Universidad de Los Andes

RUNT

Documento de Arquitectura del Sistema (SAD)

Nombre del Equipo de Trabajo: Manticore

Nombre de los Integrantes:

Carlos Echeverri e-mail: ca.echeverri964@uniandes.edu.co

Jose Aranzazu e-mail: ja.aranzazu913@uniandes.edu.co

Francisco Murcia e-mail: fa.murcia68@uniandes.edu.co

Mario Rodriguez e-mail:me.rodriguez373@uniandes.edu.co

Bogotá D.C. 2008

Versión	Modificado Por	Fecha	Comentarios
1.0	Francisco Murcia Mario Rodríguez	15 Junio 2008	Stakeholders, Concerns, Glosario, Acrónimos, Vista de Despliegue
2.0	Mario Rodríguez	21 Junio 2008	Vista Funcional: Modelo Conceptual, Casos de uso de registro de licencias y de automotores, Diagrama de Componentes
2.1	Francisco Murcia	22 Junio 2008	Vista de despliegue, diagrama de red, diagrama de despliegue y dependencia tecnológica
2.2	Mario Rodríguez	22 Junio 2008	Correcciones vista funcional
2.3	Carlos Echeverri	06 Julio 2008	Perspectiva de seguridad e información general del proyecto
2.4	Jose Aranzazu	10 Julio 2008	Vista de información: modelo de datos, flujo de la información, ciclo de vida de la información
2.5	Carlos Echeverri	21 Julio 2008	
2.6	Francisco Murcia Mario Rodríguez	25 Julio 2008	Punto de vista de Concurrencia Perspectiva de Desempeño y Escalabilidad
2.6	Francisco Murcia	26 Julio 2008	Tablas de contenido corregidas.

Tabla de Contenido

1 Contexto 3

1.1 Problemas a Resolver 3

1.1.1 Descripción General del Sistema a Desarrollar 3

1.1.2 Objetivos 3

2 Stakeholders 4

3 Atributos de Calidad 16

3.1 Perspectivas 16

3.1.1 Seguridad 16

3.1.2 Desempeño y Escalabilidad 21

4 Puntos de Vista 25

4.1 Punto de Vista de Despliegue 25

4.1.1 Descripción 25

4.1.2 Modelos de Plataforma de Ejecución 25

4.1.3 Modelos de Red 26

4.1.4 Modelos de Dependencia Tecnológica 27

4.2 Punto de Vista Funcional 28

4.2.1 Descripción 28

4.2.2 Modelo Conceptual 28

4.2.3 Diagramas de Casos de Uso 29

4.2.4 Diagrama de componentes 30

4.3 Punto de Vista de Información 33

4.3.1 Descripción 33

4.3.2 Modelos de Estructuras Estáticas de Datos 33

4.3.3 Modelos de Flujo de Información 38

4.3.4 Modelos de Ciclo de Vida de Información 39

4.4 Punto de Vista de Concurrencia 41
4.4.1 Descripción 41
4.4.2 Concerns 41
4.4.3 Modelo de Concurrencia del sistema 42
4.4.4 Modelo de estado 43

5 Directorio 45

5.1 Índice 45

5.2 Glosario de Términos 45

5.3 Acrónimos 46

Lista de Figuras

Figura 1: Diagrama de Despliegue 26
Figura 2: Modelo de Red 27
Figura 3: Diagrama de Clases (Análisis) 29
Figura 4: Casos de Uso - Registro de Automotores 30
Figura 5: Casos de Uso - Registro de Licencias 30
Figura 6: Diagrama de Componentes 31
Figura 7: Modelo de Datos 37
Figura 8: Diagrama de Flujo de Datos RUNT 39
Figura 9: Diagrama de Estado - Gestión de Trámites 40
Figura 10: Modelo de Concurrencia 43
Figura 11: Modelo de Estado 44

Lista de Tablas

Tabla 1: Listado de los Stakeholders 4

Tabla 2: Stakeholders y Concerns 5

Table 3: Tiempos de Respuesta 8

Table 4: Stakeolders Vs. Viewpoints: 15

Table 5: Recursos Sensitivos 16

Table 6: Políticas de Seguridad 17

Table 7: Dependencia Tecnológica 28

Table 8: Entidades 36

Table 9: Procesos Principales del RUNT.....38

Table 10: Estados Ciclo de Vida Proceso Gestión de Trámites 41

Table 11: Glosario.....46

1 Contexto

1.1 Problemas a Resolver

Se debe implementar una aplicación denominada por el Ministerio de Transporte RUNT (Registro Único de Transito), la cual debe estar en la capacidad de registrar y mantener centralizada, actualizada, autorizada y validada, la información relacionada con los registros de automotores, conductores, licencias de transito, empresa de transporte público, infractores, accidentes de transito, seguros, remolques y semirremolques, maquinaria agrícola y de construcción autopropulsada y de personas naturales o jurídicas.

El sistema debe cumplir con los requerimientos de seguridad, disponibilidad, confiabilidad y rendimiento de acuerdo a lo establecido por el Ministerio de Transporte y a la normatividad y estándares vigentes.

1.1.1 Descripción General del Sistema a Desarrollar

Tanto la información como la infraestructura del sistema estarán centralizadas. Los usuarios del RUNT podrán registrar, modificar, actualizar y borrar la información administrada por el sistema de acuerdo al tipo de información y privilegios del usuario. El sistema brindará los mecanismos de interconexión para compartir información con las entidades públicas y privadas establecidas por el Ministerio de Transportes. Permitirá el registro remoto de la información electrónica como huellas digitales, firma digital y fotografía. Contará con un Contact Center para la atención al ciudadano.

Todas las transacciones realizadas en el RUNT serán validadas, autorizadas y auditadas por un sistema autorizador central.

El sistema RUNT estará respaldado por un sistema alterno, el cual será idéntico en infraestructura e información. Este sistema entrará en operación cuando el sistema principal sufra algún tipo de daño.

1.1.2 Objetivos

- Centralizar toda la información procesada por la aplicación.
- Ofrecer mecanismos que permitan validar y autorizar las transacciones realizadas.
- Cumplir con los lineamientos de seguridad, disponibilidad, confiabilidad y rendimiento establecidos.
- Ofrecer mecanismos que permitan la conectividad con otras entidades públicas y privadas.

2 Stakeholders

Tabla 1: Listado de los Stakeholders

Stakeholder	Descripción
Ministerio de Transporte	Es la entidad gubernamental encargada de formular y adoptar las políticas, planes, programas, proyectos y regulación económica en materia de transporte, tránsito e infraestructura de los modos de transporte carretero, marítimo, fluvial, férreo y aéreo, como también de la regulación técnica en materia de transporte y tránsito de los modos carretero, marítimo, fluvial y férreo
Direcciones territoriales del ministerio	Son todas aquellas oficinas que representan al Ministerio de Transporte en diferentes regiones del país.
Organismos de transito regionales	Son los diferentes organismos locales encargados de facilitar el desplazamiento y movilización tanto vehicular como peatonal en los municipios del país.
Otros Actores	Son otros organismos gubernamentales o entidades establecidas por el Ministerio de Transporte con las cuales el RUNT se debe integrar para validar y autorizar los registros. Ej.: DIAN, Ministerio de protección Social, DAS, Fiscalía General de la Nación, Superintendencia de Transporte, Ministerio de relaciones Exteriores, Dirección Nacional de Estupefacientes, Ministerio de Minas y Energía, Registraduría Nacional del Estado Civil, Centrales de Inteligencia, Sistema de información de multas de la federación nacional de municipios.
Personas naturales o jurídicas	Son todas aquellas personas o empresa que de una u otra forma deben aportar o recibir información del RUNT. Ej.: conductores, empresas de transporte publico o privado, centros de enseñanza automovilística, ensambladoras de vehículos, compañías aseguradoras.

Stakeholder	Descripción
Concesionario	La empresa o grupos de empresas que va a proveer la infraestructura, servicio y operación del sistema
Entidades Financieras	Organizaciones que captarán dinero resultado de trámites realizados por los ciudadanos en el sistema

Tabla 2: Stakeholders y Concerns

Manejo de la Información

Stakeholder:

- Ministerio de Transporte
- Direcciones territoriales del ministerio
- Organismos de transito regionales
- Concesionario

Concerns:

• Permitir el registro de la información relacionada con:

Registro nacional de automotores

Registro nacional de conductores

Registro nacional de empresas de transporte público y privado

Registro nacional de licencias de transito

Registro nacional de infracciones de transito

Registro nacional de centros de enseñanza automovilística

Registro nacional de seguros

Registro nacional de personas naturales o jurídicas, públicas o privadas que presten servicios al sector publico.

Registro nacional de remolques o semirremolques

Registro nacional de accidentes de transito

Registro nacional de maquinaria agrícola y de construcción autopropulsada

• La información capturada y registrada debe estar centralizada

• Debe permitir registrar información que provenga de otros organismos diferentes al Ministerio de Transporte

• Validar la información incorporada y detectar inconsistencias.

• Validar, autorizar y registrar las transacciones resultado de los tramites de transito y transporte efectuados en los organismos de transito, en las direcciones territoriales y en el Ministerio de Transporte. Esta validación debe impedir la generación fraudulenta o incompleta de un trámite.

• Permitir la actualización y modificación de la información de trámites, manteniendo los datos históricos y el número de autorización.

• Controlar la facturación y el recaudo reportado por las entidades financieras

• Proveer un algoritmo que genere la asignación de rangos de especies venales en forma automática de acuerdo con el procedimiento establecido por el Ministerio de Transporte.

• Integrar con los otros actores la validación y autorización de la información pertinente.

• Recibir la información proveniente de los otros actores de acuerdo a los estándares y convenios establecidos por el Ministerio de Transporte.

• Generar un código de autorización cuando los organismos de transito, las direcciones territoriales y la oficina central del Ministerio de Transporte generen tramites de actualización de registros existentes.

• Generar registros de las transacciones intentadas no exitosas, cuando un intento de actualización de información sea rechazado.

• Proveer al público la información requerida de acuerdo a lo estipulado en el articulo 8 de la ley 769 de 2002 y el articulo 11 de la ley 1005 de 2006, sin perjuicio de la información confidencial, que sea considerada como tal por el ordenamiento jurídico o por el Ministerio de Transporte.

• Los documentos de licencias de conducción y licencias de transito deben ser generados con un sistema de seguridad basado en un código BI-Dimensional y con un alto nivel de encriptación.

• Proveer una herramienta de administración de gestión basada en BPM que permita el análisis de desempeño y ofrezca indicadores de ejecución de los procesos. Esta herramienta debe ser flexible, escalable, deberá centralizarse y ser única

• Debe tener una solución de presentación con sistemas de ayuda al usuario

• Generar información a partir de los datos de registros y transaccionalidad histórica que permita a la entidad competente obtener reportes. Estos reportes deben estar basados en procesos relacionados con Data Warehouse.

• El lenguaje de presentación del sistema debe ser el castellano

• El portal de trámites debe ser diseñado cumpliendo con las buenas prácticas de diseño y desarrollo de portales informáticos definidos en WCAG 1.0

• Debe generar indicadores de las autorizaciones aceptadas y rechazadas por cada organismo de transito y por cada dirección territorial del ministerio.

• Expedir certificación de los datos con los cuales cuenta el registro central vía Internet, contact center o ventanilla.

• Reportar alertas de vehículos

• Permitir la consulta de los requisitos para trámites de registros

• Para los servicios al usuario que impliquen un cobro, debe proveer mecanismos de pago a través de los convenios efectuados con bancos u otros medios de recaudo seguro, que contemplen las posibilidades de consignación en sucursales y medios de pago electrónicos.

