compAs
Grupo de capacitación e investigación pedagógica

El uso de las técnicas de la información y comunicación y su incidencia en el control de acceso vehicular a la UTEQ

Ángel Iván Torres Quijije
Byron Wladimir Oviedo Bayas

El uso de las técnicas de la información y comunicación y su incidencia en el control de acceso vehicular a la UTEQ

Ángel Iván Torres Quijije
Byron Wladimir Oviedo Bayas

El uso de las técnicas de la información y comunicación y su incidencia en el control de acceso vehicular a la UTEQ

compÁs
Grupo de capacitación e investigación pedagógica

Título original: El uso de las técnicas de la información y comunicación y su incidencia en el control de acceso vehicular a la UTEQ

Primera edición: marzo 2020

Publicado por acuerdo con los autores.

Segundo Congreso Internacional de Sociedad y Tecnología de la información en la Educación Superior
Guayaquil-Ecuador

Editado en Guayaquil - Ecuador

ISBN: 978-9942-33-193-9

compÁs
Grupo de capacitación e investigación pedagógica

Cita.
A. Torres, B. Oviedo (2020). El uso de las técnicas de la información y comunicación y su incidencia en el control de acceso vehicular a la UTEQ, Editorial Grupo Compás, Universidad Técnica Estatal de Quevedo. Guayaquil Ecuador, 68 pag

PRÓLOGO

En el trabajo del autor propone la implantación de un mecanismo de autenticación utilizando radio frecuencia (RFID) para controlar el acceso de los vehículos al campus de la Universidad Técnica Estatal de Quevedo. En el mismo se analizan diferentes tecnologías de autenticación enfatizando en las ventajas y desventajas de cada una de ellas e identifica la tecnología RFID como más favorable tanto económica como técnicamente. Además el autor desarrolla una aplicación informática que complementa la autenticación, con la cual se registra la información necesaria para realizar el control de acceso al campus. El trabajo presenta una correcta escritura, los objetivos están acorde con la necesidad de dar solución al problema detectado para la investigación. Los resultados son analizados de manera correcta haciendo un análisis de los beneficios que serán obtenidos con la implementación de la tecnología. Por lo antes expuesto y la calidad del trabajo propongo sea tomado en cuenta para su inmediata implantación en la Universidad Técnica Estatal de Quevedo.

Ing. Msc. Freddy Iván Jaramillo Chuqui,

Capítulo 1

La Universidad Técnica Estatal de Quevedo (UTEQ), fue creada mediante Decreto Legislativo, publicado en el Registro Oficial # 674 del 1 de febrero de 1984, con las Escuelas de Ingeniería Forestal, Ingeniería Zootécnica, Ingeniería en Administración de Empresas Agropecuarias, que han venido cumpliendo un rol muy importante en el desarrollo agropecuario del País y muy especialmente en su zona de influencia.

La situación actual del país evolucionó, necesitando de la formación de nuevos profesionales, consecuente de este requerimiento la UTEQ, mediante resolución Novena del Honorable Consejo Universitario (HCU) del 13 de Septiembre de 1994, creó el Instituto de Tecnologías (IT), con las Escuelas de: Administración de Microempresas, Computación, Banca y Finanzas, y, Ventas, con las carreras de sus mismos nombres respectivamente.

En atención al crecimiento de la demanda de los sectores productivos en la formación de profesionales preparados y calificados de acuerdo a las exigencias de la sociedad en plena competencia, el Instituto de Tecnologías, incorpora al currículo de las diferentes Escuelas, carreras de Licenciaturas e Ingeniarías, transformando el Instituto en lo que hoy es la Facultad de Ciencias Empresariales.

El 13 de diciembre del 2002, el Honorable Consejo Universitario aprobó la creación del instituto de informática para aportar con

el desarrollo de nuevas tecnologías con altos estándares de calidad de servicio. Además esta unidad de servicios, presta soporte a todos los departamentos que conforman la UTEQ, así como también lo hace a la comunidad externa a la institución.

El avance de la tecnología en los últimos años en relación con las telecomunicaciones, hace que surjan nuevas revisiones a la formación profesional en el campo de estudio de la Tecnología en Telemática. Es por ello que el 05 de octubre del 2004 el H. Consejo Universitario en resolución décima tercera aprueba en primera discusión el proyecto autofinanciado de la creación del PROGRAMA CARRERA TECNOLOGÍA EN TELEMÁTICA. Así mismo, el 24 de agosto del 2005 en resolución sexta el H. Consejo Universitario aprueba en segunda instancia el proyecto de creación de la carrera TECNOLOGÍA TELEMATICA adscrito a la Escuela de Informática de la Facultad de Ciencias Empresariales

Ante la necesidad de contar con profesionales en el área de Ingenierías para el desarrollo e implementación de nuevas tecnologías y agrupadas en una unidad académica que relacionen a las carreras involucradas en esta área. El 09 de septiembre del 2008, por resolución séptima del Honorable Consejo Universitario se creó la Facultad de Ciencias de la Ingeniería con las carreras de Ingeniería en Diseño Gráfico y Multimedia, Ingeniería Agroindustrial, Ingeniería Eléctrica, Ingeniería en Mecánica, Ingeniería en Telemática e Ingeniería en Sistemas.

Podemos afirmar con certeza que la incorporación de inteligencia a los tradicionales sistemas de telecomunicaciones, representa hoy en día uno de los principales motores de la productividad y del crecimiento económico en el mundo.

La carrera de Tecnología en Telemática se inició con un pensum que contenía 12 módulos por año; esto es 36 módulos asignaturas distribuidos en 3 años de estudio, agrupadas en las áreas: Matemáticas, Electricidad y Electrónica, Humanística Administrativa Informática y Económica y el área de Redes y Telecomunicaciones.

Tomando como principal referente la Misión y Visión de la UTEQ, se proyecta un nuevo reto académico al formular el Modelo Educativo por Competencia. Este modelo plantea una nueva orientación y nivel de formación de los estudiantes que los hace más efectivos en sus labores profesionales, pues se basa en el desempeño que tendrán los egresados dentro de su campo laboral.

La Tecnología en Telemática y ahora la Ingeniería en Telemática en la UTEQ constituirá en Ecuador, el lugar idóneo para pensar y proyectar la sociedad hacia nuevas áreas de desarrollo.

La creación de una nueva oferta educativa en la rama de la ingeniería tiene un gran impacto en aquellos jóvenes a los que le llega el momento de decidir la carrera que desea estudiar. Lo que usualmente ocurre es que algunos jóvenes de mejor

desempeño intelectual buscan especializarse en áreas emergentes y prósperas de la ingeniería, ya que éstas les ofrecen varias ventajas personales y perspectivas hacia el futuro.

Para dar una continuidad a los graduados de las carreras de Ingeniería en Sistemas e Ingeniería en Telemática y puedan acceder a un título de cuarto nivel, el 02 de marzo del 2004, mediante resolución decima del Honorable consejo Universitario se resolvió: Aprobar en primera discusión el PROYECTO DE CREACION DE LA MAESTRÍA EN CONECTIVIDAD Y REDES DE ORDENADORES.

La institución cuenta con el campus Ing. Manuel Haz Álvarez cuyas dimensiones son del 159.60 metros de ancho por 497.30 metros de largo teniendo como resultado una área total de 7.94 hectáreas.

La sociedad productiva en su evolución, exigió la formación de nuevos profesionales que estén acorde a la industria, comercio, servicio y el mismo campo de la agricultura con calidad de líderes empresariales del futuro con un conjunto de conocimientos, habilidades, destrezas, actitudes y aptitudes, para enfrentar los retos del nuevo milenio.

Por lo expuesto, la UTEQ, tiene la imperiosa necesidad de implementar soluciones tecnológicas acorde a las carreras técnicas que oferta la institución y así afianzara los conocimientos de sus estudiantes, las carreras técnicas

obtendrán el reconocimiento de la sociedad al observar que la UTEQ se empodera de grandes cambios tecnológicos dentro de sus predios.

El actual sistema de acceso vehicular con el que cuenta el campus Ing. Manuel Haz Álvarez es obsoleto esto contrasta con una institución de educación superior que oferta carreras técnicas por lo que es necesario automatizar sus procesos para fortalecer y crear un campus inteligente acorde a los grandes avances tecnológicos del país y el mundo.

Con la automatización del sistema de acceso vehicular en la institución mejorará la seguridad del parque automotor que a diario ingresa a la UTEQ, debido a que en los últimos semestres se han hurtado vehículos, aumentando los niveles de inseguridad.

El diseño, la implementación y pruebas del dispositivo electrónicos para la automatización del ingreso vehicular se lo realizará dentro del segundo semestre del año 2013 en los predios del Campus Ing. Manuel Haz Álvarez de la Universidad Técnica Estatal de Quevedo en el Km 1,5 de la Vía Santo Domingo de los Tsáchilas - Quito.

Del resultado positivo del proyecto, se lo instalará en Campus Ing. Manuel Haz Álvarez, para dar servicio a la comunidad universitaria que está conformada por 272 empleados (184 con Nombramiento, 36 contratados y 52 amparados en el código del Trabajo) y 427 Docentes (245 Docentes con nombramiento

y 186 Docentes por contrato), Además la institución posee una población estudiantil de 8445 estudiantes matriculados en el periodo académico 2012 – 2013, y están distribuidos en 31 carreras como lo indica el Anexo No. 01

Las organizaciones a nivel mundial reconocen como una función fundamental la seguridad patrimonial para lo cual se están implementan soluciones innovadoras en el control de acceso vehicular con un alto grado de eficiencia puesto que permiten tener un bajo tiempo de respuesta frente a ambientes hostiles de seguridad.

En muchos países la tecnología para control de acceso vehicular, se ha implementado en tele peajes los cuales permiten dinamizar los cobros en las vías concesionadas, facilitando al usuario acceder al servicio sin detener su vehículo. Una de las grandes ventajas es la disminución del congestionamiento vehicular que surge en un peaje con altos niveles de ocupación, como las Autopistas.

En el país se están diseñando controles vehiculares a grandes y pequeñas escalas implementados en parqueaderos públicos y privados, controles de acceso del personal como los relojes biométricos, y de inventarios como en las grandes cadenas de supermercados que emplean sistemas de RFID para monitorear la seguridad de sus productos.

En el país existen diversas técnicas de control de acceso empleadas en varias instituciones públicas y privadas como se

lo puede evidenciar en la cartera de clientes de empresas que proveen el servicio, tales como SYSCOM[1] que automatizó el acceso al campus Las Peñas de la Escuela Politécnica del Litoral (ESPOL), en la ciudad de Guayaquil, además el cobro de peajes tienen una propuesta de automatización que en la actualidad solo ha sido empleado en la Avenida Rumiñahui[2]

En la provincia de Los Ríos y sus cantones no existe empresa que tenga un control de acceso vehicular automatizado, muchas empresas lo hacen de forma manual y el proceso automatizado que algunas instituciones poseen es el relacionado con la revisión del personal que laboran basado en la identificación de la huella dactilar.

La Universidad Técnica Estatal de Quevedo, es una institución de educación superior con un control de acceso vehicular manual, es decir requiere de un personal permanente que valide al parque automotor, donde el conductor está en la obligación de mostrar su identificación y si todo el proceso es correcto esperar que el vigilante le emita un tiquet de forma manual y permitir ingresar al campus universitario.

La UTEQ oferta carreras técnicas como ingeniería en Telemática, Ingeniería en Sistemas, Ingeniería en Mecánica, e Ingeniería Eléctrica, con personal capacitado para la automatización de procesos que facilita la creación de un sistema electrónico para el tratamiento de la información,

[1] SYSCOM, empresa dedicada a la automatización de parqueaderos
[2] Según el diario el Comercio en su publicación del 13 de febrero del 2014

implica que la institución puede contar con control de acceso acorde a los grandes avances tecnológicos.

