Tecnología Microchip Para Acceder a Información Vehicular Como Apoyo a Procesos de Control y Seguridad

Microchip Technology for Access to Vehicular Information to Support Control and Security Processes

W. L. Aguilar-Rodríguez, W. G. Aguilar-Rodríguez, M. Á. Leguizamón-Páez

***Resumen* — El presente artículo de revisión de tema busca dar a conocer el apoyo que brinda la tecnología basada en microchips y elementos RFID en procesos de identificación y detección de vehículos, ofreciendo soluciones ante la problemática de inseguridad en vehículos automotores, evidenciada en la evasión a las autoridades y el hurto de autopartes. El uso de tecnologías de la información y las telecomunicaciones (TIC) ofrece una solución innovadora para la gestión de la información vehicular que permita contrarrestar las acciones delictivas y su impacto, puntualmente en el uso de automóviles en actividades ilícitas donde es alterada su información para evadir a las autoridades. Se plantea un sistema de apoyo basado en las TIC que promete optimizar las medidas actuales de seguridad vehicular, ofreciendo herramientas de apoyo a medidas existentes como el uso de cámaras y radares de velocidad, para ayudar a mejorar los procesos de validación de información brindando acceso más rápido y seguro. Se plantea implementar tecnología RFID en un microchip, mediante el cual se obtendrá un código único, que conectado a una red de bases de datos distribuidas, permitirá tener acceso a la información propia de los vehículos a través de un dispositivo lector de RFID, dotado de antenas compatibles con señales UHF, facilitando la recepción de la señal por encima de los 5 metros de distancia al objetivo y así identificarlo desde puntos lejanos, permitiendo obtener información de los vehículos con una mayor efectividad, buscando controlar los problemas relacionados con el uso de vehículos en actividades ilícitas.**

***Palabras clave*— Bases de datos Distribuidas, Control y manejo de la Información, Identificación por radiofrecuencia RFID, Microchip, Seguridad vehicular, Tecnologías de la Información y las telecomunicaciones (TIC).**

***Abstract*— The present topic review article will present the support provided by a technology based on microchips and RFID elements in processes of identification and detection of vehicles, offering solutions more precisely on the insecurity of them, evidenced in the evasion of the authorities and thefts of auto parts. The use of information technology and telecommunications (ICT) offers an innovative solution for the management of vehicle's information that allows to counteract criminal actions and their impact, specifically the use of cars in illicit activities in which their information is altered in order to evade the authorities. A support system based on ICT is proposed, which promises to optimize the current benchmarks of vehicular safety, offering tools to support benchmarks which are used nowadays such as the use of cameras and speed radars so that, they will help to improve the processes in the validation of information, providing faster and more secure access. This RFID technology is proposed to be implemented in a microchip, through which a unique code will be obtained, not forgetting that it allows the microchip to be connected to a network of distributed databases, which will allow access to the vehicles' own information, through an RFID reader device equipped with antennas compatible with UHF signals, facilitating the reception of the signal at distances over 5 meters away from the target and being able to identify it from far away locations, allowing to obtain information from vehicles with better effectiveness in order to control the problems about the one that are in illicit problems.**

***Index Terms*— Control and management of information, Distributed Database, Information and Telecommunications Technologies, Microchip, Radio Frequency Identification RFID, Vehicle safety.**

I. Introducción

El presente artículo busca proponer la integración de tecnologías como la presente en microchips, que se plantea sean instalados en vehículos permitiendo acceder a la información mediante la generación de ondas de radiofrecuencia, utilizando sistemas RFID, y a través de dichas señales se obtendrá la información almacenada en bases de datos distribuidas diseñadas y desarrolladas para tal fin,

Este manuscrito fue enviado el 7 de diciembre de 2018 y aceptado el 26 de junio, 2019.

Es un artículo de revisión de tema apoyado por la Universidad Distrital Francisco José de Caldas.

W. L. Aguilar-Rodríguez es Tecnólogo en Sistematización de datos de la Universidad Distrital Francisco José de Caldas (e-mail: wlaguilarr@correo.udistrital.edu.co).

W. G. Aguilar-Rodríguez. Tecnólogo en Sistematización de datos de la Universidad Distrital Francisco José de Caldas (e-mail: wgaguilarr@correo.udistrital.edu.co).

M. A. Leguizamón-Páez. Profesor asistente de la Universidad Distrital Francisco José de Caldas (e-mail: maleguizamonp@correo.udistrital.edu.co).

buscando identificar un vehículo para validar su autenticidad y evitar su falsificación y suplantación.

Se busca que dichas ondas sean leídas mediante receptores especializados, garantizando que la información sea obtenida por las autoridades y por personal calificado, siendo este un sistema de control que busca ser más eficiente que el actual, en el cual únicamente se verifica documentos físicos como la tarjeta de propiedad y se valida los números de placa, que son fácilmente falsificables dando posibilidad a la suplantación de la identificación vehicular, brindando ventajas como la validación de la información sin requerir la detención de los vehículos ni la solicitud de documentos físicos.

Basada en la tecnología RFID y sistemas UHF, se propone una solución tecnológica que, implementada en un microchip, mediante una etiqueta, tag o serial, pueda ser leída mediante un dispositivo electrónico para obtener información específica del vehículo siendo validada y determinando su estado actual frente a las autoridades y normas que regulan su desplazamiento por el territorio nacional. Dicha información solo podrá ser consultada por parte de personal autorizado, quien realizará su validación ya que estará almacenada en un conjunto de bases de datos distribuidas, permitiendo dar un correcto tratamiento de la misma.

A. Justificacion

Ante los diferentes actos delincuenciales que se presentan en la ciudad de Bogotá, tales como hurtos a residencias y personas, eventos en los que se ve relacionado el uso de motocicletas y vehículos, las autoridades han ejecutado algunas actividades reforzando la seguridad, aumentando el personal y efectuando controles en algunos de los puntos más críticos de la ciudad, medidas que no logran ser efectivas ni suficientes frente a los nuevos modus operandi de las bandas organizadas, donde se requiere fortalecer el pie de fuerza para garantizar la seguridad, especialmente en situaciones que relacionan el uso de vehículos, donde suplantar su identidad es tan fácil como cambiar las placas verdaderas por unas falsas. Para dar soporte a los procesos actuales, como la validación física de documentos, se requieren medidas que permitan fortalecer estos sistemas de seguridad.

Los actuales sistemas de control para la seguridad vehicular se basan en métodos que requieren de cercanía al vehículo y al conductor, a quien se le solicita la documentación en físico para poder acceder a la información, por esta razón, y con la necesidad de implementar métodos más efectivos que faciliten el acceso a la misma y agilicen su validación, se pretende complementar dichos sistemas con el uso de tecnologías de la información y las telecomunicaciones, que ofrecen alta disponibilidad de la información para poder ser consultada y procesada desde cualquier punto de la ciudad, en tiempo real y sin solicitar la detención del vehículo, permitiendo optimizar estos procesos de seguridad y control vehicular, validando la información sin la necesidad de requerir la documentación física de los vehículos.

