DOCUMENTO DE REQUERIMIENTOS FUNCIONALES Y NO FUNCIONALES SICOV

CONTRATO DE CONSULTORÍA 287 DE 2021

DICIEMBRE DE 2021

Contrato No. 287 de 2021

Objeto del Contrato: Contratar el servicio de consultoría especializada para la elaboración de los estudios, diseños y modelos de las condiciones técnicas, administrativas, tecnológicas, financieras y jurídicas para identificar y definir la alternativa o propuesta necesaria para el funcionamiento en la instalación, implementación, operación y mantenimiento del sistema de control y vigilancia -SICOV-, que le permita a la Superintendencia de Transporte la vigilancia, inspección y control del manejo legal y reglamentario al que están sujetos los organismos de Apoyo a las Autoridades de Transito (OAT)..

CONTROL DE VERSIONES			
VERSIÓN	**FECHA**	**ELABORADO POR**	**MOTIVO**
0.1	10/12/2021	Cesar Peña	Documento inicial.
0.2	12/12/2021	Cesar Peña	Respuesta a comentarios.
0.3	24/12/2021	Cesar Peña	Actualización de los Rq. Adicionales y de refuerzo a la normativa actual.
0.4	27/12/2021	Cesar Peña	Inclusión de modificaciones en los dominios de información y controles.
0.5	28/12/2021	Cesar Peña	Inclusión de nuevos requerimientos.
0.6	28/12/2021	Cesar Peña	Se incluye referencia entre los Arquitectura de datos y matrices de OAT`S.

REFERENCIAS CONTRACTUALES DEL ENTREGABLE:
Contrato de consultoría 287 de 2021 – SICOV entre Grow Data y la Superintendencia de Transporte, plan para la gestión del proyecto.

APROBACIÓN POR LA ENTIDAD			
NOMBRE	**ROL**	**FIRMA**	**FECHA**
Dra. Adriana Margarita Urbina Pinedo	Supervisora Contrato de consultoría 287 de 2021 - SICOV		30-12-2021
Ing. Jorge Guillermo Neira Bossa	Supervisora Contrato de consultoría 287 de 2021 - SICOV		30-12-2021

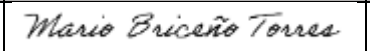
APROBACIÓN POR GROW DATA			
NOMBRE	**ROL**	**FIRMA**	**FECHA**
Ing. Mario Briceño	Gerente de Proyectos		30-12-2021
Ing. Guiovanni Serrano	Asesor Gerencia de proyectos		30-12-2021

TABLA DE CONTENIDO

TABLA DE DIAGRAMAS

TABLA DE ADJUNTOS

1. DICCIONARIO – TERMINOLOGÍA

Agudeza Auditiva: Capacidad de discriminación de estímulos auditivos.

Agudeza Visual Cinética: Capacidad de discriminar detalles de los objetos cuando existe movimiento relativo al sujeto.

Agudeza Visual: Capacidad de discriminar detalles de los objetos a una distancia determinada, teniendo en cuenta factores como condiciones de luminosidad, contraste y tamaño. Se evalúa la visión cercana y la visión lejana.

Anamnesis: Información general del candidato obtenida a partir de una entrevista inicial y que se consigna en la primera parte de la historia clínica.

ANS: ACUERDO DE NIVELES DE SERVICIO

Apelación: Solicitud presentada por un aspirante, candidato o persona que requiere la certificación, para reconsiderar cualquier decisión adversa tomada por el CRC relacionada con el estado de certificación deseada.

Application Delivery Controller: Un controlador de entrega de aplicaciones es un dispositivo de red informática en un centro de datos, a menudo parte de una red de entrega de aplicaciones, que ayuda a realizar tareas comunes, como las que realizan los aceleradores web para eliminar la carga de los propios servidores web.

Auditoría Externa: Las auditorías externas incluyen las que se denominan generalmente auditorías de segunda y tercera parte. Las auditorías de segunda parte las realizan las partes que tienen interés en la organización, por ejemplo, los clientes. Las auditorías de tercera parte las realizan organizaciones auditoras externas e independientes, con autoridad para certificar o acreditar una compañía bajo una norma de gestión establecida.

Auditoría Interna: Auditoría que realiza la organización al Sistema de Gestión de Calidad implementado. La puede realizar personal interno.

Auditoría para el mejoramiento de la calidad de la atención de salud: Es el mecanismo sistemático y continúo de evaluación y mejoramiento de la calidad observada respecto de la calidad esperada de la atención de salud que reciben los usuarios.

Auditoría: Proceso sistemático, independiente y documentado para la obtención de evidencias de cumplimiento del Sistema de Gestión de Calidad, confrontándolo con

las normas vigentes de los entes reguladores, orientadas al mejoramiento de su calidad y rendimiento.

Baremación: Los baremos iniciales serán suministrados por los proveedores de los diferentes equipos de evaluación y posteriormente el Software de Gestión ajustará los baremos de aprobación de conformidad con la población específica colombiana.

CALE: Centros de Apoyo logístico de evaluación.

Calidad de la Atención de Salud: Se entiende como la provisión de servicios de salud a los usuarios individuales y colectivos de manera accesible y equitativa, a través de un nivel profesional óptimo, teniendo en cuenta el balance entre beneficios, riesgos y costos, con el propósito de lograr la adhesión y satisfacción de dichos usuarios.

Calificación: Demostración de atributos personales, educación, formación y/o experiencia laboral.

CCTV: Circuito Cerrado de Televisión.

CDA Móvil: Centros de Diagnóstico Automotor Móvil.

CDA: Centros de Diagnóstico Automotor.

CEA: CENTRO DE ENSEÑANZA AUTOMOVISLISTICA.

CEH: El Certificado Hacker Ético es una certificación profesional proporcionada por el Consejo Internacional de Consulta de Comercio Electrónico.

Centro de Reconocimiento de Conductores: Los Centros de Reconocimiento de Conductores son las instituciones que cuentan con la facultad para realizar la evaluación y certificación de la aptitud física, mental y de coordinación motriz para conducir.

Certificado de Aptitud Física Mental y de Coordinación Motriz: Es el documento expedido por el Centro de Reconocimiento de Conductores, mediante el cual se certifica ante las autoridades de tránsito, que el aspirante a obtener por primera vez, recategorizar y/o refrendar la licencia de conducción posee la aptitud física, mental y de coordinación motriz que se requieren para conducir un vehículo automotor.

CIA: CENTROS INTEGRALES DE ATENCIÓN.

CISM: Es una certificación para el Gerenciamiento de seguridad de la información respaldada por la ISACA. Está enfocada en la gerencia.

CISSP: Es una certificación de alto nivel profesional otorgada por la (ISC)2, con el objetivo de ayudar a las empresas a reconocer a los profesionales con formación en el área de seguridad de la información

CISSP: Es una certificación de alto nivel profesional otorgada por la (ISC)2, con el objetivo de ayudar a las empresas a reconocer a los profesionales con formación en el área de seguridad de la información.

CMMI: Es un modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software. Es un modelo de evaluación de los procesos de una organización y se ha convertido en un estándar para promocionar la capacidad de desarrollar software de alta criticidad, una ventaja para las empresas que participan de proyectos complejos, riesgosos y de alto costo. De acuerdo con la Dirección de Políticas y Desarrollo TI del Ministerio TIC, las organizaciones que implementan el CMMI tienen costos predecibles y cumplen sus actividades dentro de los cronogramas indicados, lo que sin duda redunda en resultados de calidad en sus negocios, contribuyendo al mejoramiento de la competitividad de la empresa, un factor que lo hace diferenciador entre sus competidores.

COBIT: Objetivos de Control para las Tecnologías de la Información y Relacionadas es una guía de mejores prácticas presentada como framework, dirigida al control y supervisión de tecnología de la información.

Comité Técnico: Es la Instancia asesora del Ministerio de transporte y/o de la Superintendencia de Puertos y Transporte, encargada de proponer modificaciones, revisar, actualizar y avalar el esquema de certificación, las metodologías y los documentos que lo respaldan.

Competencia: Capacidad demostrada de aptitudes y/o habilidades y atributos personales, como se define en el esquema de certificación.

Condiciones de capacidad tecnológica y científica: Son los Equipos y Medios Tecnológicos idóneos y requeridos para que cada uno de los CRC pueda desempeñar sus actividades de evaluación conforme a la normatividad vigente.

Condiciones de Capacidad Tecnológica, Científica y de Infraestructura: Son los requerimientos básicos de estructura y de procesos que deben cumplir los Prestadores de Servicios de Salud por cada uno de los servicios que prestan y que se consideran suficientes y necesarios para reducir los principales riesgos que amenazan la vida o la salud de los usuarios en el marco de la prestación del servicio de salud.

CPD: Se denomina a un Centro de Procesamiento de Datos al espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización. También se conoce como centro de cómputo en Hispanoamérica y en España como centro de cálculo, centro de datos, centro de proceso de datos o centro de informática.

CRC: CENTROS DE RECONOCIMIENTO DE CONDUCTORES

DAM: Digital asset management o gestión de activos digitales, es desarrollado para organizar, almacenar y compartir los recursos digitales de una empresa.