Los visitantes del campus Ing. Manuel Haz Álvarez, observan con desagrado los bajos niveles de seguridad en los predios universitarios al enterarse de la sustracción de vehículos como lo ocurrido el día 29 de marzo del 2010[3], por tal motivo los usuarios desconfían del sistema de control de acceso al momento de parquear sus vehículos en los predios universitarios.

La Universidad Técnica Estatal de Quevedo, cuenta con un acceso vehicular manual generando congestión al tener altos tiempos de validación de certificados; requiere de personal permanente que autorice al parque automotor, donde el conductor está en la obligación de mostrar su identificación y si todo el proceso es correcto esperar que el vigilante le emita un tiquet y permitir el ingresar al campus universitario.

Por tal motivo se pretende diseñar e implementar un sistema electrónico que permita realizar el control de acceso vehicular mediante la autenticación por radiofrecuencia (RFID), en donde el usuario ingresa en un tiempo mínimo, para esto debe tener un trasmisor de radio frecuencia que será incorporado en una tarjeta o una etiqueta entregada al conductor del vehículo, está emitirá un código, el cual será recibido por un dispositivo electrónico y validado por un computador, si el código es

[3] Dato Obtenido del Diario La Hora del 31 de marzo del 2010

correcto se procederá a levantar el vástago y permitir el ingreso del automotor.

La automatización del ingreso vehicular permitirá tener un ingreso eficiente, que disminuirá el tiempo en el proceso de entrada y salida al campus Ing. Manuel Haz Álvarez, por lo que no necesitará de forma permanente personal para controlar el acceso del parque automotor al predio universitario.Técnicas de información

En líneas generales podríamos decir que las nuevas tecnologías de la información y comunicación son las que giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones; pero giran, no sólo de forma aislada, sino lo que es más significativo de manera interactiva e interconexionadas, lo que permite conseguir nuevas realidades comunicativas. (Cabero Almenara, 1998)

Control vehicular

Se puede definir como la regulación de las actividades de un vehículo con el fin de lograr un funcionamiento predeterminado, de modo que se reduzcan las probabilidades de fallos y se obtengan los resultados buscados. (Coulter., 1996)

Control de acceso

Se define como una medida de seguridad que permite limitar o restringir el acceso a determinados lugares. Esto implica que se deba contar con algún tipo de identificación para validar el acceso. (SYSCOM, 2008)

RFID

RFID (Identificación por Radiofrecuencia) es un método de almacenamiento y recuperación remota de datos, basado en el empleo de etiquetas o "tags" en las que reside la información. RFID se basa en un concepto similar al del sistema de código de barras; la principal diferencia entre ambos reside en que el segundo utiliza señales ópticas para transmitir los datos entre la etiqueta y el lector, y RFID, en cambio, emplea señales de radiofrecuencia (en diferentes bandas dependiendo del tipo de sistema, típicamente 125 KHz, 13,56 MHz, 433-860-960 MHz y 2,45 GHz). (Portilla, Bermejo, & Bernardo, 2008)

El RFID (Autenticación por Radiofrecuencia), es un proceso en el cual se emite un código a baja frecuencia (13.56 KHz estándar internacional), este es captado por una antena de RFID, el cual se validad en un computador o en un dispositivo electrónico que realice procesamiento de datos como los microcontroladores. Esta tecnología ha logrado grandes cambios ya que es la que suplantara a los códigos de barra. (Ilyas & Ahson, 2004)

La longitud de los códigos en RFID es de 15 bits lo que proporciona una capacidad de 32,768 productos que se puede codificar para el control de inventario (Telectrónica, 2009)

Tag

Una etiqueta RFID consta de un microchip montado sobre un sustrato PET flexible con una antena incorporada. Este sustrato o "inlay" es luego instalado en una etiqueta con adhesivo de

base. A pesar de que los chips son pequeños, las antenas no lo son. Ellas necesitan ser lo suficientemente grandes como para captar la señal emitida por el lector. La antena permite que una etiqueta pueda leerse a una distancia de 3 metros o más, incluso a través de distintos materiales. El tamaño de la antena tiende a determinar el tamaño de una etiqueta RFID. (Telectrónica, 2009)

El Tag es un Chip o "transponder", el cual mediante una etiqueta puede ser adherido a un producto o a cualquier elemento físico que se desee identificar dentro de la cadena de suministro, y un "radar" conocido como antena. La antena hace las veces del radar y requiere de un lector el cual genera un campo radioeléctrico que activa a la etiqueta que recibe, decodifica e interpreta la información que ésta tiene almacenada. A diferencia de los "transponder" de los aviones y por una razón de costo los tag's de RFID no cuentan con energía eléctrica propia por lo que se denominan tag's pasivos y solo envían la información que contienen una vez que son expuestos al campo radioeléctrico que proviene de las antenas. Aunque existen en la actualidad tags ACTIVOS equipados con una batería, su uso es limitado y en algunos casos la batería puede funcionar hasta por 5 años (Telectrónica, 2009).

Antena

Es un elemento pasivo diseñado para emitir y recibir ondas electromagnéticas de forma inalámbrica, es decir la antena se la puede ver como un acoplador entre un medio guiado y un

medio no guiado, las cuales pueden tener varias características entre las más importantes son las siguientes (Balanis, 1997):

- Ganancia
- Polarización
- Frecuencia de Operación
- Ancho de Lóbulo
- Impedancia

Las antenas del lector son el componente más sensible de un sistema RFID. La mayoría de las antenas son instaladas en lugares que fáciles de montar, y suelen verse como racks protegidos. Variar la ubicación de la antena del lector es una de las formas más fáciles de ajuste cuando se localizan y solucionan problemas de un sistema, y al mismo tiempo resulta una de las tareas más difíciles de llevar a cabo en forma correcta.

La antena del lector debe ser colocada en una posición donde tanto la transmisión de energía hacia la etiqueta, como la recepción de los datos emitidos sean óptimas. Debido a que existen regulaciones gubernamentales que limitan el nivel de potencia de un lector, la ubicación de las antenas es vital para alcanzar un alto grado de lectura. (Ilyas & Ahson, 2004)

Lectores RFID

Un lector RFID está compuesto por una antena, un transceptor y un decodificador. Estos lectores envían periódicamente una señal para verificar la presencia de etiquetas en su área de cobertura. Cuando detecta la presencia de una etiqueta

extrae la información contenida en el chip y la transmite al subsistema de procesamiento de datos. (Montenegro & Marchesin, 2007)

Los Lectores RFID son elementos activos que permiten identificar un bien, producto o ser vivo sin necesidad de tener contacto visual ni físico, ya que la lectura se la realiza de forma inalámbrica al acercarse los tags (Montenegro & Marchesin, 2007)

Figura 1: Lector Activo Direccional

En la actualidad podemos encontrar lectores RFID que permiten leer hasta 2000 etiquetas de forma simultánea y lo pueden realizar la autenticación hasta una velocidad de 200 kilómetro por hora, en conclusión este equipo se adaptaría a muchas aplicaciones como en el desarrollo de sistemas para tarifación basados en tele peaje. (Transcore, 2013)

Diseños Cuasi Experimental

Los diseños cuasi experimentales también manipulan deliberadamente al menos una variable independiente para ver su efecto y relación con una o más variables dependientes, solamente que difieren de los experimentos "verdaderos' en el grado de seguridad o confiabilidad que pueda tenerse sobre la equivalencia inicial de los grupos. En los diseños cuasi experimentales los sujetos no son asignados al azar a los grupo, ni emparejados; sino que dichos grupos ya estaban formados antes del experimento, son grupos intactos (la razón por la que surgen y la manera como se formaron fueron independientes o aparte del experimento). (Fernandéz Sampieri & Hérnandez Collado, 1997)

Pasos de un Cuasi Experimento

Paso 1: Definir las variables dependientes e independientes que se incluirán en el cuasi experimento.

Paso 2: Elegir los niveles de manipulación de las variables independientes y traducirlos en tratamientos experimentales.

Paso 3: Desarrollar el o los instrumentos para medir las variables dependientes.

Paso 4: Seleccionar una muestra de la población para el experimento.

Paso 5: Reclutar a los sujetos del cuasi experimento.

Paso 6: Seleccionar el diseño cuasi experimental apropiado para nuestras hipótesis, objetivos y preguntas de investigación.

Paso 7: Planificar como manejar a los sujetos que participan en el experimento.

Paso 8: Analizar las propiedades del grupo.

Método para evaluar la variable dependiente.

Independientemente de los instrumentos utilizados para medir la variable dependiente (un cambio o un efecto de cualquier tipo), es conveniente que los sujetos evalúen la experiencia después (en el momento del post-test) en términos de gusto, facilidad, eficacia, etc., incluso evaluando por separado aspectos distintos de la experiencia (que puede incluir, por ejemplo, conferencias, trabajos de equipo, etc.), que pueden ser valorados de distinta manera. Esta evaluación es otra variable dependiente. Esta información puede ser muy útil para evaluar la misma experiencia y también para verificar relaciones entre sus efectos. Puede considerarse como una información adicional que puede entrar en la triangulación ya mencionada y además enriquece la investigación. (Vallejo, 2013)

Pre test y post test sin grupo de control

Consiste en verificar un *cambio;* a los sujetos se les mide *antes* y *después* de un tratamiento o experiencia en aquella variable o variables en las que se espera que cambien. Como no hay grupo de control no se trata de un diseño experimental en sentido propio, aunque es un diseño que puede ser muy útil a pesar de sus limitaciones. (Vallejo, 2013)

Tipos de Acceso Vehicular.

Desde los inicios de la humanidad los seres humanos siempre han desarrollado experimento e innovaciones que faciliten los procesos de la vida cotidiana, este deseo ha ido evolucionando hasta nuestros días este deseo ha ido evolucionando, teniendo grandes avances tecnológicos involucrando la automatización de los procesos, por lo que podemos tener diferentes tipos de tecnología de acceso vehicular.

Control de Acceso Vehicular Accionada por Botón.

En este mundo automatizado, este es uno de los mecanismos más simples y económicos que se puedan tener en el control de acceso vehicular, y se trata de accionar las barreras de acceso vehicular atreves de botones industriales:

Ventajas:

- ✓ Fácil Instalación
- ✓ Económico
- ✓ No necesitan del desarrollo de un software para su funcionamiento
- ✓ Fácil mantenimiento

Desventajas:

- Requiere de una persona de forma permanente para su operación.
- La seguridad en el acceso está sujeta al error humano

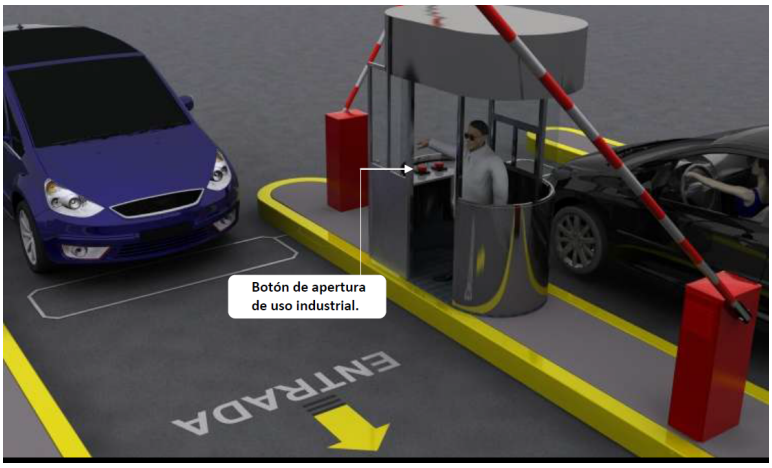


Figura 02: Control de Acceso Accionada por Botón

Esta técnica se las puede complementar con el uso de emisores y detectores de luz infrarroja para implementar seguridad al vehículo es decir que la barrera no baje hasta que el automotor supere la zona de operación de la barrera.