El uso de las Tecnologías de Información y Comunicación (TIC) aporta grandes ventajas como la efectividad en el manejo de información y el acceso a esta desde cualquier lugar, permitiendo consultarla, clasificarla y validarla de manera más efectiva y en tiempo real, con el fin de apoyar los sistemas de seguridad y vigilancia, además de permitir que se tomen acciones con tiempos de respuesta más rápidos por parte de las autoridades.

Para darle un adecuado manejo a la información, se propone el uso de bases de datos distribuidas que ofrecen facilidad y rapidez en el acceso a la información mediante la interconexión de las bases de datos de las diferentes entidades viales y del Estado operando como una sola, cumpliendo con los principios y pilares de la seguridad de la información como son la integridad, la confidencialidad y la disponibilidad, garantizando un adecuado control sobre el acceso a los datos y su veracidad.

La estructura de interconexión de estas bases de datos ofrece ventajas de capacidad y rendimiento para la administración de alta carga de información y el alto costo de procesamiento que se requiere para el manejo y almacenamiento a gran volumen de la información vehicular en diferentes sitios de la red.

Para el acceso a las bases de datos, se propone el uso de tecnología de radiofrecuencia implementada en un microchip, que generará un código único mediante el cual se pueda tener acceso a toda la información necesaria almacenada en las bases de datos distribuidas.

Estos microchips, diseñados con tecnología RFID, generarán códigos de acceso a la información mediante ondas de radiofrecuencia, y se instalarán en los vehículos para que las autoridades reguladoras de tránsito y de seguridad puedan acceder a la información de los mismos y sus propietarios. De esta manera, validar y verificar la veracidad de la información suministrada, tanto en físico (tarjeta de propiedad, SOAT, Traspaso de propiedad, tarjeta de operación, entre otros) como en digital (información en bases de datos del gobierno y la secretaria de tránsito), permitirá identificar problemas existentes con la información del vehículo.

El uso de tecnología RFID será de gran ayuda en cuestiones de control y seguridad para las autoridades competentes ya que permitirá acceder a las bases de datos para obtener la información vehicular y validarla, y así poder identificar automóviles que hayan sido hurtados, usados en acciones ilícitas o si tienen pagos pendientes por algún tipo de multa, entre otros.

B. Marco Teórico

El sistema tecnológico de apoyo a temas de seguridad vehicular propuesto está basado en el uso de tecnologías de radiofrecuencia RFID, soportados en dispositivos microchip que a su vez permiten el acceso a la información mediante un sistema de bases de datos distribuidas, logrando componer un conjunto de herramientas adecuadas que generan un sistema cuyas entradas y salidas son secuenciales dentro del proceso de consulta y validación de información vehicular, tal y como se puede apreciar en la Fig. 1.

Fig. 1. Proceso funcionamiento Sistema RFID. Fuente: Autor.

1) Sistemas RFID:

RFID es la Identificación por Radiofrecuencia, en ingles Radio Frequency IDentification, es un sistema enfocado en almacenamiento y recuperación de información remota, los cuales son usados por medio de transmisores o antenas.

La tecnología RFID fue diseñada para identificar objetos a distancia e interconectarlos dentro de una configuración existente [1], sin la necesidad de tener contacto físico directo entre estos [2]. Su origen data de la segunda guerra mundial con el uso de los radares para detectar aviones, y para poder distinguir sus aviones, los alemanes los balanceaban mientras volaban de regreso a su base, lo que generaba un cambio en la señal de radio y de esta manera identificaban los aviones aliados [3].

La tecnología RFID se puede usar donde se requiera un continuo almacenamiento de datos y se tiene un difícil acceso a datos en algunos procesos como lo son el control de inventarios, movimiento de mercancías, control de acceso a vehículos, sistemas de librerías [4], entre otros.

Esta tecnología tiene tres diferentes etiquetas para sus señales dependiendo del lugar de la alimentación de energía, estas etiquetas son:

- RFID Pasivas: No tienen fuente de alimentación propia [5], tal como se representa en la Fig. 2.

Fig. 2. RFID Pasivo [6].

- RFID Semipasivas: No tienen una fuente directa de energía pero contiene internamente una pequeña batería [7].
- RFID Activas: Estas siempre llevan su propia fuente de energía [5], como se muestra en la Fig. 3.

Fig. 3. RFID Activo [6].

Esta tecnología se divide en tres diferentes sistemas, según la banda de frecuencia en que operan [5], como se evidencia en la Tabla 1**¡Error! No se encuentra el origen de la referencia.**:

TABLA I.
BANDAS DE FRECUENCIAS

Rango de frecuencias	Descripción	Rango
120 KHz	LF (Baja Frecuencia)	Hasta 10 cm.
13,56 MHz	HF (Alta Frecuencia)	De 10 cm a 1m.
868 MHz – 956 MHz	UHF (Ultra Alta Frecuencia)	De 3 m a 12 m.
2,45 GHz – 5,4 GHz	Microondas	Más de 10 m.

- Low frequency (LF). banda espectro electromagnético de frecuencia baja que cubre frecuencias entre 30KHz a 300Khz y tiene un rango de lectura de unos 10 cm.
- High frequency/ Near Field Communication (HF / NFC)) significa frecuencia alta y/o comunicación de campos a cercanía, que opera en el rango entre 3 y 30 Mhz, generalmente 13,56 Mhz con rangos de lectura entre 10cm y 1m.
- Utra-high frequency (UHF), banda electromagnética de frecuencia ultra alta que cubren rangos de frecuencia desde 400Mhz a 1GHz y pueden tener un alcance superior a los 12 metros.
- Microondas, banda con rango de más de 10 metros, con frecuencias entre 2,45 GHz hasta 5,4 GHz.

La implementación de esta tecnología requiere de dispositivos y herramientas que soporten de manera eficiente el almacenamiento y la transmisión de la información mediante la generación y recepción de ondas. El dispositivo que cumple con las expectativas de uso acordes a lo planteado es el Transponder RFID compuesto por un microchip capaz de llevar a cabo las funciones de almacenamiento y transmisión de información [2].

2) Transponders RFID:

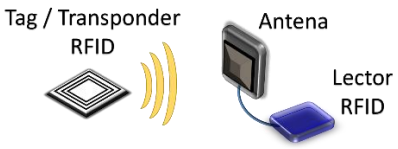

Fig. 4. Transpoder. Fuente: Autor.

Los Transponders son dispositivos inalámbricos que funcionan como mecanismos de control, supervisión o comunicación, encargados de recibir y responder automáticamente a una señal entrante [2]. También llamados "Tags", estos Transponders RFID son componentes conformados por un microchip [2] el cual almacena y transmite datos mediante una antena, estos dispositivos pueden ser pasivos, es decir que su fuente de energía es el lector y es alimentado mediante radiofrecuencia, o activos cuando poseen una batería o fuente de energía propia, además de tener un rango más alto que los pasivos. Estos Tags, como se ve en la Fig. 4, responden a peticiones realizadas por el dispositivo lector, que emite un campo electromagnético a través del cual el chip trasmite la información contenida [8]. También existen las etiquetas semi-pasivas, las cuales se comunican de la misma manera que las etiquetas pasivas, pero poseen una fuente de energía y alcanzan un rango de transmisión intermedio entre las pasivas y las activas [9].

