

Prototipo de Control de Acceso Peatonal al Campus de la Corporación Universitaria
Lasallista

Trabajo de grado para optar por el título de ingeniería informática

Diana Shirley Morales Tejada

Asesores

Cesar Ruiz Jaramillo

Ingeniero Informático

Corporación Universitaria Lasallista

Facultad de Ingeniería

Ingeniería Informática

Caldas Antioquia

2012

Tabla de contenido

Índice de Figuras	6
Índice de Tablas	8
Glosario	10
Resumen	11
Justificación	16
Objetivos	17
Objetivo General	17
Objetivos Específicos	17
Marco Teórico	18
Código de Barras	18
Tarjetas Magnéticas	20
Sistemas Biométricos	21
Tecnología RFID	22
Componentes Hardware	23
Componentes Software	23
Transponder, Tag O Etiquetas	24
Etiquetas Pasivas	25
Etiquetas Activas	25
Etiquetas Semi-Pasivas	26

Lector RFID	27
Antena	28
Rfid Middleware	29
Aplicación del computador	29
Caracterización de un sistema RFID	30
Ventajas de la identificación por radiofrecuencia	32
Ejemplo de sistemas basados en tecnología RFID	35
TIP (Tarjeta Integrada Personal)	35
Metodología	39
Análisis y Diseño para el prototipo de control de acceso a la Corporación Universitaria Lasallista	39
Modelo de dominio.....	39
Cómo se desea el funcionamiento.....	40
Análisis y diseño del Software.....	42
Diagrama Modelo De Dominio.....	42
Diagrama caso de uso SCA	44
Descripción casos de uso.....	46
Administrar Tarjeta	47
Administrar Persona	52
Consultar Información de acceso	56
Validar Acceso.....	58

Diagramas de secuencia del sistema (DSS)	59
Administrar Tarjeta	60
Administrar persona	61
Consultar Accesos	62
Validar Acceso	63
Diagramas de colaboración.....	64
Crear Persona	65
Actualizar Persona.....	66
Eliminar Persona	67
Crear Tarjeta	67
Actualizar Tarjeta	68
Eliminar Tarjeta	68
Consultar Acceso.....	69
Validar Acceso	69
Detalles de la metodología Utilizada en el análisis para el desarrollo del sistema	70
Componentes de Hardware	71
Componentes Software.....	71
Software de administración.....	71
Software de validación y registro de acceso.	73
Software Recolector de Datos	75

Resultados	76
¿Qué sugerencias nos pueden aportar al sistema?.....	81
Conclusiones.....	82
Recomendaciones.....	83
Bibliografía.....	85

Índice de Figuras

Figura 1 Tecnología Código de Barras.....	19
Figura 2 Tecnología de Identificación por Banda Magnética.....	20
Figura 3 Tecnología Biométrica	22
Figura 4 Tarjetas MIFARE PVC	24
Figura 5 Lector USB TCR-501.....	27
Figura 6 Antena RFID.....	28
Figura 7 Comunicación entre componentes de un sistema RFID	32
Figura 8 Descripción Prototipo control de acceso	42
Figura 9 Diagrama Modelo de Dominio	43
Figura 10 Diagrama Casos de uso.....	45
Figura 11 Diagrama de Secuencia Administrar Tarjeta	60
Figura 12 Diagrama de Secuencia Administrar Persona	61
Figura 13 Diagrama de Secuencias Consultar Acceso	62
Figura 14 Diagrama de Secuencia Validar Acceso.....	63
Figura 15 Diagrama de Colaboración Crear Persona	65
Figura 16 Diagrama de Colaboración Actualizar Persona	66
Figura 17 Diagrama de Secuencia Eliminar Persona	67
Figura 18 Diagrama de Colaboración Crear Tarjeta	67