Control de Acceso Vehicular Accionada por Tarjetas de Proximidad.

Este método de control de acceso a instalaciones públicas o privadas ya no necesitan de un ser humano para su operación por que la validación se la realiza mediante el uso de tarjetas magnéticas, el cual es insertada en el dispositivo de acceso si la validación es correcta se autoriza el ingreso a las instalaciones de la institución.

El sistema de tarjetas magnéticas es óptimo, pero las tarjetas magnéticas tienen un tiempo de vida corto, por cuanto la cinta magnética se deteriora fácilmente y estas pueden sufrir daños al ser sometidos a campos electromagnéticos, este puede ser

solucionado al remplazar el lector de tarjetas magnéticas por un teclado el cual el usuario deberá digitar la clave para que se le autorice el ingreso a las instalaciones de la institución.

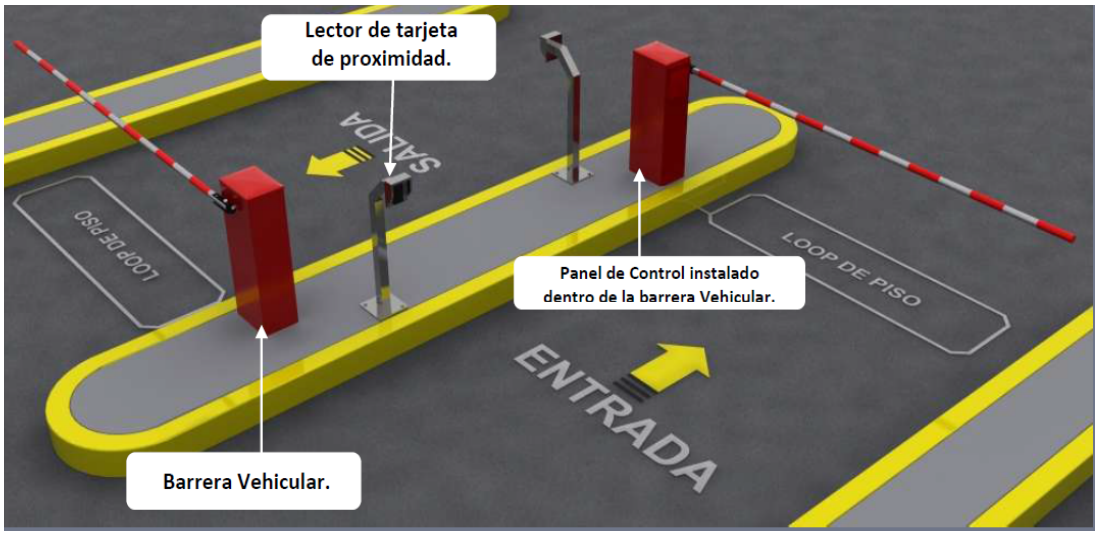


Figura 03: Control de Acceso Accionada por Tarjetas de Proximidad.

La seguridad está sujeta a la posesión de las tarjetas magnéticas y en el caso de las claves estas pueden ser olvidadas por el usuario.

Ventajas:

- ✓ Fácil Instalación
- ✓ Fácil mantenimiento
- ✓ No requieren de la operación manual de un ser humano.

Desventajas:

- Corto tiempo de vida útil de las tarjetas magnéticas.
- La seguridad en el acceso está sujeta a la posesión de las tarjetas magnéticas que se pueden extraviar fácilmente

Acceso Vehicular basado en Autenticación por Radiofrecuencia.

Esta tecnología es ampliamente empleada a nivel mundial, por ser un sistema flexible que se adecua a los requerimientos del cliente en cuanto a distancia, velocidad y presupuesto por sus ventajas: (Transcore, 2013)

- ✓ Operación manos libres, sin detención, con lo que se reduce el tráfico en el acceso a las instituciones.
- ✓ No hace falta bajar la ventanilla, con lo cual hay mayor seguridad personal.
- ✓ Accesible en precio, fácil de instalar y mantener.
- ✓ No hay equipos en la vía que puedan ser dañados por los vehículos.
- ✓ No requiere tarjetas ni tickets, los cuales suelen perderse o gastarse.
- ✓ Procesamiento automático en puertas remotas.
- ✓ Mayor seguridad personal.
- ✓ Bajos costos de reparación y mantenimiento.
- ✓ Acceso cómodo para discapacitados.

Los sistemas de RFID, se les puede incorporar mayores niveles de seguridad porque pueden operar en las frecuencias de las antenas de WIFI (2,4 GHz y 5,8GHz), para obtener un monitoreo en tiempo real (RTLS, Real Time Location Systems).

Sistemas de Radiofrecuencia

Los sistemas de radiofrecuencia es un conjunto de dispositivos que interactúan para lograr un fin mediante el uso de la radiofrecuencia es decir mediante la trasmisión y recepción de

ondas electromagnéticas a una determinada frecuencia. (Anguera & Perez, 2011)

Dentro de los sistemas de radiofrecuencia podemos tener los sistemas de telecomunicaciones, sistemas de identificación por radiofrecuencia.

Antenas.

IEEE (*Institute of Electrical and Electronics Engineers*) define una antena como "aquella parte de un sistema transmisor o receptor diseñada específicamente para radiar o recibir ondas electromagnéticas". Dicho de otro modo, la antena es la transición entre un medio guiado y el espacio libre. (Anguera & Perez, 2011)

Las ondas electromagnéticas se caracterizan por su frecuencia (f) y longitud de onda (λ):

$$\lambda = \frac{c}{f}$$

Donde c es la velocidad de propagación en el medio (aproximadamente $3x10^8$ m/s en el espacio libre).

Las antenas son un elemento pasivo pero es aquel que permite la comunicación en un sistema de radiofrecuencia, y estas se pueden clasificar por su geometría:

- ✓ Antenas Parabólicas
- ✓ Antenas tipo bocina
- ✓ Antenas Fractales
- ✓ Mono polos
- ✓ Dipolos

- ✓ Log periódicas
- ✓ Etc.

Las antenas también se la pueden clasificar según su comportamiento es decir según el rango de frecuencias de operación:

- ✓ Antenas de Banda Ancha.
- ✓ Antenas multifrecuencias.

Las antenas presentas parámetros básicos para el diseño de un sistema de radiofrecuencia como los que se mencionan a continuación:

Impedancia de entrada.

Una antena es un dispositivo de un puerto y, por lo tanto, presenta una impedancia de entrada que no es más que la relación entre la tensión y la corriente presente en el puerto de entrada. La impedancia de una antena tiene una parte real y otra imaginaria, y ambas dependen de la frecuencia. Se dice que la antena es resonante a una frecuencia f_0 si la parte imaginaria de la impedancia de entrada en f_0 es cero. Una antena presenta generalmente muchas resonancias, que se denomina "modos". (Anguera & Perez, 2011)

Lóbulos de Radiación

Un lóbulo o diagrama de radiación es una representación gráfica de las propiedades de radiación de la antena en función de las diferentes direcciones del espacio (sistema de coordenadas esférico) a una distancia fija. Con la antena

situada en el origen y manteniendo constante la distancia, expresa el campo eléctrico en función de las variables angulares. El diagrama de radiación cobra relevancia en la zona de campo lejano, es decir, en la zona donde la forma del diagrama es invariante en función de la distancia. (Balanis, 1997)

En el diagrama de radiación podemos identificar el número de lóbulos principales, el número de lóbulos secundarios, Relación delante atrás, ancho del haz de radiación.

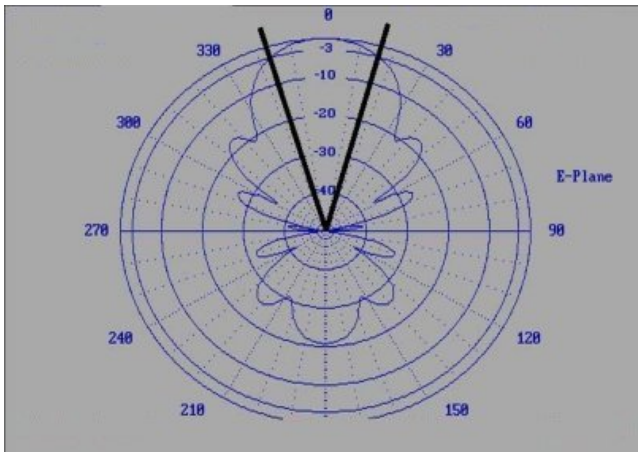


Figura 04: Diagrama de Radiación de un Dipolo.

Directividad.

La directividad de una antena se define como "la relación entre la densidad de potencia radiada en una dirección, a una distancia dada, y la densidad de potencia que radiaría a esta misma distancia una antena isotrópica que radiase la misma potencia que la antena transmisora (Balanis, 1997)

De manera gráfica, podemos decir que si una antena es muy directiva, es capaz de concentrar la potencia que radia (o

recibe) en una determinada dirección. Por ejemplo, una antena tipo reflector parabólico para observación astronómica tiene gran directividad (aproximadamente 50dB). Esto le permite apuntar en una determinada dirección para recibir la señal y no recibir en otras direcciones. Una antena de radiodifusión FM es de poca directividad ya que tiene que intentar distribuir la potencia en muchas direcciones. (Anguera & Perez, 2011)

Ganancia.

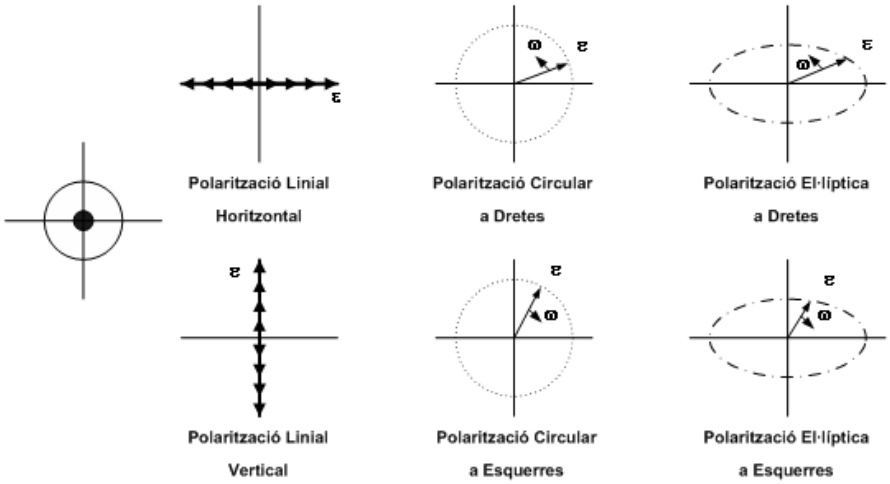
Su definición es similar al de Directividad, pero la comparación no se establece con la potencia radiada, si no con la potencia entregada a la antena. La ganancia pone de manifiesto el hecho de que una antena real no radia toda la potencia que se le suministra, si no que parte de ésta se disipa en forma de calor (RΩ). Por lo tanto, la ganancia y la directividad están relacionadas por la eficiencia de la antena. (Balanis, 1997)

Polarización.

La polarización de una antena en una dirección dada se define como "la polarización de la onda radiada cuando ésta se encuentra excitada". La polarización generalmente se define en la dirección en la que la antena radia el máximo de potencia, ya que los enlaces se diseñan para que sean eficientes en la dirección de máxima radiación. La polarización de la onda radiada varía con la dirección respecto al centro de la antena, por lo que diferentes partes del diagrama de radiación pueden tener diferentes polarizaciones. (Anguera & Perez, 2011)

- ✓ Polarización Horizontal
- ✓ Polarización Vertical
- ✓ Polarización Circular
- ✓ Polarización Elíptica

Figura 05: Tipos de Polarización.