Datasheet: Una ficha técnica es un documento en forma de sumario que contiene la descripción de las características de un objeto, material, proceso o programa de manera detallada.

DBA: Es el responsable por la Administración de las Bases de Datos. Administra las tecnologías de la información y la comunicación, siendo responsable de los aspectos técnicos, tecnológicos, científicos, inteligencia de negocios y legales de bases de datos.

Desempeño: Cada Organismo garantizará la forma como el personal cumple con lo establecido en el Esquema de Certificación, a través de la evaluación del desempeño.

Equidad: El esquema de certificación garantizará por sí mismo la igualdad de oportunidades de éxito a todos los pacientes/aspirantes.

Escáner de vulnerabilidades: Es una aplicación diseñada para realizar análisis automáticos de cualquier aplicación, sistema o red en busca de cualquier posible vulnerabilidad.

Esquema de Certificación: Requerimientos específicos de certificación relacionados con categorías especificadas de personas a las que se aplican las mismas normas y reglas particulares, y los mismos procedimientos. Es facultad exclusiva del Estado el diseño, desarrollo y validación del esquema de certificación.

Esquema de Certificación: Requerimientos específicos para evaluación y certificación, regulados en la Ley 769 de 2002 o el marco legal vigente y desarrollado en el presente anexo, que deben cumplir los aspirantes/pacientes que deseen obtener por primera vez, recategorizar o refrendar su licencia de conducción de vehículos automotores.

Ethernet: Es un estándar de redes de área local para computadoras, por sus siglas en español Acceso Múltiple con Escucha de Portadora y Detección de Colisiones. Su nombre procede del concepto físico de éter.

Evaluación: Proceso regulado en el presente anexo mediante el cual se evalúa en los aspirantes/pacientes el cumplimiento de los Requerimientos del esquema de certificación, que conduce a una decisión de certificación.

Examen: Mecanismo regulado en el presente anexo que hace parte de la evaluación, que mide la competencia de un aspirante/paciente por uno o varios medios, tales como, medios científicos, orales, prácticos y por observación.

Examinador: Persona con las calificaciones técnicas y personales pertinentes, que es competente para llevar a cabo y/o calificar un examen.

Fiabilidad: La fiabilidad de las evaluaciones, sin perjuicio del evaluador o momento en que se realicen las pruebas, será garantizada por el esquema de certificación toda vez que se aplicarán las mismas formas de evaluación en todos los Centros de Reconocimiento de Conductores a todos pacientes/aspirantes.

Firewall: Es un cortafuego, es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Los cortafuegos. pueden ser implementados en hardware o software, o en una combinación de ambos.

Forrester New Wave: Aporta recomendaciones inteligentes y comprobadas para empresas que buscan la solución ideal en inteligencia del consumidor; ahorrando meses de investigación, y ayudándoles a tomar decisiones informadas

Framework: Un entorno de trabajo, o marco de trabajo es un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar.

Gartner: El Cuadrante Mágico de Gartner permite a las empresas que contratan servicios y soluciones en TI tener una visión de conjunto de una determinada área de productos o servicios tecnológicos, y poder tomar las mejores decisiones en sus procesos de transformación digital.

Gestión: actividades coordinadas para dirigir y controlar una organización en lo referente en la calidad.

Hotfixes: Parche rápido o parche en caliente, es un único paquete que incluye información —normalmente en forma de uno o más ficheros— que es utilizado para solucionar un problema en una pieza de software.

iSCSI: Es un estándar de conexión a red de almacenamiento basado en el Protocolo de Internet (IP), que permite enlazar instalaciones de almacenamientos de datos. ... A través de iSCSI, el espacio en el servidor de almacenamiento será considerado como discos locales por el sistema operativo del cliente.

ISO 15504: Es un estándar internacional de evaluación y determinación de la capacidad y mejora continua de procesos de ingeniería del software, con la filosofía de desarrollar un conjunto de medidas de capacidad estructuradas para todos los procesos del ciclo de vida y para todos los participantes. Es el resultado de un esfuerzo internacional de trabajo y colaboración y tiene la innovación, en comparación con otros modelos, del proceso paralelo de evaluación empírica del resultado. Norma que trata los procesos de ingeniería, gestión, relación cliente-proveedor, de la organización y del soporte. Se creó por la alta competencia del mercado de desarrollo de software, a la difícil tarea de identificar los riesgos, cumplir con el calendario, controlar los costos y mejorar la eficiencia y calidad. Este engloba un modelo de referencia para los procesos y sus potencialidades sobre la base de la experiencia de compañías grandes, medianas y pequeñas.

ISO 20000: Es el estándar reconocido internacionalmente en gestión de servicios de TI (Tecnologías de la Información). La ISO/IEC 20000 es aplicable a cualquier organización, pequeña o grande, en cualquier sector o parte del mundo donde confían en los servicios de TI. La norma es particularmente aplicable para proveedores de servicios internos de TI, tales como departamentos de Información Tecnológica, proveedores externos de TI o incluso organizaciones subcontratadas. La norma está impactando positivamente en algunos de los sectores que necesitan TI tales como subcontratación de negocios, Telecomunicaciones, Finanzas y el Sector Público.

ISO 27001: Es una certificación que define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información. La ISO 27001 es para la seguridad de la información, lo mismo que la ISO 9001 es para la calidad: es una norma redactada por los mejores especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización. También permite que una organización sea certificada, lo cual significa que una entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible.

ISO 9001: Es la base del sistema de gestión de la calidad ya que es una norma internacional y que se centra en todos los elementos de administración de calidad con los que una empresa debe contar para tener un sistema efectivo que le permita administrar y mejorar la calidad de sus productos o servicios. Los clientes se inclinan por los proveedores que cuentan con esta acreditación porque de este modo se aseguran de que la empresa seleccionada disponga de un buen Sistema de Gestión de Calidad (SGC).

IT MARK: Es una certificación en métodos técnicos y de negocio, enfocado hacia la mejora de procesos en Pymes del sector de tecnologías de información. IT Mark trabaja en componentes tales como la gestión de negocios que desarrollan estrategias comerciales, financiera y de mercado. Además, evalúa las inversiones de capital de riesgo, la gestión de seguridad de la información y finalmente, la implementación de procesos de software y sistema. De acuerdo al Ministerio TIC, las empresas que implementan IT Mark, tienen mejoras representativas en el desempeño empresarial, logran enormes avances hacia la calidad, eficiencia, productividad y competitividad, hasta lograr la madurez de sus organizaciones.

MDA: Mesa de Ayuda.

Método de Evaluación: El método de evaluación será el regulado en el marco legal vigente. La validación de cada uno de los métodos deberá ser suministrado por el proveedor de los equipos utilizados por el Centro de Reconocimiento de Conductores.

Miembros del Comité Técnico: Los miembros del comité del esquema de certificación son funcionarios del Ministerio de transporte y/o de la Superintendencia de Puertos y Transporte que demuestran competencia para desarrollar, revisar y validar el Esquema de Certificación. Esta facultad podrá ser delegada en el proveedor del Sistema.

Normatividad en Seguridad LOPD: El Documento de Seguridad (DS) en materia de Protección de Datos, es como su propio nombre indica, un Documento que deben tener todos los profesionales/empresas que, están sujetos a la obligatoriedad y el cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Persona.

Normatividad en Seguridad LSSICE: es la ley que regula la venta de productos y la prestación de servicios a través de Internet.

Notificación: Son alertas que emiten ciertos programas o servicios para advertir algo al usuario.

PIN: Número de identificación único de pago.

Proceso de Certificación: Todas las actividades reguladas en el presente anexo que deben cumplir los Centros de Reconocimiento de Conductores para evaluar y expedir la certificación de aptitud física, mental y de coordinación motriz.

Protección de ENDPOINT: La seguridad de punto final o la protección de punto final es un enfoque para la protección de redes de computadoras que están conectadas de forma remota a los dispositivos del cliente.

Queja: Solicitud, en el ámbito de la evaluación de la conformidad, distinta de una apelación, presentada por una organización o persona a un OC de Certificación de Personas, de acción correctiva relacionada con las actividades de dicho CRC.

SAI: Sistema de Alimentación Ininterrumpida

SAN: Una red de área de almacenamiento, es una red de alta velocidad independiente y dedicada que interconecta y suministra depósitos compartidos de dispositivos de almacenamiento a varios servidores. Cada servidor puede acceder al almacenamiento compartido como si fuera una unidad conectada directamente al servidor.

SIEM: Son herramientas de una parte importante del entorno de seguridad de datos. Recogen datos de múltiples sistemas y analizan esos datos para detectar comportamientos anormales o posibles ataques cibernéticos o amenazas informáticas. Además, proporcionan un punto central para recopilar eventos y alertas.

Sistema de Gestión de Calidad: Es el Sistema de Gestión de Calidad que cumple con los Requerimientos de la Norma NTC ISO/IEC 17024:2013, o la norma vigente, y que asegura que los organismos de certificación de personas que operan los esquemas de certificación de la aptitud física, mental y de coordinación motriz para conducir, trabajen de forma coherente, comparable y confiable bajo un solo criterio unificado y/o modelo técnico. Este estandariza los criterios, tablas de equivalencia, técnicas de evaluación y calificación, entre otras.