• Implementar controles en el registro de la información para garantizar que los errores sean menores a uno (1) por mil (1000).

• Los nodos se clasifican de acuerdo al número de trámites diarios de la siguiente manera:

- Tipo I: Ciudades principales (Bogotá, Medellín, Cali, Barranquilla y Bucaramanga). Organismos de transito (OT) con más de 51 tramites diarios. Total 25
- Tipo II: Organismos con un número de tramites diarios entre 26 y 50. Total 27 más las 6 principales direcciones territoriales del ministerio (DT).
- Tipo III: Organismos con un número de tramites diarios entre 11 y 25. Total 36 más 14 direcciones territoriales del ministerio.
- Tipo IV: Organismos con menos de 10 tramites diarios. Total 124.

De acuerdo a lo anterior, los tiempos de respuesta del RUNT deben ajustarse a la siguiente tabla:

Procesos del RUNT	OT tipo I y II	DT tipo II	OT tipo III y IV	DT tipo III
Tiempos de respuesta de todas	1 seg.	2seg	3 seg.	3 seg.

las transacciones efectuadas contra el nodo central				

Table 3: Tiempos de Respuesta

• Cada usuario que genere información para el sistema, deberá contar con un certificado digital que permita autenticar el sitio de origen.

• La identidad del ciudadano debe ser autenticada contra la Registraduría Nacional del Estado Civil, en el primer trámite.

• Todos los sistemas de información deben contar con los mecanismos, herramientas y procesos que permitan realizar una adecuada gestión de Auditoria de Sistemas.

• La auditoria de sistemas servirá para garantizar que la información almacenada no haya sido manipulada externamente, y generará reportes y alarmas en caso de presentarse transacciones no autorizadas

• La información de firmas digitales debe ser encriptada

Stakeholder:

- Otros Actores

Concerns:

• Debe permitir registrar información que provenga de otros organismos diferentes al Ministerio de Transporte

• Integrar con los otros actores la validación y autorización de la información pertinente.

• Recibir la información proveniente de los otros actores de acuerdo a los estándares y convenios establecidos por el Ministerio de Transporte.

• Cada usuario que genere información para el sistema, deberá contar con un certificado digital que permita autenticar el sitio de origen.

• La identidad del ciudadano debe ser autenticada contra la Registraduría Nacional del Estado Civil, en el primer trámite.

Stakeholder:

- Personas naturales o jurídicas

Concerns:

• Proveer al público la información requerida de acuerdo a lo estipulado en el articulo 8 de la ley 769 de 2002 y el articulo 11 de la ley 1005 de 2006, sin perjuicio de la informa-

ción confidencial, que sea considerada como tal por el ordenamiento jurídico o por el Ministerio de Transporte.

• Debe tener una solución de presentación con sistemas de ayuda al usuario

• El lenguaje de presentación del sistema debe ser el castellano

• Expedir certificación de los datos con los cuales cuenta el registro central vía Internet, contact center o ventanilla.

• Permitir la consulta de los requisitos para trámites de registros

• Para los servicios al usuario que impliquen un cobro, debe proveer mecanismos de pago a través de los convenios efectuados con bancos u otros medios de recaudo seguro, que contemplen las posibilidades de consignación en sucursales y medios de pago electrónicos.

• Los diferentes trámites deberán contar con un sistema de autenticación basado en huella digital

• La identidad del ciudadano debe ser autenticada contra la Registraduría Nacional del Estado Civil, en el primer trámite.

Stakeholder:

- Entidades Financieras

Concerns:

• Controlar la facturación y el recaudo reportado por las entidades financieras

• Para los servicios al usuario que impliquen un cobro, debe proveer mecanismos de pago a través de los convenios efectuados con bancos u otros medios de recaudo seguro, que contemplen las posibilidades de consignación en sucursales y medios de pago electrónicos.

• Cada usuario que genere información para el sistema, deberá contar con un certificado digital que permita autenticar el sitio de origen.

Infraestructura

Stakeholder:

- Ministerio de Transporte
- Direcciones territoriales del ministerio
- Organismos de transito regionales

- Concesionario

Concerns:

• Debe existir una infraestructura central que soporte todas las operaciones establecidas.

• El sistema RUNT deberá estar interconectado con cada uno de los organismos de transito, las direcciones territoriales, el Ministerio de Transporte y los otros actores. Esta interconexión debe permitir diferentes tipos de canales

• La conexión con los otros actores debe ser en línea y en tiempo real con las medidas de seguridad pertinentes.

• Los trámites se deben ejecutar de forma electrónica y personal, contando con lectores de huella dactilar, lector de firma electrónica y video cámara para la captura centralizada y remota de la foto, la firma y la huella

• El sistema debe brindar una disponibilidad de 7 * 24 * 365.

• Deben existir sistemas de operación de contingencia que entrarán a operar en caso que falle el sistema principal.

• Proveer un Contact Center para atención al ciudadano ya sea mediante llamadas telefónicas, correos electrónicos u otros medios electrónicos

• Proveer herramientas que permitan comunicarse con aplicaciones y transmitir información desde y hacia el RUNT. Esta herramienta debe ser flexibles, escalables, deberán centralizarse y ser únicas.

• Debe ser un sistema 100% Web Based.

• Debe estar construido con una arquitectura multi-niveles (n-tier) que le permita una escalabilidad horizontal y vertical

• Debe cumplir con los niveles de seguridad establecidos por las normas ISO 17799 y 27001

• Los diferentes trámites deberán contar con un sistema de autenticación basado en huella digital

• Debe existir una base de datos central de Huellas digitales

• Durante la creación de la base de datos de huellas, se capturará la firma digital, mediante algún dispositivo electrónico.

• Los poderes para autorización de trámites serán autorizados mediante confrontación de las firmas digitales.

• La generación de las licencias se debe realizar en el sistema central, generándola con un código de barras bidimensional encriptado

• La impresión de las licencias será realizada en forma descentralizada en cada uno de los Organismos de Tránsito

• Cada uno de los computadores del RUNT debe utilizar un lector biométrico para reconocimiento de huella

• Los drivers de lectura de Huella dactilar deben cumplir con la norma ANSI / Mist ITL I-2000

• Los perfiles de usuario para los sistemas de información del RUNT deberán estar basados en el reconocimiento de huella dactilar

• El firewall debe tener un esquema de alta disponibilidad

• El concesionario deberá suministrar a cada una de las direcciones territoriales del Ministerio y de los organismos de tránsito cuya comunicación se haga a través de VPN un firewall.

• El sistema de seguridad del RUNT debe ser implementado antes del inicio de la Fase de Operación y debe ser certificado en el mismo plazo ante un organismo de certificación con la NTC- BS- 7799-2

• Se debe tener un agente de recopilación de información de cada servidor y que la transmita de forma segura al repositorio central

• Se debe tener un servidor de auditoria centralizada, donde se almacenarán los logs de los servidores

• El agente debe estar siempre disponible y no debe afectar el desempeño al registrar eventos

• Los logs se almacenarán en el repositorio central en un periodo mínimo de un mes, después se aplicarán los procesos de respaldo y recuperación

• Si la conexión entre los agentes de aplicación y el servidor de auditoria falla, las aplicaciones de manera transparente deberán continuar registrando los log localmente hasta que la conexión sea restaurada y se enviarán los registros que no se hayan transmitido

• Se debe contar con mecanismos para verificar que la información enviada por una aplicación fue recibida de manera correcta y completa al servidor de auditoria

• Se debe garantizar que los registros de log enviados desde un agente no sean alterados durante su transporte

• Debe existir un sistema de monitoreo y gestión de red para garantizar niveles de servicio

• Debe existir un antivirus, que asegure que un archivo infectado no se pierda y generar reportes con todo el archivo, la hora de atención y el origen

• Debe existir un sistema de prevención de intrusos que permita la inspección profunda de paquetes, que tenga una capacidad de filtrar en línea hasta 2 GBps, manejar en forma simultanea hasta 10000 conexiones y debe tener el desempeño equivalente a un switch

• Los sistemas de seguridad deben contar con un esquema de gestión que permitan administrar, configurar y dar soporte a toda la plataforma, desde un ambiente WEB en forma segura

• Debe existir una solución robusta para la generación automática de copias de respaldo

• Deberá existir una copia de respaldo en un municipio diferente a la ciudad de Bogota, para garantizar la continuidad en la prestación del servicio

• Las comunicaciones internas entre las direcciones territoriales del ministerio y los organismos de tránsito, se basaran sobre voz por IP. No se debe afectar el desempeño de los sistemas de información

• Se debe contar con un sistema (Servidor de Aplicaciones) que permita acceder desde cualquier Organismo de Transito, Dirección Territorial del Ministerio u oficina central del Ministerio a las aplicaciones centrales del R.U.N.T. vía WEB. Además debe permitir que las aplicaciones sean rápidas, confiables, seguras y fáciles de administrar.

• El sistema (Servidor de Aplicaciones) debe permitir integrar datos dispersos que provienen de diferentes plataformas al igual que la consolidación de aplicaciones desarrolladas en múltiples herramientas.

Servidor Web (Web Server)

• El Software de servidor WEB debe soportar configuraciones de alta disponibilidad y deberá proveer los componentes gráficos de administración.

Servidor de Aplicaciones

• El servidor de aplicaciones debe soportar configuraciones de alta disponibilidad que permita trabajar aplicaciones instaladas en múltiples nodos en forma activo-activo e incluir los componentes gráficos de administración que permitan configurar ambientes de clustering.

Servidor de Manejo de Identidad LDAP

• Los servicios del directorio deben estar en capacidad de correr en arquitectura de alta disponibilidad activo-activo en dos o más nodos configurados en cluster.

• El directorio podrá utilizar mecanismos de carga masiva de definición de usuarios.

• El directorio debe soportar mecanismos de integración con otros directorios

• El directorio debe soportar el modelo de información X.500 y soportar cambios en línea al esquema del directorio sin necesidad de reiniciar los servicios del directorio, así como

soportar replicación multimaestro a otros directorios LDAP. Con capacidad de generar y publicar certificados PKI X.509 V3.

Servidor de Portal

• La arquitectura del servidor del portal debe soportar configuraciones de alta disponibilidad activo-activo en los nodos definidos como participantes de un cluster

Servidor de Aplicaciones Business Intelligence

• Generación de reportes contra bases de datos relacionales en múltiples formatos (pdf, html, csv, txt)

• Debe permitir la creación de consultas ad-hoc por parte de usuarios no técnicos, las cuales proporcionen por lo menos dos interfases para Web, una interfaz liviana que genere código html, y una interfaz más robusta en capacidad GUI.

• Debe soportar integración con el directorio LDAP y configuraciones de alta disponibilidad activo-activo en los nodos definidos como participantes de un cluster.

Servidor de Caché

• Debe soportar configuraciones de alta disponibilidad Activo-Activo en los nodos definidos como participantes de un cluster.

Herramientas de colaboración en tiempo real

• Se debe contar con herramientas de colaboración (Servidor de correo, Chat, colaboración, gestión documental, calendarios, contactos, tablero de anuncios)

Administración y Soporte

• El sistema debe contar con una herramienta de administración centralizada, que permita implementar como mínimo las siguientes funciones: Administración de servidores, Generación y administración de niveles de servicio, Administración de la red, Administración de aplicaciones, Administración de bases de datos y Mesa de ayuda.

• La distribución de software para toda la red a nivel nacional debe llevar un registro de las solicitudes a la mesa de ayuda y la conformación de una base de conocimiento con los problemas y las soluciones

Sistema Único de Autenticación a Usuarios

• Se debe contar con una implementación de un sistema único de identificación, autenticación y contabilización mediante el uso de un único usuario y contraseña.