Figura 19 Actualizar Tarjeta Diagrama de Colaboración.....	68
Figura 20 Diagrama de Colaboración Eliminar Tarjeta	68
Figura 21 Diagrama de Colaboración Consultar Acceso	69
Figura 22 Diagrama de Colaboración Validar Acceso.....	69
Figura 23 Funcionamiento Sistema Control de Acceso	70
Figura 24 Administración de Personas.....	72
Figura 25 Administración de Tarjetas	72
Figura 26 Reporte de Accesos	73
Figura 27 Aplicación de Escritorio (Acceso Autorizado)	74
Figura 28 Aplicación de Escritorio (Acceso No Autorizado).....	74
Figura 29 Registro Acceso Visitantes	75
Figura 30 Muestra para la ejecución de las pruebas.....	77
Figura 31 Cantidad de accesos por persona.....	78
Figura 32 Estadísticas de ingresos entre empleados y visitantes.	79
Figura 33 Registro de visitantes.....	80

Índice de Tablas

Tabla 1 Descripción Frecuencias RFDI	31
Tabla 2 Tabla comparativo entre tecnologías de control de acceso	34

Tabla de Apéndice

Apéndice A - Manual Instalación Lector USB TCR-501

Apéndice B - Manual Registrar Tarjeta

Apéndice C - Manual De Usuario

Glosario

RFID: Identificación por tecnología de Radio Frecuencia.

Lector: Son los responsables de la lectura de las etiquetas RFID en un rango de acción determinado, y de la comunicación con el sistema que controla el proceso.

Tag o etiqueta: Representa el dispositivo que contiene los datos en un sistema RFID, normalmente consiste en un elemento acoplador y un microchip electrónico; este solo se activa cuando hay una señal de radio frecuencia enviada por un lector dentro de una zona de interacción entre los componentes.

SCA: Sistema para el control de Acceso.

Resumen

Para la Corporación Universitaria Lasallista se hace necesario tener un sistema que controle de forma precisa y automática el ingreso de cualquier persona o vehículo, y el acceso a diferentes puntos de la misma como laboratorios, aulas, salas de informática, sala de profesores, biblioteca, etc. El sistema propuesto tiene en cuenta el rango de pertenencia de la persona que ingresa al plantel (administrativo, servicios, alumnos, profesores, visitantes), permitiendo un mayor nivel de la seguridad al interior del campus y propendiendo la agilidad en determinados procesos. Para dar solución a esta necesidad, se propone utilizar la tecnología llamada RFID (identificación por radio frecuencia) que permite dar control a gran variedad de aplicaciones como el ingreso a establecimientos, inventarios automáticos, verificación de calidad de productos, entre otras.

Lo que se pretende entonces es desarrollar un prototipo que pueda ser utilizado por la Corporación Universitaria Lasallista para el control de acceso en diferentes áreas del campus universitario inicial y prioritariamente en el acceso a la Corporación.

Para lograr este fin, se ha implementado un prototipo basado en tecnología RFID, la cual permite que el control de acceso a la Corporación sea más eficiente, rápido y confiable permitiendo que la seguridad dentro del campus se refuerce para lograr una seguridad más confiable por parte de las personas que hacen parte de ella.

La solución está compuesta por 3 módulos:

- ✓ Un software de administración de usuarios, administración de tarjetas y consulta de acceso.

- ✓ Un software de validaciones de usuarios y registro de accesos.
- ✓ Un software recolector de datos de los tag.

Palabras claves: Prototipo, Control, Acceso, RFID, Seguridad.

Summary

For the University Corporation Lasallista it becomes necessary to have a system that controls of precise and automatic form the revenue of any person or vehicle, and the access to different points of the same one as laboratories, classrooms, rooms of computer science, teachers' room, library, etc. The proposed system bears in mind the range of belonging of the person who enters to the nursery (administrative officer, services, pupils, teachers, and visitors), allowing a major level of the safety the interior of the campus and tending the agility in certain processes. To give solution to this need, it proposes to use the technology called RFID (identification for radio frequency) that allows to give control for great variety of applications as the revenue to establishments, automatic inventories, quality check of products, between others. What is claimed then is to develop a prototype that could be used by the University Corporation Lasallista for the control of access in different areas of the university initial campus and as a priority in the access to the Corporation.