Sistema Integrado de Seguridad: Es una infraestructura tecnológica operada por cualquier ente público o privado previamente homologado por la Superintendencia de Puertos y Transporte, para asegurar el cumplimiento de los parámetros técnicos mínimos que le permita prestar con calidad el servicio para garantizar la expedición segura del certificado de aptitud física mental y de coordinación motriz.

Sistema Obligatorio de Garantía de Calidad de Atención en Salud del Sistema General de Seguridad Social en Salud (SOGCS): Es el conjunto de instituciones, normas, Requerimientos, mecanismos y procesos deliberados y sistemáticos que desarrolla el sector salud para generar, mantener y mejorar la calidad de los servicios de salud en el país.

Sistema Único de Habilitación: Es el conjunto de normas, Requerimientos y procedimientos mediante los cuales se establece, registra, verifica y controla el cumplimiento de las condiciones básicas de capacidad tecnológica y científica, de suficiencia patrimonial y financiera y de capacidad técnico-administrativa, indispensables para la entrada y permanencia en el Sistema, los cuales buscan dar seguridad a los usuarios frente a los potenciales riesgos asociados a la prestación de servicios y son de obligatorio cumplimiento por parte de los Prestadores de Servicios de Salud y las EAPB.

Sistema: conjunto de elementos mutuamente relacionados que interactúan.

SOC: Un Centro de Operaciones de Seguridad, es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet.

Software de Gestión de Calidad: Es una herramienta tecnológica cuyo fin es centralizar, unificar y controlar todas las actividades propias del Sistema de Gestión de Calidad de los CRC a nivel nacional.

Solicitante/Aspirante: Persona que requiere al Organismo de Certificación de Personas su participación en el proceso de certificación de un esquema de certificación en particular conductores.

TIC: Tecnologías de la Información y la Comunicación.

UPS: Uninterruptible Power Supply es una fuente de suministro eléctrico que posee una batería. La unidad de potencia para configurar una UPS depende de la potencia activa, también denominada potencia efectiva o eficaz, consumida por el sistema.

Validez: Los proveedores de los equipos e instrumentos utilizados en la evaluación suministrarán la información suficiente donde se garantiza que las pruebas miden lo requerido por el esquema de certificación.

VPN: Una red privada virtual es una tecnología de red de ordenadores que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet.

2. OBJETIVO LEVANTAMIENTO DE REQUERIMIENTOS.

Recabar, analizar y documentar los requerimientos expuestos en el proceso de consultoría relacionadas a las OAT`S.

2.1 NORMATIVA RELACIONADA AL LEVANTAMIENTO

A continuación, se re relacionan las normativas relacionadas para el levantamiento de cada requerimiento por cada OAT.

OAT`S	SuperTransporte	Ministerio de Transporte
CALE	No se ha expedido Resolución	Resolución 1349 de 12 MAY 2017.
CDA	Resolución No. 22180 de 01 de JUN 2017.	Resolución 13830 De 29 De septiembre De 2014
CDA Móvil	Resolución No. 14554 de 27 ABR 2017.	
CEA	Resolución No. 60832 de 2016	Resolución 20203040011355 de 2020
CIA	Resolución No. 60832 de 2016	Resolución 20203040011355 de 2020
CRC	Resolución 6246 de 2016	Resolución 20203040011355 de 2020

NOTA IMPORTANTE: Se incluyen las resoluciones que tienen impacto a nivel técnico, tecnológico o lógica de funcionamiento del Software / solución tecnológica. Las normatividades relacionadas a permisos, entes o entidades para la asignación de facultades legales no se han incluido.

3. FUNCIONES ATRIBUIDAS A LA SUPERINTENDENCIA DE PUERTOS Y TRANSPORTE

Verificar el cumplimiento de las condiciones requisitos y procedimientos establecidos en las normas legales y reglamentarias expedidas por ley o por el Ministerio de transporte.

Vigilancia, inspección y control tiene por objeto establecer orden a las actividades que se desarrollan en el sector de transporte, incluidas las actividades de apoyo al tránsito y el mejoramiento de la vigilancia y el control, a través de mecanismos sistematizados.

Procesos sancionatorios, generando modelos de supervisión de carácter preventivo, permitiendo un impacto en beneficio de la movilidad y la seguridad vial.

Mejorando los controles de ubicación de los centros y el sitio donde se realizan las pruebas, usando dispositivo hardware e incorporando todas las OAT`S.

NOTA IMPORTANTE: El cumplimiento de las disposiciones aquí establecidas, **no implica** aumento en los costos de los servicios que pagas los Centros de Reconocimiento a los Operadores autorizados, ni a los usuarios de los servicios prestados por los Centros de reconocimiento.

4. REQUERIMIENTOS

A continuación, se definen los requerimientos funcionales y no funcionales, relacionados a las normas mencionadas en el apartado Normativa relacionada al levantamiento, está dividido en 3 secciones principales:

- **Requerimientos Alto Nivel**: Contiene todos los requerimientos funcionales y no funcionales, comunes en todas las OAT`S visto desde la normatividad vigente, ubicados en los apartados:
  - Requerimientos funcionales – Alto Nivel por norma
  - Requerimientos Funcionales y NO funcionales detallados por norma

- **Requerimientos detallados por norma:** Esta detallado los requerimientos funcionales y no funcionales detallados por cada una de las OAT`S visto desde la normatividad vigente, ubicado en el apartado
  - Requerimientos Funcionales y NO funcionales detallados por norma

- **Requerimientos complementarios**: Se especifica todo requerimiento no contemplado en la normatividad vigente o que requieren de una mayor especificación, ubicado en el apartado.
  - Requerimientos Complementarios.

4.1. Requerimientos funcionales – Alto Nivel por norma

Son aquellos que el sistema debe proporcionar, debe reaccionar y debe actuar en situaciones particulares.

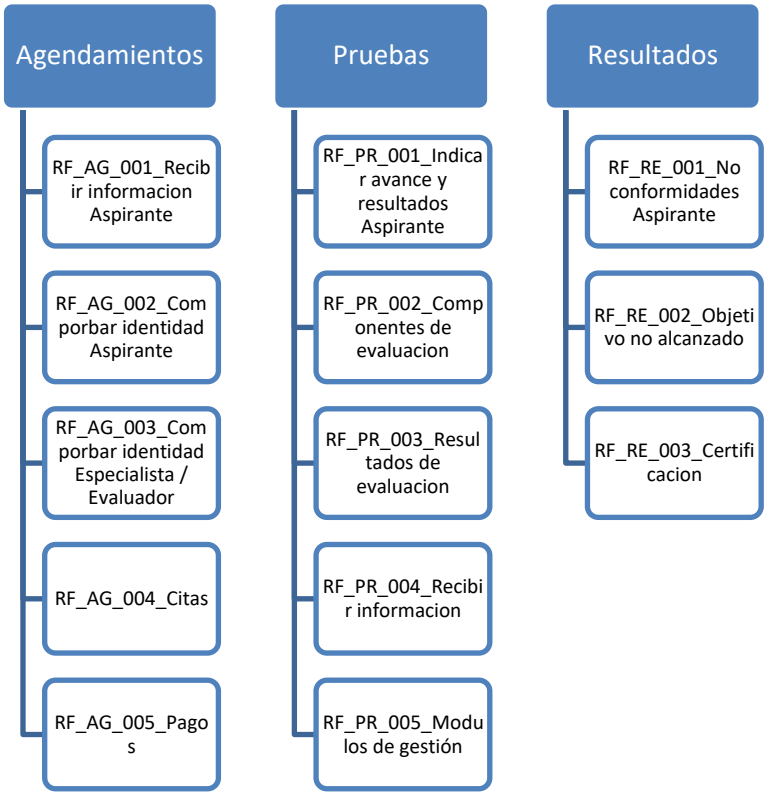
4.1.1. Diagrama alto nivel requerimientos funcionales

A continuación, se presenta una agrupación de los requerimientos funcionales que son comunes para los OAT`S.

- **Agendamientos**: Hace parte de todo el proceso inicial, en cualquiera de las OAT`S, antes de un inicio de validación o pruebas, según corresponda.

- **Pruebas**: Contempla todo el proceso intermedio de la gestión en cada una de las OAT`S, podrán ser pruebas o validaciones dependiendo de la gestión realizada.
- **Resultados**: Es la parte final en cualquiera de los procesos de las OAT`S, donde se toma una decisión de resultado y sus posibles salidas.

Diagrama 1 Requerimientos funcionales Alto nivel

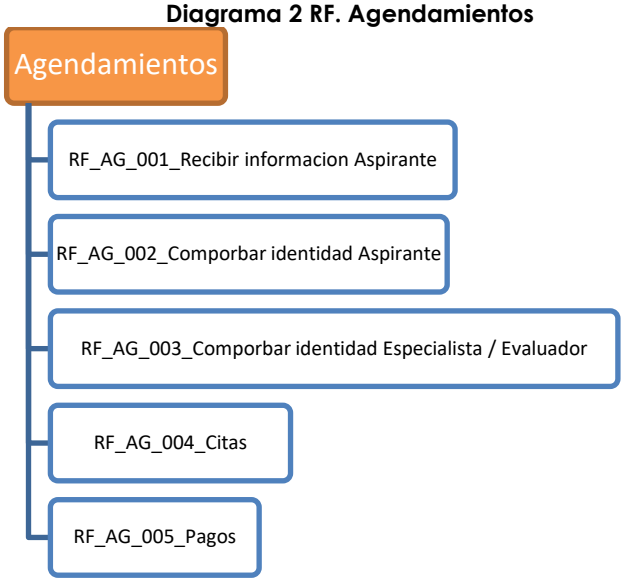


Fuente: Elaboración propia Grow Data 2021

4.1.1.1. Agendamientos

Hace parte de todo el proceso inicial, en cualquiera de las OAT`S, antes de un inicio de validación o pruebas, según corresponda.

