ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"Diseño y prototipo de un sistema de autentificación sobre una red GPRS para la seguridad en el servicio de transporte público."

TESINA DE SEMINARIO

Previa a la obtención del título de:

INGENIERO EN CIENCIAS COMPUTACIONALES
ESPECIALIZACIÓN SISTEMAS TECNOLÓGICOS

Presentado por:

Freddy Xavier Borbor Moreira

Wander Moisés Bravo Borja

Zully Esmeralda Espinoza Toala

Guayaquil – Ecuador

2011

AGRADECIMIENTO

Agradezco a Dios y mi familia por enseñarme el cariño, el calor y apoyo de un verdadero hogar sin importar las circunstancias.

A mis amigos Henry, Jota, Christian, Vancho, Socrates, Manolo, Tato, Alex, Lucy, Denisse, Leonardo, Susy, Patricia, Vanessa, Jose, Jessica, Viviana, Xavier, María, etc. que sin ser mi familia han actuado como una.

A Kerly por su apoyo y ánimos en todo momento.

A todos aquellos que de una forma u otra han contribuido para que yo esté en este punto, y a los que están por venir, Gracias.

Freddy Xavier Borbor Moreira

AGRADECIMIENTO

El mayor agradecimiento a Dios, principalmente por Él he logrado este objetivo, a mi Padre Wander Bravo, a mi madre Jackeline Borja de Bravo, quienes demostraron siempre haber confiado en mí y por apoyarme en cada momento, a mis hermanos y a toda mi familia, a todos mis amigos y personas que aunque no seamos familia de sangre, los considero mi familia, a todos ustedes quienes fueron el motor para lograr este objetivo, finalmente a mis compañeros Zully Espinoza y Freddy Borbor.

Wander Moisés Bravo Borja

AGRADECIMIENTO

Agradezco a Dios quien me ha dado salud y fuerzas para alcanzar mi meta; a mis padres Pedro Espinoza y Esmeralda Toala, porque su apoyo fue fundamental en mi camino; a mi hermana Jéssica Espinoza quien siempre me animó a creer en mí; a mi tía Gioconda Toala y a mi primita Danielita que con su sonrisa alegraba mis días. Agradezco a todos mis amigos, especialmente a Dolores Pesantez, Dennys Zambrano, Paúl Crespo y Orlando Zambrano quienes con su compañía hicieron de la universidad un hogar. Finalmente agradezco a mis profesores, a mi Facultad y a mis compañeros Freddy Borbor y Wander Bravo.

Zully Esmeralda Espinoza Toala

DEDICATORIA

Dedico este trabajo a Dios mis padres y mi familia que me indicaron el camino correcto en una noche tormentosa, la humildad en la abundancia, la perseverancia ante todo y siempre seguir el camino del bien

Freddy Xavier Borbor Moreira

DEDICATORIA

A Dios, a mis Padres, a mis hermanos, a mi sobrina; a mis profesores y Directivos de mi Facultad; a mis amigos y compañeros de siempre, a las Familias: Rada Cevallos, Sánchez Crow, Vélez Navarrete, Suriaga Quimí, a la familia de Héctor Jaramillo. Finalmente dedico este trabajo a mi compañera, amiga y novia de mi vida universitaria Denisse Katherine.

Quienes siempre mostraron su apoyo incondicional.

Wander Moisés Bravo Borja

DEDICATORIA

Dedico este trabajo a Dios, a mis padres: Esmeralda Toala y Pedro Espinoza, a mi hermana Jéssica Espinoza y a mi tía Gioconda Toala; quienes creyeron en mí y siempre mostraron su apoyo incondicional.

Ustedes fueron los motores que me empujaban día a día a luchar por alcanzar mi meta.

Zully Esmeralda Espinoza Toala

TRIBUNAL DE SUSTENTACION

Ing. Alfonso Aranda	Ing. Ronald Ponguillo
Profesor de seminario de Graduación	Profesor delegado por el Decano de la Facultad

DECLARACIÓN EXPRESA

La responsabilidad por los hechos y doctrinas expuestas en este Proyecto de Graduación, así como el Patrimonio Intelectual del mismo, corresponde exclusivamente a la FIEC (Facultad de Ingeniería en Electricidad y Computación) de la Escuela Superior Politécnica del Litoral (Reglamento de Graduación de ESPOL)

Freddy Borbor

Wander Bravo

Zully Espinoza

RESUMEN

La inseguridad que actualmente atraviesan los ciudadanos ecuatorianos en los medios de transporte público (taxis y buses), debido a las anomalías de identidad de los choferes y a las fallas de los sistemas de aplicación de sanciones de tránsito, se ha acrecentado de forma alarmante, por esta razón el proyecto actual propone una solución alternativa un prototipo de un sistema de autentificación (conductores) sobre una red GPRS, que sea fiable, aceptado por la ciudadanía y tenga un buen desempeño. Además se propone una política de seguridad que debe seguir las cooperativas de taxis con el fin de alcanzar un alto desempeño del sistema propuesto.

El sistema contiene un módulo biométrico que recibe la huella dactilar del conductor, un teclado numérico con el cual se ingresa un número de 4 dígitos. Dicha información será enviada utilizando una red GPRS, al servidor que contendrán la información pertinente, para poder validar la información requerida.

Luego de validar que el conductor es quien dice ser, se consultará el estado del conductor y del vehículo, en entidades públicas como:

Comisión de Transito: Proporciona datos de infracciones del conductor y datos del auto.

Policía Judicial: Proporciona record policial del conductor.

Luego de conocer el estado actual de dicho conductor, el sistema dará a conocer el estado actual del conductor y del vehículo mediante un indicador acorazado que utiliza un código de colores, dicho indicador acorazado, mantiene un esquema de alta seguridad, inviolable, y monitoreado continuamente, para evitar suplantaciones, o ser burlado (bypass).

Este sistema, deberá requerir que cada cooperativa de taxis, implemente políticas de seguridad, para monitorear la integridad de los dispositivos instalados, así como del estado en cada situación del conductor y del vehículo.

ÍNDICE GENERAL

ABREVIATURAS

GPRS: General packet radio service.
Servicio general de paquetes vía radio.

GPS: Global Positioning System.
Sistema de posicionamiento global

GSM: Global System for Mobile Communications.
Sistema Global para comunicaciones mobiles

HSDPA: High-Speed Downlink Packet Access
Acceso de alta velocidad de descarga de paquetes

UMTS: Universal Mobile Telecommunications System
Sistema universal de telecomunicaciones móviles

MIMO: Multiple input multiple output
Varias entradas varias salidas

Kbps: Kilo bit per second
Kilo bit por segundo

W-CDMA: Wideband CDMA
CDMA banda ancha

PKI: Public key infrastructure
Infraestructura de clave publica

SSL: Secure Sockets Layer
Capa de zócalos seguros

SDK: Software development kit
Paquete de desarrollo de software

TCP/IP: Transmission-Control-Protocol/Internet Protocol
Protocolo de control de transmisión/Protocolo de internet

DPI Dots per inch
Puntos por pulgadas

GPL General Public License
Licencia publica general

PDU	Protocol data unite Unidade de datos de protocolo
RC2	Ron's Code 2 Código de Ron 2
RC4	Ron's Code 4 Codigo de Ron 4
IDEA	International Data Encryption Algorithm Algoritmo internacional de encriptación de datos
DES	Data Encryption Standard Estándar de encriptación de datos
AES	Advanced Encryption Standard Estandar de encriptación avanzada
MD5	Message Digest Algorithm
MAC	Media Access Control Control del acceso de medios
IPSec	IP Security Protocol Protocolo de seguridad IP
NAT	Network Address Translation Traducción de dirección de red
OLTP	(On-Line Transactional Processing Procesamiento transaccional en línea

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El presente trabajo propone el prototipo de un sistema de autentificación de conductores y vehículos, que sea aceptado por la ciudadanía, sea fiable y tenga un buen desempeño con el fin de llegar a ser una solución a la inseguridad que actualmente atraviesan los ciudadanos ecuatorianos en los medios de transporte público (taxis y buses), debido a las anomalías de identidad de los choferes y a las fallas de los sistemas de aplicación de sanciones de tránsito.

El sistema consta de un conjunto de aplicaciones: una aplicación central, aplicación en la entidad reguladora, varias aplicaciones en cada cooperativa de taxi y una aplicaciones en cada vehículo, las mismas que se comunicarán a través de una red GPRS (Servicio general de paquetes vía radio o General packet radio service). La aplicación del vehículo se encuentra instalada en un dispositivo con características especiales debido a las muchas interfaces que necesita para comunicarse con diversos dispositivos, los cuales son: un lector de huellas, un teclado numérico, un dispositivo GPS (Sistema de posicionamiento global o Global Positioning System) y el dispositivo acorazado.

El sistema propone acuerdos con entidades reguladoras y las cooperativas de taxis para un correcto funcionamiento

Capítulo 1

1. Antecedentes, Objetivos y Alcance

1.1 Antecedentes

La seguridad en nuestro país en los medios de transporte público:

La seguridad es un aspecto muy importante en la sociedad, debido a que está en juego la vida de muchos ciudadanos, al exponerse diariamente ante actos delictivos, en una actividad cotidiana como es el uso de transportes públicos.

La existencia de taxis piratas, o de antisociales disfrazados de conductores de taxis, es un problema que actualmente ataca a nuestra sociedad, lo que conlleva a altos índices delictivos en Guayaquil.

Otra particularidad existente en estos actos delictivos, es el llamado “secuestro express”, donde un vehículo es interceptado por antisociales, y los pasajeros de dicho vehículo son ultrajados y víctimas de robos.

Ante esta realidad, se considera necesario, conocer el estado actual tanto del conductor como del vehículo en el marco penal, y conocer si están o no aptos para circular por la calles según el marco regulatorio de tránsito.

Un dispositivo de seguridad en cada vehículo, ayudará a notificar a cada ciudadano, el peligro al que se expone antes de embarcarse a dicho vehículo, debido a este dispositivo será inalterable, o en el caso de ser alterado, notificará aquello y se garantizará un mayor nivel de seguridad.

Mediante el uso de un dispositivo biométrico se asegurara tanto la integridad del conductor como del vehiculó en base a los marcos penales y de transito, para luego indicar a través de un dispositivo acorazado, el estado del conductor y del vehículo

1.2 Objetivos

1.2.1 Objetivo General

- Diseñar y desarrollar el prototipo de un sistema de autentificación sobre una red GPRS que pueda ser utilizado para identificar anomalías de identidad o infractores sancionados en el servicio de transporte público.

1.2.2 Objetivos Específicos

- Determinar los factores de autentificación que tendrá el sistema.
- Seleccionar el hardware y software adecuados para el sistema, teniendo en cuenta la escalabilidad de los niveles de seguridad, el precio, la disponibilidad en el mercado y la factibilidad de ser adaptados en un vehículo.
- Crear procedimientos para las entidades reguladoras y cooperativas que contribuyan al correcto funcionamiento del sistema.

1.3 Alcance

Sistema para la identificación de posibles anomalías en el servicio de transporte público tanto del personal que opera como de los vehículos. Lo conformaran tres sectores principales

1. Vehículo.
2. Cooperativa de transporte
3. Entidad reguladora.

Cada vehículo está equipado con un miniCPU y un acorazado. El miniCPU es el encargado de la recepción, procesamiento y envío de información. A este dispositivo está conectado un lector de huellas

digitales y un teclado numérico que serán los medios por los cuales los conductores se identificarán como personal autorizado a utilizar el vehículo.

Una vez que el conductor se identifica, el miniCPU se comunica a una aplicación principal la cual es la encargada de dar a conocer si el conductor tiene algún inconveniente, el cual deba impedir que opere el vehículo. Además dicha aplicación se comunica con la entidad reguladora (ya sea por medio de un webservice o directamente a una base de datos) informándole si el vehículo está autorizado a transitar por las calles.

El medio de comunicación entre el miniCPU y la aplicación principal es el servicio de internet inalámbrico que ofrecen las compañías de telefonía celular locales(GPRS), además posee un dispositivo GPS medio por el cual se informa la ubicación del vehículo en determinado momento y una cámara IP en caso de que se desee observar la situación interna del vehículo.

Además del miniCPU y los periféricos mencionados hasta el momento constará de un acorazado el cual en su interior posee indicadores por medio de los cuales se notificara el estado actual del vehículo. Dicho indicadores cambian de estado ya se al encender el vehículo por alguna anomalía que se encontrase (conductor-

vehículo) o por alguna petición remota de la cooperativa de transporte.

La cooperativa posee una aplicación desde la cual podrá:

- Ingresar o modificar la información de los conductores.
- Indicar posibles anomalías con respecto a los conductores.
- Hacer un cambio en las alertas de los acorazados.
- Observar el estado actual del vehículo por medio de fotografías.
- Observar la ubicación actual del vehículo.
- Observar una bitácora de los eventos suscitados de cada vehículo.

El uso de dicha aplicación está limitado a personal autorizado el cual se identificará por medio de un usuario y una clave. El sistema al no detectar actividad del usuario en la aplicación tras determinado periodo de tiempo cierra automáticamente su sesión.

La entidad reguladora posee acceso a una aplicación con la cual pueden obtener diverso reportes en los cuales se pueden observar el estado actual de los vehículos o conductores, entre otros.

Adicional cada cooperativa de transporte debe implementar ciertas políticas de seguridad tanto de comunicación como acceso y mantenimiento a los dispositivos

Capítulo 2

2. Marco Teórico

2.1 Biometría

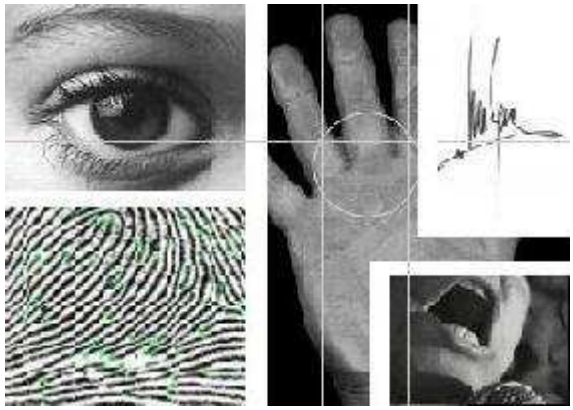

Figura 1 Biometria

La biometría emplea uno o más rasgos conductuales o físicos intrínsecos de un ser humano con el fin de crear métodos de reconocimiento únicos de personas. El término “biometría” se deriva de las palabras griegas "bios" de vida y "metron" de medida.

Para las tecnologías de la información (TI), la autentificación biométrica son tecnologías que buscan la autentificación basándose en características que son inherentes y único por sujeto, para ello miden y analizan características físicas y el comportamiento humano.

Un sistema biométrico es un sistema automatizado que realiza tareas de biometría, toma una característica personal que puede ser verificada de manera automatizada para la toma decisiones.

Modelo del proceso de identificación personal

Cualquier proceso de identificación personal postula la existencia de **tres indicadores de identidad** que definen el proceso de identificación:

1. **Conocimiento:** la persona tiene conocimiento (por ejemplo: un código),
2. **Posesión:** la persona posee un objeto (por ejemplo: una tarjeta), y
3. **Característica:** la persona tiene una característica que puede ser verificada (por ejemplo: una de sus huellas dactilares).
    - **Características físicas (estáticas);** huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano.
    - **Características del comportamiento (dinámicas);** firma, el paso y el tecleo.