Fuente: TEORÍA DE ANTENAS, J. Anguera, A. Perez, 2011, Pag, 22

Los parámetros básicos de las antenas son útiles para realizar un balance de potencias y determinar cómo cada uno de ellos afecta en la ecuación que relaciona la potencia transmitida por una antena y la potencia recibida por la antena de recepción de un sistema de radiofrecuencia.

La adaptación de una antena y su eficiencia de radiación determinan cuánta potencia se radiará en el espacio (por reciprocidad, cuánta se recibe del espacio y se entrega el receptor). El diseño de la antena determina su adaptación, que puede complementarse tanto con redes de adaptación o con

elementos discretos (ej.: bobina y condensadores) y/o distribuidos (ej.: líneas de transmisión). (Anguera & Perez, 2011)

Sistemas de RFID

La tecnología RFID tiene sus orígenes desde comienzos de la década de 1920 y está relacionada con la II Guerra Mundial, en la cual los alemanes, japoneses, americanos y británicos utilizaban radares para detectar el acercamiento de aviones. El gran inconveniente surgió porque no se podía identificar si los aviones pertenecían al enemigo o si eran pilotos del propio país que regresaban de una misión. El ejército alemán descubrió que si los pilotos balanceaban sus aviones al volver a la base cambiaría la señal de radio reflejada de vuelta, con este método se podía distinguir a los aviones alemanes de los aliados y se convirtió en el primer dispositivo de RFID pasivo. (Ilyas & Ahson, 2004)

El sistema de identificación IFF "Identification Friend or Foe" (Identificación Amigo o Enemigo) fue una tecnología para identificación de aeroplanos, inventada por Inglaterra en 1939, y utilizada en la Segunda Guerra Mundial. La primera serie de equipos electrónicos que se construyeron para la identificación recibieron el nombre de "Trasponders" (Equipos que reciben en una frecuencia y transmiten en otra) fue desarrollado por la industria inglesa y estuvo operativa a partir de 1940, recibiendo el nombre de MARK I. (Ilyas & Ahson, 2004)

Harry Stockman fue un investigador que publicó en 1948 un artículo titulado "Comunicación por medio de la energía reflejada", fue, quien dictaminó que las dificultades para la comunicación usando ondas de radio reflejadas en objetos estaban superadas, con todas las aplicaciones que esta podía permitir. (Ilyas & Ahson, 2004)

No pudo ser hasta treinta años después cuando el trabajo de Stockman fue de nuevo estudiado. Cuando se desarrollaron transistores, microprocesadores los que lograron grandes adelantos en redes de comunicación, incluso un cambio en la visión de hacer negocio, para que los sistemas RFID fueran factibles. (Ilyas & Ahson, 2004)

Fue en la década de los 50 cuando diferentes sectores de la tecnología RFID se vieron impulsados, entre ellos los sistemas con transponders de largo alcance, especialmente los conocidos como IFF. (Montenegro & Marchesin, 2007)

Trabajos como los creados por D.B. Harris "Sistema de Radio Transmisión con Respuesta Modulatoria Pasiva" fueron determinantes para que la tecnología RFID dejase de ser una idea y se convirtiese en una solución.

En la década de los 60 la actividad comercial comenzó a existir en el campo de la identificación por radio frecuencia. El primer sistema que fue usado era el EAS "Electronic Article Surveillance" (Vigilancia Electrónica de Artículos) para detectar robos en grandes almacenes. El sistema era sencillo con un único bit de información, para detectar la etiqueta o no, dentro del radio de

acción del lector y hacer sonar una alarma acústica en caso de que una etiqueta no desactivada pasase por el alcance del lector. Típicamente eran dos lectores ubicados de tal forma que el cliente tenía que pasar entre ellos para salir del establecimiento. A pesar de sus limitaciones, era económico y efectivo. (Montenegro & Marchesin, 2007)

En los 70 se lograron grandes avances y las primeras patentes para dispositivos RFID fueron solicitadas en Estados Unidos, concretamente en enero de 1973 cuando Mario W. Cardillo se presentó con una etiqueta RFID activa que portaba una memoria regrabables. El mismo año, Charles Walton recibió la patente para un sistema RFID pasivo que abría las puertas sin necesidad de llaves. Una tarjeta con un transponedor comunicaba una señal al lector de la puerta que cuando validaba la tarjeta desbloqueaba la cerradura. (Montenegro & Marchesin, 2007)

En esta década hubo un gran desarrollo técnico de los sistemas, sobre todo enfocado a aplicaciones de seguimiento de ganado, vehículos y automatización industrial. La creación de nuevas empresas dedicadas a la tecnología RFID aumentaba continuamente, era un signo positivo del potencial que tenían los sistemas RFID. (Montenegro & Marchesin, 2007)

En la década de los 80, en EEUU se implementaron sistemas de RFID en aplicaciones como el transporte, accesos y en menor grado en el control de animales. En países europeos como Francia, España, Portugal e Italia se centraron más en

aplicaciones industriales y sistemas de corto alcance para controlar animales. (Montenegro & Marchesin, 2007)

En los primeros años de los 90 en EEUU se implementó un peaje con control electrónico, como las autopistas de Houston y Oklahoma incorporaban un sistema que gestionaba el paso de los vehículos por los pasos de control. En Europa también se investigó este campo y se usaron sistemas de microondas e inductivos para controles de accesos y billetes electrónicos. Un nuevo avance en el mundo del automóvil vino con la tecnología RFID, sistema de control de encendido y de acceso del automóvil, entre otras acciones. (Montenegro & Marchesin, 2007)

Aplicaciones para autopistas y billetes electrónicos se fueron extendiendo por Asia, África, Suramérica y Australia. A partir de aquí el éxito de la tecnología RFID en estos campos hizo que se aplicaran a otros segmentos económicos.

En la actualidad el principal responsable del desarrollo e implantación de esta tecnología es Auto-ID Center, una sociedad constituida en 1999 por un centenar de empresas pioneras, universidades y centros de investigación de todo el mundo. (Montenegro & Marchesin, 2007)

El AutoID Center, ahora conocido como AUTOID Labs, está conformado por 6 laboratorios localizados en universidades de prestigio como el MIT (Massachussets Institute of Technology) de EEUU, University of Cambridge en el Reino Unido, University of Adelaide en Australia, Keio University en Japón, Fudan University

en China y University of St. Gallen en Suiza. Hace unos años el AutoID Center ubicado en el MIT con el apoyo de EAN (European Article Numbering) ahora EAN Internacional y UCC (Uniform Code Council) y las mayores empresas de consumo masivo de ámbito mundial, desarrollaron lo que hoy conocemos como la Red EPC™ y sus componentes. (Montenegro & Marchesin, 2007)

El Código Electrónico de Producto™ (EPC) es un número único que se graba en el chip contenido en una etiqueta o tag RFID y se coloca en cada producto, lo que permite hacer un seguimiento exacto de cada unidad física. La etiqueta sólo almacena el código EPC. El EPC contendrá la información asociada al Global Trade Item Number (GTIN) identificación de la empresa y producto del sistema más otros datos adicionales como el número de serie del producto que le dará una identificación única en el ámbito mundial. El EPC tiene 96 bits y es posible identificar los productos de forma inequívoca ya que cada etiqueta posee un número identificativo. (Finkenzelle, 2003)

Componentes y modelo de comunicación

Un sistema de RFID consiste de por lo menos en un transponders y un tag. Una etiqueta contiene un microchip, condensadores y una bobina que hace la función de antena la cual está dentro de un material de encapsulación, ejemplo una moneda, un cuerpo de vidrio, substrato plástico, etiqueta inteligente o una tarjeta. La bobina en un chip tecnológico permite etiquetas

muy pequeñas con sólo 6mm de diámetro y 1.5mm de espesor (Finkenzelle, 2003).

Las etiquetas se comunican vía radio, las señales con un RFID-lector que es un componente central de un Sistema de RFID. Los sistemas de RFID normalmente operan en las bandas de frecuencia ISM (Industria, Científico, Médico). Hay dos tipos de acoplamientos de etiqueta-lector (Finkenzelle, 2003).

El acoplamiento Inductivo usa frecuencias debajo de 30 MHz. El de la bobina de antena genera un campo magnético alterno e induce un voltaje en la bobina de la etiqueta. La transferencia de datos del lector a la etiqueta esta normalmente basado en un esquema de modulación digital por variación de amplitud (ASK) y la etiqueta emplea modulación de carga para transferir datos al lector. (Finkenzelle, 2003)

El Backscatter acoplando es usado para frecuencias sobre 100 MHz. Aquí la etiqueta de la antena recibe señales y energía (sólo etiquetas pasivas) del campo electromagnético emitido por el lector. Para transferir datos al lector, el poder reflejado es modulado por el transponder (moduló backscatter[4]). (Finkenzelle, 2003)

El lector normalmente envía los datos recogidos en una etiqueta a un sistema de aplicación de fondo para procesos más lejanos. Los lectores periféricos están directamente adheridos a estos sistemas (ej. Interfaces vía RS 232 o USB) y lectores

[4] Comunicación Inalámbrica sin baterías

independientes (dispositivos de handheld[5]) puede conectar vía protocolos de la red normalizados a los sistemas de respaldo, por ejemplo vía Ethernet (o un enlace inalámbrico) y TCP/IP[6]. (Finkenzelle, 2003)

El rango de la transmisión depende de varios parámetros diferentes y se pueden realizar lecturas de unos pocos centímetros a varios metros en aplicaciones prácticas. La comunicación depende del protocolo de la etiqueta, comenzado por el lector ("el lector habla primero") o por la etiqueta ("la etiqueta habla primero"). Algunos protocolos de comunicación RFID no especifican claramente las diferentes capas. (Finkenzelle, 2003)

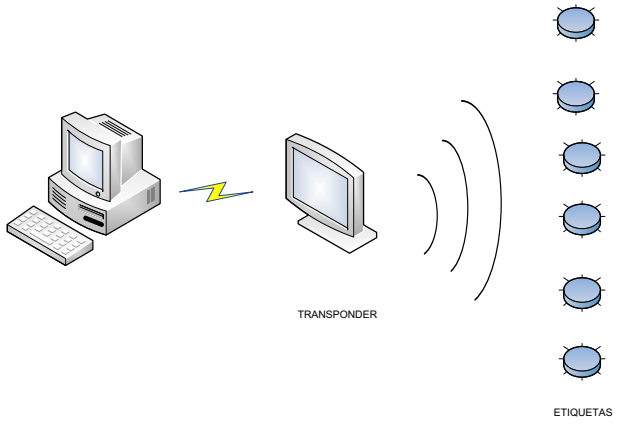


Figura 06: Esquema de un sistema RFID con etiquetas pasivas.