Diagrama 2 RF. Agendamientos



Fuente: Elaboración propia Grow Data 2021

RF_AG_001_Recibir información Aspirante
Debe permitir el ingreso de información (datos esenciales para el desarrollo de las actividades en cualquiera de las OAT`S).

RF_AG_002_Comporbar identidad Aspirante
Al empezar o finalizar alguna prueba debe validar la identidad.

RF_AG_003_Comporbar identidad Especialista / Evaluador
Al empezar o finalizar alguna prueba debe validar la identidad.

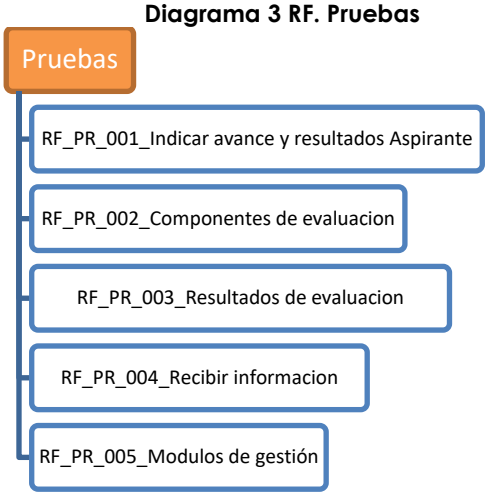
RF_AG_004_Citas
Debe permitir generar citas dependiendo su capacidad por espacio (metros cuadrados).

RF_AG_005_Pagos
Existirá procesos de pagos de forma virtual y física.

4.1.1.2. Pruebas

Contempla todo el proceso intermedio de la gestión en cada una de las OAT`S, podrán ser pruebas o validaciones dependiendo de la gestión realizada.

Diagrama 3 RF. Pruebas



Fuente: Elaboración propia Grow Data 2021

RF_PR_001_Indicar avance y resultados Aspirante
Existirá la función, para informar el avance efectuado.

RF_PR_002_Componentes de evaluación
Existen diferentes procesos de evaluación y examinación en las OAT`S, se deben contemplar e incluir en la solución tecnológica. (Se debe tener en cuenta los procesos virtuales).

RF_PR_003_Resultados de evaluación
Se debe validar cada elemento catalogado para su evaluación y composición de resultados.

RF_PR_004_Recibir información
Cada uno de los Operadores, deben cumplir con requisitos donde se debe tener en cuenta los que tienen vigencia.

RF_PR_005_Modulos de gestión
Deben implementar módulos relacionados en cada una de las normativas para los softwares de gestión.

4.1.1.3. Resultados

Es la parte final en cualquiera de los procesos de las OAT`S, donde se toma una decisión de resultado y sus posibles salidas.

Diagrama 4 RF. Resultados

Fuente: Elaboración propia Grow Data 2021

RF_RE_001_No conformidades Aspirante

Cuando no esté de acuerdo con el resultado, debe existe un método de apelación o solicitud de revalidación de cada componente de evaluación.

RF_RE_002_Objetivo no alcanzado

Cada vez que algunos de los procesos no sean alcanzados se debe implementar el proceso correspondiente según OAT.

RF_RE_003_Certificación

Una vez alcanzado y cumplido todos los elementos evaluadores, se debe generar y notificar una certificación a los distintos actores del proceso.

4.2. Requerimientos NO funcionales – Alto Nivel

Estos indican las propiedades y restricciones del sistema; también pueden ser especificados o asignados a un lenguaje de programación o aun método desarrollado. El requerimiento NO funcional puede ser más crítico que el funcional; si estos no se cumplen, el sistema es inservible.

En este apartado vamos a encontrar diferentes tipos de requerimientos NO funcionales, los cuales se relacionan a un alto nivel:

- Relativos a la interface
  - Entorno operativo: hardware, sistema
  - Operativo, de red.
  - Ergonómicos
  - Formatos intercambio información

- Desempeño y seguridad
  - Tiempos de respuesta
  - Capacidad de proceso
  - Espacio de almacenamiento
  - Fiabilidad
  - Seguridad
  - Tolerancia a fallos
  - Supervivencia

- Desarrollo
  - Producto
  - Mantenibilidad
  - Flexibilidad
  - Reusabilidad
  - Compatibilidad
  - Integración
  - Proceso
  - Tiempo de desarrollo
  - Disponibilidad de recursos
  - Estándares de desarrollo

- Operación
  - Nivel preparación usuarios
  - Accesibilidad para mantenimiento
  - Distribución espacial de componentes

- Políticos
  - Sin otra justificación que la voluntad de las personas (Normativas, resoluciones, leyes etc.…)

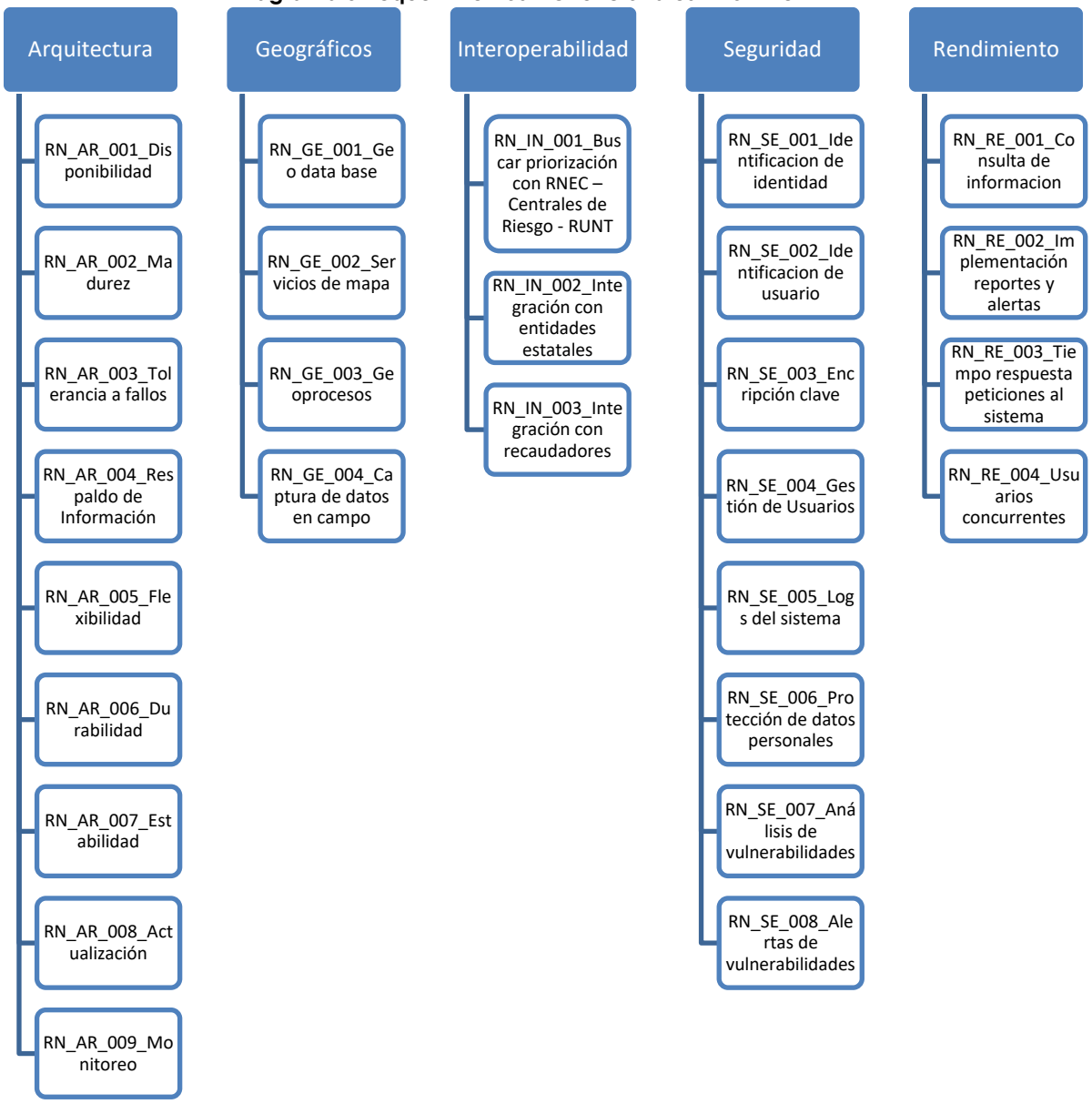
4.2.1. Diagrama alto nivel requerimientos NO funcionales

Los requerimientos NO funcionales son:

- **Arquitectura**: Se especifican requisitos generales de la arquitectura de software del sistema de información.
- **Geográfico:** Presenta los lineamientos para incluir en sistemas de información el manejo de información geográfica.
- **Interoperabilidad**: Se detallan aspectos para la interoperabilidad con otros sistemas y otras entidades.
- **Seguridad**: Describe aspectos de seguridad que se deben cumplir.