• El sistema debe contar con un esquema de redundancia que asegura la disponibilidad.

• El sistema debe estar preparado para atender un número considerable de usuarios (1500 inicialmente) y de registros (20000000) con una tasa de crecimiento constante.

• El sistema debe tener en cuenta el crecimiento de los datos y reservar el 30% del espacio de almacenamiento durante toda la operación.

• El centro de cómputo en su totalidad será redundante, para esto, se debe contar con un centro de cómputo alterno con las mismas características físicas y lógicas del centro de cómputo operacional.

• Las bases de datos de los dos centros de cómputo (principal y alterno) deberán mantenerse actualizadas asincrónicamente cada 15 segundos.

• El sistema debe proveer 3 niveles de acceso:

  • Intranet: Organismos de Tránsito, Direcciones Territoriales, Ministerios de Transporte.

  • Extranet: Otros Actores, Entidades Gubernamentales, Entidades Judiciales, etc.

  • Internet: Personas Naturales y Jurídicas.

• Los centros de cómputo deberán estar conectados por medio de un canal dedicado.

• El esquema de comunicaciones entre los organismos y dependencias del Ministerio de Transporte a nivel nacional, estará regido por los acuerdos de servicio.

Stakeholders:

- Otros Actores

Concerns:

• El sistema RUNT deberá estar interconectado con cada uno de los organismos de transito, las direcciones territoriales, el Ministerio de Transporte y los otros actores. Esta interconexión debe permitir diferentes tipos de canales

• La conexión con los otros actores debe ser en línea y en tiempo real con las medidas de seguridad pertinentes.

Stakeholders:

- Personas naturales o jurídicas

Concerns:

• Proveer un Contact Center para atención al ciudadano ya sea mediante llamadas telefónicas, correos electrónicos u otros medios electrónicos

• Debe ser un sistema 100% Web Based.

• Durante la creación de la base de datos de huellas, se capturará la firma digital, mediante algún dispositivo electrónico.

• Los poderes para autorización de trámites serán autorizados mediante confrontación de las firmas digitales.

Stakeholder	**Viewpoints**
Ministerio de Transporte	Deployment, Funcional
Direcciones territoriales del ministerio	Deployment, Funcional
Organismos de transito regionales	Deployment, Funcional
Otros Actores	Funcional
Personas naturales o jurídicas	Funcional
Concesionario	Deployment, Funcional
Entidades Financieras	Funcional

Table 4: Stakeolders Vs. Viewpoints:

3 Atributos de Calidad

3.1 Perspectivas

3.1.1 Seguridad

3.1.1.1 Recursos Sensitivos

La siguiente tabla describe los componentes, tomados de la vista funcional, más sensibles que deberían ser asegurados. Estos componentes son considerados sensibles ya que representan el core del RUNT porque concentran, en términos conceptuales, los servicios que dan un mayor valor al negocio.

Recurso	Sensibilidad	Propietario	Control de acceso
Autenticación y autorización	Es el punto de entrada a la aplicación.	RUNT	Acceso es a través de los componentes expuestos a los usuarios
Persistencia	Toda la información persistente debe ser protegida	RUNT	Acceso solo mediante los componentes de lógica de negocio.
DatawareHouse	Genera información sensible y de gran importancia para los stakeholders	RUNT	Acceso solo mediante el componente de consultas.
Recaudos	Es el mecanismo de comunicación con las entidades financieras	RUNT	Acceso solo mediante los componentes de lógica de negocio.

Table 5: Recursos Sensitivos

3.1.1.2 Políticas de Seguridad

Las políticas de seguridad se describen sobre las entidades que contienen la información principal del sistema, para cada una de ellas se menciona el control de acceso estipulado para los diferentes stakeholders. En el punto de vista de información se realiza una descripción detallada de las entidades utilizadas en este análisis.

	Licencias	Infracciones	Automotor	Conductor
Ministerio de transporte	Completo con auditoria	Completo con auditoria	Completo con auditoria	Completo con auditoria
Direcciones territoriales	Operaciones de lecto-escritura	Operaciones de lecto-escritura	Operaciones de lecto-escritura	Operaciones de lecto-escritura
Organismos regionales	Operaciones de lecto-escritura	Operaciones de lecto-escritura	Operaciones de lecto-escritura	Operaciones de lecto-escritura
Otros actores	Operaciones de solo lectura	Operaciones de solo lectura	Operaciones de solo lectura	Operaciones de solo lectura
Persona naturales o jurídicas	Operaciones de solo lectura	Operaciones de solo lectura	Operaciones de solo lectura	Operaciones de solo lectura
Concesionario	Completo con auditoria	Completo con auditoria	Completo con auditoria	Completo con auditoria
Entidades financieras	Ninguno	Ninguno	Ninguno	Operaciones de solo lectura

Table 6: Políticas de Seguridad

3.1.1.3 Árbol de Ataques

Objetivo: Cambiar la información manejada por el sistema

1. Acceso a la información por medio de la interfaz Web

   1.1 Conseguir el nombre y password de un usuario legítimo para acceder al sistema.

2. Acceso a la información utilizando los servicios Web

   2.1 Acceder a un servicio Web para tratar de realizar operaciones diferentes.

   2.2 Suplantar la identidad del usuario del servicio Web

3. Acceso directamente a la información

   3.1 Modificar la información desde la base de datos

   3.2 Modificar la información mediante le ejecución de scripts SQL

Objetivo: Denegación de los servicios del RUNT

1. Denegación por solicitudes.
   1.1 Saturar el servidor con solicitudes falsas.
   1.2 Realizar ataques desde la red interna del RUNT
   1.3 Scanear los puertos para determinar cuales pueden ser receptivos o de utilidad
2. Denegación física de los servicios.
   2.1 Apagar los servidores que prestan los servicios.
   2.2 Desconectar las fuentes de energía de las maquinas
3. Modificación del software
   3.1 Instalar o copiar virus en los servidores
   3.2 Borrar los archivos claves del software que soporta los servicios del RUNT

Objetivo: Interceptar las comunicaciones utilizadas por el RUNT

1. Redireccionamiento o cambio de los mensajes.
   1.1 Insertar mensajes falsos en la red o añadir contenido a mensajes validos.
   1.2 Redireccionar los mensajes a un destino no valido
2. Interpretación de los mensajes
   2.1 Monitorear e interpretar la información enviada y recibida

3.1.1.4 Calidad Deseada

El sistema debe cumplir con todas las necesidades de seguridad establecidas por el cliente, teniendo como más relevantes las siguientes:

- Cumplir con la norma ISO 17799 y 27001.
- Validar, autorizar y registrar las transacciones.
- Encriptar la información.
- Usar certificados digitales.

3.1.1.5 Aplicabilidad

- Punto de vista Funcional: Alto

- Punto de vista de Despliegue: Alto
- Punto de vista de Información: Alto

3.1.1.6 Concerns

- Validar la información incorporada y detectar inconsistencias.
- Validar, autorizar y registrar las transacciones resultado de los tramites de transito y transporte efectuados en los organismos de transito, en las direcciones territoriales y en el Ministerio de Transporte. Esta validación debe impedir la generación fraudulenta o incompleta de un trámite.
- Integrar con los otros actores la validación y autorización de la información pertinente.
- Los documentos de licencias de conducción y licencias de transito deben ser generados con un sistema de seguridad basado en un código BI-Dimensional y con un alto nivel de encriptación.
- Cada usuario que genere información para el sistema, deberá contar con un certificado digital que permita autenticar el sitio de origen.
- La información de firmas digitales debe ser encriptada
- La identidad del ciudadano debe ser autenticada contra la Registraduría Nacional del Estado Civil, en el primer trámite.
- Los diferentes trámites deberán contar con un sistema de autenticación basado en huella digital
- Para los servicios al usuario que impliquen un cobro, debe proveer mecanismos de pago a través de los convenios efectuados con bancos u otros medios de recaudo seguro, que contemplen las posibilidades de consignación en sucursales y medios de pago electrónicos.
- La conexión con los otros actores debe ser en línea y en tiempo real con las medidas de seguridad pertinentes.
- Debe cumplir con los niveles de seguridad establecidos por las normas ISO 17799 y 27001
- La generación de las licencias se debe realizar en el sistema central, generándola con un código de barras bidimensional encriptado
- Cada uno de los computadores del RUNT debe utilizar un lector biométrico para reconocimiento de huella
- Los perfiles de usuario para los sistemas de información del RUNT deberán estar basados en el reconocimiento de huella dactilar

- El concesionario deberá suministrar a cada una de las direcciones territoriales del Ministerio y de los organismos de tránsito cuya comunicación se haga a través de VPN un firewall.
- El sistema de seguridad del RUNT debe ser implementado antes del inicio de la Fase de Operación y debe ser certificado en el mismo plazo ante un organismo de certificación con la NTC- BS- 7799-2
- Se debe tener un agente de recopilación de información de cada servidor y que la transmita de forma segura al repositorio central
- Se debe garantizar que los registros de log enviados desde un agente no sean alterados durante su transporte
- Los sistemas de seguridad deben contar con un esquema de gestión que permitan administrar, configurar y dar soporte a toda la plataforma, desde un ambiente WEB en forma segura

3.1.1.7 Actividades

- Identificar la información que puede ser modificada.
- Definir tipos de usuario y nivel de acceso a la información.
- Identificar los servicios e interfaces que deben ser expuestos por el sistema.
- Identificar las debilidades de los componentes externos que deben ser utilizados por el sistema.
- Realizar pruebas de fallas para verificar la recuperabilidad e integridad de la información.
- Identificar las operaciones que deben ser auditadas.
- Identificar las vulnerabilidades de las redes que se deben utilizar para realizar las operaciones establecidas.

3.1.1.8 Tácticas

- Autenticar los usuarios del sistema. Para usuarios internos o conocidos utilizar nombre de usuario y password y autorización biométrica en los casos que sea necesario. Para usuarios externos utilizar certificados digitales.
- Implementar un mecanismo basado en Web-SSO para habilitar el acceso de los usuarios a los diferentes sistemas con una sola instancia de identificación.
- Involucrar políticas para la generación y administración de claves de usuario seguras.
- Encriptar la información transportada por la aplicación utilizando llaves públicas y privadas, ofrecidas por el protocolo SSL para evitar el packet sniffers.

- Validar todas las operaciones realizadas por los usuarios, verificando que la operación sea realizada por un usuario valido.
- Usar firewall físicos para restringir el acceso al sistema.
- Limitar el acceso a las instalaciones físicas donde serán alojados los servidores del sistema.
- Realizar planes de recuperación de desastres. Estos planes deben contemplar desastres naturales, fallas de software, fallas de hardware, ataques informáticos.
- Configurar los mecanismos necesarios para restringir el acceso directo a la información.
- Rechazar las conexiones que no provengan de usuarios conocidos y por medios validos.
- Usar software para monitorear toda la infraestructura de red.

3.1.2 Desempeño y Escalabilidad

3.1.2.1 Calidad Deseada

Como parte de los pliegos de especificación para el sistema RUNT, el Ministerio de Transporte estableció unos requerimientos mínimos de desempeño que deben ser cumplidos por la aplicación; adicionalmente, debido al crecimiento que se tiene estimado para los datos y el acceso concurrente de usuarios, la arquitectura deberá estar preparada para adaptarse en el tiempo sin afectar el desempeño.

Para suplir la necesidad inicial de soportar miles de usuarios en línea concurrentes, el Ministerio sugiere utilizar una infraestructura basada en redundancia, esto es, que los puntos sensibles de acceso a la aplicación, deberán estar funcionando en cluster para asegurar el continuo funcionamiento y la mayor cantidad de usuarios concurrentes en el sistema.