[5] Computador portátil llamado PDA (Asistentes Digitales Personales)
[6] Conjunto de protocolos de internet en los que se basa internet permitiendo la transmisión de datos
TCP Protocolo de Control de Transmisión
IP Protocolo de Internet

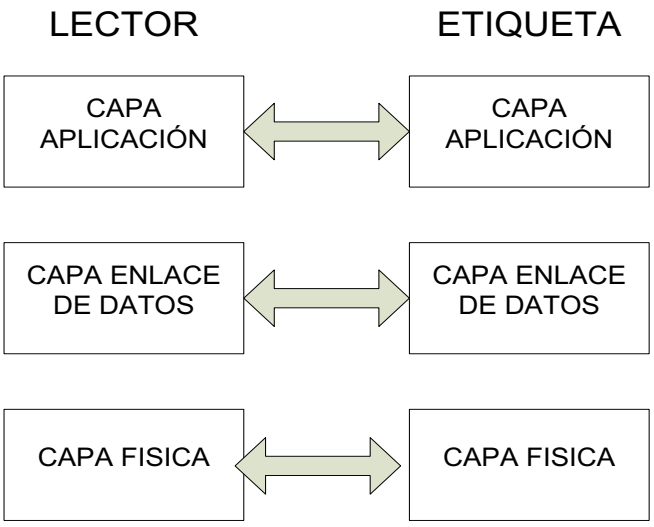


Figura 07: Modelo de Comunicaciones RFID

Propiedades de Funcionamiento

Los Transponders RFID considerados tienen las siguientes características funcionales:

- Agregar un mínimo, Estos permiten enviar un único identificador (UID) en respuesta. Entonces llamado "Transponders de 1 bit" sin un chip, el cual es usado para artículos electrónicos de vigilancia (EAS).
- Poseen protocolos anticolisión y de multiacceso (uno probabilístico y otro determinístico) implementado el cual permite la detección y direccionamiento de múltiples etiquetas en el rango de un solo lector. Los protocolos de anti-colisión entre diferentes lectores en la proximidad pueden ser considerados una emisión abierta.

- Su propósito primario es identificación de objetos, es decir tarjetas inteligentes con un poder de procesamiento considerable (para operaciones criptográficas avanzadas)
- La etiqueta RFID puede poseer memoria de lectura y escritura aparte de UID. La tecnología de memoria es usualmente EEPROM (Memoria de solo lectura programable y borrable eléctricamente) y los rangos de capacidad típicos están entre los cientos de Bits y varios Kbytes.
- El transponder es controlado por una máquina de estados (transponder de bajo-fin) u otro por un microprocesador (transpondedor alto-fin).
- La etiqueta puede poseer una unidad de encriptación y autenticación de mensajes e implementar algunas funciones de seguridad, con el propósito de proteger la etiqueta y sus comunicaciones.

La tecnología RFID fue desarrollada para remplazar códigos de barras en algunos puntos en el futuro. Las mayores ventajas de sistemas RFID sobre identificación óptica con código de barras son:

- La posibilidad de rescribir y modificar datos
- La operación sin línea de vista

En algunas etiquetas RFID, el control de acceso es implementado en las cuales no es posible con código de barras. La lectura rápida (en particular relevante para un número largo de artículos) puede ser más alta que usando código de barras. El almacenamiento puede no ser una ventaja desde modernos

código de barras 2D pueden almacenar 16 Kbit de datos o más, aunque muchos scaners desplegados no pueden leer estos códigos.

Estándar de los sistemas RFID

Existe una gran variedad de sistemas RFID y sus principales características son definidas por estándares. En particular sus interfaces inalámbricas (frecuencia, codificación, modulación), protocolos de comunicación, ancho de banda, anti-colisión y mecanismos de seguridad. Otras características son: etiquetas de lectura y memoria, tipo de chip, diseño de etiqueta, rango de comunicación). (Sánchez, 2008)

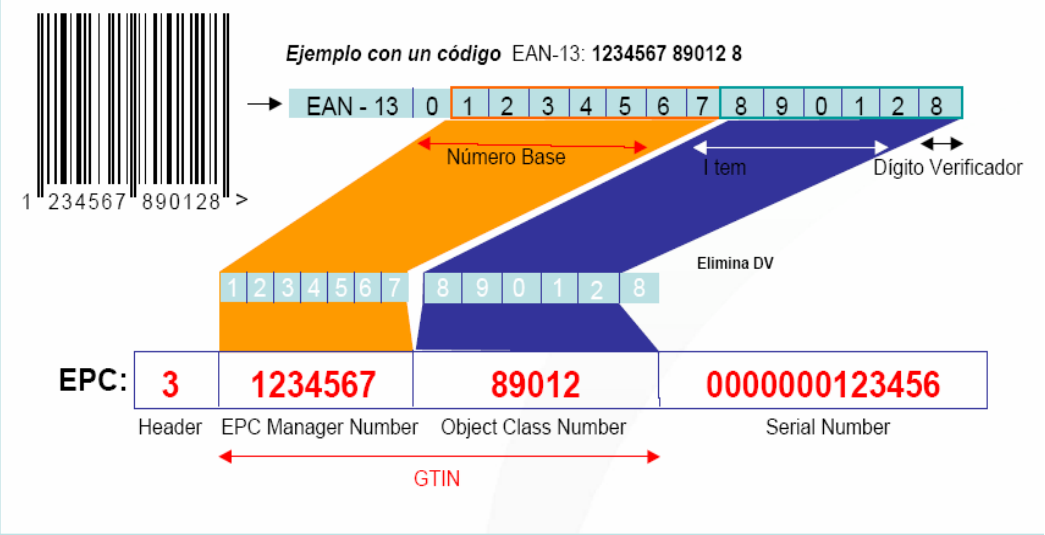
Existen diversos tipos de tags RFID en el mercado. Esto guarda relación con las frecuencias utilizadas, la cantidad de memoria, los tipos de códigos y una serie de otros puntos en los cuales no existen claros consensos. Es por esto que luego de varias reuniones entre los actores fundamentales del mercado se llegó a un consenso con respecto a la identificación de los artículos proponiéndose un sistema estándar, específicamente el Código Electrónico de Producto (EPC). Algunos de los actores que intervinieron en dicho acontecimiento fueron EAN International, Uniform Code Council, The Gillette Company, Procter & Gamble, Wal-Mart, Hewlett-Packard, Johnson & Johnson, Checkpoint Systems and Auto-ID Labs. (Sánchez, 2008)

El Código Electrónico de Producto (EPC) es "un esquema de identificación para objetos físicos que se identifican universalmente a través de las etiquetas de Identificación por Radio Frecuencia (RFID) y otros medios. Los datos EPC

estandarizados consisten en un EPC (o Identificador EPC) que identifica únicamente a un objeto individual, así como también un Valor de Filtro opcional, cuando se considera que éste es necesario para permitir una lectura efectiva y correcta de las etiquetas EPC. Además de estos datos estandarizados, ciertas clases de etiquetas EPC permitirán incluir datos definidos por el usuario. (Sánchez, 2008)

Los Estándares de Datos de la Etiqueta EPC definirán las longitudes y posición de estos datos, sin definir su contenido. Actualmente no existen especificaciones de datos definidas por el usuario, ya que aún no se han definido las etiquetas de esta Clase". (Sánchez, 2008)

El EPC utiliza una cadena de números para identificar fabricante, producto y un número de serie exclusivo para cada unidad de artículo. Esta cadena de números se graba en el chip de la etiqueta RFID pudiendo obtenerse una infinidad de información complementaria, asociando el número *EPC* a una base de datos. (Sánchez, 2008)



Fuente: EPCglobal Inc, http://www.epcglobalinc.org/

Figura 08: Formato del código EPC

Tarjetas de circuitos integrados de poco contacto.

Las tarjetas de circuitos integrados de poco contacto son una instancia especial de las tarjetas de identificación como se definido en ISO 7810. Específicamente hay tres tipos de tarjetas de poco contacto las cuales pueden ser distinguidas en términos de sus rangos de comunicación:

- Tarjetas de par-cerrado (ISO 10536). Estas operan en distancias bien pequeñas al lector (< 1 cm). Pueden ofrecer pocas ventajas sobre las clásicas tarjetas inteligentes de contacto (ISO 7816).
- Tarjetas de Proximidad (ISO 14443) operan a aproximadamente 10 cm de distancia desde el lector. Estas usualmente poseen un microprocesador y puede ser considerado como traspondedor RFID alto-fin. Estas tarjetas pueden implementar más

aplicaciones sofisticadas tales como ticketing. Existen dos diferentes estándares (tipo A y tipo B) para el interfaz aéreo, inicialización y anti-colisión. El estándar describe el protocolo de capa enlace (T=CL) qué permite intercambiar las Unidades de Aplicación de Datos (APDUs) similar a ISO 7816 - 3 (el protocolo T=1) para tarjetas inteligentes de contacto.

- Tarjetas vecinas (ISO 15693) tienen un rango superior a 1 metro. Estas tarjetas pueden usarse para la identificación y aplicaciones simples como control de acceso. El estándar describe el interfaz aéreo, anti colisión y el protocolo de transmisión (capa enlace).

RFID en los animales

ISO 11784, ISO 11785 e ISO 14223 específica etiquetas para la identificación animal en la banda de frecuencia por debajo de 135 Khz. Los estándares originales definieron sólo un único identificador fijo de 64 bits, pero con el estándar ISO 14223 se permite la lectura/escritura y los bloques de datos protegidos contra escritura. El protocolo de comunicación ISO 14223 se relaciona estrechamente con ISO 18000. (Ilyas & Ahson, 2004)

Elemento de direccionamiento

ISO 18000 (RFID para elemento de direccionamiento) define el interfaz aéreo, mecanismos de detección de colisión y el protocolo de comunicación para el elemento de etiqueta en diferentes bandas de frecuencia, describe la referencia de arquitectura y especifican las características de las diferentes frecuencias. (Ilyas & Ahson, 2004)

Específica etiquetas de bajas frecuencias (<135 Khz.), para los sistemas de HF (13,56 Mhz) es compatible con ISO 15693 (pero con más flexibilidad en los diseños de etiquetas), y especifica una próxima generación del sistema RFID en la misma banda de frecuencia con superior ancho de banda (sobre los 848 kBit/s) y scanner más rápido de etiquetas múltiples. Especifica sistemas de 2,45 Ghz en un sistema del backscatter pasivo y con un rango mayor, sistema de alta tasa de datos con etiquetas activas. (Finkenzelle, 2003)

Comunicación de campo cercano (NFC)

NFC evolucionó de la tecnología RFID y está diseñada para las interacciones entre las etiquetas y dispositivos electrónicos en las proximidades (<10 centímetro). Los estándares ETSI TS 102.190, ISO 18092 y ECMA 340 definen idénticamente el interfaz de Comunicación de Campo Cercano y el Protocolo (NFCIP-1). (Ilyas & Ahson, 2004)

Describen el interfaz aéreo, inicialización, la anulación de colisión, un formato de trama y un bloque orientado al protocolo de intercambio de datos con manejo de error. Hay un modo de comunicación activo (ambos dispositivos usan sus propios campos RF) y un modo pasivo de comunicación (el iniciador es generado en el campo RF y los usos designados a la carga del esquema de la modulación). NFC no es diseñado para todas las conexiones de redes o la transmisión de grandes cantidades de datos, pero debe permitir un intercambio de datos conveniente entre las etiquetas económicas (por

ejemplo, las etiquetas inteligentes) y los dispositivos electrónicos (por ejemplo, PDAs). Otra aplicación es la comunicación entre los periféricos de la computadora (por ejemplo, para propósitos de configuración). (Ilyas & Ahson, 2004)

El interfaz de Comunicación de Campo Cercano y el Protocolo -2 (NFCIP-2) especifican el mecanismo de selección de modo de comunicación (ECMA 352). Este protocolo distribuye la ubicación todos los dispositivos NFCIP-1, ISO, 14443 e ISO 15693 operen a 13,56 Mhz, pero con diferentes protocolos. Está especificado que NFCIP-2 los dispositivos dóciles puedan entrar en cada uno de estos tres modos de comunicación y son diseñados para no perturbar otros campos de RF a 13,56 Mhz. (Ilyas & Ahson, 2004)

Código Electrónico del Producto (EPC)

EPC fue desarrollado por la Auto ID (La Identificación automática) Centro del MIT. La estandarización está ahora dentro de la responsabilidad de EPCglobal que es una especulación entre EAN Internacional y el Consejo de Código Uniforme (UCC) [EPCglobal 2003]. El tan llamado red EPC está compuesto de cinco elementos funcionales:

- El Código Electrónico del Producto es un número de 96 Bits identificando el número de la versión de EPC, dominios, clases de objeto y los casos individuales (Quantifying the value of RFIDand the EPC Global Architecture Framework in Logistics, 2012).