- **Rendimiento**: Se listan las necesidades de rendimiento de la solución tecnológica, en los requerimientos no funcionales de alto nivel.

Diagrama 5 Requerimientos NO funcionales Alto nivel

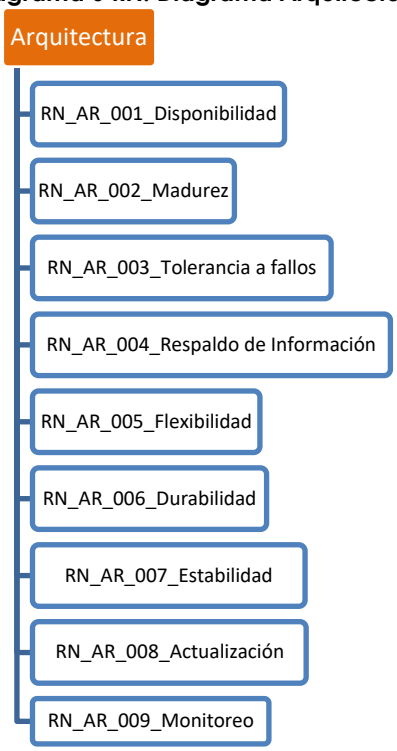


Fuente: Elaboración propia Grow Data 2021

4.2.1.1. Arquitectura

Se especifican requisitos generales de la arquitectura de software del sistema de información.

Diagrama 6 RN. Diagrama Arquitectura



Fuente: Elaboración propia Grow Data 2021

RN_AR_001_Disponibilidad

La infraestructura debe soportar una operación en alta disponibilidad, debe estar provisto de mecanismos o componentes que aseguren la continuidad del servicio procesamiento distribuido y almacenamiento en múltiples servidores. Se espera una disponibilidad mínima del 99.6 %.
El sistema deberá estar disponible las 24 horas del día, 7 días de la semana, 365 días del año.

RN_AR_002_Madurez

La infraestructura debe enfocarse en la utilización de componentes base o reconocidos en el mercado, 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 componente que permita el mejoramiento y acceso a nuevas versiones de acuerdo con la evolución de las plataformas.

RN_AR_003_Tolerancia a fallos

La infraestructura deberá mantener el nivel especificado de rendimiento en casos de fallos del hardware.

RN_AR_004_Respaldo de Información
Contar con procedimientos automáticos para copias de seguridad y restauración encaminados a realizar copias periódicas de seguridad de todos elementos dentro del sistema (carpetas, documentos, metadatos, usuarios, roles, permisos, configuraciones específicas).

RN_AR_005_Flexibilidad
Cuando se produzca un fallo del hardware, debe resultar posible devolver la operación a un estado conocido con el hardware disponible.
El sistema debe ser fácil de instalar en todas las plataformas de hardware y software de base requeridas, así como permitir su instalación en diferentes tamaños de configuración.

RN_AR_006_Durabilidad
Capacidad de la infraestructura para continuar en funcionamiento sin necesidad de revisión a través del tiempo debido al desgaste, manteniendo sus características físicas y de funcionalidad.

RN_AR_007_Estabilidad
Capacidad de la infraestructura para mantener el rendimiento esperado bajo carga de trabajo.

RN_AR_008_Actualización
La infraestructura debe tener la capacidad de gestionar las diferentes actualizaciones (parches de seguridad, versiona miento, etc.)

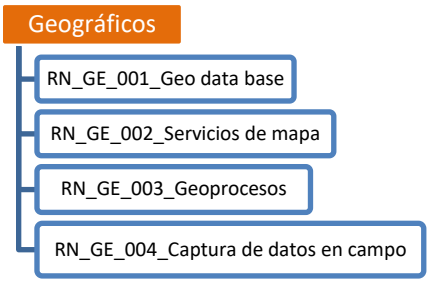
RN_AR_009_Monitoreo
La infraestructura debe tener la capacidad de monitorear los diferentes componentes relacionados a la operación, buscando evitar y/o reaccionar ante posibles amenazas que puedan afectar su funcionamiento.

4.2.1.2. Geográficos

Para los sistemas de información que requieran captura, almacenamiento, algún procesamiento o visualización de información geográfica, se deberá hacer uso del componente geográfico.

Se debe validar los aspectos geográficos y detectar si las necesidades del sistema son cubiertas con el componente o se requieren incluir nuevas funcionalidades o modificaciones a las a funcionalidades ya construidas.

Diagrama 7 RN. Geográficos



Fuente: Elaboración propia Grow Data 2021

RN_GE_001_Geo data base

La base de datos geográfica deberá detallarse en su funcionamiento si se requiere captura de información, tanto de imágenes como datos espaciales. Si la herramienta requiere establecer una estructura de tablas para los componentes, entonces debe validar y comparar el requerimiento con el esquema actual de ministerio para evitar duplicidad.

RN_GE_002_Servicios de mapa

Se deben identificar los servicios de mapa que se requieran en la solución, bien sean de ministerio, superintendencia o de una entidad exterior.

RN_GE_003_Geoprocesos

Un geo proceso es todo aquel desarrollo de software que tenga como entrada una o más capas geográficas y que en su operación transforma, filtra o genera nueva información geográfica.

En la solución tecnológica se debe plantear sus características como su lenguaje, operabilidad, etc.

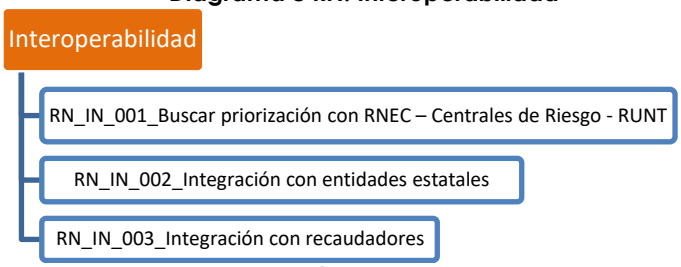
RN_GE_004_Captura de datos en campo

Se debe generar captura de información en campo, de ubicación real, posicionamiento, recorrido, fecha, hora, etc... Esto aplica para puntos fijos, móviles o automóviles.

4.2.1.3. Interoperabilidad

Se relaciona los sistemas de identidades en las cuales se debe realizar algún tipo de consulta.

Diagrama 8 RN. Interoperabilidad



Fuente: Elaboración propia Grow Data 2021

RN_IN_001_Buscar priorización con entidades.

Se debe detectar las necesidades de interoperabilidad y buscar su priorización ante la red de conexión.

- Registraduría Nacional del estado civil (RNEC)
- Registro Nacional de Infractores de Tránsito.
- Registro Único Nacional de Transito (RUNT)
- Centrales de riesgo

RN_IN_002_Integración con entidades estatales

Para la integración con entidades estatales se debe validar las formas de conexión con cada una de ellas, de acuerdo con los recursos que se tengan para dichos procesos de interoperabilidad.

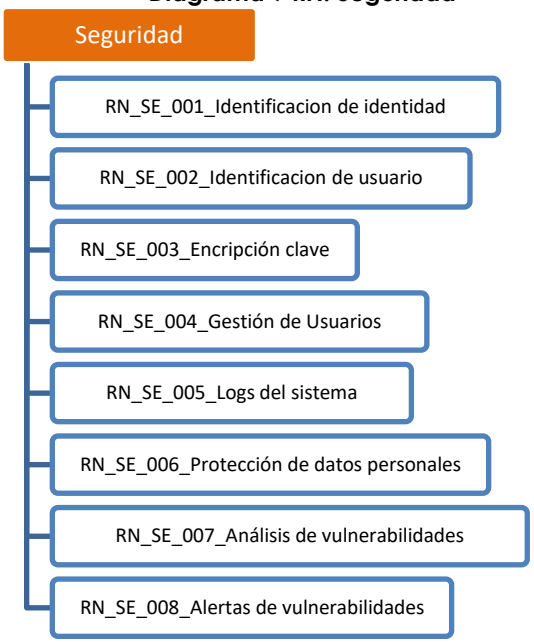
RN_IN_003_Integración con recaudadores

Para la integración con entidades encargadas al apoyo del recaudo de las diferentes actividades generas en las OAT`S.

4.2.1.4. Seguridad

Describe aspectos de seguridad que se deben cumplir en las descripciones de los requerimientos no funcionales –Alto nivel.

Diagrama 9 RN. Seguridad



Fuente: Elaboración propia Grow Data 2021

RN_SE_001_Identificacion de identidad

Se debe usar los métodos de validación de identidad con las entidades RNEC y Centrales de riesgo o métodos para gestión de excepciones.

RN_SE_002_Identificacion de usuario

La solución informática o Software de gestión, debe tener un método de validación de usuarios asignados al personal a interactuar en el ecosistema.