Los indicadores anteriores pueden ser combinados con el fin de alcanzar altos grados de seguridad y diferentes niveles de

protección. La tarea de identificación personal depende de la situación. Es importante considerar el valor que está siendo protegido, los diversos tipos de amenazas, la reacción de los usuarios y el costo del proceso.

Características de un indicador biométrico

Un indicador biométrico es alguna característica con la cual se puede realizar biometría. Cualquiera sea el indicador, debe cumplir los siguientes requerimientos:

1. **Universalidad:** toda persona posee esa característica;
2. **Unicidad:** la existencia de dos personas con una característica idéntica tiene una probabilidad muy pequeña;
3. **Permanencia:** la característica no cambia en el tiempo; y
4. **Cuantificación:** la característica puede ser medida en forma cuantitativa.

Características de un sistema biométrico para identificación personal

Un sistema biométrico debe tener una utilidad práctica por lo que debe considerar lo siguiente:

1. El **desempeño**, busca comprobar si el sistema posee una exactitud y rapidez aceptable con un requerimiento de recursos razonable.
2. La **aceptabilidad**, indica si las personas están dispuestas a aceptar un sistema biométrico en su vida diaria. Por lo que el sistema debe inspirar confianza.
3. La **fiabilidad**, indica si el sistema puede ser burlado fácilmente.

2.1.1 Sistemas biométricos actuales

Las técnicas biométricas más conocidas son nueve y están basadas en los siguientes indicadores biométricos:

1. Rostro,
2. Termograma del rostro,
3. Huellas dactilares,
4. Geometría de la mano,
5. Venas de las manos,
6. Iris,
7. Patrones de la retina,
8. Voz,
9. Firma.

2.2 Tecnología GPRS

2.2.1 Antecedentes

GSM: Es el antecesor de GPRS, es considerado por sus características; como velocidad de transmisión, un estándar de segunda generación (2G).

GSM ha servido al mundo de las comunicaciones móviles por más de 2 décadas, y ha cumplido su papel muy bien, y actualmente aun es el más utilizado en la tecnología de las comunicaciones de telefonía móvil.

2.2.2 Definición

GPRS es una tecnología que transmite datos por medio de 'paquetes' y comparte un rango de frecuencias que pertenecen a una red GSM.

La conmutación de paquetes es el procedimiento más apropiado para la transmisión datos, debido a que los datos anteriormente se transmitían mediante conmutación de circuitos, dicho procedimiento es el más adecuado para la transmisión de voz.

2.2.3 Características

- Velocidad de transferencia de hasta 144 Kbps

- Conexión permanente. Tiempo de establecimiento de conexión inferior al segundo
- Pago por cantidad de información transmitida, no por tiempo de conexión
- Beneficios de un computador personal pero de menor tamaño.

2.2.4 Ventajas

VENTAJAS PARA EL USUARIO

Las ventajas que obtiene el usuario con el sistema GPRS son consecuencia directa de las características vistas en el punto anterior.

- Característica de "Always connected": un usuario GPRS puede mantener una conexión permanente, debido a que no utiliza ningún recurso de red, y tampoco se le cobrara ningún valor, mientras no esté recibiendo ni transmitiendo datos.
- El cobro de valores es por la cantidad de datos transmitidos, y no por tiempo de conexión.
- El establecimiento de conexión a la red GPRS, posee un costo nulo en comparación a los quantum de conexiones utilizando la tecnología GSM.

- Mejor velocidad de transmisión en GPRS, se pueden tener varios canales asignados, tanto en el sentido de transmisión del móvil a la estación base, como viceversa, a diferencia de GSM que sólo se puede tener un canal asignado ("timeslot"), por lo tanto la velocidad de transmisión aumentará con el número de canales asignados.

  Además, GPRS permite el uso de esquemas de codificación de datos que permiten una velocidad de transferencia de datos mayor que en GSM.

- Posibilidad de realizar/recibir llamadas de voz mientras se está conectado o cuando se está utilizando cualquiera de los servicios disponibles en esta tecnología.
- Modo de transmisión asimétrico, más adaptado al tipo de tráfico de navegación html o wml (un terminal GPRS 4+1)

  (4 slots downlink y 1 uplink) tendrá cuatro veces mayor capacidad de transmisión de bajada que de subida).

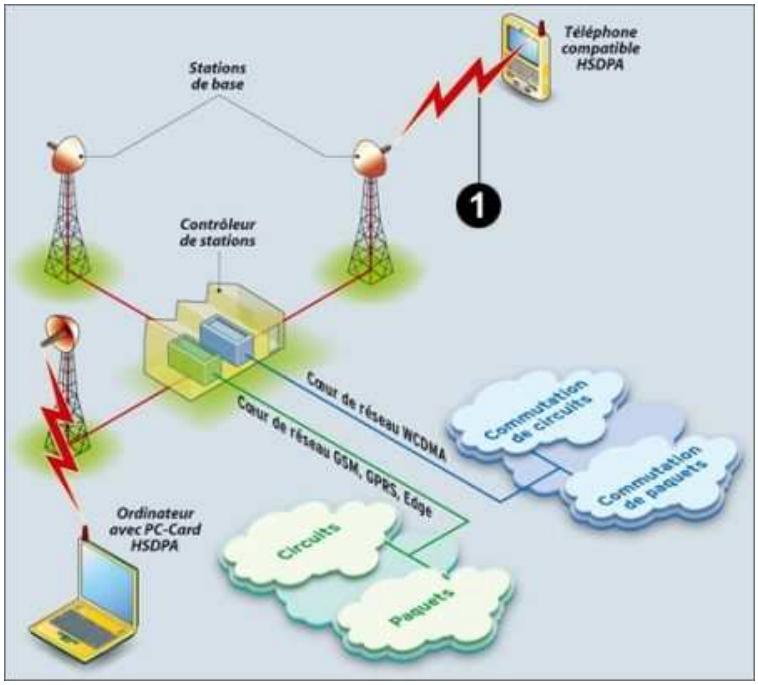

Figura 2 Funcionamiento de Red HSPDA

VENTAJAS PARA LA OPERADORA.

La operadora obtendrá el uso eficiente de los recursos de la red, ya que los usuarios sólo ocuparan los recursos de la red si y solo si están transmitiendo o recibiendo datos, adicionalmente se podrán compartir los canales de comunicación entre distintos usuarios a diferencia de los canales dedicados como en el modelo GSM.

2.2.5 HSDPA

Es una tecnología móvil también conocida como 3.5G, ya que es una mejora de la tecnología UMTS o de tercera generación (3G).

Esta tecnología provee velocidades altas en el canal de bajada (downlink), hasta 14.4 Mbps (y 20 Mbps con antenas MIMO), superando altamente a los 384 kbps de UMTS, y aumentando así su eficiencia espectral.

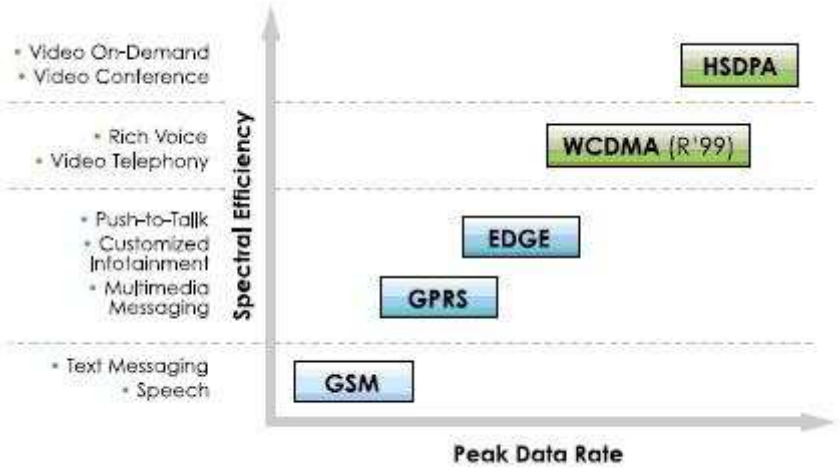

Figura 3 Servicios por tecnologías

2.3 Protocolo SSL

Si se requiere autenticación y privacidad de la información una opción es usar criptografía mediante el protocolo Secure Socket Layer (SSL), entre extremos sobre Internet.

Comúnmente, sólo el servidor es el que se autentifica (en otras palabras garantiza que él es quien dice ser) mientras que el cliente permanece sin autenticar; si se requiere implementar autenticación mutua, se necesita un despliegue de infraestructura de claves públicas (o PKI) para los clientes, con la finalidad de prevenir escuchas (eavesdropping), falsificación de la identidad del remitente (phishing) y alterar la integridad del mensaje.

SSL implica una serie de fases básicas que son las siguientes:

- Negociar entre las partes el algoritmo que se usará en la comunicación.
- Intercambio de claves públicas y autenticación basada en certificados digitales.
- Cifrado del tráfico basado en cifrado simétrico.

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

- Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza;
- Para cifrado simétrico: Ron's Code 2 (RC2), Ron's Code 4 (RC4), IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard);
- Con funciones hash: Message Digest 5 (MD5) o de la familia SHA.

SSL poseen una variedad de medidas de seguridad:

- Numerando todos los registros y usando el número de secuencia en el media access control (MAC).
- Usando un resumen de mensaje mejorado con una clave (de forma que solo con dicha clave se pueda comprobar el MAC). Esto se especifica en el RFC 2104).
- Protección contra varios ataques conocidos (incluyendo ataques man-in-the-middle), como los que implican un degradado del protocolo a versiones previas (por tanto, menos seguras), o conjuntos de cifrados más débiles.
- El mensaje que finaliza el protocolo handshake (Finished) envía un hash de todos los datos intercambiados y vistos por ambas partes.

- La función pseudo-aleatoria divide los datos de entrada en 2 mitades y las procesa con algoritmos hash diferentes (MD5 y SHA), después realiza sobre ellos una operación XOR. De esta forma se protege a sí mismo de la eventualidad de que alguno de estos algoritmos se revelen vulnerables en el futuro.

SSL es un protocolo en capas y consiste en cuatro sub-protocolos:

- SSL Protocolo de saludo (SSL Handshake Protocol)
- SSL Protocolo de cambio de especificaciones de cifrado (SSL Change Cipher Spec Protocol)
- SSL Protocolo de alerta (Alert Protocol)
- SSL Registro de Capa (SSL Record Layer)

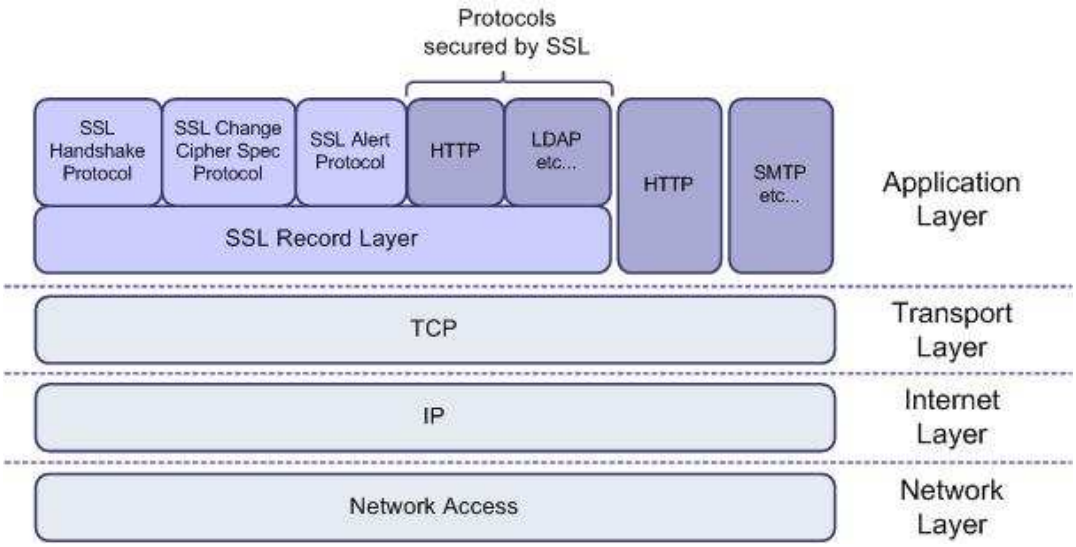

Figura 4 SSL en el protocolo TCP/IP

Como el diagrama superior muestra, SSL se encuentra en la capa de aplicación del modelo TCP/IP (Transmission-Control-Protocol/Internet Protocol). SSL puede ser implementado en casi cualquier sistema operativo que soporte TCP/IP, sin la necesidad de modificar el kernel del sistema. Esto le da a SSL una ventaja muy fuerte sobre otros protocolos como IPSec (IP Security Protocol), el cual requiere soporte de Kernel y una modificación a TCP/IP. SSL también puede ser implementada a través de firewalls y proxys, al igual que NAT (Network Address Translation) sin problemas.

2.4 Java Secure Socket Extention (JSSE)

Es un conjunto de paquetes de java que permite tener una comunicación segura en Internet. Implementa los protocolos SSL y TLS, pero en una versión java, además posee funcionalidades como cifrado de datos, autenticación del servidor, integridad de mensajes y autenticación del cliente.

Comando para generar un Almacenador de claves (KeyStore)

- Keytoo
- Genkey
- Keystore
- mySrvKeystore

- keyalg RSA

Algoritmo que pueden ser utilizados al momento de crear un keystore:

- Java keystore (Jks).
- pkcs12

2.5 GPS

Figura 5 Receptores GPS

El GPS (Global Positioning System) permite obtener la ubicación de cualquier de objetos en cualquier lugar del planeta gracias a un sincronizado grupo de 24 satélites que se encuentran a una altura de 20200 Km sobre la superficie terrestre

Los 24 satélites se encuentran en orbitas sincronizadas cubriendo todo el globo terráqueo distribuidos en 6 planos orbitales, cada plano tiene 4 satélites

Los receptores GPS son los terminales finales con los que interactúa el usuario y por medio del cual puede fácilmente puede conocer su posición en la tierra.

Inicialmente los receptores GPS eran grandes y costosos equipos pero con el pasar del tiempo ha disminuido su tamaño y costo. Existe una gran variedad de receptores desde complejos equipos independiente hasta receptores USB para ser utilizados en computadores personales.

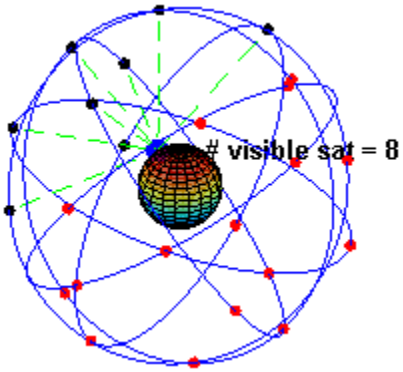

Figura 6 Ejemplo visual de la constelación GPS.

El receptor GPS para determinar su posición necesita localizar como mínimo 3 de los 24 satélites luego sincronizan sus relojes GPS, una vez hecho esto midiendo el tiempo que tardan en llegar unas señales desde el satélite al receptor se puede determinar la distancia entre estos dos, el receptor procede a determinar su posición relativa a los satélites localizados utilizando triangulación (método de triangulación inversa).

La posición de cada satélite es determinada de antemano por el receptor utilizando la información llamada almanaque (un conjunto de valores con 5 elementos orbitales), dicha información es transmitida por los satélites. Un receptor tarda entre 12 y 20 minutos en recolectar el almanaque de todos los satélites.

Con la posición relativa del receptor y la posición de cada satélite se puede establecer la posición real sobre la tierra del receptor GPS.