Las siguientes son las estimaciones iniciales:

- Se deberá soportar inicialmente 1550 usuarios concurrentes.
- Se deberá soportar inicialmente 200 millones de registros (conductores, multas, rangos de vehículos, etc.)
- Se deberá soportar inicialmente un mínimo de 5 millones de consultas mensuales.
- Se estima que la tasa de crecimiento anual de los datos será del 4%.

Adicional a los mencionados, debido al requerimiento de registro de operaciones a nivel global de la aplicación, la recolección de dichos datos deberá ser lo más eficiente posible para que no se vea afectado el desempeño.

3.1.2.2 Aplicabilidad

- Punto de vista Funcional: Alto; el sistema debe estar en capacidad de asegurar funcionalmente que los requerimientos de desempeño y escalabilidad son cumplidos a cabalidad.
- Punto de vista de Información: Alto; el manejo de la información, teniendo en cuenta los requerimientos estimados iniciales de desempeño y escalabilidad, debe presentar un modelo muy flexible y eficiente para el almacenamiento y transporte de datos.
- Punto de vista de Concurrencia: Alto; este punto de vista es uno de los más afectados por esta perspectiva, ya que la concurrencia es un factor que afecta desempeño de forma drástica, y es directamente proporcional con la escalabilidad, debido a que si la concurrencia aumenta, para que el desempeño no se vea afectado, la escalabilidad entra a jugar un papel importante en el crecimiento a nivel de infraestructura y funcionalidad.
- Punto de vista de Desarrollo: Alto; se deben establecer estándares y patrones de desarrollo que giren en torno del desempeño, por ejemplo, optimización de algoritmos, delegación de responsabilidades a componentes especializados, etc.
- Punto de vista de Despliegue: Alto; la infraestructura del sistema determina en gran parte el desempeño y escalabilidad del sistema, ya que la infraestructura debe estar planeada, pensando en la carga a nivel de procesamiento que pueda generar el sistema. Cómo estamos hablando de un sistema que se encontrará disponible a nivel nacional, la infraestructura deberá estar acorde a la cantidad de operaciones que podría llegar a manejar el sistema y es por ello que se sugiere usar una plataforma redundante.
- Punto de vista Operacional: Alto; para el RUNT de antemano se asume, que tendrá una considerable cantidad de operaciones desde distintos puntos de entrada en un momento determinado.

3.1.2.3 Concerns

- Tiempos de Respuesta
    - Creación de un conductor: 5 segundos
    - Actualización de un conductor: 5 segundos
    - Eliminación de un conductor: 5 segundos
    - Radicación de un trámite: 20 segundos
- Rendimiento
    - Reporte de trámites en el mes (miles de cientos de registros): 2 horas
    - Consulta de trámites para un usuario determinado dentro de un rango de fechas: 5 registros / 10 segundos

- Escalabilidad
    - El sistema debe contar con la infraestructura necesaria para soportar el crecimiento de datos estimado (4% anual). Para esto se planea utilizar un sistema SAN, que conste de arreglos de discos a los que se les pueda agregar más capacidad de forma dinámica y en caliente.
    - El sistema debe mantenerse sincronizado con el centro espejo de respaldo, que entrará en funcionamiento en caso de falla del sistema principal. La base de datos espejo debe ser una fiel copia de la base de datos principal; para llevar esto a cabo, el sistema deberá ejecutar un proceso de actualización con periodicidad de 15 segundos.
    - La aplicación tramitadora debe tener en cuenta que los procedimientos realizados en los diferentes trámites ofrecidos por el sistema están sujetos a la ley y a las disposiciones gubernamentales. Por esto, los componentes deben poder ser reemplazados o refabricados de manera que no afecte el normal funcionamiento del sistema.
    - La infraestructura del sistema debe estar preparada para el aumento, con el paso del tiempo, de los usuarios que estarán accediendo los servicios ofrecidos, por ello, deberá permitir agregar servidores a los diferentes clusters establecidos que aumenten la capacidad de procesamiento.

3.1.2.4 Actividades

- Analizar los modelos de desempeño
    - Caracterizar las cargas de trabajo: Identificar la carga que deberá ejecutar los componentes del sistema, cada uno de los niveles de la arquitectura tiene funciones que son utilizadas por los demás niveles, aunque puede que tengan cargas diferentes.
    - Estimar el rendimiento: Realizar estimaciones por medio de pruebas o prácticas que permitan encontrar el punto óptimo de desempeño sobre condiciones ambientales preestablecidas, para así determinar los niveles de servicio.
- Llevar a cabo pruebas prácticas
    - Estimar las métricas de desempeño: Por medio de pruebas de stress y carga, establecer las medidas óptimas de desempeño que estén de acuerdo con los acuerdos de servicio.
    - Llevar a cabo las pruebas: Ejecutar dichas pruebas y obtener datos y medidas como base de estimación y comparación.
- Evaluar contra los requerimientos

  - Identificar los riesgos: Establecer los costos derivados de los riesgos potenciales que se puedan presentar al analizar los resultados de las pruebas prácticas. Se deben priorizar de acuerdo al efecto que tengan sobre los acuerdos de servicio.
  - Revisar los requerimientos: Comparar los resultados obtenidos con los requerimientos establecidos por el cliente para así llegar a acuerdos aceptados por éste último.

- Iterar sobre la arquitectura: En caso de no llegar a un acuerdo o de que los resultados se encuentren muy desfasados con respecto a las estimaciones, se deben realizar nuevas iteraciones hasta alcanzar la medida más cercana.

3.1.2.5 Tácticas

- Buscar utilizar tecnología que permita realizar cambios estructurales en caliente.
- Desarrollar componentes muy desacoplados, que permitan ser cambiados y refabricados sin afectar el sistema.
- Controlar constantemente, por medio de los agentes de registro, el estado de ejecución del sistema, para detectar y planear con tiempo posibles estados de actualización tanto de hardware como de software.
- Clasificar los procesos que se ejecutarán en el sistema, para determinar los patrones o buenas prácticas más eficientes y convenientes para su desarrollo

4 Puntos de Vista

4.1 Punto de Vista de Despliegue

4.1.1 Descripción

Este punto de vista describe el ambiente en el cual el sistema será instalado, identificando los diferentes nodos, la relación entre ellos y la forma como se comunican. Los nodos que representan toda la infraestructura servidor (servidores, firewall, balanceadores de carga), estarán ubicados en una misma instalación física de acuerdo a los requerimientos del cliente.

4.1.2 Modelos de Plataforma de Ejecución

Éste modelo describe los diferentes nodos de ejecución, sobre los que el RUNT será ejecutado y operado. La plataforma consta de una serie de servidores en cluster, que pretenden ofrecer un servicio continuo, en los puntos más sensibles de la infraestructura. Los servidores Web, de Aplicaciones y de Bases de Datos tendrán una carga transaccional muy fuerte durante la ejecución del sistema, ya que se espera atender usuarios desde cualquier punto del país, concurrentemente. Adicionalmente, los organismos y direcciones del ministerio de transporte a nivel nacional, tendrán un canal dedicado de conexión con el nodo principal, para asegurar un servicio seguro y de alta confiabilidad.

Los clientes, internos y externos, usarán un navegador Web como medio de interacción primario con el sistema. Para esto, se dispondrán balanceadores de carga que se encargaran de seleccionar el servidor más adecuado de acuerdo a parámetros de desempeño configurados previamente.

Adicional al servidor de autenticación LDAP especificado en el problema, se hará uso de un servidor especializado en el almacenamiento de Biométricos. Los biométricos hacen referencia a huellas, retinas y demás información que pueda ser tomada del cuerpo humano para ser usada como referencia de seguridad.

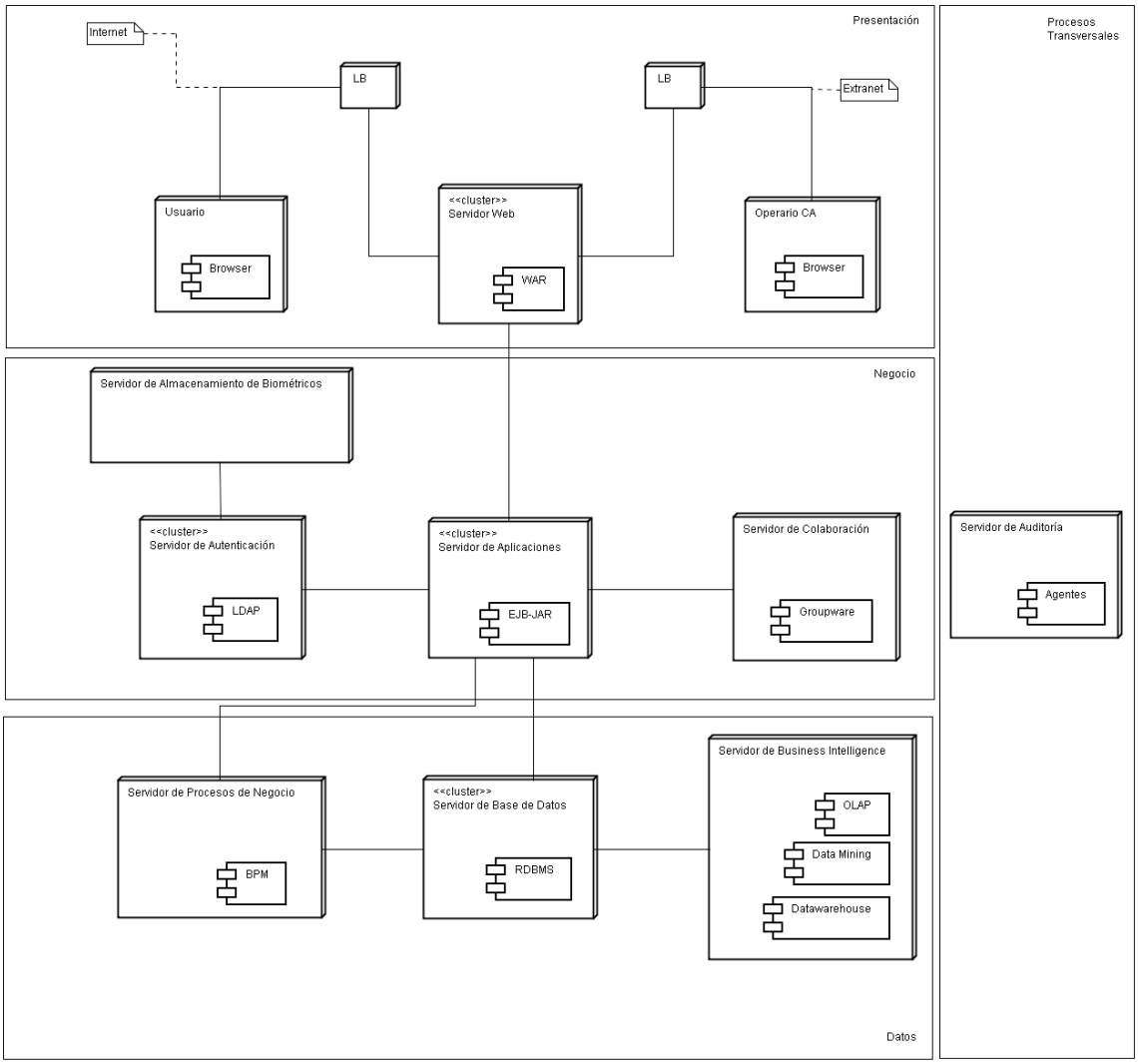

Figura 1: Diagrama de Despliegue

4.1.3 Modelos de Red

Los usuarios del sistema serán atendidos principalmente usando el protocolo HTTP desde sus navegadores Web. Los organismos y direcciones territoriales del ministerio a nivel nacional, contarán con un canal dedicado, establecido por medio de una red privada virtual (VPN) que asegurará que la información que sea intercambiada por este medio, viaje de forma segura y confiable. Para los dos medio mencionados, se dispondrá de un punto de entrada único, cuyo primer filtro será un sistema de detección de intrusos (IDS) encargado de denegar acceso a cualquier acción o intento de ejecución riesgoso.