To achieve this end, there has been implemented a prototype based on technology RFID, which allows that the control of access to the Corporation should be more efficient, rapid and reliable allowing that the safety inside the campus should be reinforced to achieve a more reliable safety on the part of the persons who do part of she.

The solution is composed by 3 modules:

- ✓ Software of users' administration, administration of cards and consultation of access.
- ✓ Software of users' validations and record of accesses.
- ✓ Software recollection of information of the tag.

Keywords: Prototype, Control, Access, RFID, Security.

El objetivo de esta investigación es encontrar un sistema alternativo, basado en tecnologías de identificación por radio frecuencia que ayuden a identificar las personas que ingresen al campus de la corporación, es por tanto que se desea comparar los sistemas que en la actualidad se utilizan en las industrias en la identificación de personal y así obtener el proceso más adecuado para la implementación de un prototipo que permita garantizar una seguridad más fuerte en la Corporación Universitaria Lasallista.

Principalmente el prototipo estará basado en controlar con mayor seguridad el ingreso peatonal al Campus de la Corporación, identificando las personas por el rol que desempeñen en la institución, privilegios y necesidades de la corporación, también está dentro del alcance apoyar a grupos externos al sistema en la consulta de reportes de ingreso, sea de visitantes o ingresos frecuentes de las personas que integran la comunidad Lasallista.

La metodología con la cual se desarrollara el proyecto de investigación está compuesta de aspectos como apoyo en investigaciones relacionadas con el control de acceso por medio de la tecnología por radio frecuencia (RFID) en industrias, establecimientos públicos y instituciones educativas esto con el fin de encontrar el proceso más adecuado para ser implementado en la corporación, esto en la parte de investigación de procesos. En la parte de análisis y diseño del prototipo se utilizaran metodologías de desarrollo de software entre las cuales están UML y la metodología adoptada por Craig Larman para el análisis y diseño de software basado en objetos, y para la implantación del sistema se tendrán en cuenta metodologías ágiles de desarrollo de software.

Justificación

Actualmente en la Corporación Universitaria Lasallista la seguridad está a cargo de una empresa de vigilancia privada, que cumple a cabalidad su función y que como otros procesos, este necesita de ayudas adicionales para lograr la perfección en su desarrollo y es por eso que hoy se trabaja en un proyecto de investigación orientado en el apoyo a la seguridad de la Corporación y así mejorar el sistema y garantizar mayor confianza en cuanto a seguridad a toda la comunidad que hace parte de la Institución.

Objetivos

Objetivo General

Implementar un prototipo, basado en tecnología de identificación por radiofrecuencia, para el control de acceso en la Corporación Universitaria Lasallista.

Objetivos Específicos

- Definir los requerimientos para la implementación de un sistema automático de control de acceso en la Corporación.
- Comparar los diferentes sistemas de control de acceso disponibles en el mercado evidenciando porqué el basado en RFID es el más apropiado para su implantación en la Corporación.
- Implantar, mediante un prototipo funcional, un sistema de control de acceso basado en la tecnología RFID para la Corporación Universitaria Lasallista
- Diseñar una interfaz que permita la integración del SCA con otros sistemas de la Corporación.

Marco Teórico

El control de acceso es la habilidad de permitir o denegar el uso de un recurso físico (áreas restringidas según rango del visitante) o virtual (acceso a información) a personas o entidades en particular. Para dar claridad al proyecto, se quiere implementar un control de acceso físico que está basado en el control de ingreso y salida en edificios, inmuebles, cuartos o áreas específicas únicamente a personas autorizadas.¹

El control de acceso físico está enfocado en tres preguntas: ¿quién?, ¿cuándo? y ¿cómo?; es decir ¿quién está autorizado a entrar o salir?, ¿cuándo entrará o saldrá del área? y ¿cómo lo realizará?