- EPC evolucionó del ampliamente usado EAN-UCC (European Article Numbering / Universal Code Council) código de barras que identifica los productos, pero no los objetos individuales.

- Un Sistema de Identificación que consiste de etiquetas de RFID y lectores. Grupo de etiquetas 0 ofrece sólo un programa empresarial EPC y las etiquetas de la clase más alta proporcionan funcionalidades adicionales, por ejemplo, las funciones de seguridad. La Auto-ID Center publicó una especificación de protocolo para las etiquetas de Clase 1 en la banda HF (compatible con ISO 15693 y ISO 18000-3), y etiquetas de Clase 0 y 1 en la banda UHF [Auto-ID Center 2003a, 2003b, 2002a]. Hay discusiones continuas sobre normalización de las especificaciones de la EPC banda UHF y el estándar ISO 18000-6.

- El Savant Middleware ofrece "tratamiento de Módulos o Servicios" reducir carga y tráfico de la red dentro de los sistemas back-end. Puede realizar varias tareas relacionadas a la información de la etiqueta adquirida (Ilyas & Ahson, 2004).

- El Servicio de Denominación de Objeto (ONS) es un servicio de conexión de red similar al Servicio del nombre de Dominio (DNS). Con ONS, el Código Electrónico del Producto puede unirse a la información detallada del objeto. Los servidores de ONS regresan a la dirección IP del servicio de información EPC el cual guarda la información relacionada (Ilyas & Ahson, 2004).

- El lenguaje físico Markup (PML) es basado en XML y provee de un Standard de representación de información desde la red EPC (Ilyas & Ahson, 2004).

- Hay discusiones en marcha sobre la armonización del EPC y del ISO 18000 para la banda de frecuencia de UHF. Esto sería notado por aquella especificación global EPC como un complemento de los sistemas RFID incluidas las aplicaciones de capas la cual no es el caso de ISO 1800.

Seguridad de la tecnología RFID

La radio comunicación entre transpondedores RFID y lectores provoca, como básicamente todas las tecnologías inalámbricas, un número de problemas de seguridad. Objetivos fundamentales de la seguridad en información, tales como confidencialidad, integridad, disponibilidad, autenticidad, autorización, no rechazo (aceptación) y anonimato frecuentemente no son alcanzados a menos que mecanismos de seguridad especial sean integrados dentro del sistema. (Ilyas & Ahson, 2004)

El aspecto de privacidad ha ganado especial atención por los sistemas RFID. Consumidores pueden llevar objetos con transpondedores de comunicación silenciosa incluso sin la existencia de etiquetas. Etiquetas pasivas usualmente envían su identificador sin la verificación de seguridad complementaria cuando están potenciados por ondas electromagnéticas desde un lector. La información ID puede también ser enlazada a otros datos idénticos y a localización de información. Los

consumidores podrían emplear un lector personal para identificar etiquetas en sus entornos, pero el amplio número de diferentes modelos (patrones, criterios) puede traer esta dificultad. Las compañías están enfrentando los miedos de los clientes y los problemas de privacidad pueden llegar a ser más allá un mayor obstáculo para la proliferación de RFID. Hay sugerencias para una política estructural. (Ilyas & Ahson, 2004)

Propiedades de la Seguridad:

Confidencialidad

La comunicación entre lector y etiqueta no está protegida en muchos de los casos (a excepción de algunos sistemas de altas-salidas ISO 14443). Las personas que escuchan a escondidas (curiosos) pueden luego escuchar si hay una proximidad inmediata. El canal siguiente desde el lector a la etiqueta tiene un largo rango y es más riesgoso que el canal anterior. Además, la memoria de la etiqueta puede ser leída si el acceso al control no es implementado. (Ilyas & Ahson, 2004)

Integridad

Con excepción de los sistemas de alta-salida ISO 14443 que usan mensajes de códigos de autenticidad (MACs), la integridad de la información transmitida no puede ser asegurada. (CRCs) son frecuentemente empleadas sobre la interface de comunicación, pero protegen solo contra fallas aleatorias. Además, la memoria de etiqueta escribible puede ser manipulada si el control de acceso no es implementado. (Ilyas & Ahson, 2004)

Disponibilidad

Algunos sistemas RFID pueden fácilmente ser perturbados por una interferencia de frecuencia. Pero, el rechazo del servicio es un ataque factible también para las altas capas de comunicación. Los llamados "bloques RFID" en singular etiquetas expansivas (anticolisión) mecanismos para interrumpir la comunicación de un lector con todo o con una etiqueta específica. (Ilyas & Ahson, 2004)

Autenticidad

La autenticidad de una etiqueta está en riesgo desde el identificador único (UID) de una etiqueta puede ser manipuladas. Las etiquetas en general no son resistentes. Engañado o manipulado. La etiqueta es en general no resistente a sabotajes. (Ilyas & Ahson, 2004)

Anonimato

El único identificador puede ser usado para rastrear a una persona o a un objeto que porta una etiqueta en tiempo y espacio. Este no puede ser avisado por la persona rastreada. La información recopilada puede ser anexada y enlazada en orden para generar un perfil personal. Algo similar ocurre en aplicaciones suplementarias donde la búsqueda de productos indeseados es posible. La lectura automatizada de etiquetas permite el conteo de objetos ejemplo (banco de objetos con etiquetas adjuntas) que pueden ser indeseados. (Ilyas & Ahson, 2004)

Mecanismos de Seguridad y su Propósito

Efectivamente los mecanismos de seguridad pueden brindar protección de amenazas. Pero estas podrían ser tomadas entre aquellas que el propósito principal de la tecnología RFID es la realización de bajo costo e identificación automatizada así los mecanismos de seguridad estándar pueden duramente ser implementadas porque su complejidad relativa comparada con etiquetas forzadas calculando recursos. A continuación describiremos la implementación y propósito de los mecanismos de seguridad RFID. (Ilyas & Ahson, 2004)

Control de Acceso y Autentificación

Algunas etiquetas implementan mecanismos de control de acceso para sus memorias de lectura y escritura. El acceso para el UID es más abierto y lo mejor de los procedimientos de control de acceso varían. (Finkenzelle, 2003)

Las etiquetas RFID no protegen el identificador único con raíces mencionadas en las citas de privacidad. Algunas etiquetas (la ISO 14443 y etiquetas MIFARE) fuerzan los mecanismos de autentificación antes de entregar el acceso de lectura y escritura en bloques específicos de memoria. Aquí, cada uno de una simple autentificación de password o una unilateral o bilateral respuesta de cambio de autentificación (la ISO 9798-2) con claves simétricas están actualmente en la práctica. La autorización puede ser granular y dependiente en claves que son usados por el solicitante (por ejemplo, el lector.) Para la próxima parte cuatro del estándar ISO 15693 se producen

cambios una respuesta de cambio en el protocolo de autentificación los transponders cumplen con la ISO; que pueden ser empleadas en aplicaciones con niveles de autentificación de contactos por medio de smart card. (Finkenzelle, 2003)

Los riesgos de seguridad y privacidad inducidos por los identificadores de etiquetas no protegidas dan razones para un número de contribuciones y protocolos. Así los recursos construidos con etiquetas de bajo costo tienen que ser consideradas. (Finkenzelle, 2003)

Una opción podría ser para destruir las tarjetas después de haber sido usadas, por ejemplo, en los puntos de venta. El comando destroy de un password protegido sido integrado en las especificaciones Electronic Product Code (EPC). Pero este podría también destruir recursos importantes y borrar información la cual puede ser importante. El consumidor o las aplicaciones domésticas pueden por ejemplo obtener información relacionada de productos o las etiquetas podrían ser usadas para reciclar. Inventado "RFID blocker tag" el cual explota etiquetas para la singularización de protocolos en orden para interrumpir la comunicación con todas las etiquetas con un ID específico. (Finkenzelle, 2003)

Encriptación y Autentificación del Mensaje

Algunos sistemas high-end de RFID (basados en ISO 14443 y MIFARE®) pueden encriptar y autentificar el tráfico de los datos con protocolos propietarios. Desde el intercambio de datos

apartado de los identificadores no juega un papel importante en los sistemas de RFID, la mensajería segura no se mira usualmente como cuestión clave. El encriptado de los bloques de la memoria puede ser revisado en la capa de aplicación y es transparente para la etiqueta de RFID. El identificador Único (UID) es generalmente inalterable y muchos transponders de RFID (ejemplo. las etiquetas ISO 15693 o 18000-3) permiten una escritura permanente de los bloques de la memoria. Esto puede asegurar integridad de datos pero, por supuesto, no autentificación del mensaje. (Ilyas & Ahson, 2004)

Los tiempos de validación del acceso manual con el que contaba la UTEQ fue realizada durante los días lunes 06, martes 07, miércoles 08, jueves 09 y viernes 10 de enero del 2014, estos tiempos fueron considerados al momento de ingresar a los predios universitarios a bordo del auto Nissan placa GRZ 9958, en horario en los que se tenía una gran afluencia vehicular es decir a las ocho de la mañana.

Una vez implementado el sistema de autenticación por radiofrecuencia se procedió a medir los tiempos de validación durante los días jueves 16 y viernes 17 de enero del 2014, las muestras no deberían variar, pero se obtuvo una pequeña variación por motivo de errores humano al momento de acercar la credencial para su validación, los factores climáticos es otro de los motivos para provocar diferentes lectura por cuanto las credenciales se humedecen dificultando su lectura.

El sistema de monitoreo que contaba la UTEQ, consistía en entregar un tiquet, que en muchas ocasiones los vigilantes

obviaban para evitar la congestión vehicular y debía ser entregado al abandonar los predios universitario.

Determinamos los tiempos que tardaban en constatar que un vehículo abandonó la institución es impreciso, dado que el personal procedía a la revisión de los tiquets emitidos manualmente, sin considerar que no a todos los usuarios se les entregaba tiquet, es decir no se puede establecer en qué hora ingreso o salió de los predios Universitarios.

Para el sistema de control de acceso se desarrolló una aplicación de escritorio basada en C# el mismo que interactúa con una base de datos desarrollada en SQL el cual permite registrar tiempo de ingreso i/o egreso de cada vehículo que requiere hacer uso de los parqueaderos del campus universitario, en conclusión se pueden generar reportes en un tiempo aproximado de 10 segundos.

Además se realizó pruebas con los docentes que poseen vehículo de la carrera de Ingeniería en Telemática, se los escogió a ellos por tener mejor destreza para interactuar y evaluar con nuevas tecnología, los usuarios no tuvieron inconveniente alguno al momento de hacer uso de la autenticación por radiofrecuencia para acceder a los parqueaderos de la UTEQ.

En el proyecto acceso del parque automotor empleando la tecnología de autenticación por radio frecuencia para la evaluación de las variables dependientes y su posterior comprobación de la hipótesis se empleó el diseño pre test – post

test, por cuanto es el que más se ajusta al método cuasi experimental mencionado en el presente proyecto.

Radica en verificar un *cambio;* a los sujetos se les mide *antes* y *después* de un tratamiento o experiencia en aquella variable o variables en las que se espera que cambien. Como no hay grupo de control no se trata de un diseño experimental en sentido propio, aunque es un diseño que puede ser muy útil a pesar de sus limitaciones.