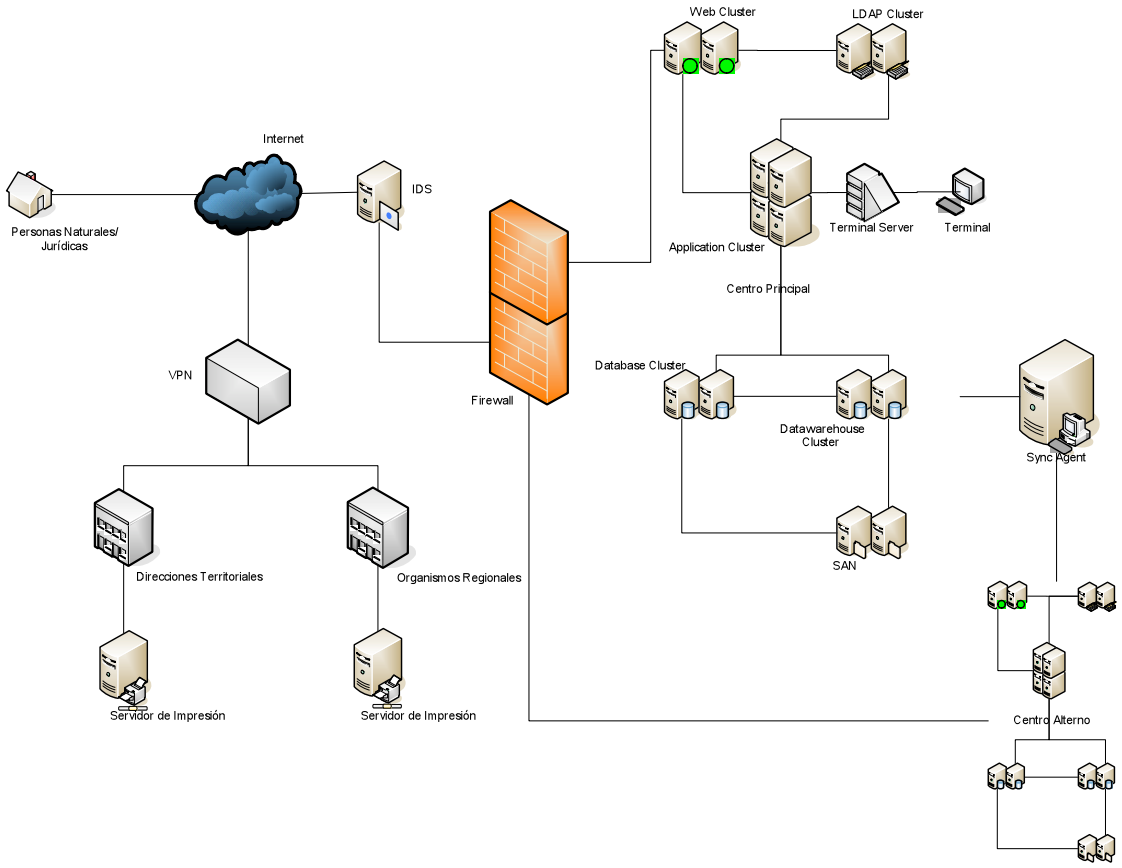

Figura 2: Modelo de Red

4.1.4 Modelos de Dependencia Tecnológica

Componente	Requiere
PC Cliente	Windows XP Profesional SP3 Browser IE 6.X SP2
Servidor WEB	Windows Server 2003 R2 Enterprise Edition SP 2 WebSphere Application Server 6.0.1
Servidor Aplicaciones	Windows Server 2003 R2 Enterprise Edition SP 2 WebSphere Application Server 6.0.1
Servidor Base De Datos	Windows Server 2003 R2 Enterprise Edition SP 2 Oracle Database 10g Release 10.2.0.1.0

	PL/SQL Release 10.2.0.1.0 CORE 10.2.0.1.0 TNS for 32-bit Windows: Version 10.2.0.1.0 NLSRTL Version 10.2.0.1.0
Conexión Base de Datos	ojdbc14 for release 10.2.0.1.0
WebSphere Application Server 6.0.1	Java 2 Technology Edition, V1.4.2 SR1a
IBM Tivoli Directory Server	LDAP DB2 9

Table 7: Dependencia Tecnológica

4.2 Punto de Vista Funcional

4.2.1 Descripción

Mediante este puntote vista se describirán los elementos funcionales del sistema, así como sus principales responsabilidades, interfaces e interacciones.

4.2.2 Modelo Conceptual

Mediante este diagrama, se abstraen las entidades más relevantes, que expresan la interacción entre los elementos y la cobertura de los requerimientos funcionales.

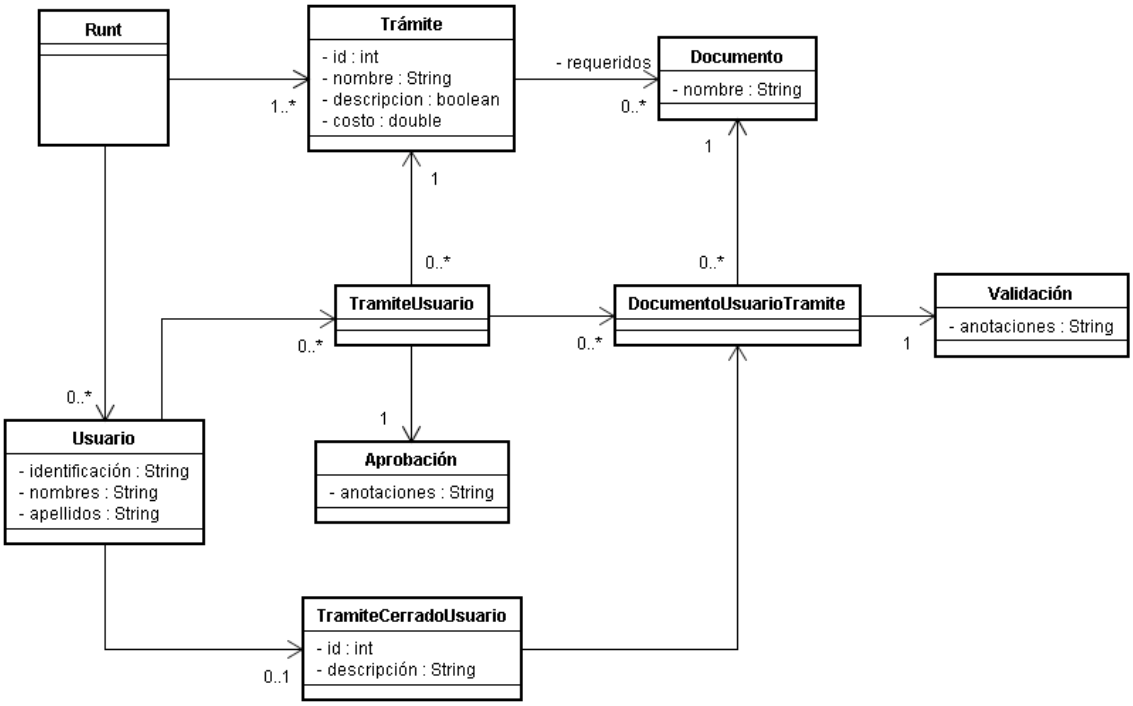

Figura 3: Diagrama de Clases (Análisis)

4.2.3 Diagramas de Casos de Uso

Estos diagramas expresan los requerimientos funcionales para las aplicaciones “Registro de Automotores” y “Registro de Licencias de tránsito”