Este sistema ha sido implementado en el arranque de los vehículos incorporando un microchip transponder en las llaves (denominado *Llave transponder*) que, al momento de hacer contacto con el switch del encendido, emite una señal por radiofrecuencia, generando un código que es captado por una antena o unidad lectora, la cual compara el código emitido con el código memorizado, al igual que el código emitido por la

unidad de arranque. Al encontrar coincidencia en estos códigos emitidos, la unidad de mando autoriza el encendido del vehículo [10].

3) Microchip:

La Real Academia Española define un chip como *"Pequeña pieza de material semiconductor que contiene múltiples circuitos integrados con los que se realizan numerosas funciones en computadoras y dispositivos electrónicos."* [11]. También definido como una pastilla semiconductora protegida dentro de un encapsulado de plástico o cerámica [12].

Es también llamado "*circuito integrado o electrónicos*", desarrollado en 1958 por Jack St. Clair Kilby, un ingeniero eléctrico y físico Norteamericano [12], algunos de los circuitos integrados más avanzados que se crearon con mayor avance y utilidad fueron los microprocesadores que se usan para los computadores y algunos elementos electrónicos.

Los microchips son elementos que se utilizan en diferentes elementos o seres vivos como los animales, para poder identificarlos, destacándose para que las instituciones de control animal obtengan la información de los animales domésticos o mascotas e incluso de quienes lo adoptan. Por su capacidad de almacenar información estos microchips pueden obtener los datos y reconocer las características reales y verídicas del quién o el que lo porta [13].

Los procesadores son elementos pequeños fabricados con Silicio, tanto como para compararse con la uña de un dedo meñique, pero tienen la capacidad de procesar gran información con bastante rapidez, pueden procesar aproximadamente 10.000 millones de instrucciones por segundo [14].

Bajo el enfoque funcional de la propuesta, los microchips son herramientas tecnológicas por medio de las cuales se generan impulsos eléctricos que se traducen en códigos de enlace, de esta forma, brindan acceso a información almacenada en las diferentes bases de datos existentes, y cuyo uso representa un recurso óptimo que se utilizará para integrar un sistema eficaz de seguridad vehicular.

4) Bases de Datos:

Una base de datos es una colección de datos lógicamente coherente para un propósito específico [15]. También se considera un almacenamiento virtual de grandes volúmenes de información de manera organizada ordenada para un acceso fácil a datos específicos [16], que se compone de filas y columnas, guardados en uno o varios servidores.

4.1) Bases de Datos Distribuidas:

Las bases de datos distribuidas son aquellas que almacenan información y datos que pertenecen lógicamente a un único sistema pero se encuentran físicamente diversas y repartidas en diferentes lugares donde su ubican los diferentes servidores conectados en la red. Es un conjunto de bases de datos construidas e interconectadas en una red de computadoras formando un sistema [17], donde la información estructurada en la base de datos se almacena en varios lugares de la propia red, y los diferentes sistemas pueden acceder a los datos desde múltiples posiciones geográficas [18].

La información almacenada en varios computadores servidores, puede ser accedida y modificada simultáneamente a través de la red de las bases de datos distribuidas. Cada servidor de las bases de datos del sistema de Bases de Datos Distribuidas es controlado por su Sistema Gestor de Base de Datos DBMS (Data Base Management System) local, cooperando para mantener la coherencia de la base de datos global [18].

Estas bases de datos tienen su arquitectura cliente – servidor como las demás con su propio DBMS, pero su interconexión se define con nodos, los cuales pueden ser clientes o servidores, donde se puede acceder a sus datos desde cualquier otro nodo. Las conexiones a bases de datos entre sus diferentes tablas se realizan mediante rutas o enlaces de la base de datos [19].

5) Antenas VHF/UHF

Las antenas son dispositivos para transmitir señales por medio de ondas de radiofrecuencia, algunas son para transmitir únicamente y otras solo para receptar señal [20] que solo operan con frecuencia de entrada. Esta funciona dependiendo del espectro electromagnético que se gradué en la señal.

Estas antenas se clasifican en VHF y UHF dependiendo de los rangos de frecuencia con que operan, tal y como se describe a continuación:

- **VHF** (Very High Frequency o Muy Alta Frecuencia) es uno de los rangos de frecuencia en la banda de onda de radio, comúnmente usada para las transmisiones de televisión, radio FM y comunicaciones bidireccionales de los departamentos de policía y otros servicios de emergencia [21]. Las antenas VHF reciben ondas VHF que tienen una longitud de onda entre 1 y 10 Metros, y abarcan frecuencias desde los 54 MHz a 88 MHz y entre 174 MHz y 216 MHz [22].
- **UHF** (Ultra High Frequency o Ultra Alta Frecuencia) opera entre las frecuencias 470 MHz a 806 MHz [22]. Tiene una longitud de onda entre 10 Centímetros y un Metro. Las longitudes de onda cortas de las señales UHF permiten pasar más fácilmente a través de los obstáculos y rebotar en la ionosfera, para que puedan viajar más allá del horizonte de la torre de transmisión [23].
  Entre las antenas UHF se encuentran las antenas Yagi-Uda, diseñada para recibir ondas de radio entre los 300 MHz y los 3 GHz [24].

II. Tecnologias De La Informacion Y Las Telecomunicaciones Aplicadas En Soluciones Para La Seguridad Vehicular

En la actualidad, las medidas de seguridad vehicular existentes en Colombia no han dado el mayor resultado a pesar del trabajo y coordinación de la institución de la policía nacional, quienes han diseñado algunas estrategias para combatir la problemática. Como parte de estas estrategias, la policía nacional realiza como método una investigación para recolecta de información de los delincuentes capturados, para conocer los modos de operación en los delitos [25].

Estas investigaciones las realizan los agentes de la Policía Nacional para encontrar los diferentes métodos y estrategias usadas por los delincuentes para lograr los diferentes robos, el

incentivo que los lleva a cometer los robos, descubrir los vehículos, elementos o lugares donde se concentrar para realizar el hurto. La policía se basa en indagar y entrevistar a los involucrados para conocer la forma en que operan los delincuentes y bandas organizadas y así poder actuar en ese frente de manera más puntual y lograr las capturas.

Aunque estas estrategias son bien planteadas, están orientadas en un sentido más correctivo que preventivo, lo que se plantea con el uso de la tecnología es un cambio con el fin de que se desarrollen nuevas estrategias enfocadas en la prevención de actos delictivos. Las autoridades realizan seguimientos sobre delitos identificados por su continua ocurrencia y así poder ejecutar acciones para evitar que se repitan las diferentes infracciones y delitos.

Acciones como la instalación de puestos de control, requisas y solicitud de documentos son algunas de las actividades de prevención que se han ido fortaleciendo con el objetivo de controlar situaciones como el hurto y la suplantación de vehículos, para reducir, por ejemplo, el número de casos presentados donde las placas de estos son falsificadas para poder cometer diferentes delitos [26].