2.6 Tecnología aplicada a seguridad pública - Casos de estudio

La tecnología aplicada a la seguridad pública es un campo nuevo en el que se está innovando constantemente, a continuación se muestran los siguientes casos de estudio en los que la tecnología ha contribuido en alguna medida a la seguridad de las personas

2.6.1 Proyecto Voice your view

La inseguridad que hoy en día enfrentan los ciudadanos al salir a las calles o inclusive en su propio hogar se ha incrementado a tal punto que muchos ciudadanos no se sienten a salvo en ningún momento del día.

Es este el motivo del sistema llamado Voice Your Vew (vYv) desarrollado por científicos del Programa de Economía Digital del Engineering and Physical Sciences Research (EPSRC) en

Reino Unido. El objetivo principal del vYv es permitir a los ciudadanos expresar el nivel emocional respecto a su barrio o cualquier espacio público utilizando terminales de acceso público o software en los teléfonos celulares, luego el sistema mediante procesamiento del lenguaje natural convierte los comentarios en datos significativos. Un ciudadano que ha realizado un comentario puede saber si algún otro ciudadano está de acuerdo con su opinión y observar las opiniones del resto de ciudadanos.

Los siguientes son algunos de los escenarios donde se ha probado esta tecnología:

- Librería publica de Lancaster
- Campus de la Universidad de Coventry
- Condado de Derry en Irlanda del Norte

Con los datos recolectados se realiza un grafica de muestra la satisfacción ciudadana de un sector. Esta puede llegar a ser información valiosa a las entidades que velan por el bien público ya que no hay mejor fuente de la situación actual de sector de una ciudad que las personas que día a día circulan por la misma.

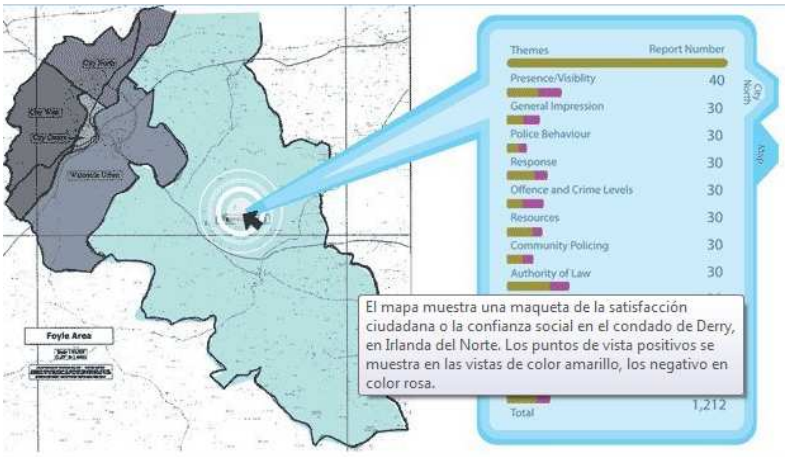

Figura 7 Satisfacción ciudadana del condado de Derry – Irlanda del Norte

2.6.2 Celulares Anti-secuestro

A lo largo del tiempo de nuestra sociedad las medidas de seguridad han avanzado y con ellas las diversas formas de delitos, uno de ellos que en los últimos años afecta al público en general es el secuestro. Acto en el cual un individuo o grupo de individuos es privado de su libertad y para ser liberados las víctimas o familiares deben proporcionar fuertes sumas de dinero a los captores.

Una medida para contrarrestar este tipo de delito es una aplicación Antisecuestros desarrollada por la empresa mexicana

Futuro Móvil para los dispositivos Iphone, se asegura que en un futuro existirá para Nokia, Android y Blackberry.

La aplicación se divide en tres partes:

- Preventiva:

  El usuario mediante la aplicación recibirá consejos de expertos en seguridad para evitar se víctimas de algún delito agravado.

- Alerta

  El usuario acciona un botón de pánico, una vez accionado la aplicación reportara a sus familiares o amigos que va a ser víctima de un delito mediante las principales redes sociales (Facebook, Twitter), SMS o correo electrónico en un intervalo de 5 minutos. Adicionalmente a sus contactos telefónicos envía su ubicación utilizando el GPS.

- Denuncia

  El usuario puede reportar a las autoridades acerca de un delito o accidentes del que ha sido víctima o presenciado

Figura 8 Software móvil anti secuestros

2.6.3 Próxima Generación de Seguridad Pública

MOTOROLA

Figura 9 *Logo Motorola*

Motorola incluye entre sus productos equipos diseñados para América latina orientados a la seguridad pública en una estrategia llamada Próxima Generación de seguridad pública.

El gigante de las telecomunicaciones incluye equipos que trabajan en una frecuencia de 4.9 GHz la cual es una excelente para los fines a ser utilizados.

Promueven sistemas banda ancha inalámbrica que proporcionan conectividad en lugares de difícil acceso donde otras tecnologías fallan, además de una alta rentabilidad y escalabilidad al poder ser adaptados tanto a sistemas de radiocomunicaciones (APCO25, TETRA YH MOTOTRBO) como a computadores móviles.

La utilización de conexiones punto-punto y punto-multipunto facilita una conexión veloz y segura a bases de datos en internet además de eliminar líneas dedicadas y cableadas que tienen un mayor costo

Todas estas tecnologías cumplen con las más altas normas de de confiabilidad que son necesarias al momento de hablar de redes de seguridad pública y pueden ser implementadas tanto a pequeñas como grandes ciudades.

2.6.4 Proyecto Tire Iq

Ilustración 1 Logo TireIQ

Desde el comienzo de la era industrial el proteger su inversión ha sido uno de los mayores intereses de los grandes

empresarios. Ya sea por falta de tiempo o recursos no pueden realizar un correcto monitoreo del correcto manejo de su inversión, un gran mercado poco explotados en este sentido es el de los neumáticos.

A este mercado es a donde el gigante de neumáticos Good Yeard está introduciendo un nuevo sistema llamado Tire Iq en colaboración con Vector Technology en Latino América.

El sistema se basa en el uso de tecnologías inalámbricas (GPRS, Bluetooh y Radio Frecuencia) para el seguimiento del desempeño de los neumáticos durante su vida útil. Consta de las siguientes partes.

- Chips para neumáticos y vehículos
- Equipos recolectores de datos
- Aplicación cliente

En cada neumático y vehículo se coloca un chip el cual se va a encargar de almacenar información relevante del neumático la cual va a ser ingresada con ayuda del Colector de datos, todos estos implementos totalmente inalámbricos en su funcionamiento. Una vez obtenida la información por los equipos recolectores de datos esta es enviada a un servidor por

medio de GPRS, una vez realizado el envío la información puede ser visualizada por la aplicación cliente. La aplicación clientes es un sistema de control gerencial desde el cual se puede observar estado de todas las flotas de vehículos que tenga a su cargo.

Gracias al avanzado uso de las tecnologías se disminuye en un gran porcentaje la incidencia del factor humano en el proceso de control de neumáticos. El usuario puede observar y analizar información actualizada en tiempo real y así poder tomar decisiones tanto preventivas como correctivas en base a información mucho más fiable.

Capítulo 3

3. Diseño General

3.1 Hardware

3.1.1 Dispositivo Lector de huellas

Nombre: Lector de huellas de Microsoft (Microsoft Fingerprint Reader)

Descripción:

Dispositivo biométrico lector de huellas digitales. El esquema de su funcionamiento es muy sencillo al momento que el usuario coloca su huella en el dispositivo este envía una captura de la huella a la aplicación la cual puede ser procesada para obtener una plantilla, es esta la información la que distingue entre individuos la cual puede ser almacena en base de datos y difícilmente recreada. Microsoft no proporciona las librerías para el manejo de dicha información pero en el mercado existen una gran variedad de SDK para que los desarrolladores manipulen dicha información.

Características:

- **Tipo:** óptico

- **Fabricante:** Microsoft.
- **Resolución:** 512 DPI-Dots per inch
- **Tamaño de la imagen:** 355x390 pixeles
- **Colores:** 256 niveles, escala de grises
- **Conexión:** USB 1.0, 1.1 o 2.0
- **S.O. soportados:** Windows Vista/XP/2003/2000 y **Linux**

3.1.2 Receptor GPS

Es un receptor basado en la arquitectura SiRF Star III, que se comunica con otros dispositivos electrónicos compatibles a través de la interfaz USB, y guarda la información importante transmitida desde de los satélites en su memoria temporal. Tiene un bajo consumo de energía, y su información proviene de 20 satélites al mismo tiempo, dicha señal de los satélites se adquiere cada 100 ms y actualiza el posicionamiento cada segundo.

Características:

- **Tasa de actualización:** 1 Mhz
- **Fabricante:** Holux.
- **Tiempo de actualización :**
  - Re adquisición: 0.1 s
  - Arranque en caliente (Hot start): 8 s.
  - Arranque en tibio (Warm Start): 38 s.

- Arranque en frio (Cold start): 42 s.

- **Protocolo:** NMEA V.2.2
- **Exactitud de posicionamiento:** 5 – 25 m
- **Peso:** 84 g
- **Consumo de energía:** menos de 80mA con 4.5- 5.5V de entrada.

3.1.3 Dispositivo acorazado

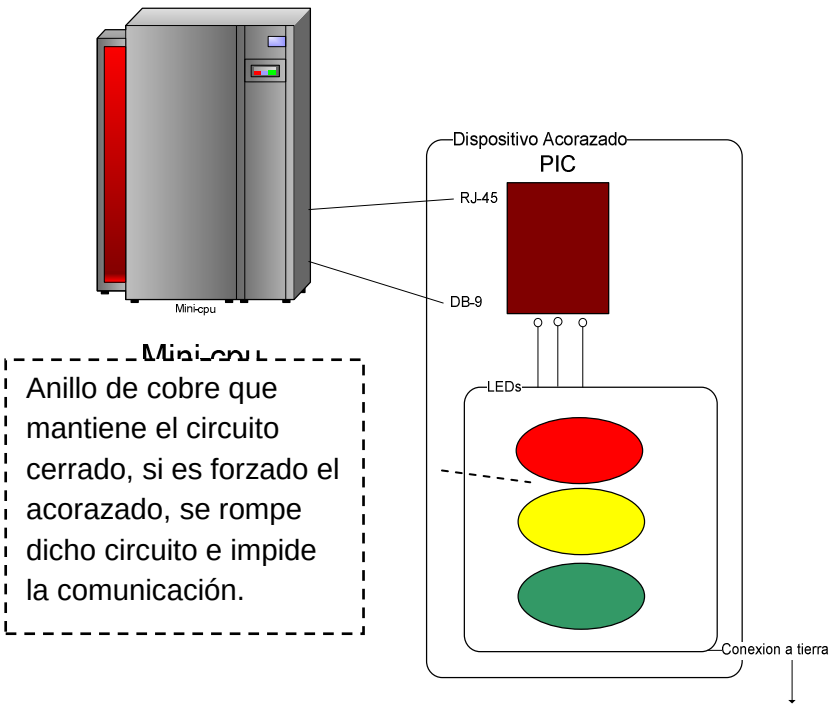

Figura 10 Arquitectura del dispositivo acorazado

Dispositivo electrónico utilizado para emitir alarmas visuales recibidas por medio de una interfaz DB-9. El dispositivo consta de un puerto RJ45 por medio del cual puede ser

monitoreada su actividad, adicional consta de una línea de cobre que se encuentra unida a la estructura externa y cierra el circuito del puerto RJ45, si la estructura externa del acorazado es abierta la línea de cobre se corta y el monitoreo se interrumpe este mecanismo puede ser utilizado como seguridad física del dispositivo.

3.2 Software

3.2.1 Sistema operativo

Ubuntu 7

Ubuntu es una distribución Linux basada en Debian GNU/Linux orientado a un usuario medio que no necesita un alto nivel de conocimiento informático para poder utilizarlo e instalarlo. Tanto el sistema operativo como los paquetes que lo conforman son distribuidos bajo licencia GPL-General Public License.

3.2.2 Librería Java Fingerprint SDK 2009

El Fingerprint Software development kit (SDK) es un paquete de desarrollo utilizado para agregar la autenticación biométrica por huella dactilar de los usuarios a tus propias aplicaciones, agregando un mayor nivel de seguridad al acceso a las aplicaciones.

Características

- Soporte a múltiples lectores de huellas: Fingerprint SDK admite 19 dispositivos.
- Soporte a los lectores de Microsoft y Digital Persona, el SDK incluye su propio manipulador para este tipo de dispositivos para así obviar de driver o API de los fabricantes.
- Provee una gran escalabilidad y portabilidad, al ser desarrollado en java no está ligado a un sistema operativo en específico.
- Identificación de huellas uno – muchos.

3.2.3 Librería java Jposition

Librería distribuida bajo licencia GNU Lesser GPL, esta librería es utilizada para mostrar mapas de google docs en una aplicación java

3.2.4 Librería java Rxtx

Librería para java utilizada para una correcta comunicación de la aplicación con los puertos seriales (COM Y LPT).

3.2.5 Librería Java NMEA Api

Libraría para java para la manipulación de datos GPS utilizando el protocolo de National Marine Electronics Association (NMEA),

El protocolo NMEA es utilizado para que despóticos marinos y receptores GPS puedan comunicarse

3.2.6 Proyecto v4l4j

Libraría java distribuida bajo licencia GLP que provee un fácil acceso a la captura de video.

Permite un control a las características del video (contrastes, brillo, foco, etc.)

3.3 Arquitectura del Sistema

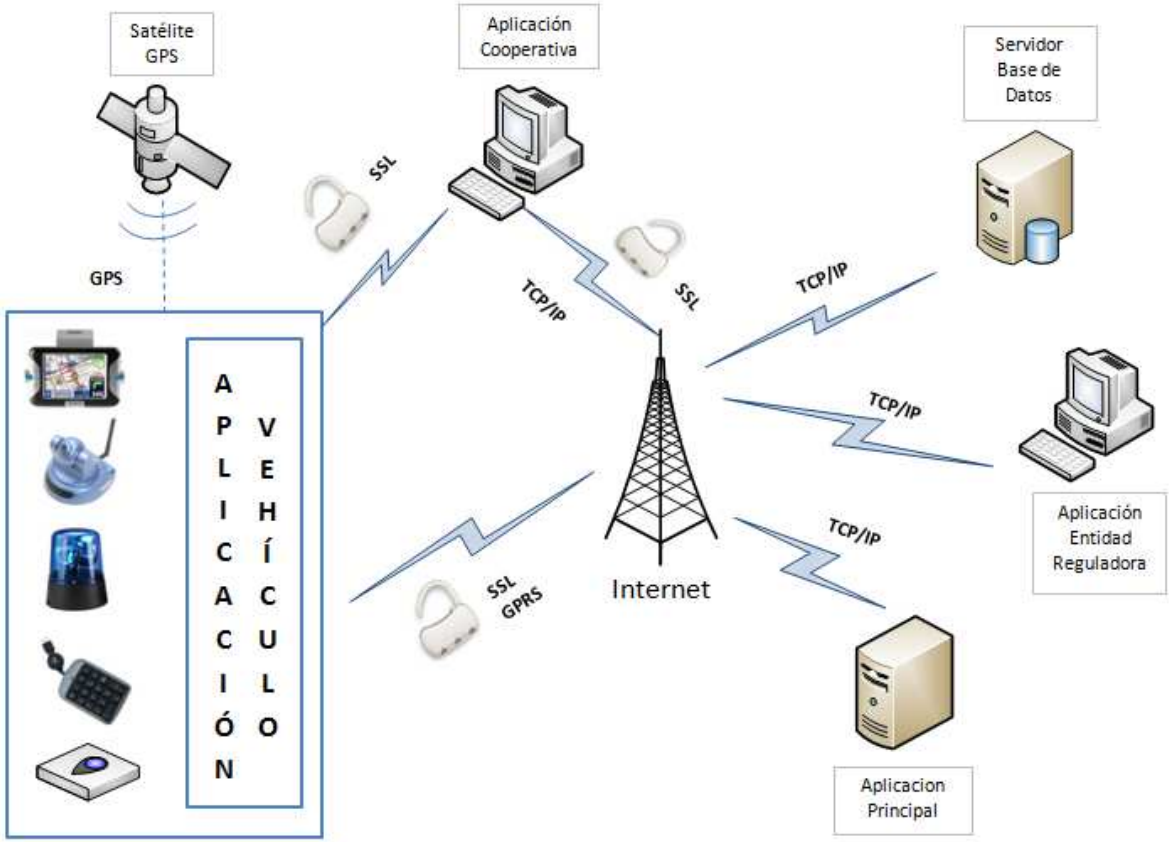

Figura 11 Arquitectura del Sistema

El sistema trabaja sobre una red GPRS y está conformado por los siguientes módulos:

- Aplicación Principal
- Aplicación en la Entidad Reguladora
- Aplicaciones en las Cooperativas
- Dispositivos en los Vehículos
- Servidor de Base de Datos de la Aplicación Principal

La comunicación entre cada uno de estos módulos se la realiza utilizando el protocolo TCP/IP.