En la actualidad se cuenta con una gran variedad de tecnologías que pueden ayudarnos a suplir esta necesidad, entre las cuales están:

Código de Barras

Los códigos de barra son una técnica de codificación gráfica que representa datos en forma de barras y espacios de diferentes dimensiones y representaciones que ha ayudado a los comerciantes en la identificación de productos y precios. Las imágenes son leídas por equipos especiales de lectura óptica a través de los cuales se puede comunicar información al

¹ Mediante diferentes tecnologías podemos gestionar la digitalización de la identificación con la que se controla los accesos físicos de personas, como la entrada y salida de edificios, casas, instituciones e instalaciones por medio de tarjetas y dispositivos biométricos.

computador.²

La principal ventaja del código de barras es que su implementación es muy barata pues la creación de códigos no es muy compleja y es de fácil aplicación a las tarjetas que contendrán los códigos. Sus desventajas son de gran variedad, pero las que más priman son: la vulnerabilidad a falsificaciones y los problemas en las lecturas cuando la superficie se encuentra sucia, borrosa o manchada. Estas razones pueden ser incluso significativas para descartar esta tecnología en sistemas de control de acceso.

Figura 1 Tecnología Código de Barras



Fuente: I <http://2.bp.blogspot.com>

² El código de barras consiste en un sistema de codificación creado a través de series de líneas y espacios paralelos de distinto grosor. Generalmente se utiliza como sistema de control ya que facilita la actividad comercial del fabricante y del distribuidor, por lo que no ofrece información al consumidor, si no datos de operaciones aplicados a identificar productos, llevar control de inventarios, carga y descarga de mercancías, disminuir tiempos de atención en ventas.

Tarjetas Magnéticas

Son tarjetas que contienen una banda magnética que posee un código que permite identificarse rápidamente. Este sistema utiliza señales electromagnéticas para registrar y codificar la información. Una de las aplicaciones más comunes de esta tecnología son las tarjetas de crédito.

Las tarjetas magnéticas poseen una alta difusión y popularidad, además son de bajo costo. Sin embargo, su uso continuo las deteriora físicamente debido a la fricción en el momento de la lectura; también si la tarjeta es acercada a una fuente electromagnética, relativamente fuerte, la información contenida en ella puede ser modificada, con lo cual pierde su utilidad.(Green, 2007)

Figura 2 Tecnología de Identificación por Banda Magnética



Fuente: II <http://www.kimaldi.com>

Sistemas Biométricos

Estos sistemas fundamentan sus decisiones de reconocimiento mediante una característica personal, donde los lectores reconocen automáticamente la característica física de la persona eliminando por completo el uso de tarjetas electrónicas o magnéticas.

Las principales características físicas que se trabajan en el reconocimiento de las personas son: reconocimiento de iris, reflexión retina, geometría de la mano, geometría facial, termografía mano-facial, huellas dactilares y patrón de la voz.

La biometría ofrece una ventaja significativa: El alto grado de seguridad, ya que sólo identifica la característica de la persona autorizada por tanto es difícil la suplantación de información ya que los rasgos físicos son únicos e intransferibles.

Las desventajas de este sistema son su alto costo de implementación (por los lectores que se manejan para detectar los rasgos la persona), la reducida velocidad de lectura (comparada con la de otros sistemas) y la carencia de una eficiencia necesaria para grandes corporaciones pues los retardos en las lecturas de personal disminuirían tiempos en las labores. (Jaramillo, 2009).

Figura 3 Tecnología Biométrica



Fuente: III <http://tecnoseguridad.netii.net>

Tecnología RFID

RFID es una tecnología para la identificación de objetos, personas y animales a distancias sin necesidad de contacto o línea de vista; se trata de una tecnología muy versátil y de fácil uso, aplicable en situaciones muy variadas, que abre la puerta a un conjunto muy extenso de aplicaciones en una gran variedad de ámbitos, desde la trazabilidad y control de inventario, hasta la localización y seguimiento de personas y bienes, o la seguridad en el control de accesos a establecimientos comerciales y educativos.³

³ La RFID es una tecnología de identificación por radiofrecuencia, que permite almacenar y enviar información de objetos, animales o hasta de una persona. Se basa en la transmisión de datos por campos electromagnéticos y una identificación sin contacto visual directo.(Sistema de información y control de acceso basado en tecnología RFID, Tesis)

El sistema de RFID está compuesto por una serie de subsistemas los cuales se dividen en dos:

Componentes Hardware

- ✓ Transponder, TAG o etiqueta: Es el objeto que será identificado.
- ✓ Lector: Dependiendo del diseño y la tecnología usada, podría ser un dispositivo lector o lector/escritor.
- ✓ Antena: Es el conductor para la comunicación de datos entre el tag y el lector.