Para hacer frente a estas problemáticas, los procesos actuales requieren de asistencia de las autoridades de seguridad pública, mediante la instalación de retenes y recorridos por las diferentes zonas de la ciudad de Bogotá y en las demás ciudades de Colombia solicitando soportes físicos como los documentos de identidad o tarjeta de propiedad en el caso de los vehículos.

La información registrada en documentos como la tarjeta de propiedad, registro de revisión tecno mecánica, SOAT (seguro contra accidentes), incluso las placas que tenga un vehículo en Colombia, son fácilmente falsificables, y muchas de las bandas organizadas delincuenciales se encargan de realizar estas falsificaciones para poder ejecutar sus actividades delictivas, contando con complicidad de personal empleado en entidades Distritales o Estatales.

En algunos casos, al momento de realizar las inspecciones de los vehículos, las autoridades encuentran que las placas se encuentran sobrepuestas o detectan anomalías en su diseño, incluso al verificar los números de placa en las bases de datos de tránsito o la SIJIN (Seccional de Investigación Judicial), no se encuentra información coherente o hace referencia a un vehículo con características diferentes como su marca, tipo de vehículo, entre otras características.

La SIJIN junto a la DIJIN (Dirección de Investigación Judicial) son unidades operativas de la Policía Nacional encargadas de ejercer las funciones de Policía Judicial, llevando a cabo actividades y procedimientos de investigación criminal, además de dirigir y coordinar la recepción de información en materia criminal.

Estas condiciones dificultan la validación de la información básica de los vehículos por parte de las autoridades, permitiendo llevar a cabo actividades ilícitas y delictivas, en las que en ocasiones no se deja ningún rastro real de los autores y vehículos utilizados.

A. Una solución tecnológica para optimizar procesos de control en seguridad vehicular.

La implementación tecnológica en sistemas de seguridad vehicular busca brindar apoyo y soporte en actividades como la prevención, gestión y control de incidentes que afectan la estabilidad y seguridad de una persona, empresa o comunidad, además de ofrecer herramientas para la verificación y recopilación de pruebas que permitan tomar las decisiones y medidas adecuadas para reducir las amenazas y el impacto de cualquier ataque. Por ejemplo, la implementación de cámaras es una de las herramientas tecnológicas más usadas en temas de seguridad ciudadana [27], y cuya implementación es visible incluso en diferentes puntos de las principales ciudades de Colombia como Bogotá D.C., incluso instaladas en los radioteléfonos de uso privativo de la Policía Nacional.

Para algunas empresas, tanto Estatales como privadas, es importante implementar mecanismos de seguridad en sus productos, y han optado por adquirir soluciones tecnológicas para hacer frente a temas de seguridad, como por ejemplo Goodyear, una de las empresas más grandes de fabricación de llantas, y que también ha innovado en temas de tecnología en pro de la seguridad, incorporó microchips en los neumáticos con el fin de reducir el riesgo de hurto, almacenando información de su procedencia, como por ejemplo su propietario original [28], además de las características propias del neumático como su tipo, tamaño y número exclusivo de identificación, y que a futuro podrá almacenar información como presión y temperatura de los mismos. Estos microchip están basados en tecnología RFID (Radio Frequency IDentification - Identificación por Radiofrecuencia) que permite identificar un elemento, incluso seguir su ruta de movimiento. El microchip por medio de la señal de radiofrecuencia enviaría un código a un lector específico Middleware RFID con el cual se accederá a la información requerida para la identificación del vehículo [29].

En la **¡Error! No se encuentra el origen de la referencia.**2 se puede evidenciar y comparar las mejoras en los procesos de seguridad vehicular.

TABLA II.
PROCESOS DE REQUERIMIENTO DE INFORMACIÓN VEHICULAR

	Proceso actual	**Proceso planteado**
Identificación del vehículo.	Se realiza mediante la detención de los vehículos, solicitando la documentación al conductor.	Disminución de velocidad del vehículo para una mejor captura de la señal generada por el tag RFID.
Consulta de la información.	Después de solicitar la documentación del vehículo, se ingresa al sistema de consulta o se solicita a la central por radioteléfono. Proceso que puede llevar algo de tiempo mientras la	Una vez obtenido el código descifrado emitido desde el microchip, este funcionará como un enlace directo a la información almacenada en el sistema de bases de datos distribuidas.

	comunicación se efectúa.	
Validación de la información.	La información se obtiene desde la central a respuesta de la solicitud de los agentes que ejecutan los operativos de control, se debe esperar para tomar acciones necesarias acordes a los datos obtenidos. Si la información se obtiene mediante plataformas, actualmente no está integrada la información legal que maneja la agencia de transito SIMIT con la información judicial de la SIJIN-DIJIN.	La consulta realizada mediante el código obtenido desde el microchip retornara toda la información relacionada al vehículo, desde los datos de sus propietarios, impuestos y comparendos, hasta información legal sobre embargos o pendientes con la justicia.

B. Microchips basados en tecnología RFID para transmitir información.

Los sistemas RFID-UHF permiten la transmisión de datos muy rápida y son muy sensibles a interferencias. Actualmente ya existen tags, antenas y lectores que brindan alto rendimiento [7], y los tags UHF son más eficientes y con menos interferencias en comparación con los LF (Low Frequency) y HF (High Frequency).

La adaptación de un dispositivo de tecnología de identificación por Radiofrecuencia RFID en los automóviles que reemplace la existencia de documentos físicos como la tarjeta de propiedad y certificados de revisiones técnico mecánicas, además de brindar un acceso más rápido y en tiempo real a la información, permitirá optimizar los procesos de validación de la información que llevan a cabo las autoridades en los diferentes puntos de control instalados en las ciudades de Colombia.

Estos dispositivos RFID tienen la capacidad de almacenar y transmitir información mediante "transponders" o "tags" , que son dispositivos que reciben y envían señales [8] o simplemente amplían o modifican una señal. Su principal función es la de transmitir información mediante la generación de una señal, como números de serie o códigos únicos que permitirán consultar la información del vehículo en el cual se encuentre instalado el microchip en las diferentes bases de datos conectadas al sistema de información vehicular.

C. Funcionamiento de la tecnología RFID para el acceso a la información vehicular.

Teniendo en cuenta el análisis de la tecnología RFID y las ventajas que ofrece en cuanto a su alcance, practicidad y usabilidad, y el complemento con un sistema de bases de datos distribuidas, se requiere adicionar un dispositivo intermedio que se encargará de traducir las señales emitidas desde el microchip y que permita obtener la información almacenada en las bases de datos.

Fig. 5. Funcionamiento Sistema RFID. Fuentes: Autor [30] [31].

Como se puede apreciar en la Fig. 5**¡Error! No se encuentra el origen de la referencia.**, un microchip, instalado en el vehículo, generará señales mediante tecnología RFID-UHF, que tiene un campo de cubrimiento por encima de los 12 metros, suficiente para que esta señal sea recibida mediante un dispositivo dotado con una antena compatible con UHF [8]. Esta señal emitida desde el microchip enviará un código único que será traducido por el dispositivo receptor [5], el cual permitirá acceder a un sistema de información o aplicación, para consultar la información relacionada al vehículo portador del microchip.