3.3.1 Aplicación Principal

La aplicación principal tiene como objetivo escuchar y responder las peticiones que realizan las aplicaciones de los vehículos.

Las peticiones que realizan los vehículos son las siguientes:

- **Petición A :** Verificar clave

  La petición enviada por el vehículo tiene el siguiente formato:

  C:CodigoConductor:IdCooperativa:Placa

  Una vez que se verifica que el Código ingresado por el conductor utilizando el teclado numérico existe, realiza la consulta de los antecedentes penales y de tránsito que

pertenecieran al conductor o al vehículo y esta responde a la aplicación del vehículo los estados correspondientes de ambos.

La aplicación principal responde al vehículo con el siguiente formato:

RC:StVehiculo:StConductor

Donde STVEHICULO significa el estado del vehículo, y STCONDUCTOR significa estado del conductor.

Los valores que puede tomar STVEHICULO son:

- NN: falló la conexión con la entidad reguladora
- VP: vehículo penalizado
- OK: vehículo con estado ok

Los valores que puede tomar STCONDUCTOR son:

- NN: falló la conexión con la entidad reguladora
- CP: conductor penalizado
- OK: conductor con estado ok

Si STCONDUCTOR y STVEHICULO son OK, la aplicación procede a la verificación biométrica del conductor para comprobar que es él quien dice ser.

Si el valor STCONDUCTOR ó STVEHICULO no es OK, la aplicación del vehículo establece el color correspondiente en el acorazado el cual indicará la anomalía existente.

- **Petición B:** Verificar si el código del conductor coincide con la huella ingresada.

  La petición enviada por el vehículo tiene el siguiente formato:

  H:HUELLA

  La aplicación responde al vehículo con el siguiente formato:

  RH:RESULTADO.

  Donde RESULTADO puede tomar los siguiente valores:

  - S: si coincide
  - N: no coincide

  Si el valor de RESPUESTA es S entonces la aplicación del vehículo establece el estado del acorazado en verde caso contrario no enciende el acorazado.

3.3.2 Aplicación en la Entidad Reguladora

La aplicación ubicada en la Entidad reguladora tiene como objetivo realizar consultas referentes a los vehículos, las cooperativas y conductores.

La aplicación tiene las siguientes opciones:

- Conductores en línea

- Conductores que fallaron en el login
- Conductores en estado Ok
- Vehículos en estado OK

3.3.3 Aplicación en las Cooperativas

La aplicación ubicada en las cooperativas tiene como objetivo realizar las siguientes operaciones:

- Crear Cooperativa
- Crear Vehículo
- Consultar Vehículo
- Ingresar Marcas de Vehículos
- Ingresar Modelos de Vehículos
- Crear usuario
- Crear Conductor
- Control de vehículos
- Cambiar estado del Acorazado de un vehículo.

3.3.4 Dispositivos en los Vehículos

El dispositivo ubicado en los vehículos está formado por los siguientes bloques:

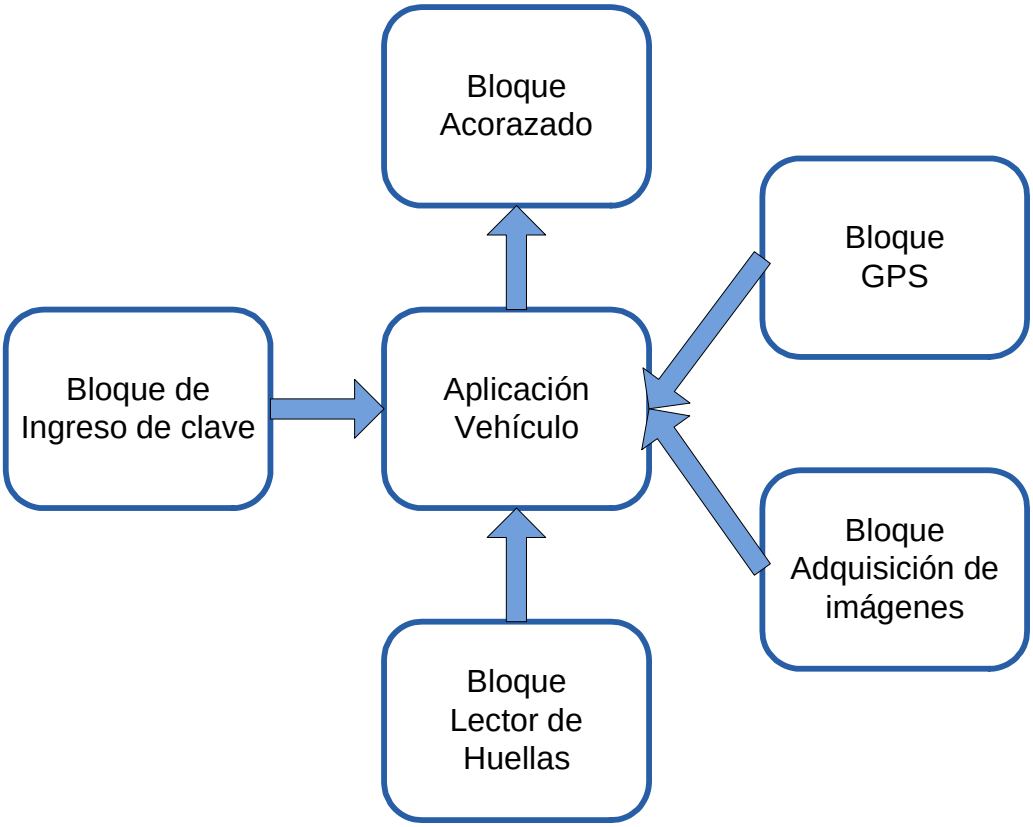

Figura 12 Diagrama de bloques de comunicación entre el vehículo y los dispositivos

Bloques de Entrada

Bloque de Ingreso de clave

Bloque Lector de Huellas

Bloque GPS

Bloque Adquisición de imágenes

Bloque de Salida

Bloque Acorazado

3.3.4.1 Aplicación Vehículo

Esta aplicación es la encargada de procesar la información receptada por los bloques de entrada y a su vez es la encargada de enviar los datos correspondientes a los bloques de salida.

Este bloque realiza varias funciones:

- Recepción de la huella digital del conductor.
- Recepción del código del conductor.
- Envío de la huella digital y código del conductor a la aplicación principal.
- Asignación del estado del acorazado en base al estado del vehículo y conductor o por solicitud de la aplicación de la cooperativa
- Recepción del posicionamiento del vehículo calculado por el bloque GPS.
- Envío de la posición del vehículo a la aplicación de la cooperativa.
- Recepción de las imágenes tomadas por el bloque de Adquisición de imágenes.
- Envío de las imágenes receptadas a la aplicación de la cooperativa.

3.3.4.2 Bloque de Ingreso de clave

Este bloque es el encargado de obtener los dígitos correspondientes al código del conductor utilizando un teclado numérico USB, que luego será usado junto con la huella digital para verificar que el conductor es quien dice ser.

3.3.4.3 Bloque Acorazado

Es el encargado de mostrar a los usuarios el estado de la unidad (conductor y vehículo).

Los estados son los siguientes:

Estado	**Conductor**	**Operación**	**Taxi**
Verde	Ok	And	Ok
Naranja	Ok	And	No Ok
Rojo	No Ok	And	Ok
Rojo	No Ok	And	No Ok

Tabla 1 Estados del indicador del acorazado

El acorazado permanece apagado cuando:

- El vehículo está apagado.
- La huella no corresponde a la clave ingresada.

3.3.4.4 Bloque Lector de Huellas

El bloque lector de huellas es el encargado de la captura y digitalización de la huella dactilar del conductor al momento de realizar el login.

3.3.4.5 Bloque GPS

Este bloque es el encargado de la recepción de la ubicación geográfica del vehículo.

3.3.4.6 Bloque de Adquisición de imágenes

Este bloque es el encargado capturar fotos del interior del vehículo al momento que la cooperativa de taxis realiza el monitoreo periódico.

3.3.5 Servidor de base de datos

Computador servidor que posee un motor de base de datos relacional con características para bases OLTP (On-Line Transactional Processing o Procesamiento transaccional en línea), de este modo puede responder correctamente a las constantes peticiones de las aplicaciones.

Las características recomendadas para el servidor serian

- Procesador inter core 2 duo.
- Memoria Ram 2GB.
- Disco duro 120 GB.

3.4 Procesos

Para un mejor entendimiento del sistema, se detalla los procesos que se consideran relevantes:

- Proceso de Autentificación.
- Proceso de Búsqueda de Anomalías.
- Proceso de Monitoreo de taxis.

3.4.1 Proceso de Autentificación

Aplicación Principal – Autentificacion

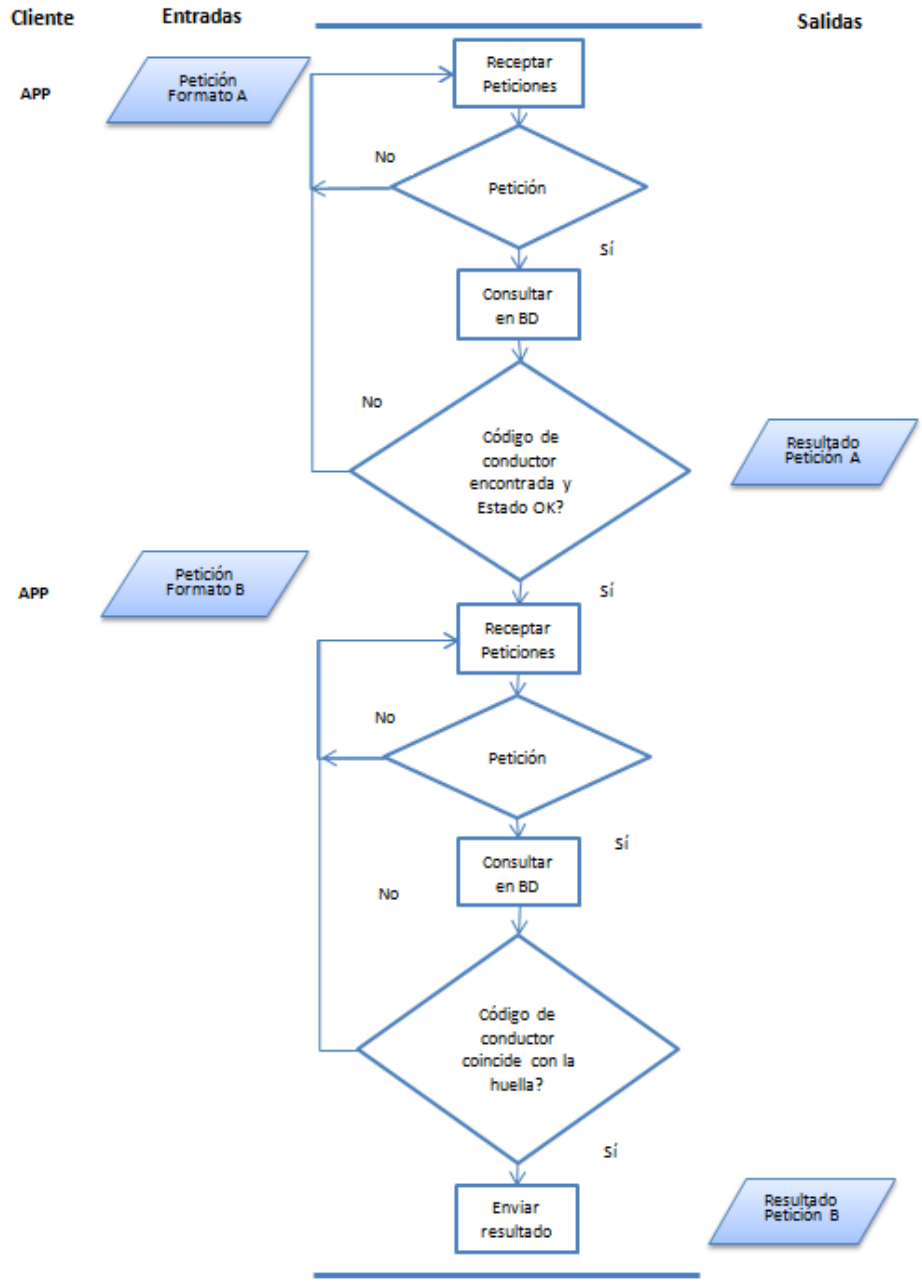

Figura 13 Proceso de autentificación – Aplicación Principal

Vehículo - Autentitificacion

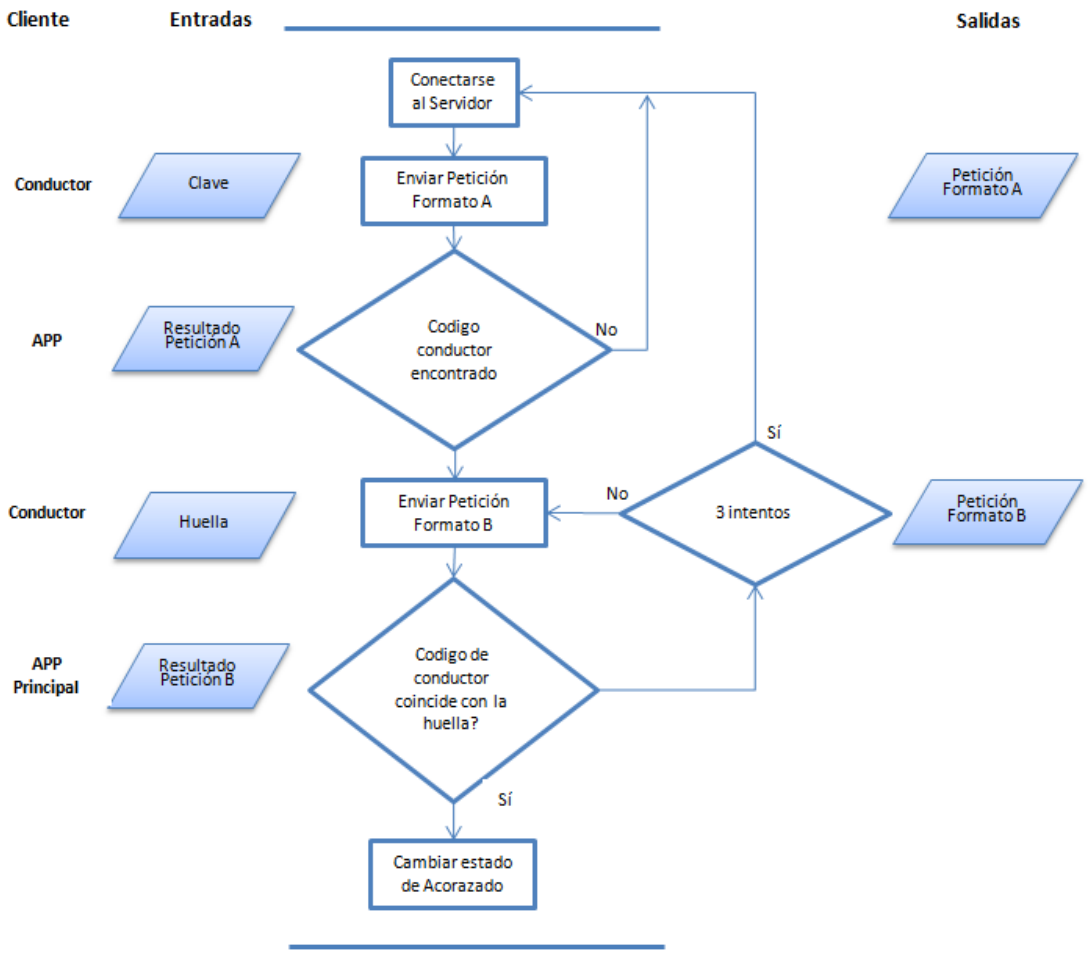

Figura 14 Proceso de Autentificación – Aplicación de Vehículos

3.4.2 Proceso de Búsqueda de Anomalías

Este proceso es el que se debe seguir para indicar el estado del conductor y vehículo por parte de la entidad reguladora.