Componentes Software

- ✓ Software del Sistema RFID: Es una colección de funciones necesarias para habilitar la interacción básica entre el tag y el lector.
- ✓ RFID Middleware: Consiste en un conjunto de componentes software que actúan como puente entre los componentes de un sistema RFID y software de aplicación del computador.
- ✓ Aplicación del Computador: La aplicación del computador recibe datos procesados y normalizados enviados de la etiqueta, vía lector y el software RFID middleware.

Transponder, Tag O Etiquetas

Representa el dispositivo que contiene los datos en un sistema RFID, normalmente consiste en un elemento acoplador y un microchip electrónico; este solo se activa cuando hay una señal de radio frecuencia enviada por un lector dentro de una zona de interacción ente los componentes.

Las etiquetas se utilizan dependiendo de su fin entre los tipos de etiquetas están:

- ✓ Etiquetas Pasivas
- ✓ Etiquetas Activas
- ✓ Semi- Pasivos
- ✓ Semi- Activos

Figura 4 Tarjetas MIFARE PVC



Fuente: IV <http://image.made-in-china.com>

Etiquetas Pasivas

Los tags pasivos no poseen ningún tipo de alimentación. La señal que les llega de los lectores induce una corriente eléctrica mínima que basta para operar el circuito integrado del tag para generar y transmitir una respuesta al lector y están compuestas por una antena y un microchip.⁴

Los tags pasivos suelen tener distancias de uso práctico comprendidas entre los 10 cm y llegando hasta unos pocos metros según la frecuencia de funcionamiento, el diseño y tamaño de la antena.

Como carecen de autonomía energética el dispositivo puede resultar muy pequeño: pueden incluirse en una pegatina o insertarse bajo la piel (tags de baja frecuencia).

Etiquetas Activas

Las etiquetas RFID activas poseen su propia fuente de poder que incorporada, energiza el microchip y el transmisor para propagar su señal al lector y así establecer una sección de comunicación con este.⁵

⁴ Los tags pasivos no requieren ninguna fuente de alimentación interna y son en efecto dispositivos puramente pasivos (sólo se activan cuando un reader se encuentra cerca para suministrarles la energía necesaria). Los otros dos tipos necesitan alimentación, típicamente una pila pequeña.

⁵ A diferencia de los tags pasivos, los activos poseen su propia fuente autónoma de energía, que utilizan para dar corriente a sus circuitos integrados y propagar su señal al lector. Estos tags son mucho más fiables (tienen menos errores) que los pasivos debido a su capacidad de establecer sesiones con el reader.

Las etiquetas activas pueden recibir y transmitir señales a largas distancias y en ambientes demasiado pesados por ejemplo ambientes compuestos por agua y metales.

Muchos tags activos tienen rangos efectivos de cientos de metros y una vida útil de sus baterías de hasta 10 años.

Etiquetas Semi-Pasivas

Los tags semipasivos poseen una fuente de alimentación propia, aunque en este caso se utiliza principalmente para alimentar el microchip y no para transmitir una señal, para realizar la transmisión de datos usan la energía del lector para transmitirlos.

Las etiquetas semipasivas funcionan de modo similar a las etiquetas pasivas RFID. Sin embargo, ellas contienen una batería que permite la lectura a mayor distancia y la batería puede permitir al circuito integrado de la etiqueta estar constantemente alimentado y eliminar la necesidad de diseñar una antena para recoger potencia de una señal entrante.

Las etiquetas RFID semipasivas responden más rápidamente, por lo que son más fuertes en el radio de lectura que las pasivas⁶.