RN_SE_003_Encripción clave

En el momento de uso de claves para ingreso de usuarios en el ecosistema / Software, se deben encriptar con el fin de que ni el administrador de la aplicación pueda tener conocimiento de cuales con (Debe permitir parametrización).

RN_SE_004_Gestión de Usuarios

El sistema debe permitir la gestión de usuarios (creación, suministros de acceso, asignación de privilegios, revocatoria de accesos, o los necesarios dispuestos en el detalle de cada OAT, contenidos en el apartado Matrices adjuntas de requerimientos por OAT.), roles y perfiles, grupos de usuarios, asociación de acciones para cada rol y administración exclusiva del administrador de la aplicación.

RN_SE_005_Logs del sistema
Debe permitir generar registros de los ingresos a la aplicación y las actividades realizadas por los usuarios.

RN_SE_006_Protección de datos personales
El sistema debe garantizar el cumplimiento del régimen general de protección de datos personales. Cuando el sistema solicita información personal al usuario final, se debe establecer un mecanismo para obtener la autorización y tener prueba de ellos (log). Cumplir la Ley 1581 de 2012.

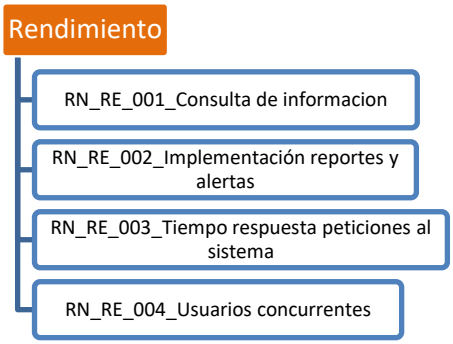
RN_SE_007_Análisis de vulnerabilidades
Se deben analistas y establecer las posibles vulnerabilidades que este expuesto el ecosistema.

RN_SE_008_Alertas de vulnerabilidades
Se generar procesos de alertas o notificaciones donde se informe posibles vulnerabilidades generadas al SOC.

4.2.1.5. Rendimiento

Se listan las necesidades de rendimiento de la solución tecnológica, en los requerimientos no funcionales de alto nivel.

Diagrama 10 RN. Rendimiento



Fuente: Elaboración propia Grow Data

RN_RE_001_Consulta de información
La información de las distintas OAT`S, sus transacciones, registros, grabaciones, usuarios, roles y cualquier información que este registrada en las diferentes BBDD`S, debe estar disponible 24*7*365.
Su información debe estar en tiempo real, a excepción de la ubicación de geoposicionamiento de algunas OAT`S, que máximo será cada 60 minutos.

RN_RE_002_Implementación reportes y alertas

El sistema de control y vigilancia debe tener procesos para consulta y extracción de información, así mismo creando métodos para generar alertas sobre procesos parametrizados o fuera de lo habitual.

RN_RE_003_Tiempo respuesta peticiones al sistema

El sistema debe ser de alta disponibilidad, minimizando todos los tiempos en los procesos solicitados por alguno de los usuarios / procesos que interactúan en el ecosistema.

RN_RE_004_Usuarios concurrentes

Debe estar pensado para poder recibir aumentos de consultas de usuarios múltiples, N cantidad, sin afectar su rendimiento y funcionamiento.

4.3. Requerimientos Funcionales y NO funcionales detallados por norma

A continuación de relaciona los requerimientos detallados por resolución, ley o norma emitida desde el Ministerio de transporte o Supertransporte.

Estos requerimientos se han generado desde la Visión del SICOV (Control y Vigilancia).

Ya que son extensos, sean han clasificado en otro documento, se disponen de 1 tipo de formato donde se encuentran cada una de los requerimientos de forma detallada.

4.3.1. Matrices adjuntas de requerimientos por OAT.

Se relacionan matrices por cada OAT, donde se encuentran de forma detallada los requerimientos funcionales para el funcionamiento de la solución tecnológica.

NOTA IMPORTANTE: Para generar descarga de cada una de las matrices, dar doble clic sobre cada archivo adjunto ubicado en frente de cada del título de cada OAT.

Adjunto 1 Matriz de requerimientos Funcionales y NO funcionales

Fuente: Elaboración propia Grow Data 2021

4.4. Requerimientos Complementarios.

Dentro de los requerimientos complementarios encontraremos todos aquellos criterios necesarios para la implementación del nuevo SICOV, que en algunos casos no están establecidos dentro de la norma o la norma no da alcance suficiente a los requerimientos tecnológicos actuales, pero son indispensables para el correcto funcionamiento de la nueva solución informática.

IMPORTANTE: En ambos casos se debe generar procesos de análisis, validación e implementación normativa, para que puedan ser exigibles en la nueva solución informática.

4.4.1. Diagrama Requerimientos complementarios

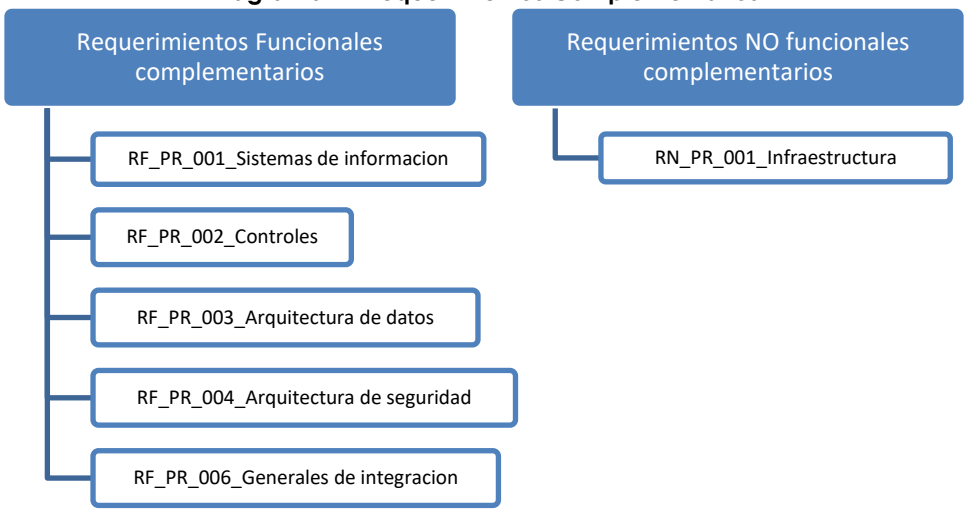
Se han catalogado en:

- **Sistemas de información (SI)**: Se encontrara los componentes interrelacionados que trabajan juntos para recopilar, procesar, almacenar y difundir información para apoyar la toma de decisiones.
- **Controles**: Se relacionan los que no se contemplan en la norma y están relacionados en la documentación de "Controles de dominio", donde se encontraran procesos para mejora de supervisión y vigilancias desde la nueva solución tecnológica.
- **Arquitectura de datos**: Están relacionados todos los artefactos, políticas, reglas y como

se almacena, organiza, integran y utilizan los sistemas de información.

- **Infraestructura**: Son todos los elementos o componentes físicos e informáticos, necesarios para garantizar una correcta operabilidad y funcionamiento óptimo de la solución tecnológica y sus componentes periféricos.
- **Arquitectura de seguridad:** Son todos aquellos elementos que garantizan la seguridad e integridad de información, componentes y gestión de todo el ecosistema.
- **Generales – propuestos de integración:** Se incluyen componentes del ciclo de vida, aspectos generales de la solución tecnológica.

Diagrama 11 Requerimientos Complementarios

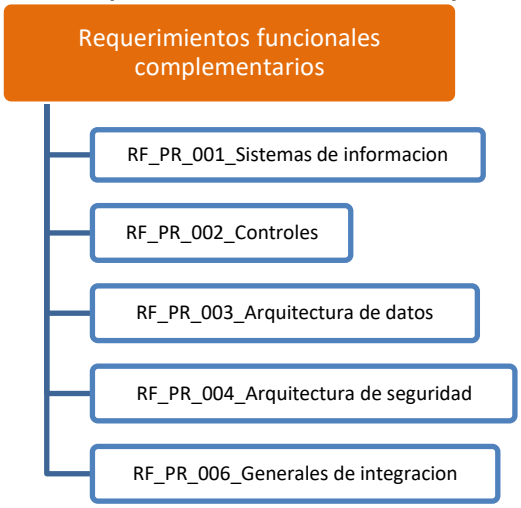


Fuente: Elaboración propia Grow Data 2021

4.4.1.1. Requerimientos funcionales complementarios.

A continuación, se relaciona el detalle de cada de los requerimientos funcionales asociados a cada uno de los elementos del apartado.

Diagrama 12 Requerimientos funcionales complementarios



Fuente: Elaboración propia Grow Data 2021

RF_PR_001_Sistemas de información

Se relacionan requerimientos relacionados a sistemas de la información no relacionados a la norma o su respectivo refuerzo.