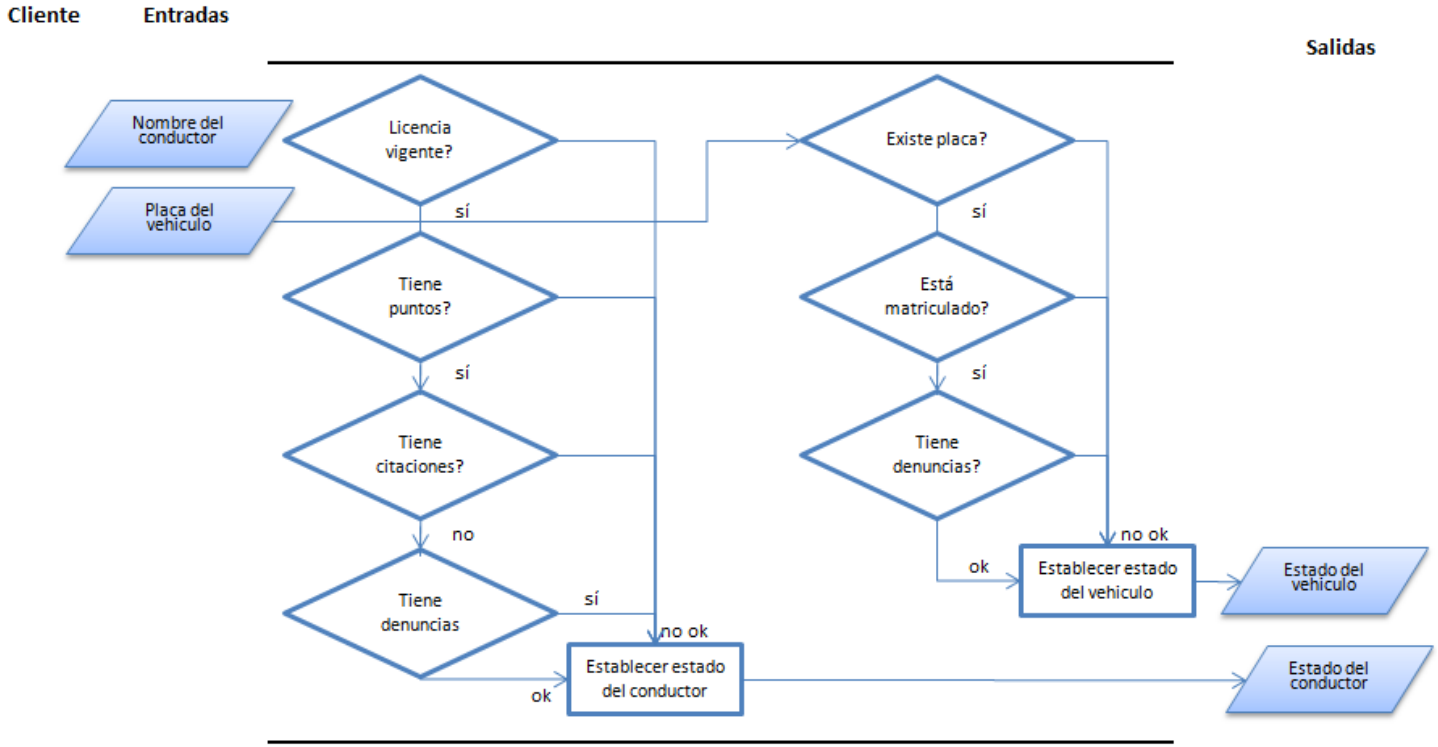

Figura 15 Proceso de búsqueda de anomalías

3.4.3 Proceso de Monitoreo de taxis

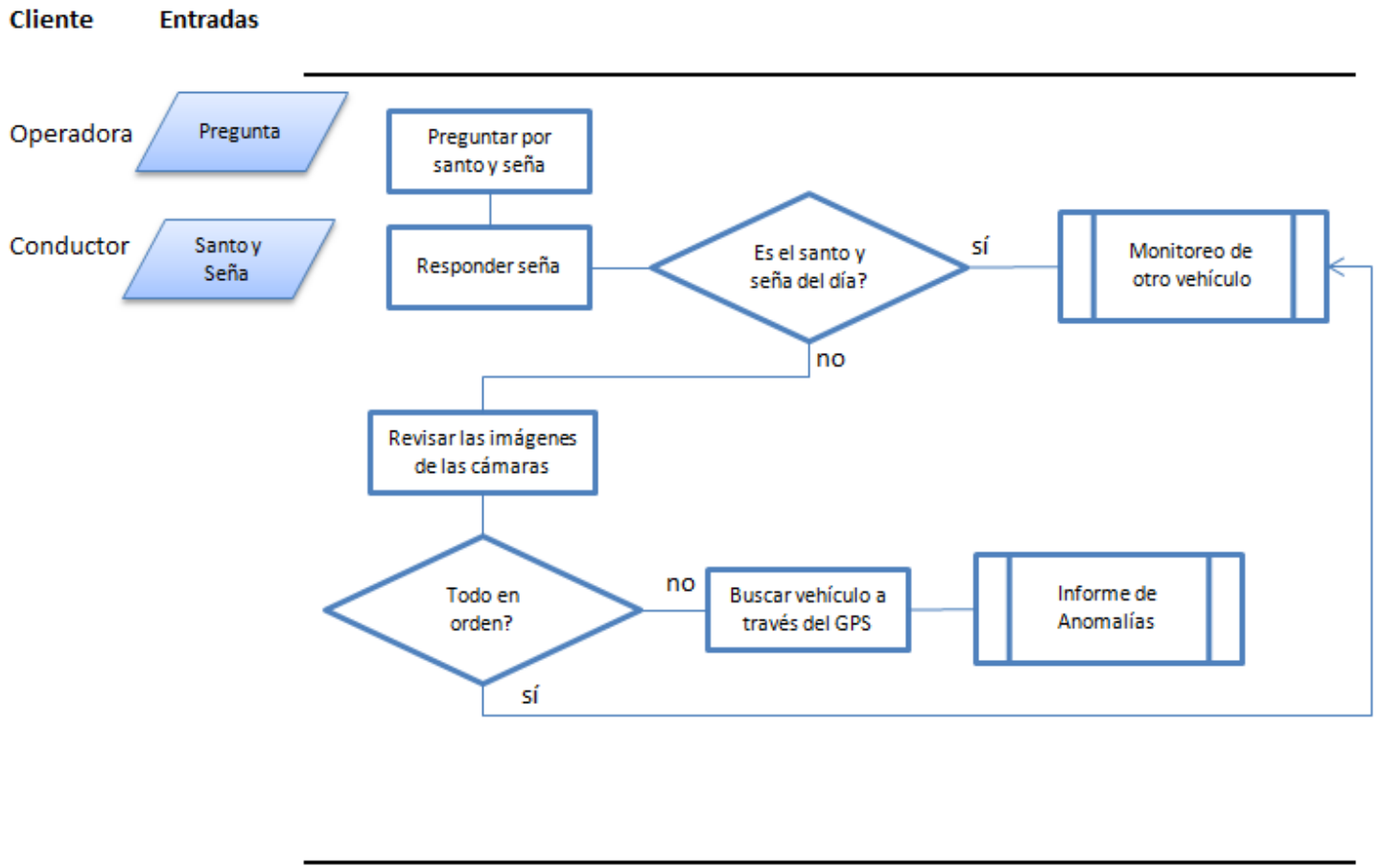

Figura 16 Proceso de monitoreo de Taxis

3.5 Interfaces, protocolos y PDUs

3.5.1 Interfaz entre el Bloque Lector de huellas y el Bloque de Aplicación

La interfaz utilizada es usb.

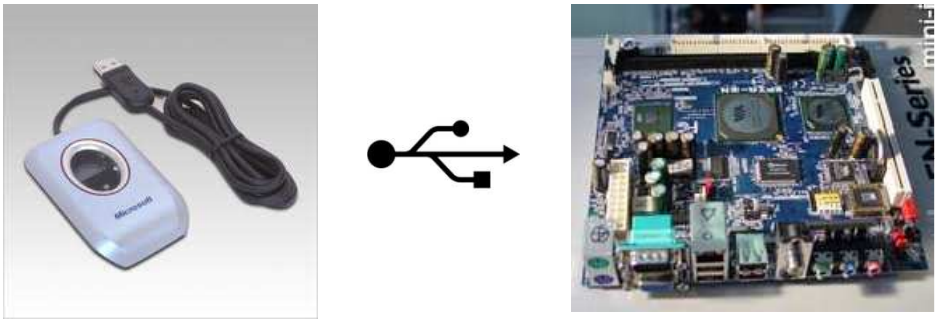

Figura 17 Interfaz del lector de Huellas

3.5.2 Interfaz entre el Bloque de Ingreso de clave y el Bloque de Aplicación

La interfaz utilizada es usb.

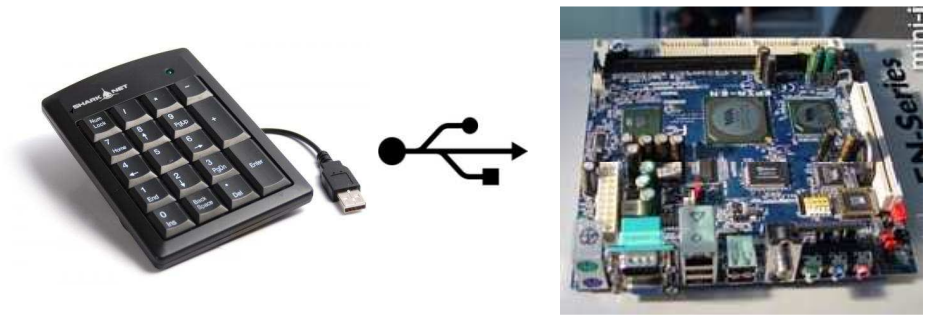

Figura 18 Interfaz del Teclado numérico

3.5.3 Interfaz entre el Bloque GPS y el Bloque de Aplicación

La interfaz utilizada es usb.

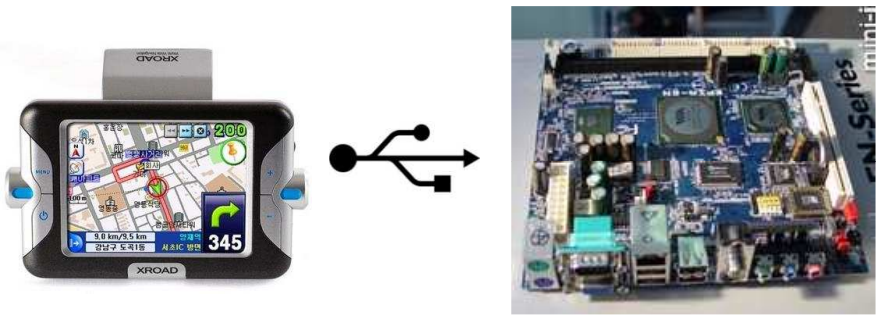

Figura 19 Interfaz del dispositivo GPS

3.5.4 Interfaz entre el Bloque Adquisición de Imágenes y el Bloque de Aplicación

La interfaz utilizada es TCP/IP.

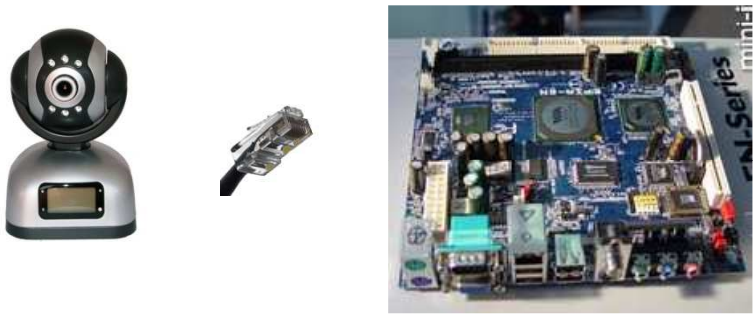

Figura 20 Interfaz de la camara

3.5.5 Interfaz entre el Bloque Acorazado y el Bloque de Aplicación

La interfaz utilizada es TCP/IP.

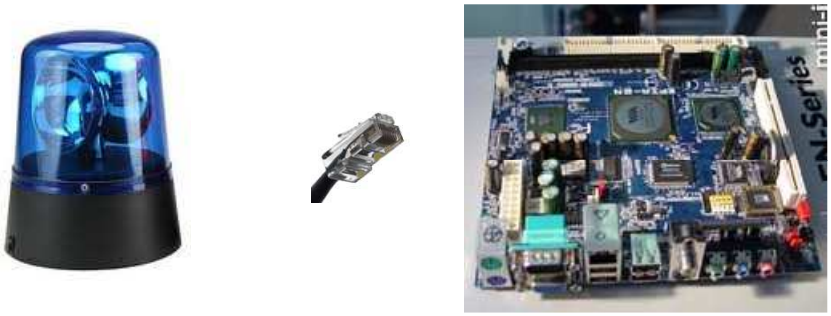

Figura 21 Interfaz del dispositivo acorazado

3.6 Acuerdos con entidades reguladoras

Para un adecuado funcionamiento del sistema de autentificación que estamos presentando es necesario realizar acuerdos con entidades reguladoras para poder disponer de la siguiente información de los conductores y los vehículos:

Anomalías de los conductores

- Licencia no vigente
- Falta de puntos
- Citaciones por situaciones graves en su contra.
- Denuncias penales graves, tales como robos, secuestros, asesinatos, estafas.