⁶ Los tags semipasivos poseen una fuente de alimentación propia, aunque en este caso se utiliza principalmente para alimentar el microchip y no para transmitir una señal. (Lagos, Diego Fernando, Diseño y construcción de un modelo de control de acceso para los armarios de CNT de la ciudad de Ambato, p. 15)

Lector RFID

Es uno de los elementos más importantes en un sistema RFID ya que si él no existiera la comunicación, no se completaría.

Los lectores son los encargados de enviar una señal de radio frecuencia para detectar las posibles etiquetas en un determinado rango de acción, los lectores suelen ser utilizados para validar diversos tags en un espacio corto de tiempo.

La máxima distancia a la que puede establecerse la comunicación entre el lector y la etiqueta depende de la potencia del lector y de la frecuencia que se utiliza para la comunicación entre el lector y la etiqueta.

Figura 5 Lector USB TCR-501



Fuente: V Corporación Universitaria Lasallista

Antena

Cada sistema RFID incluye como mínimo una antena para transmitir y recibir las señales de radio frecuencia⁷. En algunos sistemas usan una única antena que transmite y recibe las señales. En otros sistemas una antena transmite y otra recibe las señales. La cantidad y el tipo de las antenas dependen de la aplicación (velocidad de paso, nº de transponders a detectar etc.).

Figura 6 Antena RFID



Fuente: VI <http://www.gaorfid.com>

⁷ “Cada sistema RFID incluye como mínimo una antena para transmitir y recibir las señales de radio frecuencia” (Introducción a los sistemas RFID pág. 5, Recuperado de www.kifer.es.)

Rfid Middleware

Middleware es un término genérico utilizado para describir el software que se encuentra entre el lector de RFID.

Es un componente crítico de cualquier sistema RFID, debido a que el middleware toma los datos en bruto del lector y los pasa a unos sistemas back-end. Middleware juega un papel clave en conseguir la información correcta para la aplicación correcta en el momento adecuado⁸.

Los sistemas middleware ayudan con lo siguiente:

1. Recuperación de datos del lector.
2. Filtrar datos que llegan al sistema y no pertenecen a este.
3. Generación de notificaciones de inventario de movimiento.
4. Seguimiento de etiquetas y funcionamiento de lectores de la red.
5. Captura de historiales de los tag.

Aplicación del computador

Estas aplicaciones se desarrollan de acuerdo al negocio del sistema y deben ser sincronizados con el middleware ya que estos dos en conjunto forman el sistema de Identificación de datos de acuerdo a las especificaciones del sistema o negocio en función.

⁸ Software que se encuentra instalado desde fábrica dentro de los lectores RFID, los cuales son los que inicialmente imponen el core del negocio bajo el cual se implementará con el sistema que se desea montar con dicho lector.

Caracterización de un sistema RFID

Un sistema RFID puede estar caracterizado por una serie de variables las cuales trabajando conjuntamente logran que un sistema RFID cumpla su función dentro del ámbito del negocio.

Una de esas variables es la comunicación que para que se lleve a cabo entran a jugar otras variables como alcance de lectura, velocidad de transmisión y seguridad de transmisión, esto dentro de la comunicación, y la otra variable que caracteriza los sistemas RFID es el rango de frecuencia donde entran el tipo de antena, el tipo de etiquetas entre otras más.