Dicha información es almacenada en un sistema de Bases de datos distribuidas y se podrá acceder a esta desde un sistema o aplicación mediante el serial generado por el dispositivo receptor, permitiendo una consulta de datos segura y eficiente.

D. Instalación de la tecnología planteada.

Para la instalación de este microchip se debe tener en cuenta que se debe ubicar de manera que sea fácil su detección y lectura con los dispositivos adecuados por parte de cualquier personal encargado del control, además que la señal alcance un rango ideal de radiofrecuencia para que su lectura no se vea afectada por la distancia entre el dispositivo emisor y receptor, o por interferencias, incluso si el vehículo se encuentra en movimiento. También se debe garantizar que el microchip se instale en un lugar donde no se pueda retirar o acceder por personas no autorizadas, igualmente que no esté expuesto a sufrir daños o afectaciones en casos de accidente.

Las autoridades encargadas de las actividades de control, tienen la capacidad de decidir acerca de la instalación de los dispositivos lectores de los microchips, que pueden ser instalados en puntos fijos como semáforos, en intersecciones viales y avenidas principales, con la debida señalización, informando a la población en general; o simplemente ser asignados a los agentes para que estos los porten y puedan realizar controles en diferentes puntos de las ciudades Colombianas. Esta portabilidad de los dispositivos receptores permitirá reducir la evasión por parte de los conductores como lo hacen con los detectores de velocidad [32]. Los dispositivos receptores de señal requieren tener, entre sus componentes, antenas tipos VHF/UHF [23], suficientemente robustas para lograr obtener una señal clara entre los 5 y 10 metros, compatibles con sistemas RFID-UHF.

E. Administrar la información vehicular mediante un sistema de Bases de datos distribuidas.

En los procesos de seguridad es de gran importancia el manejo de la información, desde el acceso seguro a esta, ofreciendo canales seguros que garanticen su integridad y permitan validar su autenticidad, hasta el correcto almacenamiento, asegurando su confidencialidad y disponibilidad en tiempo real. El adecuado manejo de la información permitirá ejecutar medidas de control en poco tiempo, ofreciendo una rápida respuesta por parte de las autoridades, fortaleciendo las acciones, obteniendo resultados favorables en la reducción del uso de vehículos en actividades ilícitas.

Para esto, es necesario apoyar el sistema de seguridad con herramientas de alta tecnología que optimicen los procesos y recursos actuales, ofreciendo un alto nivel de conectividad y gran capacidad de almacenamiento, tal y como lo ofrecen los sistemas de bases de datos distribuidas.

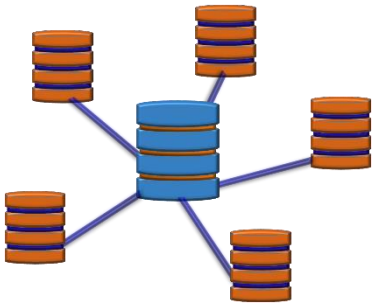

Fig. 6. What is Distributed Database. Fuente: Autor.

El modelo de las bases de datos Distribuidas, como se observa en la Fig. 6**¡Error! No se encuentra el origen de la referencia.**, permite apreciar que es todo un conjunto de bases de datos que opera como una sola, ofreciendo ventajas en seguridad, disponibilidad y accesibilidad de la información, permitiendo que se pueda realizar consultas desde cualquier punto o nodo de una red, sin necesidad de mantener la base de datos en un host principal [33]. El objetivo principal de procesar la información a través de bases de datos distribuidas es el de reducir tanto los costes en la carga de la información como los tiempos de consulta para obtener mayor eficiencia en el acceso a la información.

El Sistema Gestor de Bases de Datos Distribuidas (SGBDD), para realizar las consultas y obtener la información, se basa en un algoritmo de optimización de consultas, el cual verifica la cantidad de bytes que se transfieren de acuerdo a la tabla de donde se obtienen los datos y la forma como se realizan los joins para obtener los datos con menor peso [33]. Las consultas también se pueden optimizar mediante la técnica conocida como "semireunion", que consiste en transferir únicamente las tuplas y atributos necesarios, evitando que se transfieran bytes innecesarios.

Un método para conectar bases de datos distribuidas es haciendo la conexión como bases de datos fragmentadas, es decir, llamando desde una base de datos a otra base de datos por medio de su IP o nombre de equipo, para ligar entre ellas.

Para realizar las consultas llamando los datos de las dos tablas, se realiza haciendo un *select* a las tablas, la tabla de la base de datos agregada se llama por medio de la IP y nombre de la base y se realiza un *Union* con una de las tablas de la base principal [34] , por ejemplo:

*"Select * from [IP]nombreBasedeDatos.dbo.nombreTabla;*

Unión

*Select * from nombreTabla;*

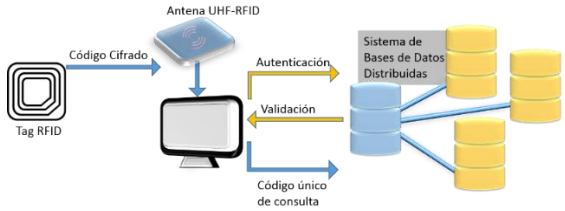

Fig. 7. Acceso a información en una base de datos distribuida mediante RFID. Fuente: Autor.

El acceso a la información vehicular en el sistema de bases de datos distribuidas, como se muestra en la Fig. 7, se realiza mediante el código emitido por radiofrecuencia desde el dispositivo RFID, el cual llega cifrado hasta el dispositivo lector. Este es un código principal y único (llave primaria), lo que permite generar una consulta más rápida y exacta, relacionando la información básica de las tablas que almacenan la información del vehículo, de su propietario, incluso de multas y accidentes en los cuales se haya visto involucrado.

Este sistema de bases de datos distribuidas va a estar compuesto por bases de datos de la secretaría de tránsito, del Simit (Sistema Integrado de información sobre multas y sanciones por infracciones de tránsito) y la Sijin, proponiendo así un esquema completo de información vehicular.

F. Seguridad en Bases de Datos Distribuidas:

La seguridad de las bases de datos distribuidas para proteger la información y el acceso a las bases y su información para ser compartida se definen en niveles llamados niveles de sensibilidad, a estos se le les asigna restricciones o reglas de clasificación. Las restricciones proporcionan seguridad a los datos en cuanto a contenido, contexto del contenido y fechas. [35].

Estas bases de datos requieren ser fuertes en seguridad ya que obtienen conexión a muchos usuarios desde diferentes puntos, alta transaccionalidad y acceso a la totalidad de la información almacenada, esto puede presentar espacios vulnerables en acceso a la información por parte de usuarios no permitidos, lo que genera amenazas como la perdida de información, perdida de integridad de los datos, denegación de acceso a usuarios con permisos y acceso a información privada [36]. En las bases de datos distribuidas se da el acceso a múltiples usuarios en el mismo tiempo, estas garantizan que los cambios que se realizan simultáneamente como inserciones, actualizaciones y eliminaciones se reflejen en tiempo real tanto en la misma conexión como en las demás ubicaciones y datos almacenados en otros lugares [37].