Anomalías de los vehículos

- Placa no existe
- No se encuentra matriculado
- Tiene denuncias en su contra

También es necesario que:

- Todas los vehículos pertenezcan a una cooperativa.
- Las cooperativas de taxi cumplan con el procedimiento de monitoreo descrito a continuación:

  El procedimiento de monitoreo que se propone requiere de la utilización de una medida de seguridad comúnmente conocido como santo y seña de la cual la cooperativa será responsable de darla a conocer a los conductores así como el cambio de la misma diariamente.

  La cooperativa debe verificar el estado del conductor, para lo cual deberá establecer comunicación con el mismo cada 15 minutos; el conductor deberá citar el santo y seña del día; la operadora observará las imágenes capturadas por la cámara que se encuentra en el vehículo y comprobará que todo esté en orden.

  En caso de que el santo y seña no sea el correcto o que la operadora observe alguna anomalía, se procederá a avisar a la

comisión de tránsito para que realice la tarea de búsqueda del vehículo.

3.7 Escenarios

El sistema propuesto contempla los siguientes escenarios:

3.7.1 Escenario 1 – Ideal

El usuario y el conductor son personas comunes sin ninguna mala intención con el fin de recibir y prestar servicio respectivamente

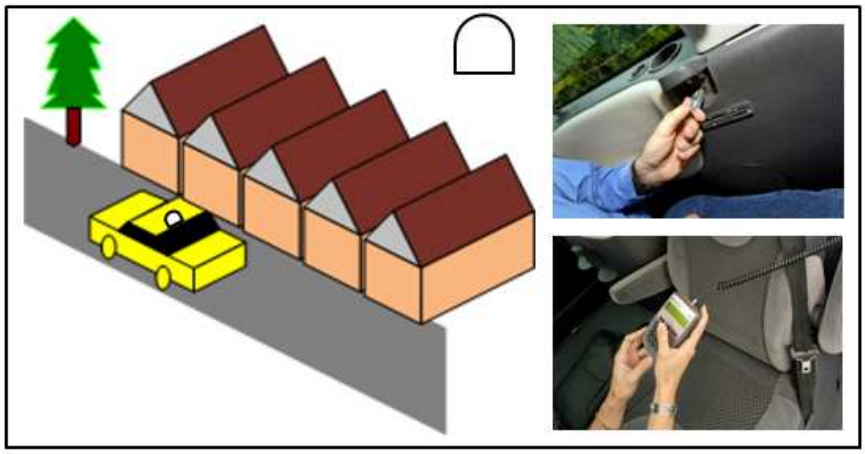

Figura 22 Escenario 1 - inicio

1. El conductor ingresa su huella digital y su código

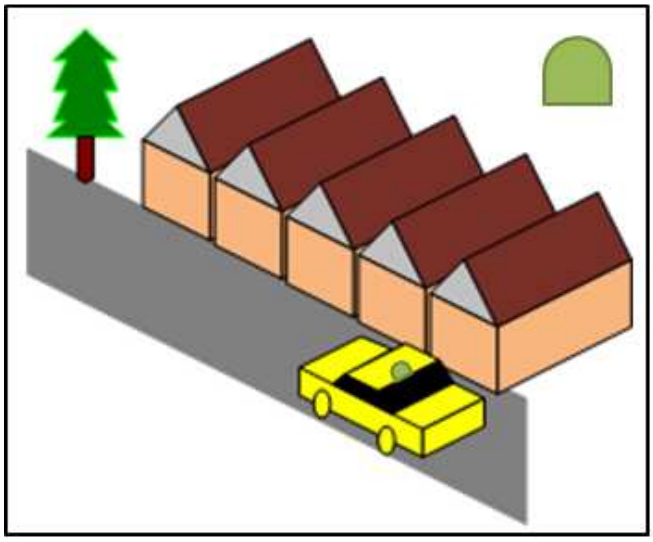

Figura 23 Escenario 1 - recorrido

1. Huella digital y código son correctos.
2. Conductor no tiene problemas con la CTG y el vehículo está en condiciones de ser operado; acorazado se enciende en color verde.

Figura 24 Escenario 1 – verificación de anomalías

3. Operador(a) de la cooperativa pregunta por el santo y seña; el conductor responde correctamente; la operadora revisa las imágenes enviadas por la cámara que se encuentra en el vehículo y observa que todo está en orden.

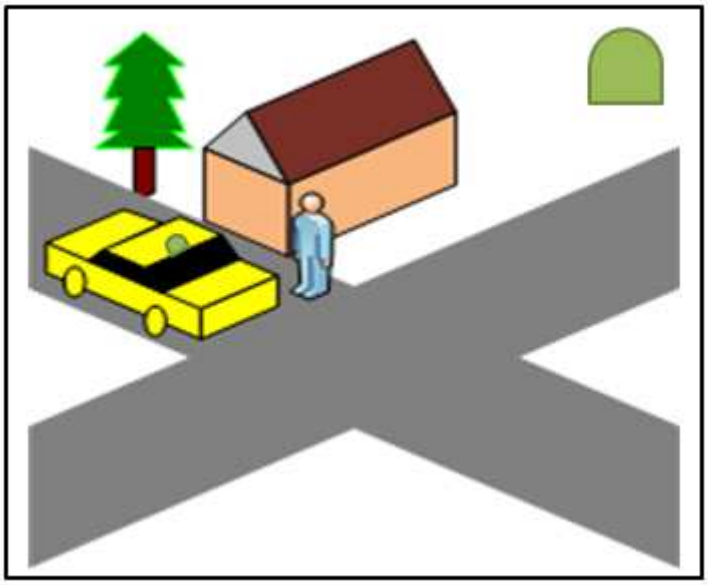

Figura 25 Escenario 1 – Indicador acorazado en verde

4. Al estar el acorazado en verde, una persona se sube al taxi.

3.7.2 Escenario 2 – Robo del vehículo

El vehículo es intersecado por un segundo vehículo obligando al conductor a abandonar el mismo.

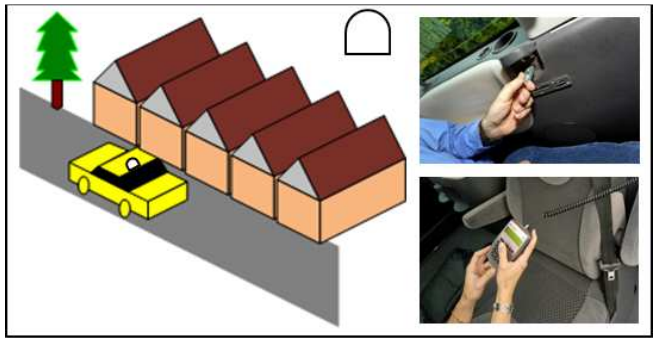

Figura 26 Escenario 2 - inicio

1. El conductor ingresa su huella digital y su código.

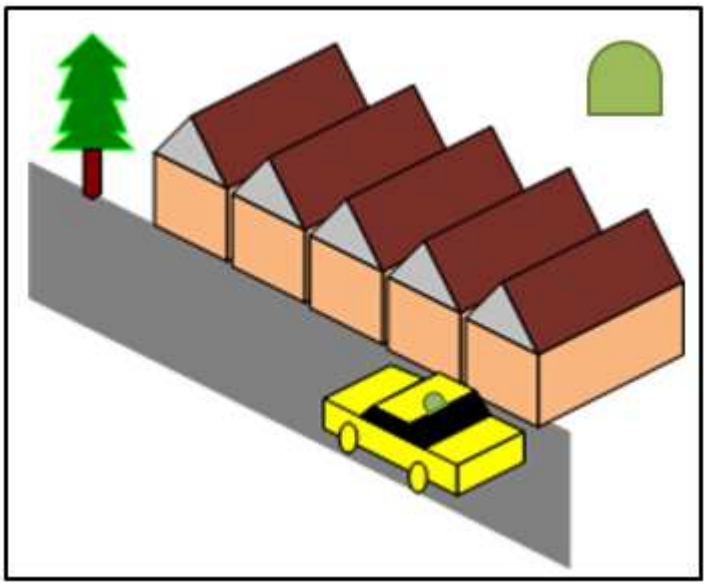

Figura 27 Escenario 2 - recorrido

2. Código y huella digital son correctas.

3. Conductor no tiene problemas con la CTG y el vehículo está en condiciones de ser operado; acorazado se enciende en color verde.

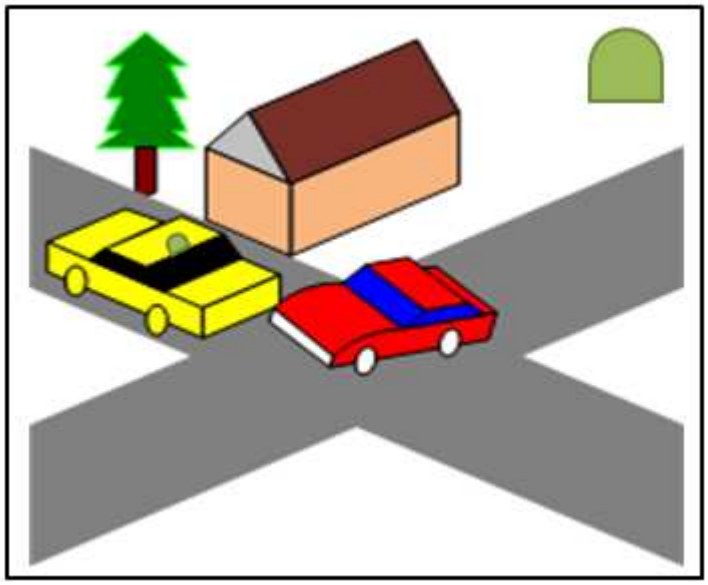

Figura 28 Escenario 2 – vehículo interceptado

4. El vehículo es interceptado.

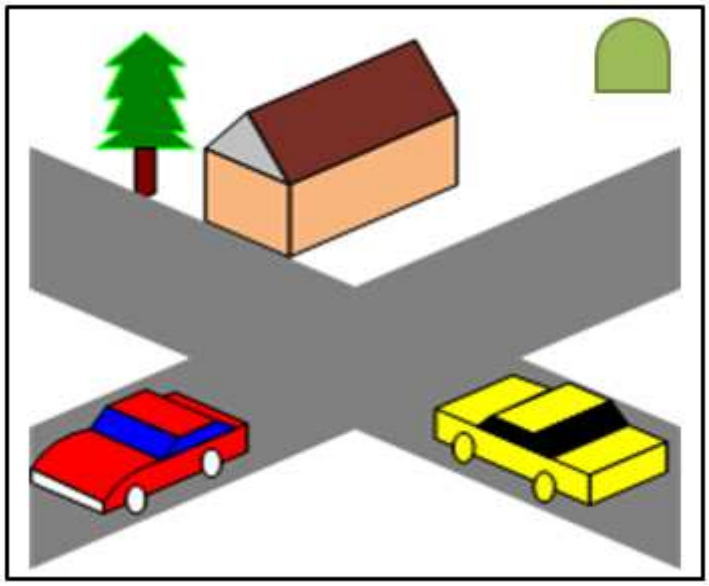

Figura 29 Escenario 2 – vehículo robado

5. El conductor es obligado a salir del vehículo.

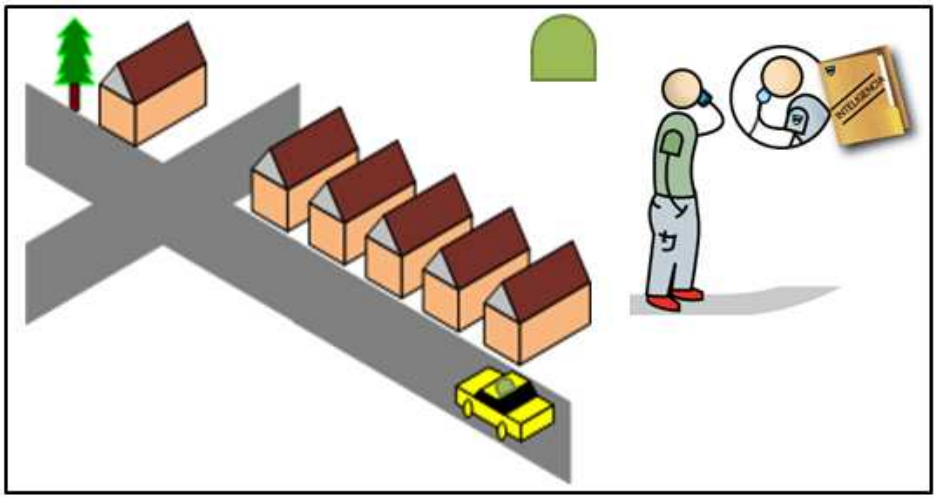

Figura 30 Escenario 2 – denuncia de robo

6. El delincuente se lleva el vehículo con el acorazado en luz verde.
7. El conductor se comunica por teléfono a la cooperativa.

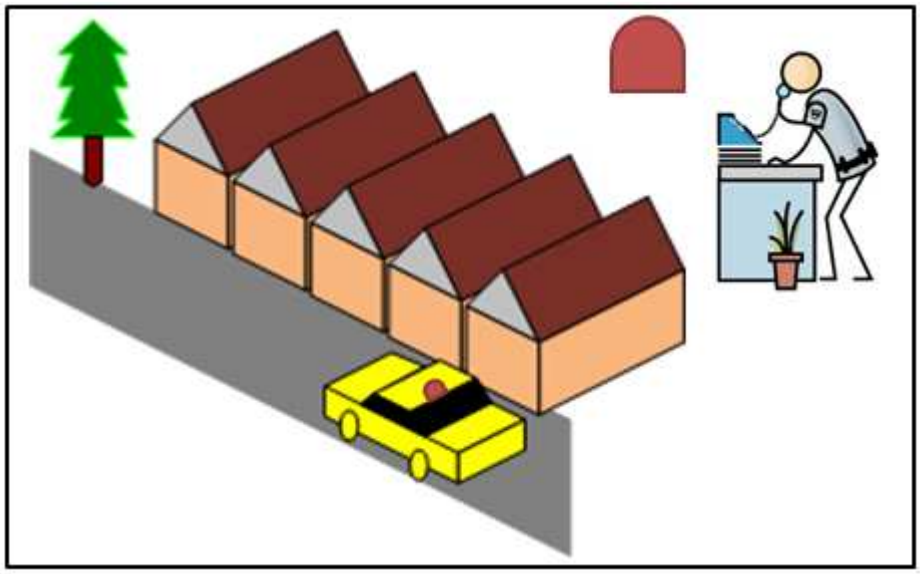

Figura 31 Escenario 2 – indicador acorazado en rojo

8. En la cooperativa cambian el estado del acorazado a rojo y comienzan a rastrear al vehículo.

3.7.3 Escenario 3 – Pasajero asaltante

El usuario aborda el taxi con la finalidad de asaltar al conductor del vehículo haciéndose pasar por un pasajero común.