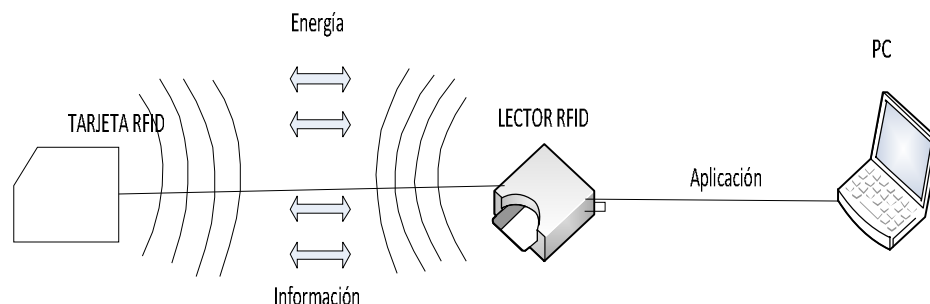
Para la creación de un sistema RFID hay que tener en cuenta factores como el rango de alcance donde se pueda mantener la comunicación entre el lector y el transponder, la cantidad de información que el tag puede almacenar y a su vez transmitir, la cantidad de datos que se puede obtener entre el lector y la etiqueta al momento de una transmisión y la más importante, que capacidad posee el lector para responder y mantener una comunicación entre varias etiquetas, todo lo anterior se debe tener en cuenta para la generación de un sistema totalmente acoplable al negocio que se desee desarrollar. (Herrera, 2011)

La otra variable es la frecuencia de funcionamiento del sistema, para esto debemos tener en cuenta que las frecuencias corresponden a unos rangos de transmisión y recepción de datos entre las cuales están las que se muestran en la tabla 1.

Tabla 1 Descripción Frecuencias RFDI

Banda	LF Baja frecuencia	HF Alta Frecuencia	UHF Ultra-alta frecuencia	Microondas
Rango de frec.	30-300KHz	3-30MHz	300MHz-2GHz	2-30GHz
Frecuencias RFID	125-134KHz	13.56MHz	868MHz (Europa) 915MHz (USA)	2.45GHz
Distancias (aprox) tags pasivos	<0.5m	Hasta 2m	6m	Activo: >100m No habitual pasivo
Velocidad	<1kbps	25kbps	Hasta 640kbps	
Ventajas	Buen comportamiento con metal y agua	Buena distancia, mejor velocidad y anticolisión	Muy alta velocidad (600 tags/s), estandarización global ePC, mayores distancias	
Inconvenientes	Corta distancia, baja velocidad, poca capacidad anticolisión	Peor comportamiento con agua y metales	Muy sensible al agua y al metal	
Uso habitual	ID Animal, coches, controles de accesos	Accesos y seguridad, smart cards, pasaporte	Logística procesos de fabricación	Activos: autopistas, contenedores
Otras características	Campo cercano Acop. Magnético	Campo cercano Acop. Magnético	Campo lejano Acop. Eléctrico	

Figura 7 Comunicación entre componentes de un sistema RFID



Ventajas de la identificación por radiofrecuencia

- **Seguridad:** Por el diseño tecnológico que tienen las tarjetas no pueden duplicarse, cada tag (tarjeta) posee un código único, por lo cual no permite que varios usuarios puedan tener una tarjeta duplicada.
- **Sin necesidad de alineación o línea vista:** En comparación con los otros sistemas, éste es el más ágil y práctico porque para reconocer la tarjeta no es necesario que sea pasado por una ranura ni por el lector en un sentido ya que la tarjeta es reconocida por los dos lados.
- **Inventarios de alta velocidad:** Múltiples dispositivos pueden ser leídos simultáneamente, lo que ahorra un tiempo significativo en comparación con otras tecnologías a las cuales los productos deben ser pasados uno por uno.
- **Lectores sin mantenimiento:** Los lectores son unidades sin partes móviles, lo que garantiza un correcto funcionamiento sin límite de uso y sin que haya que

hacerles algún tipo de mantenimiento. También se pueden instalar a la intemperie sin que las inclemencias del tiempo, como altas y bajas temperaturas ambientales, los dañen.

- **Tarjetas sin desgaste:** Las tarjetas no presentan ningún tipo de fricción con el lector por lo cual no se desgastan. Esto garantiza una vida útil prolongada para ambas partes.
- **Reescribible:** Algunos tipo de tarjetas (tag) RFID pueden ser leídas y escritas en múltiples ocasiones.
- **Factibilidad:** La tecnología RFID puede ser aplicada en gran cantidad de campos y aplicaciones.
- **Otras Tareas:** Además de almacenar y transmitir datos, una etiqueta de RFID, puede ser diseñada para desempeñar otras funciones como medir condiciones de humedad o temperatura en el ambiente.