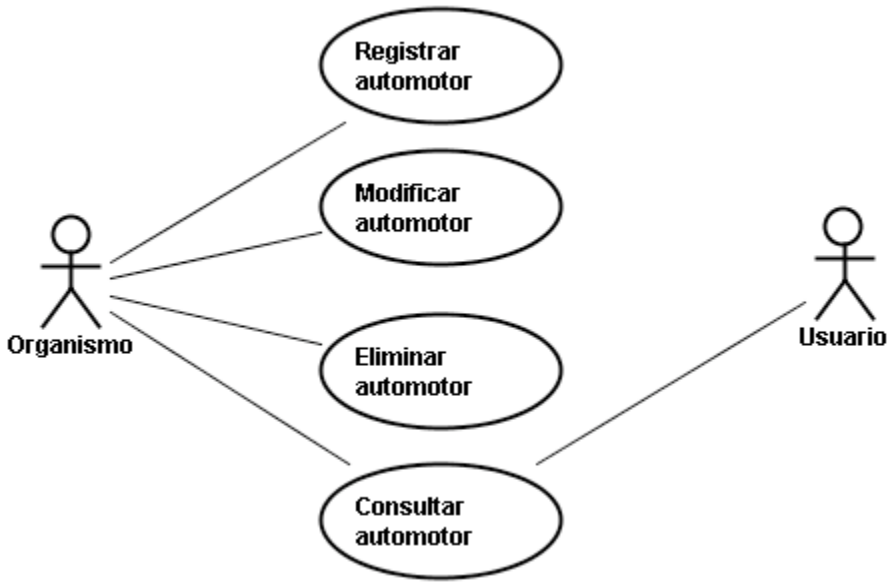

Figura 4: Casos de Uso - Registro de Automotores

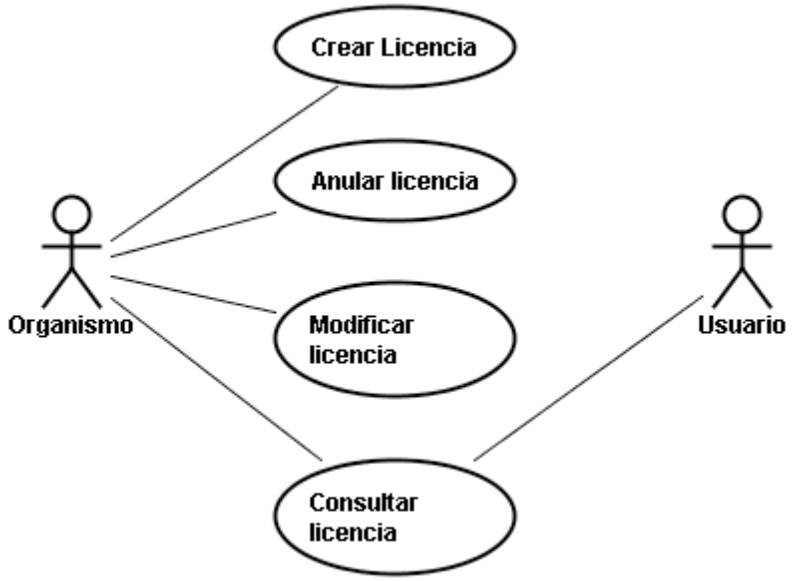

Figura 5: Casos de Uso - Registro de Licencias

4.2.4 Diagrama de componentes

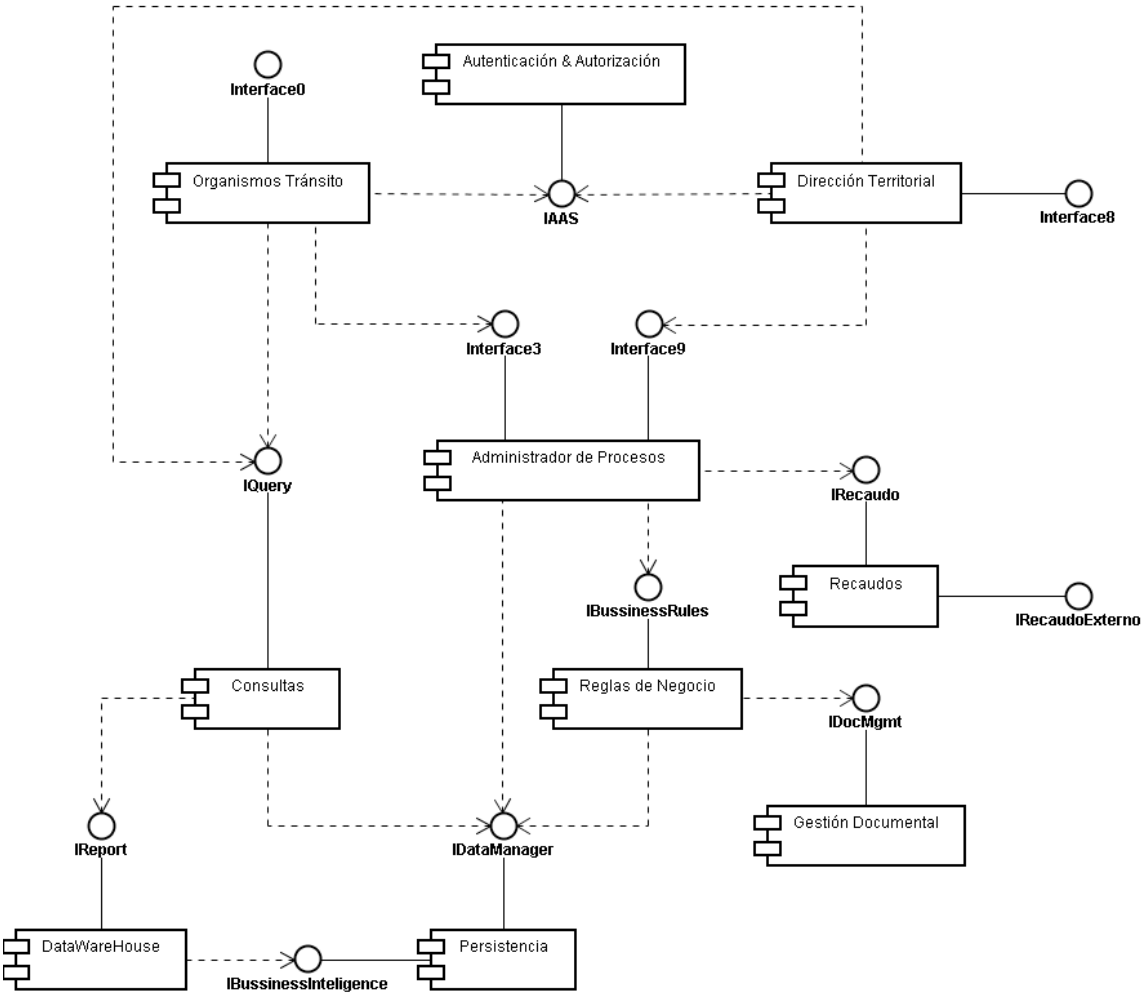

Figura 6: Diagrama de Componentes

Componentes y responsabilidades:

- Autenticación y autorización:
    - Encargado de establecer y confirmar la autenticidad de un usuario, mediante cuentas, contraseñas, lecturas biométricas (huella digital, firma electrónica, etc)
    - Ofrecerá una credencial electrónica a los usuario autenticados, que servirá para autorizar el acceso a las diversas funcionalidades del sistemas
    - En el primer trámite de los usuarios, validará la información de la persona contra la registraduría nacional.
- Organismos de tránsito
    - Punto de entrada para las funcionalidades especificas ofrecidas a los organismos de tránsito

- Dirección territorial
    - Punto de entrada para las funcionalidades especificas ofrecidas a las direcciones territoriales
- Administrador de procesos
    - Motor de actividades, transiciones, reglamentaciones y modelamiento de los trámites que se pueden realizar en el sistema
- Recaudos
    - Conjunto de interfaces de comunicación con las entidades financieras que realizan los recaudos de trámites de los usuarios.
- Reglas de Negocio
    - Conjunto de componentes lógicos de validación de información, detección y prevención de incongruencias de data y aseguramiento de cumplimiento de restricciones y comportamientos de procesos en los trámites
- Gestión Documental
    - Encargado de la administración de documentos electrónicos requeridos para el cumplimiento de los trámites
- Consultas
    - Modulo para obtener información almacenada en el sistema y punto de entrada para obtener reportes
- Persistencia
    - Encargado del almacenamiento de la información y registro de modificaciones, consultas, inserciones, etc para efectos de auditoria.
- DataWareHouse
    - Grupo de funcionalidades para minería de datos, optimización de procesos de negocio, indicadores de gestión, etc.

4.3 Punto de Vista de Información

En esta sección se presenta el punto de vista de Información

4.3.1 Descripción

Este punto de vista permite definir un conjunto de elementos y estrategias que apoya el modelamiento de la información generada por los procesos de negocio. Teniendo en cuenta que el RUNT es un sistema de información con un alto flujo de datos, enmarcado en un conjunto de requerimientos no funcionales que busca asegurar un modelo óptimo de administración de la información, es necesario plantear una estructura de datos sólida que garantice un cubrimiento total de los requerimientos definidos por la organización y enfocada en los principios de flexibilidad, crecimiento, consistencia e integridad de la información.

4.3.2 Modelos de Estructuras Estáticas de Datos

A partir de este modelo se define una arquitectura de la información a un alto nivel, que involucra las entidades de negocio de mayor impacto para el sistema y esquematiza la estructura de datos a seguir durante la fase de construcción.

Para la definición del modelo se categorizaron los procesos de negocio más importantes del RUNT en un conjunto de entidades estáticas que representan su respectivo depósito de datos.

Entidad	Descripción
Automotor	Información de los automotores matriculados • Características vehiculares • Identificación vehicular • Revisión técnico mecánica y de gases • Autorizaciones • Situación jurídica de los vehículos • Historial de trámites • Identificación de autoridad de tránsito • Propiedad
Conductor	Información de los conductores de vehículos de servicio particular o público y los conductores de motocicletas • Identificación del conductor • Características licencias de conducción • Identificación de autoridad de tránsito • Historial de trámites
Empresa	Información de las empresas de transporte pú-

	público y privado • Identificación de la empresa • Identificación vehicular • Características vehiculares • Propiedad • Representación legal • Autorizaciones para transporte colectivo urbano • Autorizaciones para transporte mixto urbano • Autorizaciones para transporte individual • Autorizaciones para transporte colectivo de pasajeros de radio de acción nacional • Autorizaciones para transporte especial de estudiantes y asalariados • Autorizaciones para transporte de carga • Autorizaciones para transporte mixto de radio de acción nacional • Autorizaciones para transporte internacional de carga • Historial de trámites
Licencia	Información de las licencias de tránsito • Características vehiculares • Identificación vehicular • Situación jurídica de los vehículos • Propiedad • Revisión técnico mecánica y de gases • Identificación de autoridad de tránsito • Historial de trámites
Infracción	Información de las infracciones de tránsito y transporte en Colombia • Características del comparendo • Características licencias de conducción • Características vehiculares • Identificación de autoridad de tránsito • Identificación del infractor • Identificación vehicular • Propiedad • Historial de trámites (Antecedentes de infracciones) • Autorizaciones
Centro Enseñanza	Información de centros de enseñanza automovilística, centros de reconocimiento, centros integrales de atención, centros de diagnostico automotor • Identificación centro de enseñanza • Representación legal del centro • Autorizaciones • Características vehículos asociados • Identificación vehículos asociados • Identificación Instructor • Características licencias de conducción solicitadas • Base de datos de pruebas • Identificación autoridad de tránsito

	• Historial de trámites
Seguro	Información de seguros obligatorios para automotores que se expidan en Colombia • Características del seguro • Características vehiculares • Identificación vehicular • Propiedad
Tercero	Información de las personas naturales o jurídicas que presten algún tipo de servicio al tránsito, que presten apoyo o reciban delegación de los organismos de tránsito o las autoridades de tránsito • Autorizaciones • Identificación de autoridad de tránsito • Identificación (persona natural o jurídica) • Historial de trámites
Remolque / Semirremolque	Información de los remolques y semirremolques legalmente matriculados • Características Remolque / Semirremolque • Identificación Remolque / Semirremolque • Identificación vehicular • Autorizaciones • Características del seguro • Propiedad • Identificación de autoridad de tránsito • Historial de trámites
Accidente	Información de los accidentes de tránsito que ocurran en Colombia • Características del seguro • Características licencia de conducción • Características vehiculares • Identificación vehicular • Identificación autoridad de tránsito • Identificación conductor • Información reporte de accidente • Propiedad vehículos involucrados
Maquinaria	Información de la maquinaría agrícola y de construcción autopropulsada • Características de la maquinaría • Registro de maquinaría nueva importada, fabricada o ensamblada • Identificación de la maquinaría • Propiedad de la maquinaría • Situación jurídica • Identificación autoridad de tránsito

Trámite	Entidad transaccional que debe soportar la información generada por los diferentes trámites derivados de los procesos de negocio.
Autoridad de tránsito	Información de las diferentes autoridades de tránsito habilitadas en el país, las cuales son responsables de la información generada sobre su rango de acción.

Table 8: Entidades

El modelo propuesto (*Ilustración 1*) presenta una vista de alto nivel, conformado por las entidades de negocio representativas del RUNT y las relaciones básicas de navegación entre estás.