GRUPO EXPERIMENTAL: O1  **X**  **O2**

INDICADOR	DEFINICIÓN
O1	Pretest o primera observación se lo realizó al obtener los tiempos de validación del acceso vehicular con el sistema manual y se estudió los niveles de seguridad que este poseía
X	Es el efecto que la Tecnología RFID causa en la variable dependiente que es el control de acceso del parque automotor
02	Post-test, o segunda medida u observación, posterior a X. se lo realizó al obtener los tiempos de validación del acceso vehicular con el sistema de autenticación por radiofrecuencia y se estudió los niveles de seguridad que este poseía

Fuente: INVESTIGACIÓN EXPERIMENTAL, DISEÑO Y CONTRASTE DE MEDIAS
Autor: Pedro Morales Vallejo

Tabla 7: *Indicadores del Pre test-Post test*

La prueba de hipótesis: es un procedimiento, basado en evidencia de la muestra y en la teoría de las probabilidades, usado para determinar si la hipótesis es una afirmación razonable y debería no ser rechazada o si no es razonable debería ser rechazada.

Para la comprobación de la hipótesis de este trabajo de investigación se empleó la distribución T-studet., está se basa en el cálculo estadísticos descriptivos previos, el número de observaciones, la media y la desviación típica de cada grupo.

Fórmula:

$$t = \frac{\bar{X}_1 - \bar{X}_2}{\sigma\rho\sqrt{\frac{1}{N_1} + \frac{1}{N_2}}}$$

Dónde:

t = valor estadístico de la prueba t-student

X_1 = Valor promedio del grupo 1

X_2 = Valor promedio del grupo 2

σρ = Desviación estándar ponderada de ambos grupos

N_1 = tamaño de la muestra del grupo 1

N_2 = tamaño de la muestra del grupo 2

Ecuación para obtener la desviación estándar ponderada:

$$\sigma\rho = \sqrt{\frac{SC_1 + SC_2}{N_1 + N_2 - 2}}$$

Dónde:

σρ = Desviación estándar ponderada de ambos grupos

SC = suma de cuadrados de ambos grupos

N = tamaño de la muestra

Planteamiento de la Hipótesis.

Para la comprobación de la hipótesis del presente trabajo de investigación, se realizaron dos pruebas, la primera radicó en el sistema de acceso manual que poseía la UTEQ, y la segunda se efectuó con la implementación de la tecnología de autenticación por radiofrecuencia, para calcular el tiempo de validación del acceso vehicular.

Se realizaron diez muestras en ambos casos los que se encuentran tabulados en la tabla 3 del presente capítulo,

Acceso Manual (seg)	**Acceso Rfid (seg)**	$(X_1 - \bar{X}_1)$	$(X_1 - \bar{X}_1)^2$	$(X_2 - \bar{X}_2)$	$(X_2 - \bar{X}_2)^2$

40	4	-12,2	148,84	-0,4	0,16
49	4	-3,2	10,24	-0,4	0,16
56	4	3,8	14,44	-0,4	0,16
57	5	4,8	23,04	0,6	0,36
48	4	-4,2	17,64	-0,4	0,16
60	6	7,8	60,84	1,6	2,56
56	4	3,8	14,44	-0,4	0,16
45	4	-7,2	51,84	-0,4	0,16
49	5	-3,2	10,24	0,6	0,36
62	4	9,8	96,04	-0,4	0,16
52,2	4,4		44,76		0,44

Fuente: Investigación
Autor: Ing. Ángel Torres Q

Realizados los cálculos, se procede a consultar la tabla de la distribución T-student (anexo 3) y se realiza la prueba con 18 grados de libertad a un nivel de significancia de 0,05 donde se encuentra una razón de t igual a 1,7341.

La razón calculada es de 67,435 es mucho mayor que 1,7341, con lo que demuestra que la diferencia entre las pruebas realizadas es mayor al valor que se requiere para rechazar la hipótesis nula con un nivel de significancia de 0,05 por lo tanto, los datos son lo suficientemente significativo para aceptar la hipótesis alternativa.

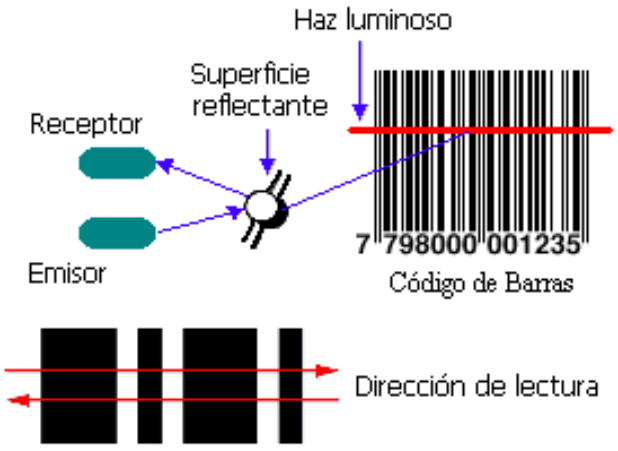
La tecnología RFID se encuadra dentro del grupo de los sistemas de identificación automática, empleado para realizar el seguimiento de productos, artículos, objetos o seres vivos, además las tecnologías para autenticación son ampliamente conocidas y aceptadas en el Ecuador, sin embargo la tecnología RFID es la llamada a sustituirlas, por lo que se realiza

un análisis comparativos de las tecnologías relacionada a la validación de credenciales de acceso.

Código de Barras frente RFID

A finales del siglo veinte el código de barras ha sido el principal medio de identificación automática de productos en la cadena de abastecimiento. Los códigos de barra han probado ser muy efectivos, no obstante, también tienen limitaciones.

Las atribuciones claves a ser consideradas cuando se compara RFID con el código de barras giran entorno de la capacidad de legibilidad, la rapidez en la lectura, la durabilidad de la etiqueta, la cantidad de información, la flexibilidad de la información, los costos de la tecnología y los estándares. Una migración hacia RFID involucra un conjunto de consideraciones, siendo una de las principales si el código de barras debe ser complementario o si será reemplazado definitivamente. (Telectrónica, 2009)



Fuente:
http://www.monografias.com/trabajos11/yantucod/yantucod.shtml/

Los lectores ópticos de código de barra requieren una verificación visual directa. El lector indica cuándo obtiene una buena lectura dentro de su rango, y una mala lectura es inmediatamente asociada con una etiqueta y un ítem específicos. Este tipo de relaciones es establecido uno a uno. La lectura por RFID no requiere línea de vista para obtener la información de la etiqueta.

La señal de la frecuencia de radio (RF) es capaz de viajar a través de la mayoría de los materiales. Esto es particularmente ventajoso en las operaciones de recepción de mercaderías en depósitos y en aplicaciones donde la información debe ser recolectada a partir de ítems que tengan una orientación heterogénea. Un lector RFID es capaz de distinguir e interactuar con una etiqueta individual a pesar de que múltiples etiquetas se encuentren dentro del rango de lectura dado. No obstante, la discriminación de etiquetas no provee la ubicación física absoluta de un ítem que sí ofrece el código de barras cuando el objetivo es un punto específico en la línea de empaque.

Además las etiquetas RFID pueden ser leídas más rápidamente que las etiquetas de código de barras en grados teóricos de 1.000 por segundo o más. Esto supera ampliamente la velocidad de lectura a nivel de cada unidad que posee el código de barras. (Telectrónica, 2009)

Para mayor protección, las etiquetas RFID pueden ser insertadas en sustratos de plástico duro u otros materiales. A pesar de que son significativamente más duraderas que las etiquetas de papel de código de barra, ambas dependen del adhesivo que

las mantiene intactas y pegadas a un ítem. La naturaleza de las etiquetas RFID les permite perdurar más que las de código de barras. El código de barras puede ser impreso en una tarjeta plástica pero está tiende a perder su color por el uso constante, lo que altera su estructura y dificulta su lectura.

La desventaja de una etiqueta RFID es el punto de unión de la antena con el chip. Un corte que dañe el punto de unión inutilizará la etiqueta, mientras que el código de barras solo sería levemente degradado. (Telectrónica, 2009)

El código UPC identifica la clasificación de un ítem genérico a través de la asignación de la información en una longitud de 12 dígitos, pero EPC permite identificar un ítem en forma individual a través de un número serial asignado. Los tags RFID de alto valor contendrán varios kilobits de memoria (miles de caracteres).

Por la capacidad de almacenamiento de información algunas etiquetas RFID soportan la combinación de palabras claves que pueden hacerlas ilegibles para los sistemas de lectura que no usan las claves de acceso del código EPC.

Los principales costos están representados por el equipamiento (impresoras, lectores, antenas y tags) y por los servicios profesionales (relevamientos, ingeniería de proyectos, instalación y puesta en marcha, capacitación de los usuarios).

Características	Código de barras	RFID
Capacidad	Espacio limitado	Almacena mayor cantidad de información
Identificación	Estandarizada	Unívoca por producto
Actualización	Solo lectura	Lectura/Escritura
Flexibilidad	Requiere línea de visión para la lectura	No requiere línea de visión para la lectura
Lectura	Una lectura por vez	Lectura simultanea
Tipo de lectura	Lee sólo en superficie	Lee a través de diversos materiales y superficies
Precisión	Requiere intervención humana	No requiere intervención humana, 100% automático.
Durabilidad	Puede dañarse fácilmente	Soporta ambientes agresivos (interperie, químicos, humedad, temperatura).

Fuente: (Telectrónica, 2009)
Autor: Ing. Ángel Torres Q

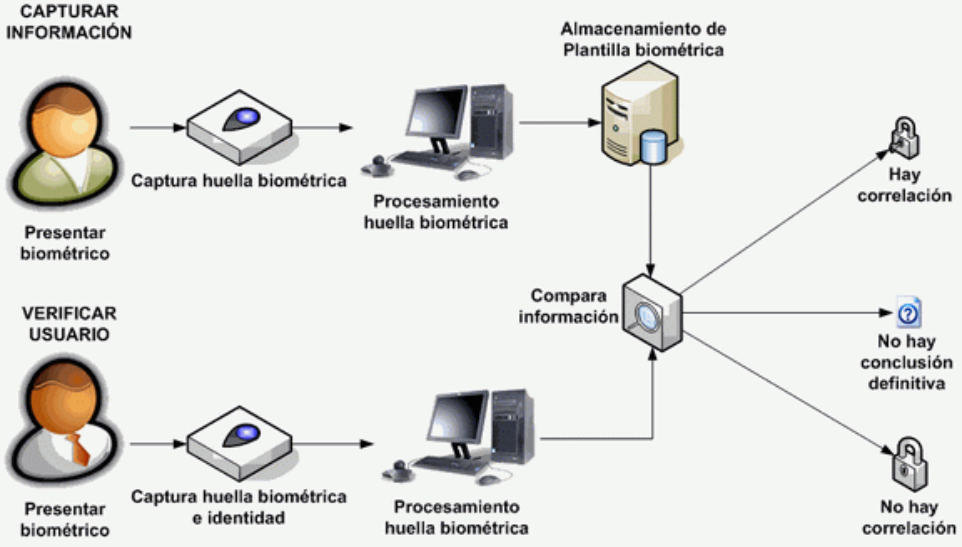
Reconocimiento Óptico de Caracteres (OCR)

El sistema OCR (Optical Character Recognition) fue utilizado por primera vez en la década de los 60.Los sistemas OCR identifican automáticamente símbolos o caracteres, a partir de una imagen para almacenarla en forma de datos. Algunas de sus aplicaciones, entre otras, son: reconocimiento de matrículas a

través de radares, registro de cheques por parte de los bancos, etc. Los inconvenientes de este sistema de identificación residen en su alto precio y la complejidad de los lectores en comparación con otros sistemas de identificación. (INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN, 2013)

Sistemas Biométricos

Son sistemas que identifican personas por comparación de características unívocas[7]. Su principal cualidad es que transforman una característica biológica, morfológica o de comportamiento del propio individuo, en un valor numérico y lo almacenan para su posterior comparación.