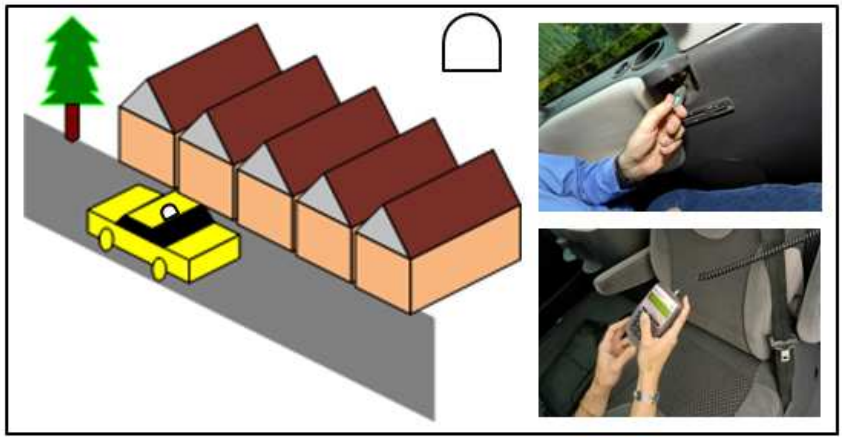

Figura 32 Escenario 3 - inicio

1. El conductor ingresa su huella digital y su código.

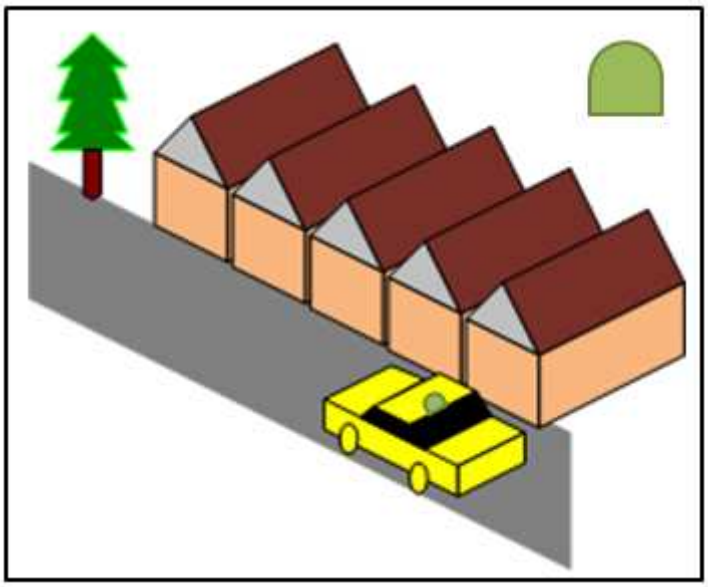

Figura 33 Escenario 3 - recorrido

2. Código y huella digital son correctas.

3. Conductor no tiene problemas con la CTG y el vehículo está en condiciones de ser operado; acorazado se enciende en color verde.

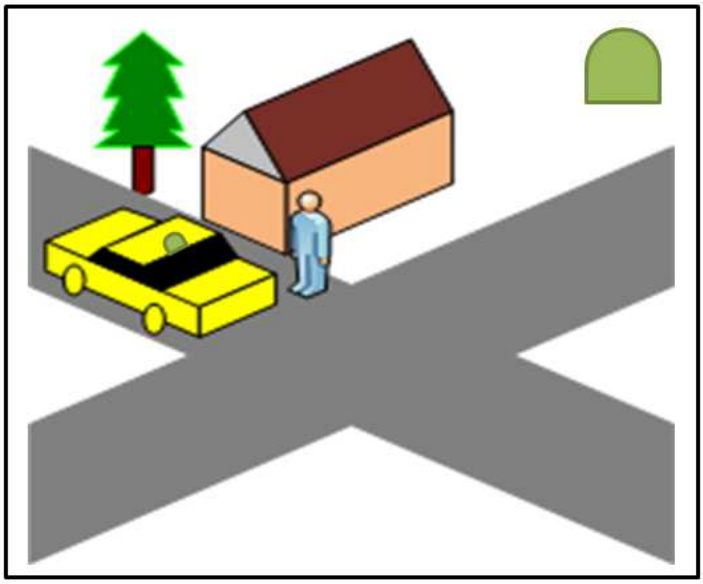

Figura 34 Escenario 3 – indicador acorazado en verde

4. Una persona se sube al vehículo.

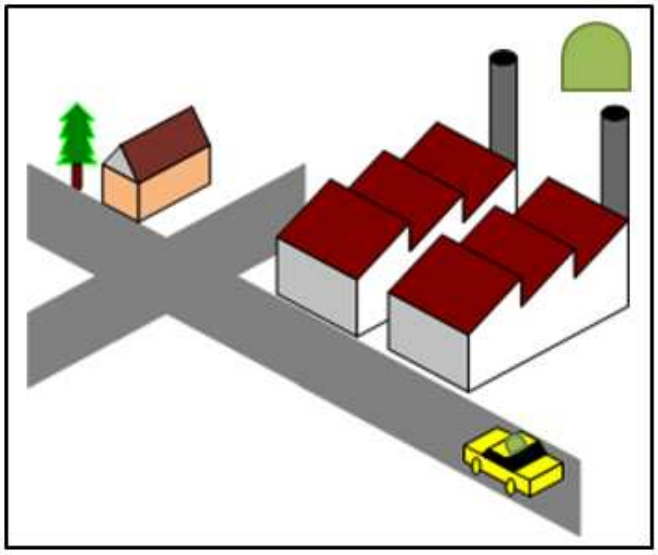

Figura 35 Escenario 3 – conductor secuestrado

5. El pasajero amenaza al conductor con un arma y le pide que lo lleve a un lugar para robarle.

Figura 36 Escenario 3 – verificación anomalías

6. Operador(a) de la cooperativa, pregunta por el santo y seña; el chofer responde correctamente; el(la) operador(a) revisa las imágenes enviadas por la cámara que se encuentra en el vehículo y se da percata de la irregularidad.
7. El (la) operadora llama a la comisión de tránsito para que comience el rastreo del vehículo.

3.7.4 Escenario 4 – Alteración del acorazado

El acorazado es alterado con el fin de reportación información incorrecta y así engañar a otras personas.

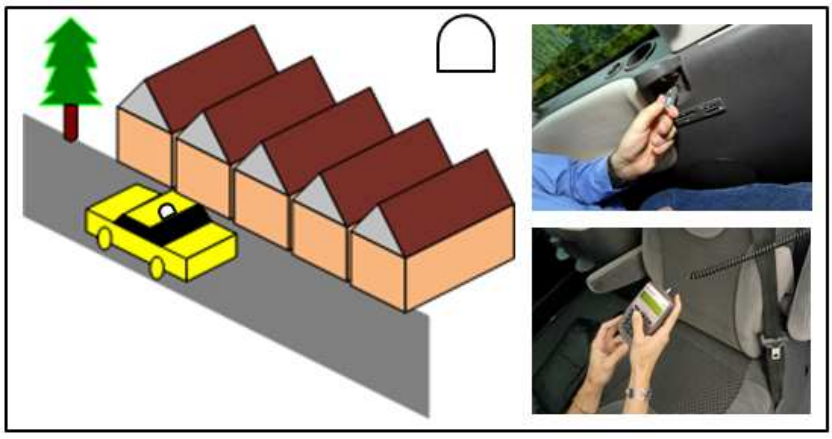

Figura 37 Escenario 4 - inicio

1. El acorazado es violentado con el fin de mostrar siempre luz verde.

2. El conductor ingresa su huella digital y su código.
3. Código y huella digital son correctas.

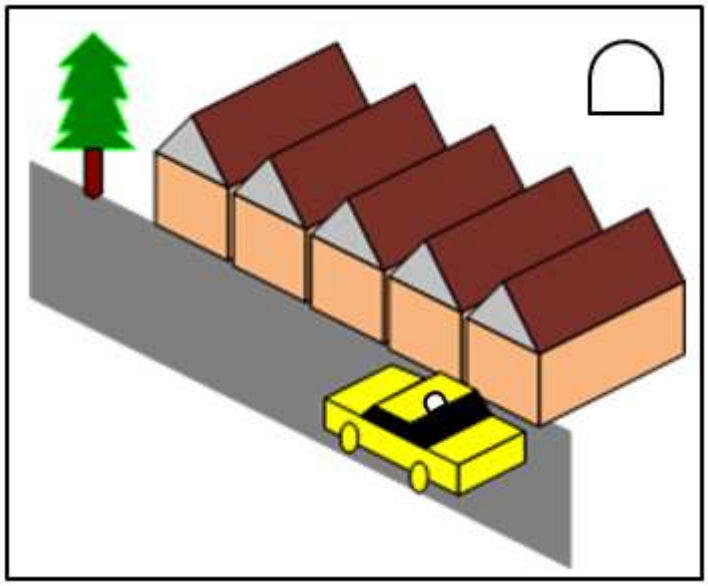

Figura 38 Escenario 4 – acorazado violentado

4. Independientemente de si el conductor tiene o no problemas con la CTG o si el vehículo está o no está en condiciones para ser operado; el acorazado no enciende.

Capítulo 4

4. Puesta en marcha

4.1 Consideraciones técnicas

Para un buen funcionamiento del sistema propuesto es necesario prestar atención las siguientes consideraciones técnicas:

4.1.1 Mini CPU

El mini CPU ubicado en el vehículo, debe tener instalado una versión light de Linux (sin interfaz gráfica), el mismo debe ser capaz de ejecutar java y el Fingerprint SDK Java 2009. Para las comunicaciones a través del internet se utilizará un modem de internet móvil, el cual es distribuido por las compañías de telefonía móvil local. El criterio para elegir el proveedor de dicho dispositivo será aquel que ofrezca una mayor cobertura en las zonas donde los vehículos circulen con mayor frecuencia. Para el monitoreo del interior del vehículo existirá una cámara IP con la cual el operario de la aplicación ubicada en la cooperativa podrá capturar imágenes cuando la situación lo amerite. Se utilizarán una interfaz Ethernet y un puerto DB9 para el monitoreo y comunicación respectivamente con el acorazado.

Por medio del acorazado a los pasajeros se les mostrarán alarmas visuales (luces de distintos colores) que indicaran estado actual del vehículo.

Teclado numérico (Numpad) para que el conductor pueda identificarse por medio de un código de cuatro dígitos que junto con la placa del vehículo y la huella conforman la identificación del conductor.

Lector de huellas digitales, dispositivo biométrico con el cual se puede asegurar que los datos del conductor están registrado en el sistema y él es quien dice ser.

GPS, dispositivo con el cual se podrá conocer la ubicación exacta del vehículo en un momento dado y utilizando la comunicación GPRS se podrá reportar la ubicación de dicho vehículo bajo la petición que realice el operador de la aplicación ubicada en la cooperativa.

Todas las comunicaciones entrantes o salientes ya sea con el servidor de Datos o con la cooperativa, serán encriptados utilizando el protocolo SSL. Las comunicaciones con el Servidor de Datos y la cooperativa utilizarán puertos distintos predefinidos previamente.

El teclado numérico, la cámara y modem GSM se comunicarán por puertos USB cada uno al mini CPU.

La interfaz Ethernet (conector RJ45) se utilizará para monitorear constantemente la comunicación entre el mini CPU y el acorazado y de existir alguna anomalía la reportarán al servidor de datos por medio del modem GPRS.

4.1.2 Servidor de Aplicaciones

El servidor de Aplicaciones contendrá una versión estable y segura de Linux, deberá soportar Java, y estará apto para manejar comunicaciones en paralelo.

Todas las comunicaciones entrantes o salientes con los vehículos serán encriptados utilizando el protocolo SSL.

Este servidor debe estar en la capacidad de recibir un número de conexiones en paralelo equivalente al número total de vehículos registrado de la aplicación.

Para facilitar la implementación el protocolo SSL utilizara el puerto 9000 y utilizara tramas UDP para manejar velocidades de transmisión de datos aceptables.

4.1.3 Dispositivo Indicador Acorazado

El dispositivo indicador acorazado, en nuestro prototipo del sistema, tiene las siguientes características:

- El circuito del dispositivo es simulado, utilizando las herramientas, tales como: proteus, para simular los

circuitos integrados, VMWare para la maquina virtual quien se comunica con el computador principal, virtual Serial Port Driver, para simular puertos virtuales ya que físicamente dichos puertos no existen en el computador.

- Debe mantener un alto grado de seguridad, por lo tanto, tiene una conexión, que permanece monitoreada constantemente, y en el momento en que se pierde la conexión, se envía un mensaje a la cooperativa a la que pertenece dicho vehículo.
- El mini-cpu se comunica con un integrado PIC16F877A, quien a través del puerto serial, recibe las órdenes para poder procesar la información hacia los indicadores LED.

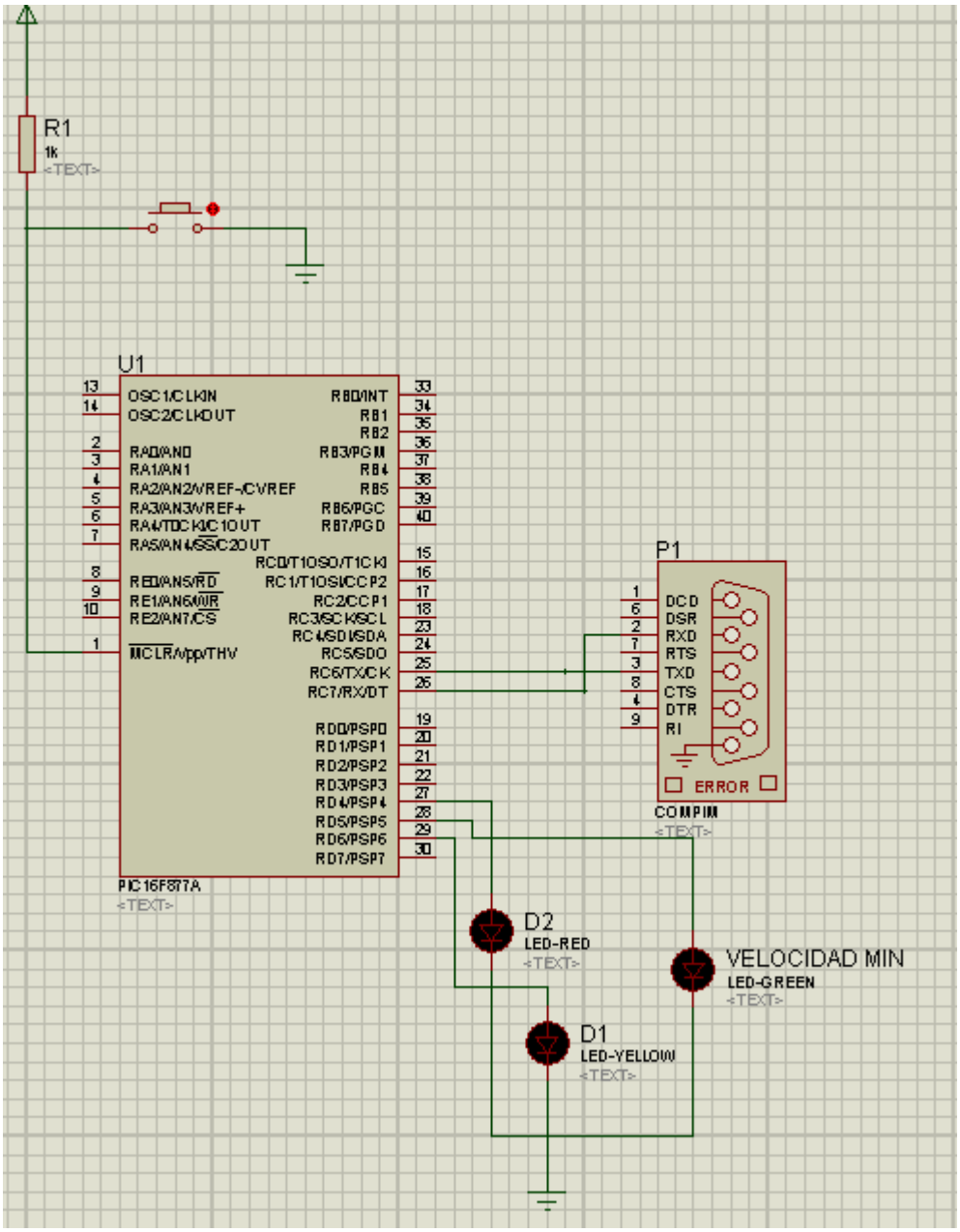

Figura 39 Simulación del circuito electrónico del Acorazado

4.2 Prototipo

Debido a la falta de recursos económicos y operativos el prototipo planteado difiere en cierta cantidad con respecto a la solución planteada los cual es analizado en los siguientes puntos.