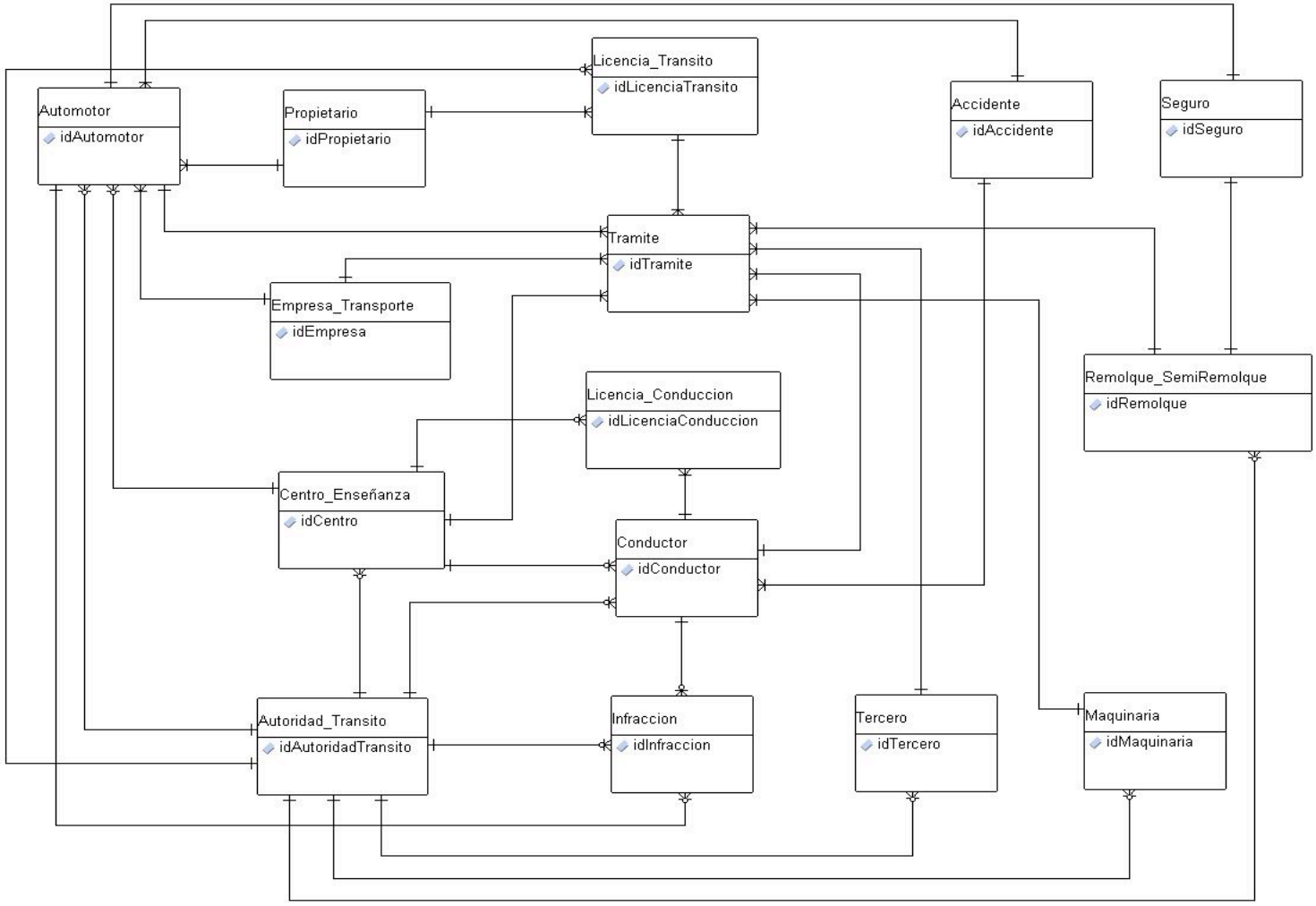

Figura 7: Modelo de Datos

4.3.3 Modelos de Flujo de Información

Este modelo nos permite tener un enfoque global de la forma como interactúan entre si los principales procesos de negocio del RUNT, definiendo claramente el flujo de información entre estos.

El objetivo que se busca con este modelo es definir una línea base del flujo de datos entre los procesos identificados, que permita dimensionar a gran escala los elementos de mayor impacto en la construcción del modelo detallado de la infraestructura de datos requerida para cubrir los requerimientos funcionales.

Proceso	Descripción
Cargue Inicial	* Realización del proceso inicial de todos los registros estipulados en los artículos 8 de la ley 769 de 2002 y 11 de la Ley 1005 de 2006. * Preparación del sistema con la información base necesaria para dar inicio a su operación por parte de las autoridades de tránsito habilitadas.
Cargue de información	* Cargue de Información suministrada por todos los actores que intervienen en el R.U.N.T, depuración, reporte de inconsistencias y planeación e implementación de su solución. * Integración con los Otros Actores para las validaciones y autorización de los registros. Recibir la información de los Otros Actores según los estándares y convenios establecidos por el Ministerio de Transporte.
Gestión de trámites	* Validación, autorización y registro de las transacciones resultado de los trámites de tránsito y transporte efectuados por todos los actores que intervienen en el R.U.N.T y el almacenamiento y custodia de dicha información. * Generar un código de autorización cuando cualquier actor que intervenga en el R.U.N.T, genere un trámite que actualiza el registro existente.
Gestión de Recaudo	* Control y seguimiento de recaudo de las especies venales y de Tarifas. Así como proveer el algoritmo que genere la asignación de rangos de especies venales en forma automática por Organismo de Tránsito o dirección territorial, de acuerdo con el procedimiento establecido por el MINISTERIO DE TRANSPORTE. * Recaudo de las Tarifas. * Asignación de rangos de especies venales.
Atención al ciudadano	Brindar servicios de información dentro del marco jurídico establecido por la ley, asesorando en respuestas o procedimientos a seguir en caso de quejas o reclamos.

Table 9: Procesos Principales del RUNT

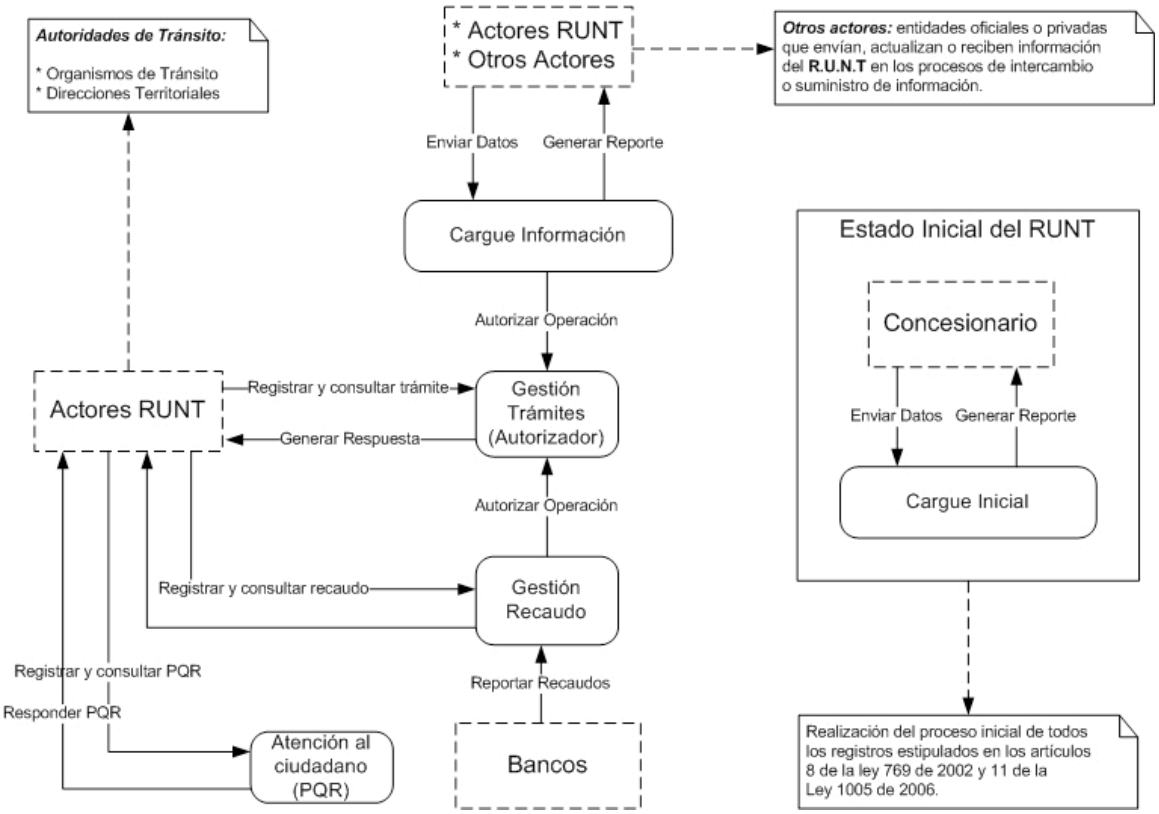

Figura 8: Diagrama de Flujo de Datos RUNT

4.3.4 Modelos de Ciclo de Vida de Información

Este tipo de modelo nos permite tener un panorama claro de los puntos de evaluación e interpretación por los cuales debe pasar un proceso y los cuales determinan la dinámica de los datos dentro del sistema.

De acuerdo a la naturaleza del problema enmarcado en los requerimientos del RUNT, dentro de los procesos de negocio identificados existe uno que canaliza el flujo principal de la información, este proceso es ***Gestión Trámites (Autorizador)***. A partir de lo anterior, a continuación se presenta el modelo de ciclo de vida de la información sustentado en un conjunto de estados de transición que determinan los puntos de control y evaluación del proceso.

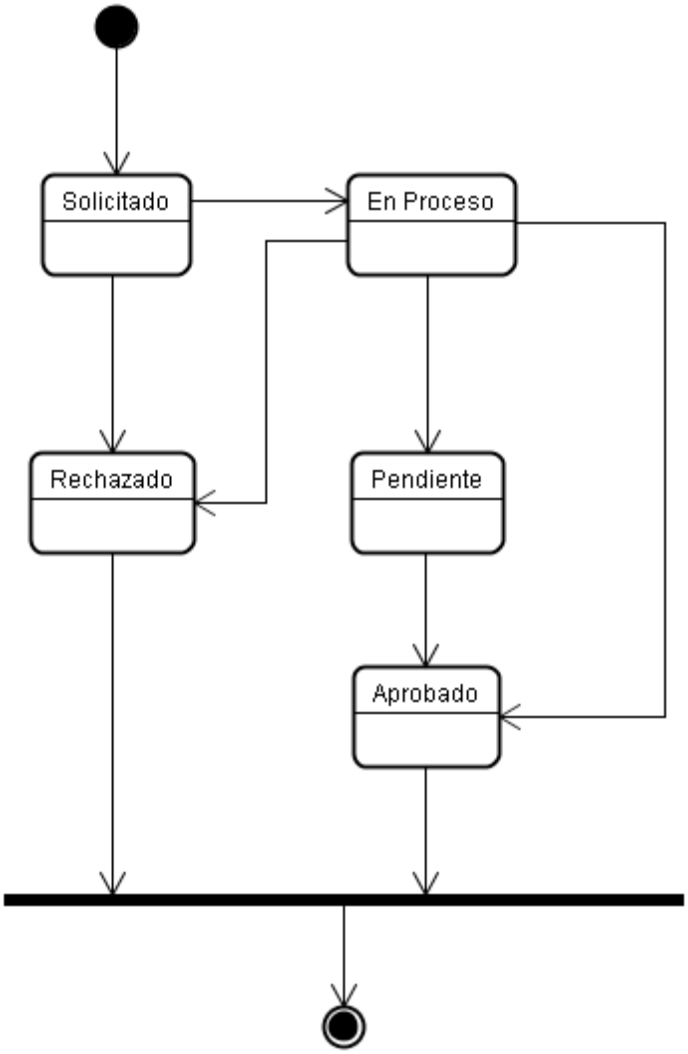

Figura 9: Diagrama de Estado - Gestión de Trámites

Estado	Descripción
Solicitado	Estado inicial con el cual se referencia un trámite. Indica que éste se encuentra en un proceso de validación genérico (común a todos los trámites).
En proceso	Estado de transición que indica que el trámite inicia un proceso de validación, el cual es ajustado de acuerdo al tipo de procedimiento en ejecución (Enfocado al trámite).

Pendiente	Estado asignado como resultado de un proceso de validación incompleto, es decir, se requiere información complementaria (documentos, firmas, sellos, entre otros).
Aprobado	Estado asignado como resultado exitoso del proceso de validación. Indica que el sistema generó satisfactoriamente el número de autorización o especie venal.
Rechazado	Estado asignado como resultado negativo del proceso de validación inicial o de procedimiento particular.

Table 10: Estados Ciclo de Vida Proceso Gestión de Trámites

4.4 Punto de Vista de Concurrencia

4.4.1 Descripción

Este punto de vista, busca describir la concurrencia del sistema, identificando las partes que pueden ejecutarse de manera simultánea y la sincronización de unidades de ejecución.

Para efectos de este documento, se analizará el sistema de agentes de auditoria requerido por el cliente.