- Debe existir un módulo en la solución tecnológica, donde se administre los controles (crear, desactivar, Editar y suspender)
  - Control de accesos por usuarios, roles y permisos
  - Debe almacenar log de transacciones.
    - Usuarios que generan cualquier modificación.
    - Fecha y hora
    - Ubicación (IP, nombre del equipo)

- Debe generar procesos de recepción, validación y notificación de todos los documentos, certificaciones u autorizaciones que tengan vigencia, implementado procesos de alerta / notificaciones informando la perdida de vigencia X días antes y cuando se pierde.
  - Debe incluir procesos de notificación (A quien, como, periodicidad)
  - Control de accesos por usuarios, roles y permisos
  - Debe almacenar log de transacciones.
    - Usuarios que generan cualquier modificación.
    - Fecha y hora
    - Ubicación (IP, nombre del equipo)

NOTA: Este requerimiento está enfocado a certificaciones u autorizaciones actuales o futuras, como el SOAT y tecnomecanica de los carros que se usan para las clases prácticas, el detalle de cada uno está relacionado en el documento "Controles".

- Debe generar procesos de recepción, validación y notificación de todas autorizaciones de funcionamiento que NO tienen vigencia, pero pueden llegar a suspenderse, implementado procesos de alerta / notificaciones informando la perdida de la autorización, esta validación debe realizarse cada X días.
    - Debe incluir procesos de notificación (A quien, como, periodicidad)
    - Control de accesos por usuarios, roles y permisos
    - Debe almacenar log de transacciones.
        - Usuarios que generan cualquier modificación.
        - Fecha y hora
        - Ubicación (IP, nombre del equipo)

NOTA: Este requerimiento está enfocado a todas autorizaciones de funcionamiento o ejercicio de funciones, como el registro en el RETHUS de los especialistas de la salud, y todos los actuales o futuros cumplan esta condición.

- Se debe implementar un gobierno de datos, el detalle de cada uno está relacionado en el documento "Controles"
    - Se debe desarrollar políticas y procedimientos.

- Control de datos en múltiples niveles.

- Custodia de datos en múltiples niveles.
    - Así como las conductas necesarias para gestionar los datos como un activo de manera exitosa.

- Se debe implementar los datos maestros y referencia
    - Se debe tener acceso a los mismos conjuntos de datos,
    - Deben ser datos confiables, completos, actuales y consistentes.

- Se debe garantizar la calidad de los datos
    - Deben tener consistencia.

RF_PR_002_Controles

Se relacionan requerimientos relacionados a controles no relacionados a la norma o su respectivo refuerzo.

- **CRC**

- Se debe implementar procesos de protocolos para el mantenimiento preventivo de

los instrumentos.

- **CEA - CIA**

  - Debe Implementar restricción y control de horas laboradas para cada instructor.
    - Esta restricción del sistema debe ser parametrizable, ya que puede cambiar en el tiempo.

  - Debe garantizar el tiempo de asistencia en las clases prácticas y teóricas, implementando procesos de validación y notificación.
    - Estar implementado para aspirante e instructor.
    - Debe ser parametrizable el % de asistencia para las notificaciones.

  - Para poder iniciar una nueva clase o examen, no debe tener ninguna en curso.

- **CDA**

  - Debe Implementar evaluación de conocimiento teórico practicas inspectores o técnicos, operarios o su equivalencia.
    - Debe Implementar procesos de análisis basadas en los resultados, para implementar capacitaciones / formación, con el único fin de garantizar la correcta evaluación.

  - Debe Implementar nuevos procesos de capacitaciones para las nuevas tecnologías.

  - Debe implementar procesos de vigencia de calibración de cada uno de los instrumentos de medición.

  - Debe generar más validaciones de identificación del automotor, al inicio, durante y al finalizar las pruebas.
    - Evidencia fotográfica de Numero de chasis.
    - Evidencia fotográfica de Numero de motor.

  - Debe implementar procesos en la estación de inspección sensorial, el técnico de pista revisa adecuadamente el vehículo automotor y transmite información al sistema sin alteraciones.

  - Debe implementar procesos en la estación de inspección con herramientas de medición, el técnico de pista revisa adecuadamente el vehículo automotor y transmite información al sistema sin alteraciones.
    - Revisión frenos.
    - Alineación.

- Suspensión.
- Llantas.
- Vidrios.
- Luces.
- Gases.

- Se debe generar revisión de identidad del personal inspectores o técnicos, operarios o su equivalencia, cada vez que incluya información al sistema.

- Se debe garantizar el uso de las herramientas de medición.

RF_PR_003_Arquitectura de datos

Se relacionan requerimientos relacionados de arquitectura de los datos no relacionados a la norma o su respectivo refuerzo.

- Se debe unificar las fuentes de información de las distintas OAT`s, transmitida por medio de Web Service.
  - Toda la información ingestada debe ser estructurada.
  - Debe persistir en dimensionamientos y tablas de hechos.

- Se debe garantizar procesos donde la información resultante de todas las gestiones, se almacenen en su totalidad y con traza de gestión.

- Se debe implementar un módulo de creación, modificación, desactivación de informes.
  - No debe permitir creación de informes duplicados.
  - Debe ser flexible, escalable, intuitivo.
  - Sus procesos de creación y modificación no deben demorar más de X tiempo.
  - Debe tener control de accesos por usuarios, roles y permisos.
  - Debe almacenar log de transacciones.
    - Usuarios que generan cualquier modificación.
    - Fecha y hora.
    - Ubicación (IP, nombre del equipo).

- Se debe implementar un módulo de consulta / extracción de informes.
  - Debe ser flexible, escalable, intuitivo.
  - Sus procesos de creación y modificación no deben demorar más de X tiempo.
  - Debe tener control de accesos por usuarios, roles y permisos.
  - Debe almacenar log de transacciones.
    - Usuarios que generan cualquier descarga.
    - Fecha y hora.

        - Ubicación (IP, nombre del equipo).

    - Debe tener una temporalidad de uso, una vez un informe no se use durante más de **XX** días, una vez alcanzada este tiempo se desactivará de forma automática, evitando una sobre carga de informes en el sistema.

- Se debe implementar un módulo de creación, modificación, desactivación de KPI, métricas e indicadores que alimente un (Dashboard).
    - Debe ser flexible, escalable, intuitivo.
    - Sus procesos de creación y modificación no deben demorar más de X tiempo.
    - Debe tener control de accesos por usuarios, roles y permisos.
    - Debe almacenar log de transacciones.
        - Usuarios que generan cualquier modificación.
        - Fecha y hora.
        - Ubicación (IP, nombre del equipo).

- Se debe actualizar los documentos como catálogos y matrices mínimo 1 vez por año.

- Se debe implementar procesos con estrategia de analítica tradicional que permita realizar modelos para descubrir información y poder tomar decisiones a partir de estos. Por ejemplo, algoritmos para predecir el número de solicitudes de licencia de conducción en un periodo de tiempo determinado o los posibles automotores que probablemente no pasaran la revisión tecno-mecánica.

- Se debe implementar procesos con estrategia de analítica avanzada basada en modelos y técnicas de inteligencia artificial que permitan realizar video analítica y minería de opinión.
    - El análisis de sentimiento a partir de redes sociales, para poder captar las opiniones (PQR, manejo de redes) de los usuarios de los diferentes Organismos de Apoyo al Tránsito y tomar acciones de mejoras.

- Se debe garantizar la disponibilidad de la información para que los distintos procesos de analítica, informes, reportes y demás elementos que puedan implementarse en la solución tecnológica funcionen correctamente.
    - En los casos que se supere los límites de espera para recepción de información, debe generar procesos de reporte, notificaciones para alertar el retraso de la data.

RF_PR_004_Arquitectura de seguridad

Se relacionan requerimientos relacionados de arquitectura de la seguridad no relacionados a la norma o su respectivo refuerzo.

- Se deben implementar controles para mejorar la protección de la confidencialidad, integridad y disponibilidad de los datos
    - Se debe implementar gestión de identidades y usuarios
        - Debe tener control de accesos por usuarios, roles y permisos
    - Se debe implementar Control de EndPoint
        - 360 total security endpoint
    - Se debe implementar Prevención de fuga y perdida de información – DLP
    - Se debe implementar Gestión de dispositivos móviles
    - Se debe implementar Ofuscación de código

RF_PR_005_Generales de integración

Se relacionan requerimientos funcionales y NO funcionales no especificados en la normatividad y también aquellos que requieren un refuerzo o dar más alcance.

- Se debe implementar un módulo para cada OAT, donde se relaciona todos las tarifas asociadas o generadas al usuario / aspirante final.
    - Únicamente debe crear y desactivar tarifas.
    - Por cada tipo de tarifa en cada OAT podrá existir una activa, con el fin de evitar incoherencias en las tarifas.
    - No debe permitir creación de tarifas duplicadas
    - Debe ser flexible, escalable, intuitivo.
    - Debe tener control de accesos por usuarios, roles y permisos
    - Debe almacenar log de transacciones.
        - Usuarios que generan cualquier modificación.
        - Fecha y hora
    - Ubicación (IP, nombre del equipo)

- Se debe contemplar en la solución tecnológica que sea capaz de integrarse con los distintos navegadores actuales.
    - Tener compatibilidad con la última versión en producción de cada navegador.
    - En el caso de que alguno de los complementos de las APP`S no sea compatible con algún navegador, debe informar por algún método la restricción del navegador.

- NO debe permitir iniciar un proceso de enseñanza a un aspirante que no tenga un certificado de aptitud física, mental y de coordinación motriz.