4.2.1 Arquitectura

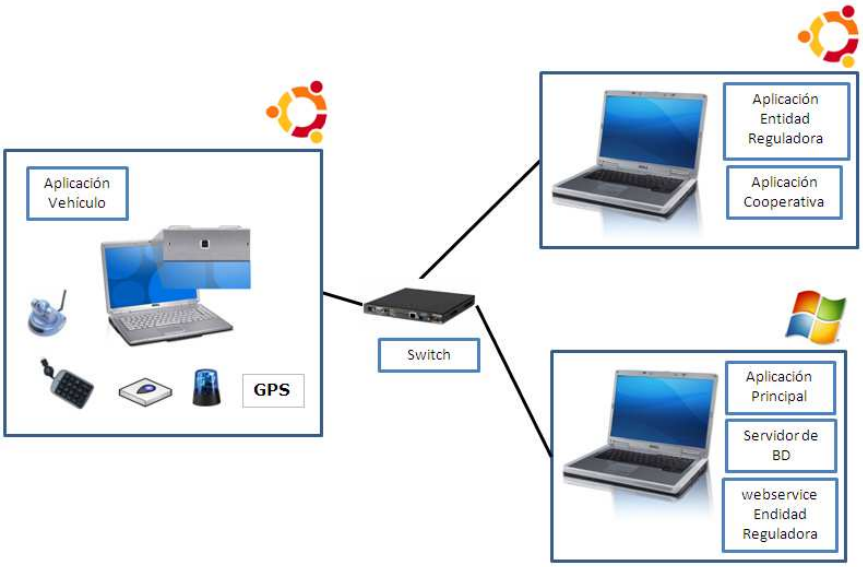

Figura 40 Arquitectura del Prototipo

A diferencia del sistema planteado, la red sobre la que trabaja el prototipo es una red Ethernet virtual.

Las aplicaciones están distribuidas en varios computadores como muestra la Imagen 19, pero distribuidas entre computadores y la máquina virtual.

La aplicación del vehículo se encuentra en una computador y el acorazado en una maquina virtual que se ejecuta en el mismo computador.

La aplicación principal, Servidor de base de datos y el web service de la entidad reguladora se encuentran en un mismo computador y la aplicación de entidad reguladora junto con la aplicación cooperativa están en una maquina virtual dentro del mismo computador antes mencionado.

4.3 Análisis de tráfico de datos

Para ejecutar el sistema propuesto, es necesario realizar un análisis de la cantidad de datos que serán transmitidos por la red GPRS con la finalidad de establecer el ancho de banda que se requiere, así como el contrato paquete datos que deberá adquirir la cooperativa a la compañía de telefonía móvil con el fin de evitar latencia en la red.

En el anexo A se encuentra los detalles del análisis de factibilidad del tráfico de datos.

4.4 Prototipo vs. Puesta en Marcha

Prototipo	**Caso Real**
La aplicación no controla el encendido del vehículo	El conductor no podrá encender el vehículo, si es que no pone su huella digital, y se valida que es la persona que debería estar conduciendo dicho vehículo.
Para la comunicación entre las distintas aplicaciones se utilizará una red LAN local	Para la comunicación del vehículo se utilizara la red de datos de las operadoras de telefonía móvil. El resto de aplicaciones (cooperativa, servidores y entidad reguladora) se comunicarán utilizando el proveedor de servicio más conveniente
El acorazado será simulado utilizando una máquina virtual y un simulador de circuitos electrónicos.	Se elaborará el dispositivo en base a circuitos integrados.
El servicio web que debe proporcionar la entidad reguladora se encuentra de	El servicio web debe ser implementado por la entidad reguladora.

forma local en una PC	
La información proporcionada por el webservice va a provenir de una base de datos de prueba	La información proporcionada por el webservice de la entidad reguladora mostrara información actualizada a la fecha
La aplicación utiliza la cámara integrada en la PC de prueba.	La aplicación utiliza una cámara IP, para monitorear la conexión
La seguridad física no será controlada ya que el acorazado solo es simulado	El acorazado posee una alta seguridad física.

Tabla 2 Consideraciones y Limitantes

Consideraciones:

El manejo de la energía eléctrica es crítico dentro de nuestro sistema, por lo que se recomienda, implementar la aplicación en lenguaje C, debido a que se administran mejor las peticiones enviadas al CPU, y con esto el consumo eléctrico va a ser menor.

Para consumir un menor ancho de banda, dentro de la aplicación, las imágenes que se envíen a través de la red, pueden ser comprimidas; considerando el riesgo de perder calidad en dichas imágenes.

CONCLUSIONES

1. El análisis de las operaciones del sistema de transporte público mostró que existe mucha inseguridad debido a que las medidas para contrarrestar los riesgos son aisladas unas de otras, por lo cual concluimos que para lograr el objetivo de disminuir la inseguridad, el sistema propuesto debe ser colaborativo entre cada uno de los siguientes: entidad reguladora, cooperativas de vehículos, conductores y usuarios.

2. Se analizó y se concluyó que la red GPRS es la mejor opción de comunicación para el sistema, debido a la madurez de esta tecnología, se aprovechará la cobertura de la red y se evita realizar gastos adicionales para efectos de comunicación.

3. Un análisis del medio mostró que para que el sistema tenga éxito el mismo debe ser de bajo costo y fácil uso

4. Se utilizó un lector de huellas como dispositivo biométrico debido a su facilidad de uso y a su bajo costo.

5. La transmisión de información crítica a través de la red dio lugar a que se utilizará el protocolo SSL como mecanismo para protegerla.

6. La creación de procedimientos tanto para las cooperativas como para las entidades reguladoras ayudará a que se fomente una cultura de orden y colaboración conjunta.

RECOMENDACIONES

1. Dentro de la aplicación se debería manejar el caso en el que la batería del vehículo se desconecte, escenario en el cual se debería guardar la última ubicación de dicho vehículo y almacenarlo dentro del LOG de eventos del sistema.

2. Se recomienda que el sistema sea financiado y auspiciado por una entidad reguladora.

3. Se recomienda que se actualicen los datos de las cooperativas en la Unión de cooperativas de Taxis del Guayas, debido a que durante la elaboración de la presente tesis se encontró que existen datos de cooperativas que tienen hasta 4 años sin ser actualizados.

4. Se recomienda que los usuarios de los vehículos soliciten a los conductores la autentificación al momento de subirse en una unidad.

5. Se recomienda que haya un mayor control a las cooperativas de taxis con el fin de garantizar que se cumplan los procedimientos propuestos en la tesis.

6. Se recomienda que la entidad responsable del sistema llegue a un acuerdo con las operadoras de telefonía celular con la finalidad contratar planes adecuados para las cooperativas, que se ajusten a las necesidades de las mismas.

ANEXO A

Análisis de la cantidad de información transmitida por vehículo mensualmente

Detalle de del tamaño en KB de las tramas que son enviadas y recibidas por el vehículo

Autentificacion

Detalle del tamaño de las tramas								Total	
								Bytes	KB
	Petición formato A								
Nombre del campo	C	:	CODIGO CONDUCTOR	:	ID COOPERATIVA	:	PLACA	26	0,025
Tamaño en bytes	1	1	4	1	10	1	8		
	Resultado formato A								
Nombre del campo	RC	:	STVEHICULO	:	STCONDUCTOR			8	0,008
Tamaño en bytes	2	1	2	1	2				
	Petición formato B								
Nombre del campo	RH	:	HUELLA					603	0,589
Tamaño en bytes	2	1	600						
	Resultado formato B								
Nombre del campo	RH	:	S|N					4	0,004
Tamaño en bytes	2	1	1						
							Total Autentificacion	0,626	KB

Tabla 3Detalle del tamaño de trama de Autentificación

Peticion Foto

Detalle del tamaño de las tramas				Total	
				Bytes	KB
	Peticion de Foto a vehículo				
Nombre del campo	F	:		2	0,002
Tamaño en bytes	1	1			
	Respuesta de peticion de Foto por parte del vehiculo				
Nombre del campo	Foto			0	50
Tamaño en bytes	51200				
			Total P. Foto	50,002	KB

Tabla 4 Detalle del tamaño de trama de Petición de una foto

Detalle del tamaño de las tramas							Total	
							Bytes	KB
Peticion Ubicación								
Peticion de Ubicación	Peticion de Ubicación a vehículo							
Nombre del campo	P	:					2	0,002
Tamaño en bytes	1	1						
	Respuesta Peticion de Huvicacion a vehículo							
Nombre del campo	RP	:	LATITUD	:	LONGITUD		20	0,020
Tamaño en bytes	2	1	8	1	8			
						Total P. Ubicación		0,021 KB

Tabla 5 Detalle del tamaño de trama de Petición de ubicación

Estimación de KB consumidos mensualmente por un vehículo en un mes.

Accion	KB por accion	# acciones diarias por vehiculo	KB dirario por acción de vehiculo
Autentificacion	0,626	3	1,878
Peticion de Foto	50,002	40	2000,078
Peticion de ubicación	0,021	40	0,859

Total de Kb diario por vehiculo	2002,815	1,956 MB
Consumo mensual por vehiculo	60084,463 KB	58,676 MB

Tabla 6 Consumo de KB diario por vehículo

En la tabla 6 se realiza una estimación de los KB consumidos por un vehículo. El número de acciones de las peticiones de Foto y ubicación se planteo asumiendo que el operador de cada cooperativa realiza una verificación de cada taxi cada 15 minutos frecuencia con la que se realiza la verificación por radio actualmente en la mayoría de cooperativas de taxis.

En base a los cálculos cada vehículo requiere aproximadamente 60 MB mensuales los cual es aceptable ya que a la fecha las operadoras ofrecen

paquetes de 2000 MB para internet móvil y 5000 MB para teléfonos inteligentes.

ANEXO B

Costo del prototipo

El costo del prototipo propuesto es el siguiente:

Componentes	Estimación 1		Estimación 2	
	Marca	**Precio**	**Marca**	**Precio**
Lector de huellas	Microsoft Finger Print	35	Digital Person	99
GPS	ND 100S GPS DONDLE	35	GR-213-USB:Holux USB Mouse GPS	49.95
Teclado Numérico	Targus PAUK10U Ultra Mini USB Keypad	9.14	New USB Numeric KeyPad Number Keyboard	7.55
Módem USB	Modem Internet Huawei Claro MODELO E173 - USB STICK	70	Internet Movil Modem Zte Movistar	70
Cámara IP	Camara Web Genius Islim 300x	10	Camara Web Genius Eye 312	15
Acorazado		22.39		22.53
Mini CPU		280		284
Total	$	**461.53**	$	**490.53**

Tanto el acorazado como el Mini CPU, no existen en el mercado; por dicho motivo hemos realizado un estimado de su costo, teniendo en cuenta el costo de sus componentes.

Algunos de los componentes solo se los pueden adquirir fuera del territorio ecuatoriano.

- Acorazado

Componentes	Estimación 1		Estimación 2	
	Marca	**Precio**	**Marca**	**Precio**
Microcontrolador	PIC16F877	4.41	PIC16F876	4.53
3 leds	Led 10mm	0.98	Led 10mm	1
Puerto DB9 Macho		0.5		0.5
Puerto RJ45		0.5		0.5
Bus		1		1
Placa		5		5
Estructura externa		10		10
Total	$	22.3898	$	22.53

- Mini CPU

Componentes	Estimación 1		Estimación 2	
	Marca	**Precio**	**Marca**	**Precio**
Memoria Ram	512Mb	25	1Gb	29
Disco duro	20Gb	20	20Gb	20
Mainboard	Quanmax Industrial KEEX-2030 Atom 3.5"	235	Quanmax Industrial KEEX-2030 Atom 3.5"	235
Total	$	280	$	284

BIBLIOGRAFÍA

[1] Gloria Navas Jiménez, Una nueva tecnología hará más seguras las ciudades, http://www.tendencias21.net/Una-nueva-tecnologia-hara-mas-seguras-las-ciudades_a4660.html, Ultima actualización 12 de Julio del 2010.

[2] Voice your View, Proyecto Voice your View, http://www.voiceyourview.com/site/content_about.php, Ultima actualización 06 de Mayo del 2011.

[3] Futuro Móvil, Aplicación antisecuestro para Smartphone, http://futuromovil.com/?p=292, Ultima actualización 18 de Agosto del 2010.

[4] Código Venezuela, Motorola y la Seguridad Pública, http://www.codigovenezuela.com/2010/05/negocio/empresas-negocio/motorola-y-la-seguridad-publica, Ultima actualización 20 de Mayo del 2010.

[5] Canal Tecnológico, Soluciones Motorola para optimizar la seguridad de las ciudades, http://www.canal-tecnologico.com/index.php?option=com_content&task=view&id=191&Itemid=12, Ultima actualización 29 de Junio del 2010.

[6] Juan Carlos Díaz M - Corresponsal EL TIEMPO, Presentan chip inteligente que permite monitoreo de los vehículos a control remoto, http://identicocolombia.blogspot.com/2010_07_01_archive.html, última actualización 26 de Julio del 2010.

[7] Wikipedia, Sistema de posicionamiento Global, http://es.wikipedia.org/wiki/Sistema_de_posicionamiento_global, Última actualización 27 de Mayo del 2011.

[8] Griaule Biometrics, Java SDK para Lector de Huellas de Microsoft, http://www.griaulebiometrics.com/page/en-us/downloads, Última actualización Julio del 2009.

[9] Usuario Blassoto – Proyectos Google, Biblioteca para desplegar mapas de Google Maps desde Java – Jposition, http://code.google.com/p/jposition/, Ultima actualización Junio del 2010.

[10] Keane Jarvi, Librería Java para manejo de Puerto Serial, http://rxtx.qbang.org/wiki/index.php/Main_Page. Ultima actualización 21 de Marzo del 2011.

[11] Olivier LE DIOURIS, Librería Java para manejo del protocolo NMEA, http://sourceforge.net/projects/javanmea/. Ultima actualización 17 de Julio del 2009.

[12] Usuario gilles.gigan – Proyectos Google, Proyecto v4l4j para manejo de Cámaras de video para Java, http://code.google.com/p/v4l4j/, Ultima actualización 26 de Marzo del 2011

[13] Noticias de la tecnología de la información (IT News), Implementación del protocolo SSL en Java, http://www.itnews.ec/marco/000024.aspx, Ultima actualización 10 de Mayo del 2011.

[14] EcuRed, Que es GRPS, http://www.ecured.cu/index.php/GPRS, Última actualización Mayo del 2011.

[15] Wikipedia, HSDPA, http://en.wikipedia.org/wiki/High-speed_Downlink_Packet_Access. Ultima actualización 7 de Mayo del 2011.