4.4.2 Concerns

El sistema de agentes para auditoría debe contar las siguientes características:

- Un agente debe recibir y transmitir de forma segura al repositorio central, la información de los logs que cada aplicación genere.
- El agente siempre debe estar disponible para recibir la información de las aplicaciones y/o trasmitir los logs, de tal manera que no se afecte el desempeño del sistema.
- Los registros generados por cada aplicación deben estar claramente identificados, con fecha, hora, tipo, aplicación, consecutivo y usuario.
- Los tiempos de escritura de eventos no deben generar represamientos en el registro central de los logs y se almacenarán en el repositorio central por un periodo mínimo de 1 mes.

- El repositorio centra dispondrá de un servicio de recepción de las transacciones enviadas por cada agente, de tal manera que este sea el único autorizado para escribir en la base de datos centralizada.
- Si la conexión entre los agentes de la aplicación y el servidor de auditoría falla, las aplicaciones de manera transparente deberán continuar registrando los logs localmente hasta que la conexión sea restaurada, momento en el cual se deben enviar los registros que no hayan sido transmitidos.
- Se debe contar con mecanismos para verificar que la información enviada por una aplicación fue recibida de manera correcta y completa al servidor de auditoría.
- Garantizar que los registros de log enviados desde un agente no sean alterados durante su transporte y que sean originados por el agente respectivo.

4.4.3 Modelo de Concurrencia del sistema

El sistema de auditoria por agentes solicitado por el cliente, es un foco importante para analizar en esta vista arquitectural. Dado que muchos procesos, aplicaciones y servicios deben utilizar las funcionalidades de auditoria, se debe sincronizar el acceso a dicho recurso; además, múltiples agentes deben publicar todos sus registros en el servidor central de auditoria. Estas operaciones no pueden afectar el desempeño del sistema, y deben contar con mecanismos de recuperación y alta disponibilidad.

- Estrategias en el diseño de la multitarea

El acceso a un agente debe considerarse como un punto crucial concurrente, por tanto su acceso debe sincronizarse. La estrategia sugerida es utilizar un mecanismo de exclusiones mutuas (Mutex).

La publicación de los registros de auditoria no deben afectar el desempeño, se debe asegurar la entrega y debe contar con un mecanismo de recuperación. Se plantea el uso de colas de mensajes, tipo publicador/subscriptor con validación de aceptación, tolerancia a fallas, reintentos y serialización local.

- Priorización de acceso

Dados los requerimientos del sistema, todo trámite, proceso y acción realizada en las aplicaciones debe ser registrada en el repositorio central de auditoria. El acceso a los recursos compartidos para realizar estas labores ofrecerá un esquema de igual prioridad a las aplicaciones que consuman estos servicios.

- Abrazos mortales

Para evitar posibles escenarios de abrazos mortales, se optó por el mecanismo de colas de mensajes para la publicación en el repositorio central, y en los instrumentos de exclusión mutua (Mutex) en los agentes locales se evitará el uso de recursos comunes que puedan ocasionar una condición de carrera entre las aplicaciones.

- Modelo de concurrencia

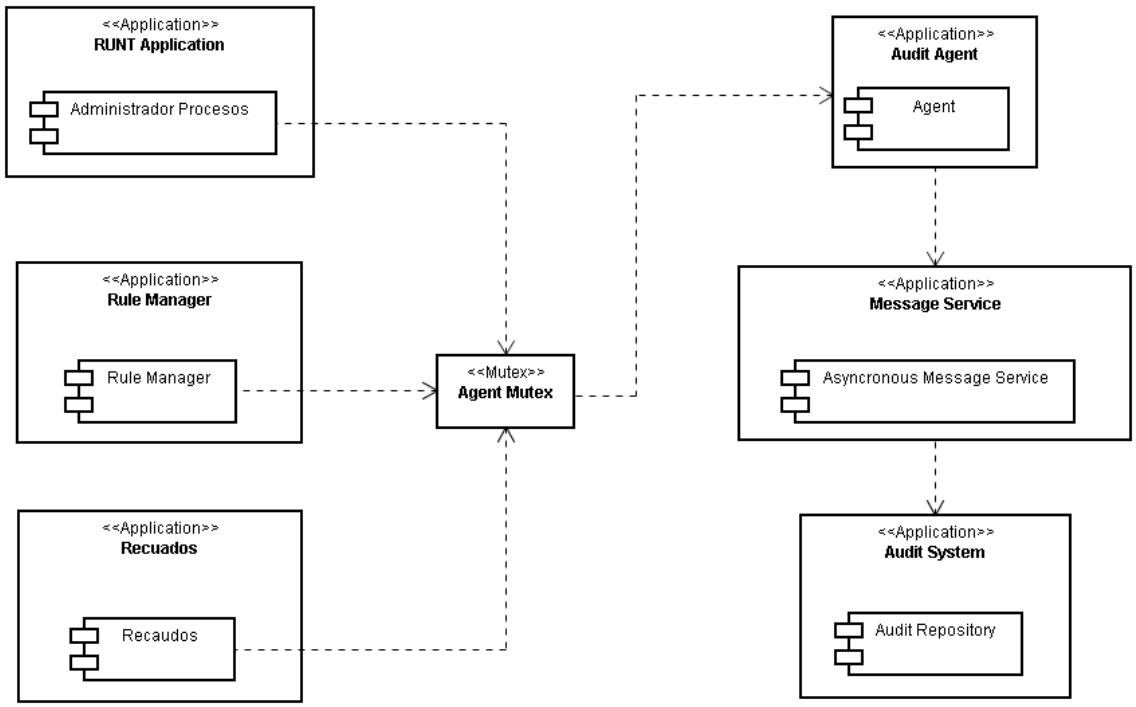

Figura 10: Modelo de Concurrencia

Los componentes funcionales de Recaudos, motor de reglas de negocio y administrador de procesos, usarán un Mutex (Exclusión mutua), para registrar los eventos en el agente local de auditoria. Este además utilizará un servicio de colas de mensajes publicador / subscriptor para enviar los registros al repositorio central. Dado que la cola de mensajes es asíncrona y no transaccional el desempeño general de la aplicación no se verá afectado.

4.4.4 Modelo de estado

Este modelo representa el ciclo de vida de la información de auditoria desde que es publicada por una aplicación, hasta que es almacenada en el repositorio central.

Dado que los agentes de auditoria requieren contar con un mecanismo de recuperación, la información que no se haya publicado al repositorio central, se almacenará localmente y se eliminará hasta que el agente reciba una confirmación.

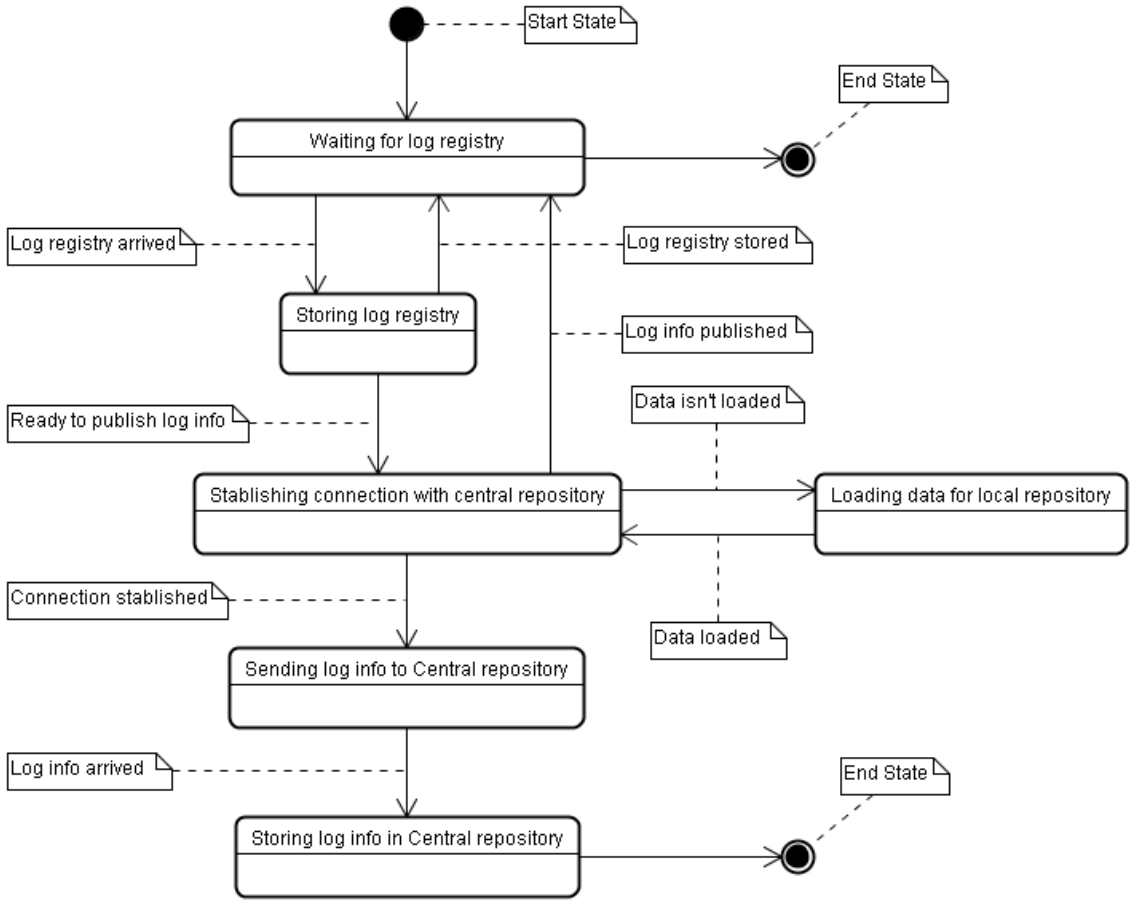

Figura 11: Modelo de Estado

5 Directorio

5.1 Índice

5.2 Glosario de Términos

Término	Definición
Especies Venales.	Son documentos tales como certificados de movilización, formulario único nacional, licencias de transito, placa única nacional para automotores, placa única nacional para motocicletas y formulario de informe policial de accidentes de transito
WCAG (Web Content Accessibility Guidelines):	Es una guía elaborada por la W3C que explica como hacer accesible contenido Web para personas con discapacidades
Certificado Digital	Garantiza la autenticidad de quien remite un mensaje o realiza una transacción, integridad del mensaje, confidencialidad frente a terceros y reconocimiento e imposible negación de las partes involucradas.
X.500	Conjunto de estándares de redes de ordenadores de la UIT-T sobre servicios de directorio, entendidos estos como bases de datos de direcciones electrónicas (o de otros tipos).
X.509	Estándar UIT-T para infraestructuras de claves públicas. Especifica formatos para certificados de claves públicas y un algoritmo de validación de la ruta de certificación.
ISO9001	Norma de Administración de calidad
ISO15408	Criterios comunes para la evaluación de seguridad de la Tecnología Informática

ISO17799	Guía para la administración de la seguridad de la información.
ISO27001	Guía para la administración de la seguridad de la información.
ANSI / Nist ITL I-2000	Estándar de formato de datos para el intercambio de biométricos
NTC- BS- 7799-2	Principal certificación para el estándar internacional de la administración de la seguridad.
DES, 3DES, IKE	Algoritmos de cifrado
SHA-1, MD5	Sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology (NIST).

Table 11: Glosario

5.3 Acrónimos

RUNT	Registro Único Nacional de Transporte
AICPA	American Institute of Certified Public Accountants
CISA	Canadian Institute of Chartered Accountants
RUNT	Registro Único Nacional de Transporte
LDAP	Lightweight Directory Access Protocol
GUI	Graphical User Interface

PKI	Public key infrastructure
UIT	Unión Internacional de Telecomunicaciones
WCAG	Web Content Accessibility Guidelines
BPM	Bussiness Process Management