- Volver obligatoria la consulta contra la registraduría o validaciones alternas que puedan existir y no permitir guardar datos personales de los aspirantes en los sistemas de los proveedores.

- NO permitir multi sesiones (Tener varias sesiones abiertas sobre la solución tecnológica), a cualquier usuario conectado en la solución.

- Se debe tener en cuenta clases virtuales (Creación de modulo dedicado para generar los procesos de clases virtuales).
    - Se debe incluir las condiciones y características de clases presenciales de las diferentes OAT`S, para que sea la base de integración a clases virtuales.

- Los exámenes teóricos deben implementarse desde la solución tecnológica.
    - Debe ser flexible, escalable, intuitivo.
    - Debe tener control de accesos por usuarios, roles y permisos.
    - Debe validación de respuestas deber hacerlo el mismo sistema y almacenar la información.
    - Debe asegurar la identidad de cada participante.
    - Debe almacenar log de transacciones.
        - Usuarios que generan cualquier modificación.
        - Fecha y hora.
    - Ubicación (IP, nombre del equipo).

- Implementar uso de la CC digital.

- Implementar token de sesión, por actividad, al momento de iniciar cesión en la solución tecnológica.

- Al momento de no ser satisfactorio el reconocimiento Biométrico, se debe implementar procesos de respaldo, para validación / identificación de identidad.
- Debe poder adicionar, modificar o eliminar los nuevos componentes de inventario para la conexión de sistema, estandarizando las condiciones mínimas para la aceptación en el sistema.
    - Tipos de vehículos (autorizados para impartir cursos prácticos).
    - Dispositivos para evaluación o validación.

- Implementar protocolos para los casos donde el aspirante no supere un examen o validación.
    - Estos dependen de las motivos y condiciones de cada OAT.

- Al momento de ingresar el documento de identidad debe, traer información básica (Nombre, apellidos, grupo sanguíneo o los necesarios para el funcionamiento de cada una de las OAT`S) ya almacenada en las bases, permitiendo actualizar o incluir (Poder extraer información desde RUNT).

- Una vez el aspirante inicie un proceso o examen y no lo completa, debe existir una temporalidad para poder continuar con el proceso.

- La información del árbol genealógico de los funcionarios, debe validar contra el sistema, indicando donde no puede ir por restricción de lasos sanguíneos.

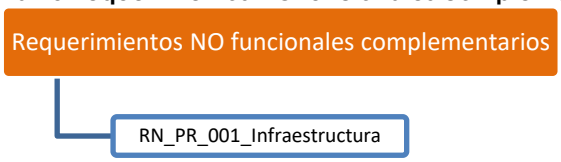
- Implementar historia clínica.
  - Ir almacenando la información de cada uno de los exámenes de cada uno (a) de los aspirantes, con el fin de crear una historia y poder facilitar los procesos de restricciones y validaciones en cada una de las OAT`S.

- En el momento de generar error la APP por algún motivo, debe guardar un Log relacionado a un código de error informado en el momento que ocurra.

4.4.1.2. Requerimientos NO funcionales complementarios.

A continuación, se relaciona el detalle de cada de los requerimientos funcionales asociados a cada uno de los elementos del apartado.

Diagrama 13 Requerimientos NO funcionales complementarios



Fuente: Elaboración propia Grow Data 2021

RN_PR_001_ Infraestructura

Se relacionan requerimientos relacionados a infraestructura no relacionados a la norma o su respectivo refuerzo.

- Se debe actualizar la especificación técnica de los equipos ubicados en las OAT`S, con el fin de garantizar los procesos de alta disponibilidad de la información.
  - SSD SATA 2 TB
  - Memorias RAM Ddr4 16 GB
  - Procesador máximo 3 generaciones inferiores a la actual
  - Tarjeta De Red Gigabit Giga

- Se debe implementar para los procesos de respaldo de conexiona a internet.
  - Balanceador de cargas (Enrutador VPN) el cual debe tener:
    - Mínimo 1 puerto WAN Gigabit SFP
    - Mínimo 1 puerto de Gigabit
    - Sesiones simultaneas
    - Equilibrio de cargas
    - Respaldo de enlaces
    - Firewall basado en políticas

- Enrutamiento estático
- Enrutamiento basado en políticas
- VLAN
- DHCP de múltiples redes

- Los dispositivos móviles usados en cualquiera de las OAT`S y tengan funcionamiento directo o indirecto con la solución tecnológica, deben soportar el ultimo software de sistema operativo del mercado.

4.4.1. Matrices adjuntas de requerimientos por OAT.

5. ANEXOS

- CRC Matriz requerimientos V1.1
- CALE Matriz requerimientos V1.0
- CEA - CIA Matriz requerimientos V1.0
- CDA Matriz requerimientos V1.0

5.1. REFERENCIA DE ARQUITECTURA DE INFORMACIÓN

Esta relacionado todos los apartados que componen la arquitectura de información basados en las matrices.

- Anexo - CALE Matriz requerimientos, sus puntos y subpuntos:
  - 2.1 Requisitos para habilitarse como CALE
  - 4.2 Artículo 11. Condiciones previas a la presentación del examen teórico.
  - 5 DEL EXAMEN PRÁCTICO
  - 5.3 Artículo 18. Definición de procesos y metodología de evaluación.

- Anexo - CDA Matriz requerimientos, sus puntos y subpuntos:
  - 3.1 Procesos de verificación de la presencia del vehículo en las instalaciones del CDA a través de la captura de videos "Registro fílmico"
  - 3.4 Proceso de cruce de información e interconexión.
  - 5 Requisitos funcionales, tecnólogos y lógicos de funcionalidad del sistema de control y vigilancia para los CDA`S
  - 5.2.5 Seguridad lógica
  - 5.3.5 Gestión de almacenamiento de la información (Seguridad 27001)
  - 5.3.7 Encriptación de la información
  - 5.3.8 Normatividad en seguridad LOPD Y LSSICE

- Anexo - CEA – CIA Matriz requerimientos, sus puntos y subpuntos:
  - 4.1 Partes del proceso
  - 5.6 Requerimientos técnicos
  - 5.6.2 Aspectos técnicos generales
  - 5.6.4.3 CPD (Centro de protección de datos)
  - 5.6.4.3.5 Seguridad lógica
  - 5.6.4.3.7 Gestión de almacenamientos de la información
  - 5.6.4.3.8 Normatividad en seguridad LOPD y LSSICE
  - 5.6.5.2 Módulo de enrolamiento o registro
  - 5.6.5.6 Módulo de registro de los resultados
  - 5.6.5.9 Módulo de certificación

- Anexo - CRC Matriz requerimientos, sus puntos y subpuntos:
  - 5.1 Partes del proceso
  - 6.2 Requerimientos del aspirante
  - 6.6 Requerimientos técnicos
  - 6.6.2 Aspectos técnicos generales
  - 6.6.4.2 CPD (Centro de protección de datos)
  - 6.6.4.2.5 Seguridad lógica
  - 6.6.4.2.7 Gestión de almacenamientos de la información
  - 6.6.4.2.8 Normatividad en seguridad LOPD y LSSICE
  - 6.6.4.3 Requerimientos Relativos del personal
  - 6.6.4.5 Requerimientos relativos a los registros y la información
  - 6.6.4.6 Información Publica
  - 6.6.5 Seguridad
  - 6.6.5.1.4 Alcance de la certificación
  - 6.6.6.4 Módulo de enrolamiento o registro
  - 6.6.6.6 Módulo de certificación

5.2. COMPROMISOS POSTERIORES

Una vez otorgado el permiso el proveedor / homologado se comprometerá a realizar las actividades, las cuales dependen de cada OAT (Descritas en cada adjunto de matrices de requerimientos).

- Anexo - CALE Matriz requerimientos, sus puntos y subpuntos:
  - No especificada por norma

- Anexo - CDA Matriz requerimientos, sus puntos y subpuntos:

- 5.3.11 Compromisos posteriores

- Anexo - CEA – CIA Matriz requerimientos, sus puntos y subpuntos:
  - 5.6.7 Compromisos posteriores

- Anexo - CRC Matriz requerimientos, sus puntos y subpuntos:
  - 6.6.8 Compromisos posteriores

6. REFERENCIAS

https://www.mintransporte.gov.co/documentos/14/resoluciones/genPag=2&genPagDocs=2
https://www.supertransporte.gov.co/index.php/resoluciones-generales/2020/
https://www.supertransporte.gov.co/index.php/resoluciones-generales/2017/
https://www.supertransporte.gov.co/index.php/resoluciones-generales/2016/
https://www.supertransporte.gov.co/index.php/resoluciones-generales/2014/
https://www.cessi.org.ar/perfilesit/detalle-de-administrador-de-base-de-datos-dba-12
https://www.ac-cc.com/blog/como-funciona-una-ups#:~:text=UPS%20(por%20su%20nombre%20en,el%C3%A9ctrico%20que%20posee%20una%20bater%C3%ADa.&text=La%20unidad%20de%20potencia%20para,eficaz%2C%20consumida%20por%20el%20sistema.
https://protecciondatos-lopd.com/empresas/lssi-ce/
https://es.wikipedia.org/wiki/Wikipedia