Fuente: http://www.monografias.com/trabajos57/huellas-lofoscopicas/huellas-lofoscopicas3.shtml

[7] La tecnología tiene inherente ciertas tasas de error

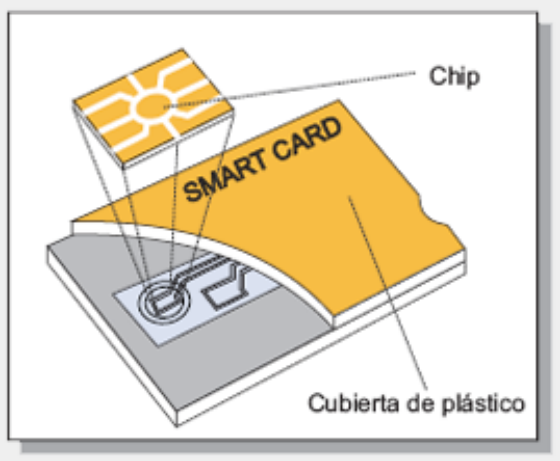
Se puede hablar de sistemas identificadores por huella dactilar, por voz, por pupila, por forma de la cara, por forma de la oreja, por forma corporal o por patrón de escritura, entre otros. En sistemas de autenticación se suelen utilizar diferentes factores como por ejemplo "lo que tengo (Ej.: una tarjeta), lo que sé (Ej.: un número PIN) y lo que soy (Ej.: mi huella dactilar)". Los sistemas biométricos representarían el tercer factor: "lo que soy". (INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN, 2013)

La identificación biométrica ofrece una ventaja significativa, dado que bajo este sistema, se identifica explícitamente a la persona, no así a alguna credencial u otro objeto. La razón por la cual no es aplicable para ciertos problemas se produce porque no existen sistemas que ofrezcan una confiabilidad cercana al 100 por ciento. La mayoría de los sistemas de este tipo tienen una eficiencia menor a lo deseable. Otra desventaja de este tipo de sistemas es que son más costosos. (Sánchez, 2008)

Tarjetas Inteligentes

Una tarjeta inteligente o smart card, es un sistema de almacenamiento electrónico de datos con capacidad para procesarlos (microprocesador). Por seguridad está instalado dentro de una estructura de plástico similar, en forma y tamaño, a una tarjeta de crédito. Una de las principales ventajas de las tarjetas inteligentes es que aportan protección frente a posibles accesos indeseados ya que poseen características de

seguridad avanzadas y además son más económicas. (INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN, 2013)



Fuente: http//www.scssa.com.ar/tarjetas-inteligentes.htm

	Código de Barras	**Memorias de contacto**	**Biometría**	**OCR**	**Tarjetas Magnéticas**	**Tarjetas inteligentes**	**RFID**	
							PASIVO	ACTIVO
Modificación de datos	No modificable	Modificable	No modificable	No modificable	Parcialmente modificable	Modificable	Modificable	Modificable
Seguridad de datos	Seguridad mínima	Altamente seguro	Altamente seguro	Seguridad media	Seguridad media	Alta seguridad	Rango de baja a alta seguridad	Alta seguridad
Cantidad típica de datos(byte)	1 a 100	De 8Mb en adelante	Ninguno	Ninguno	16 a 64K	1MB	Alrededor de 64 Kbyte	Alrededor de 8MB

Coste	Muy Bajo	Alto (más de $1 por etiqueta)	Ninguno	Medio	Medio	Medio	Medio (Unos 0.25 por tag)	Muy alto (más de 10 $ por tag)
Estándares	Estable implantado	Propietario, sin estándar	Ninguno	Estable	Estable implantado	Estable implantado	Con estándares en fase de implantación	Propietario y estándares abiertos
Desgaste	Limitado	Limitado	Indefinido	Limitado	Limitado	Limitado	Ninguno	Ninguno
Distancia de lectura	Pocos centímetros	Contacto necesario	Contacto directo	Contacto directo	Contacto directo	Contacto directo	Del orden de 1 metro	Del orden de 100 metro
Interfaz	Lectura óptica directa	Contacto	Contacto	Contacto	Contacto	Contacto	Sin barrera aunque puede haber interferencias	Sin barrera aunque puede haber interferencias
Susceptible a la sucieda d líquidos	Alto	Alto	Ninguno	Medio	Posible	Posible	Ninguno	Ninguno
Influencia en la dirección y posición	Ligero	Ligero	Muy Alto	Alto	Muy Alto	Ligero	Ninguno	Ninguno

Fuente: (Percy E. De la Cruz Vélez de Villa, 2010)

Prototipo de control de Acceso

Realizado el análisis en la sección 4.1 sobre las tecnologías acceso, se determinó que la autenticación por RFID, es la que más se ajusta a las necesidades de la UTEQ, por ser fácil de implementar y aportará en el control y monitoreo del parque automotor de la institución.

Para implementar el prototipo se realizó la adquisición de dos lectores RFID de marca D-LOGIC con doce tags (anexo 11) que garantice un óptimo funcionamiento acorde a las condiciones en las que va a trabajar, además se consiguió dos cables de 10 metros, que permite conectar los lectores con el computador en el que se instalará la aplicación para la gestión de la información.

Se diseñó una estructura mecánica que permita el movimiento de un pívot para garantizar la aprobación o no del acceso vehicular, el movimiento lo realiza a través de un motor de corriente continua de 12 v mediante la ley de la palanca.[8] El diseño de las barreras se lo muestra en el anexo 09.

Empleando Visual estudio 2010 como lenguaje de programación se desarrolló una aplicación de escritorio que permite validar, administrar y configurar los tags RFID, haciendo uso de una base de datos desarrollada en SQL (anexo 07), el que constan información relevante de los docentes empleados y trabajadores de la UTEQ.

[8]En Física, La ley de la palanca es la que relaciona la fuerza de una palanca en equilibrio.

Con el prototipo en funcionamiento en la garita principal de la UTEQ (anexo 09) se procedió a realizar las pruebas con los docentes de la carrera de Ingeniería en Telemática que hacen uso de los parqueaderos de la institución.

Conclusión Parcial

Al realizar un análisis cualitativo de las tecnologías que permiten automatizar el control de acceso vehicular se determinó que la autenticación por radio frecuencia es la adecuada para ser instalada en el campus Ing. Manuel Haz Álvarez por ser relativamente más económica frente a un sistema de reconocimiento de caracteres pero con mejores prestaciones que aquellas de lectura códigos de barras o de tarjetas magnéticas en el cual la vida útil de estás son menores.

Además, basados en la distribución T-student, se analizó los cálculos determinando que se acepta la hipótesis alterna, donde $\mathbf{X_1 > X_2}$, es decir que en base a los resultados obtenidos y calculador de la comprobación de la hipótesis podemos establecer que la tecnología de autenticación por radiofrecuencia, incide positivamente en el control de acceso del parque automotor al campus Ing. Manuel Haz Álvarez, es decir que se puede dar por aceptada la hipótesis alterna.

Un sistema de control de acceso basado en la autenticación por radiofrecuencia resulta beneficioso dado que la validación del ingreso es casi inmediata y con esto evitamos congestión vehicular en el ingreso de los predios universitarios.

El análisis comparativo realizado como consta en la *Tabla 6: Cuadro Comparativo de las tecnologías de Identificación* Automática seleccionados por comparación, se determinó que la técnica más efectiva de autenticación es la RFID dado que los costos de implementación no son tan elevados en relación a los beneficios para la gestión de la información que requiere la institución. La aplicación de escritorio facilita la administración y toma de decisiones en lo relacionado a la validación del control de acceso vehicular y ha permitido aumentar los niveles de seguridad, por cuanto los usuarios poseen una tarjeta o credencial RFID, misma que es intransferible y única, es decir imposible de clonar; sin tener la tarjeta el control de ingreso no permitirá el paso del vehículo sea este para ingresar o salir de los predios universitarios.

El sistema electrónico RFID controla y ordena el ingreso del parque automotor de la UTEQ, puesto que se lleva un control del número de plazas disponibles en los parqueaderos internos de la institución, si no existiera lugar disponible el sistema no lo deja ingresar.(Anexo 10, figura 22)

BIBLIOGRAFÍA

(2012). En D. Uckelmann, *Quantifying the value of RFIDand the EPC Global Architecture Framework in Logistics* (pág. 143). Stugard: Springer.

Anguera, J., & Perez, A. (2011). *Teoría de Antenas.*

Balanis, C. A. (1997). *Antenna Theory, Analisis and desing.* New York: John Wiley & Sons INC.

Coulter., S. R. (1996). *Administración.* México.: Quinta Edición.

Fernandéz Sampieri, R., & Hérnandez Collado, C. (1997). *METODOLOGÍA DE LA INVESTIGACIÓN.*

Finkenzelle, K. (2003). *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication.* wiley.

Ilyas, M., & Ahson, S. (2004). *RFID HANDBOOCK, Aplications Technology Security, and Privacy.* Estados Unidos de America: CRC Press.

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. (2013). *Guía sobre seguridad y privacidad.* España: CELARAYN, s.a.

Montenegro, G. A., & Marchesin, A. E. (2007). *SISTEMA DE IDENTIFICACIÓN POR RADIOFRECUENCIA (RFID.*

Percy E. De la Cruz Vélez de Villa, M. R. (2010). Radiofrecuencia de identificación (RFID):. *Revista de investigacion de sistemas informáticos* , 77-86.

Portilla, J. I., Bermejo, A. B., & Bernardo, A. M. (2008). *TECNOLOGIA DE IDENTIFICACIÓN POR RADIOFRECUENCIA (RFID) Aplicaciones en el ámbito de la Salud.*

Sánchez, J. A. (2008). *Sistema de Control de Acceso con RFID.* Mexico.

SYSCOM. ((2008).). *Introducción a los sistemas de control de acceso.* Obtenido de Introducción a los sistemas de control de acceso: (2008).

Telectrónica. (2009). *INTRODUCCIÓN A LA IDENTIFICACIÓN POR RADIOFRECUENCIA*.

Transcore, S. (2013). *Sistema de Gestión y Administración para Peaje-Telepeaje*. http://www.sictranscore.com.ar/Peaje.html.

Vallejo, P. M. (2013). *Investigación Experimental, Diseño y Contraste de Medias.*

- SISTEMA DE IDENTIFICACIÓN POR RADIOFRECUENCIA (RFID); Guillermo A. Montenegro, Antonio E. Marchesin; 2007;
- INTRODUCCIÓN A LA IDENTIFICACIÓN POR RADIOFRECUENCIA; Telectrónica
- TEORIA DE ANTENAS, J. Anguera, A. Perez, 2011
- APLICACIONES DEL RFID COMO HERRAMIENTA PARA EL PROCESO DE MARKETING; Rodrigo Ramírez, Miguel Henríquez; 2006
- METODOLOGÍA DE LA INVESTIGACIÓN; M en C Roberto Fernández Sampieri, Dr. Carlos Hernández Collado, Dra., Pilar Baptista Lucio; McGRAW-HILL; 1997.
- The global Language of business. Consulta: 06 de Noviembre del 2012.

http://www.12manage.com/methods_rfid_technology.html

Descubre tu próxima lectura

Si quieres formar parte de nuestra comunidad,
regístrate en **https://www.grupocompas.org/suscribirse**
y recibirás recomendaciones y capacitación

compÁs

Grupo de capacitación e investigación pedagógica

@grupocompas.ec
compasacademico@icloud.com

compAs
Grupo de capacitación e investigación pedagógica

@grupocompas.ec
compasacademico@icloud.com

ISBN: 978-9942-33-193-9

@grupocompas.ec
compasacademico@icloud.com

compAS
Grupo de capacitación e investigación pedagógica