Para el acceso a la información del vehículo se requiere custodiar los datos transmitidos a través del cifrado del código que emite el microchip y desencriptarlo en el receptor, así la base de datos podrá leer dicho código para consultar la información del vehículo, manteniendo este oculto de posibles interceptaciones.

Frente a esto se generan controles de acceso, de flujo de datos y cifrado de la información [36], se puede tener en cuenta métodos de encriptación para proteger el acceso a la base de datos como lo son las llaves públicas, llaves privadas y las firmas digitales.

La seguridad en la comunicación entre nodos de la base de datos contiene la verificación de que los datos no estén dañados, que el canal de comunicación este protegido de espías y que contenga los protocolos bien definidos. Así mismo debe contener sistema de registro y monitoreo y para esto se implementan auditorias en los diferentes registros y procesos realizados [38].

Aunque las bases de datos se muestren cada vez más con complementos que han generado mayor seguridad, los problemas más comunes son la autenticación y la identificación de los usuarios como controles de acceso. Existen algunas sentencias SQL como GRANT y REVOKE para dar accesos y privilegios a algunos usuario [37].

En el impacto de la seguridad debe tenerse en cuenta las políticas del manejo de información, por ejemplo quien puede acceder a esta y modificarla, y las políticas de seguridad de las diferentes bases de datos, tales como verificar y mantener reglas de seguridad durante los procesos de consulta y modificación de los datos, así mismo auditar cada proceso como seguimiento y control [37].

Las diferentes consultas, los accesos a las bases de datos, la información de los códigos y datos de los vehículos deben ser auditados para conocer que la información sea correcta, que no se haya modificado sin permisos y que el acceso a la misma no sea de usuario no permitidos.

G. Seguridad de la información en un sistema RFID:

Los sistemas RFID ofrecen esquemas de alta seguridad en cuanto a la posible vulneración, alteración y clonación de los tags pero que también generan dudas en términos de manejo y acceso a la información [9]. Partiendo de los propósitos básicos de los protocolos de seguridad RFID: identificación y autenticación, los riesgos a los que se puede ver expuesta la información radica en la pérdida de la Privacidad en cuanto a que la información que llega a los lectores RFID pueda ser interceptada por terceros [39].

Otros factores a tener en cuenta referente a la seguridad de los sistemas RFID incluyen la estandarización, costos, la falta de profesionales capacitados y las lecturas falsas de las etiquetas. Para este último se han propuestos algoritmos de lectura y reconocimiento de acuerdo a la detección de la etiqueta [40].

El sistema RFID es una tecnología que se destaca en los nuevos entornos informáticos, aunque se tienen en cuenta protocolos de comunicación y de seguridad, ha sido un sistema que ha tenido fallas en el blindaje y protección en el intercambio de datos, y no se ha logrado mejorar la privacidad en él envió de información y mensajes entre estos sistemas, por lo cual se busca obtener un protocolo que mejore esta deficiencia [41].

Frente a esto se han propuesto diferentes soluciones de algoritmos de cifrado, que algunas veces son limitados en relación al tamaño reducido y bajo costo de los dispositivos [8], y cuyos esfuerzos han llegado a proponer complejos algoritmos basados en técnicas Hash, o incluso YA-TRAP que proporciona autenticación resistente al seguimiento mediante medidas de sellos de tiempo [39]. Los sellos de tiempo son certificaciones que indican el estado del certificado electrónico en el momento de la firma y que comprueba que un conjunto de datos existente en un instante de tiempo no han sido modificados posteriormente [42].

Otro protocolo es el de autenticación mutua, basado en Hash y secreto sincronizado, utiliza la sincronización mediante valores secretos compartidos entre la etiqueta y el servidor Back-End. Aquí el ID se divide en grupos y a su vez cada grupo se divide en números aleatorios [39]. En la Fig. 8 se presenta un esquema de cifrado con autenticación mutua y firma digital, entre un dispositivo lector y otro emisor utilizados en los sistemas de ignición o encendido de los vehículos.

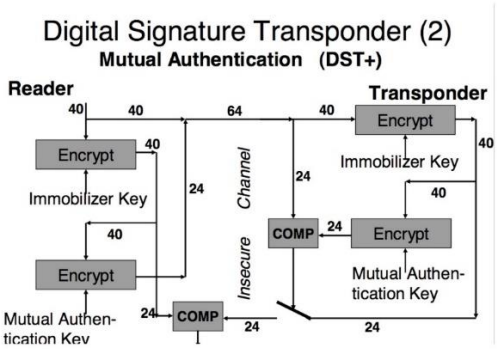

Fig. 8. Digital Signature Transponder [43].

Otro sistema que resulta bastante eficaz está basado en el uso de firmas digitales en etiquetas RFID [9], permitiendo asegurar la confianza en el paso de la información mediante la autenticación de dispositivos, evitando la clonación de etiquetas y falsificaciones de la transmisión [44]. Este sistema está basado en un esquema de identificación cryptoGPS y funciones hash SHA-1, lo que ofrece una arquitectura de hardware de bajo costo [44].

Teniendo en cuenta los protocolos relacionados anteriormente, se propone una implementación de un sistema que incluya cifrado con uso de firmas digitales, y a su vez basado en autenticación mutua, pero con el beneficio de que sus funciones se utilizarán en un solo sentido [45], donde el servidor de autenticación calculara tiempos limitados para encontrar el identificador de la etiqueta RFID y en el cual la respuesta de la etiqueta cambia en cada autenticación. De esta manera se obtiene ventajas en cuanto a detección de clonación de etiquetas, interceptación, espionaje e incluso ataques de denegación de servicio. [45]

La ventaja en seguridad del sistema propuesto se encuentra en que el tag no contendrá información en claro del vehículo, sino que almacenará un código único cifrado que incluye una firma digital, que funcionará como un enlace directo que permitirá acceder a la información de manera rápida y segura. Para leer y descifrar dicho código se requiere de un lector con un software compatible con el sistema de cifrado, ejerciendo

funciones de middleware, traduciendo el código recibido en una llave de acceso a la base de datos y poder así obtener la información del vehículo.

Es decir, que, aunque la información viaje a través del espectro y pueda ser fácilmente interceptada, solamente se obtendrá un conjunto de caracteres, que mientras no se obtengan con el debido receptor, no se podrá tener acceso a la información. Adicionalmente, al estar la información almacenada en un sistema de bases de datos distribuidas, permitirá aumentar las barreras a los posibles ataques que tengan como finalidad robar información.

Las bases de datos deben tener como prioridad la protección de los datos y la información; en cuanto a eso, se han creado políticas en varios países del mundo. En el caso de Colombia, existe el Habeas Data, que es la ley estatutaria que decreta la protección de datos personales, con la cual deben regirse todas las organizaciones del Estado [46].

H. Ventajas sobre el uso de la tecnología RFID y bases de datos distribuidas en procesos de seguridad:

Acceso a la información: El uso de tecnología RFID permite que la captura de información y los seriales en los dispositivos lectores, sea más rápida y ágil, al igual que la consulta de la información en las bases de datos. El sistema de bases de datos distribuidas garantiza que el acceso sea más seguro, además de garantizar la disponibilidad de la información.

Veracidad de la información: La información almacenada en las diferentes bases de datos aporta un alto nivel de seguridad en el acceso a la información. Por parte de la tecnología RFID, esta permite que la información se envíe cifrada y con códigos de seguridad o firmas digitales, asegurando que se mantenga la integridad de la información y esta no sea modificada ni alterada.

Optimización en el proceso: Dentro de la dinámica de los procesos de seguridad, la validación de información vehicular no requerirá que se establezca un contacto directo con los conductores, basta con capturar la señal generada por el microchip desde el vehículo, permitiendo verificar la información de manera más rápida y tomar las medidas de seguridad necesarias al instante.

Reducción de tiempos: La captura de la información transmitida desde el transponder hacia el dispositivo lector, al igual que el acceso a la información en las bases de datos es un proceso que requerirá de tan solo algunos segundos, lo cual permite validar la información en tiempo real.

III. CONCLUSIONES

El acceso a la información mediante tecnologías RFID ofrece alta velocidad de respuesta permitiendo consultar y validar datos en tiempo real optimizando el consumo de los recursos informáticos.

El uso de la tecnología permite optimizar labores de control y verificación de información en bases de datos de gran tamaño por parte de entidades de seguridad para apoyar diferentes tareas que combaten actos delictivos.

La tecnología basada en radio frecuencia es una herramienta que facilita llevar a cabo actividades donde la distancia es un factor fundamental para su implementación y aplicación, haciendo posible que se pueda tener acceso a diferentes tipos de información como audio, video o data.

La implementación de interconexión de redes y la tecnología de sistemas de información, integrada con dispositivos emisores y receptores de radiofrecuencia, dan la posibilidad de encontrar y/o manipular información a determinadas distancias en tiempo real, lo que beneficiaria los procesos de validación de información haciendo que estos sean más agiles y prácticos.

Las tecnologías RFID tienen mayor cantidad de estándares en el envió de datos cifrados y firmas digitales de datos, ofreciendo mayor seguridad y protección a la información que se envía.

REFERENCIAS

[1] M. Bayani, A. Segura, M. Alvarado y M. Loaiza, “IoT-Based Library Automation and Monitoring system: Developing an Implementation framework of Implementation”, E-Ciencias de la Información, vol. 8, nº 1, junio 2018. DOI:10.15517/ECI.V8I1.30010

[2] V. J. Acevedo Duran, A. García Sandoval y J. S. Sandino Ariza, “Sistema de Registro y Control de Salida de Elementos mediante Dispositivos RFID”, Pontificia Universidad Javeriana, Bogotá D.C., 2004.

[3] R. J. Ramírez Lazón, “Aplicaciones del RFID como herramienta”, Universidad de Chile, Santiago de Chile, 2006.

[4] P. Kumar, M. Ruba, R. Kumar, D. Sowmiya y S. Varsha, “RFID BASED LIBRARY MANAGEMENT SYSTEM”, International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST), vol. 2, 2016.

[5] J. M. Ciudad Herrera y E. Samà Casanovas, “Estudio, Diseño y Simulación de un Sistema de RFID Basado en EPC”, 2005.

[6] Logistica Empresarial, Logistica Empresarial, 2018. [En línea]. Available: http://logisticaparalaempresa.blogspot.com/2015/09/radio-frecuency-identification-rfid.html.

[7] J. M. García Barceló, “Análisis y Prueba de un Sistema en Tecnología de Identificación por Radiofrecuencia”, Madrid, 2016.

[8] E. Gotor Carrasco, “Estado del Arte en Tecnologías RFID”, Universidad Politécnica de Madrid, Madrid, 2009.

[9] M. A. Leguizamón Páez, J. Martínez Pinzón y J. A. Misnaza Morales, “Análisis de una Implementación RFID dentro de la Industria Farmacéutica”, *Ingenierías USBMed*, p. 11, 2017. DOI: 10.21500/20275846.2936

[10] M. Green, “A Few Thoughts on Cryptographic Engineering”, Septiembre 2011. [En línea]. Available: https://blog.cryptographyengineering.com/2011/09/24/where-things-fall-apart-protocols-part/.

[11] Real Academia Española, “Real Academia Española”, Julio 2018. [En línea]. Available: http://dle.rae.es/?id=8pzz8q5.

[12] M. G. Mondaza, “Entorno histórico y Social de la Aparición del Microchip”, Universidad Politécnica de Madrid, 2014.

[13] R. Felmer, R. Chávez, A. Catrileo y C. Rojas, “Tecnologías actuales y emergentes para la identificación animal y su aplicación en la trazabilidad animal,» Archivos de medicina veterinaria, nº 38, 2006. DOI: 10.4067/S0301-732X2006000300002

[14] C. S. Mena Quiñones, “microchipfunciones”, 02 mayo 2012. [En línea]. Available:

http://microchipfunciones.blogspot.com/2012/05/funciones-claves.html.
[15] R. A. Elmasri y S. B. Navathe, "Fundamentos de Sistemas de Bases de datos", 5a. ed., Madrid: PEARSON EDUCACIÓN S.A., 2007.
[16] D. Pérez Valdés, "Maestros de la Web", 26 octubre 2007. [En línea]. Available: http://www.maestrosdelweb.com/que-son-las-bases-de-datos/.
[17] M. T. Özsu y P. Valduriez, Principles of Distributed Database Systems, 3a. ed., Springer Science & Business Media, 2011, p. 846.
[18] A. M. Díaz García y F. A. Acosta, "Sistema Telemático Basado en Servicios Web, Georreferenciación y Bases de Datos Distribuidas para Gestionar la Información del Departamento de Ventas de una Organización Dedicada al Comercio de Materiales para la Construcción", Universidad Distrital Francisco José de Caldas, Bogotá D.C., 2017.
[19] Oracle, «Oracle Help Center, » Julio 2018. [En línea]. Available: https://docs.oracle.com/cd/A57673_01/DOC/server/doc/SCN73/ch21.htm.
[20] W. J. Hidalgo Bucheli, "Diseño de Antenas Planares para Tags RFID pasivos en Bandas UHF sobre Sustrato Polimérico con Características de Flexibilidad y Transparencia para la Aplicación en Sistema de Transporte Inteligente", Universidad Nacional de Colombia, Bogotá D.C., 2017.
[21] Techlandia, "Techlandia", 2018. [En línea]. Available: https://techlandia.com/antena-vhf-info_257647/.
[22] RoudianTong.com, "Electronica Tecnología En Línea" [En línea]. Available: http://www.inteligentes.online/TV/Accesorios-TV/La-diferencia-entre-una-antena-UHF-y-VHF-.html.
[23] Techlandia, "Techlandia", 2018. [En línea]. Available: https://techlandia.com/antena-uhf-vs-vhf-info_214567/. [Último acceso: febrero 2018].
[24] Techlandia, "Techlandia", 2018. [En línea]. Available: https://techlandia.com/tipos-antena-uhf-lista_90017/.
[25] E. N. Céspedes, L. F. Castillo Romero, Y. A. Duarte Velásquez y G. A. Torres Guzmán, "Policia Nacional de Colombia", [En línea]. Available: https://www.policia.gov.co/sites/default/files/Hurto%20Automotores.html.
[26] [26] J. A. Restrepo Morales, S. Medina Hurtado y A. Bedoya, "Pérdidas Esperadas y Detrimento Patrimonial por Hurto de Vehículos en Colombia", Cuadernos de Economia, vol. 36, nº 71, Julio 2017. DOI: 10.15446/cuad.econ.v36n71.47450
[27] F. Falck Duran, "Cámaras Versus Drones: Las Políticas Públicas Latinoamericanas En La Encrucijada. El Caso de Honduras y Colombia", Pontificia Universidad Javeriana, Bogotá D.C., 2016.
[28] D. Clavero, "Diariomotor", enero 2012. [En línea]. Available: http://www.diariomotor.com/tecmovia/2012/01/20/goodyear-inserta-un-microchip-en-los-neumaticos-para-evitar-que-sean-robados/.
[29] K. N. Figueroa Niño, "Aplicación de la Tecnología de Identificación por Radio Frecuencia en Estudios de Transito y Transporte", Univesidad Nacional de Colombia, Bogotá D.C., 2016.
[30] StudioMarLin, Artist, Transporte/Tráfico. [Art]. 2018.
[31] Clker-Free-Vector-Images, Artist, GPS. [Art]. 2014.
[32] E. Espectador, "El Espectador", 14 Julio 2011. [En línea]. Available: http://www.elespectador.com/content/bogotanos-evaden-controles-de-velocidad-con-detector-de-radares.
[33] A. J. Elizondo, "Universidad de la Rioja", 2009. [En línea]. Available: http://www.unirioja.es/cu/arjaime/Temas/09.Distribuidas.pdf.
[34] B. Chavoya, Dirección, Consultas (BASE DE DATOS DISTRIBUIDOS). [Película]. Billy Chavoya, 2015.
[35] B. Thuraisingham y W. Ford, "Security constraint processing in a multilevel secure distributed database management system", IEEE Transactions on Knowledge and Data Engineering, vol. 7, pp. 274 - 293, 1995. DOI:10.1109/69.382297
[36] Tutorials Point, "Tutorials Point", [En línea]. Available: https://www.tutorialspoint.com/distributed_dbms/distributed_dbms_database_security_cryptography.htm. [Último acceso: 2018].
[37] Z. Zakaria Suliman, "On Distributed Database Security Aspects", ResearchGate, p. 5, 2014. DOI:10.1109/MMCS.2009.5256696
[38] Tutorials Point, "Tutorials Point", [En línea]. Available: https://www.tutorialspoint.com/distributed_dbms/distributed_dbms_security_distributed_databases.htm. [Último acceso: 2018].
[39] K. Hyunsung, "RFID Mutual Authentication Protocol based on Synchronized Secret.", International Journal of Security and Its Applications., vol. 7, nº 4, p. 14, 2013.
[40] Y.-J. Tu y S. Piramuthu, "Reducing False Reads in RFID-Embedded Supply Chains", Journal of Theorical and Applied Electronic Commerce Research, vol. 3, nº 2, Agosto 2008. doi:10.4067/S0718-18762008000100006
[41] K. Rhee, J. Kwak, S. Kim y D. Won, "Challenge-Response Based RFID Authentication", notas de Ciencias de la computación, vol. 3450, 2005.
[42] Cecarm, "Cecarm Comercio electrónico", [En línea]. Available: http://www.cecarm.com/emprendedor/estrategia/consultas-y-faqs/que-son-los-sellos-de-tiempo-3763. [Último acceso: Agosto 2018].
[43] Where Things Fall Apart: Protocols (Part 2 of 2)., "Where Things Fall Apart: Protocols (Part 2 of 2).", [En línea]. Available: https://blog.cryptographyengineering.com/2011/09/24/where-things-fall-apart-protocols-part/.
[44] M. O'Neill y M. Robshaw, "Low-cost digital signature architecture suitable for radio frequency identification tags", IET Computers & Digital Techniques, vol. 4, nº 1, p. 12, 2010. DOI:10.1049/iet-cdt.2008.0165
[45] Y. Liu, "An Efficient RFID Authentication Protocol for Low-Cost Tags", de 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Shanghai, China, 2008. DOI:10.1109/EUC.2008.135
[46] [EnColombia, "EnColombia", 2018. [En línea]. Available: https://encolombia.com/derecho/leyes/ley-habeas-data/ambito-aplicacion-definiciones/.

Wilson Leonardo Aguilar Rodriguez. Nacido en Bogotá D.C. en 1990. Estudió Tecnología en Sistematización de datos de la Universidad Distrital Francisco José de Caldas sede tecnológica, graduado en el año 2014. Ha trabajado desde 2013 en desarrollo de software en lenguaje Java y Pl-sql (2014). Actualmente es desarrollador para la empresa española Vector ITC Group haciendo parte de proyectos para cargue de información y apoyando la administración de bases de datos Oracle. Se ha especializado en el manejo y administración de bases de datos Oracle y desarrollo en lenguaje PL-SQL.

ORCID: https://orcid.org/0000-0003-3528-6902

Wilmar Giovanni Aguilar Rodriguez. Nació en 1990 en la ciudad de Bogotá D.C. Graduado como Tecnólogo en Sistematización de datos de la Universidad Distrital Francisco José de Caldas sede tecnológica en el año 2015. Desde el año 2014 se ha desempeñado como desarrollador de software en lenguaje Java, desarrollo en capa web con framework PrimeFaces y en servicios rest.

En la actualidad hace parte del equipo de desarrollo de la empresa española Vector ITC Group en proyectos destinados a la generación de reportes y administración de riesgos para SARLAFT. En sus años de experiencia ha trabajado especialmente en desarrollo de aplicaciones web.

ORCID: http://orcid.org/0000-0002-8953-9381

Miguel Angel Leguizamón Páez. Nació en Tunja Boyacá en 1974. Estudio Ingeniería de Sistemas en la Universidad de Boyacá en Tunja, graduado en el año 1998. Luego, en el año 2000 recibió el título de Especialista en Gerencia de Sistemas Informáticos en la misma Universidad de Boyacá. Posteriormente en el año 2013 se graduó como Magíster en Ciencias de la Información y las Comunicaciones en la Universidad Distrital Francisco José de Caldas. Acumula 19 años de experiencia docente universitaria: en el período comprendido entre 1999 y 2009 estuvo vinculado con la Universidad pedagógica y Tecnológica de Colombia en la ciudad de Tunja, Boyacá; actualmente y desde 2010 es docente de planta, categoría asistente en la Universidad Distrital Francisco José de Caldas en la ciudad de Bogotá. Autor de 9 artículos publicados en revistas nacionales.

Sus campos de interés se centran en procesos gerenciales a nivel de Tecnologías de la Información y las Comunicaciones, sistemas distribuidos, Internet de las cosas, Tecnologías emergentes y docencia universitaria, entre otras.

ORCID: http://orcid.org/0000-0003-0457-0126