Tabla 2 Tabla comparativo entre tecnologías de control de acceso

<u>Tecnología de Lectura</u>	<u>Seguridad</u>	<u>Desgaste tarjeta</u>	<u>Desgaste de Lector</u>	<u>Costo Mantenimiento</u>	<u>Precio Tarjeta</u>	<u>Precio Lector</u>
<u>Código de Barras</u>	<u>Baja</u>	<u>Medio</u>	<u>Bajo</u>	<u>Medio</u>	<u>Bajo</u>	<u>Medio</u>
<u>Tarjeta Magnética</u>	<u>Medio</u>	<u>Alto</u>	<u>Muy Alto</u>	<u>Alto</u>	<u>Muy Bajo</u>	<u>Bajo</u>
<u>Sistema Biométrico</u>	<u>Muy Alta</u>	<u>No Posee</u>	<u>Bajo</u>	<u>Medio-Alto</u>	<u>No Posee</u>	<u>Muy Alto</u>
<u>Tecnología RFID</u>	<u>Alta</u>	<u>No Posee</u>	<u>No Posee</u>	<u>Muy Bajo</u>	<u>Medio-Bajo</u>	<u>Medio</u>

Ejemplo de sistemas basados en tecnología RFID

Sistemas de RFID implementados en instituciones de educación superior

TIP (Tarjeta Integrada Personal)

La tarjeta integrada personal (TIP), (CVNE, Centro Virtual de noticias de la educación), es una tarjeta de proximidad implementada por la Universidad de Antioquia. A continuación se explican sus alcances mediante fragmentos de un artículo escrito por el ingeniero electrónico Eduard Emiro Rodríguez Ramírez con el fin de generar claridad y reflexión sobre el tema:

“La TIP es una tarjeta de identificación electrónica sin contacto o de proximidad, que funciona almacenando una información y transmitiéndola de manera inalámbrica hacia un dispositivo lector sólo cuando tarjeta y lector están muy cercanos. Las características de esta tarjeta están definidas por el estándar internacional ISO/IEC 14443 y la transmisión inalámbrica está basada en la tecnología de Identificación por Radio Frecuencia o RFID.

El estándar internacional ISO/IEC 14443 define aspectos físicos de la tarjeta y aspectos de la transmisión de información que se realiza entre tarjeta y lector. El estándar define también dos tipos de tarjetas, A y B, diferenciados por aspectos técnicos de tratamiento de la información (en este caso, la TIP es tipo A). Es importante resaltar que las entidades que formularon este estándar gozan de prestigio y credibilidad al garantizar a los usuarios que un proceso o producto satisface las especificaciones técnicas indicadas por un estándar, lo cual finalmente se traduce para los usuarios en características como calidad, confiabilidad y seguridad, entre otras.

Como la TIP utiliza tecnología de Identificación por Radio Frecuencia -RFID-, es conveniente presentar algunos conceptos sobre ésta. El propósito de la tecnología RFID es transmitir de forma inalámbrica información hacia un dispositivo lector. Una tarjeta RFID (en este caso, la TIP) guarda en su memoria la información de identificación del portador y de las aplicaciones o servicios disponibles, toda información adicional que se requiera o se genere es guardada en los sistemas de información conectados con el lector, no en la tarjeta.

En esta implementación de la tecnología RFID, la tarjeta es llamada pasiva porque no utiliza una fuente de energía o batería, lo cual significa que no puede haber una transmisión permanente de información desde la tarjeta, ya que ésta no funciona de manera autónoma y sí dependiente de la cercanía a un lector y de la energía que reciba el circuito electrónico de la tarjeta, proveniente de una señal emitida por el lector; la transmisión sólo ocurre cuando la tarjeta se ubica dentro de la zona de alcance de un lector, correspondiente a no más de 10 centímetros, de acuerdo con especificaciones del estándar y del fabricante.

Pensar que una tarjeta y un lector puedan interactuar a distancias mayores a 10 centímetros no es adecuado; la transmisión se hace imposible en la medida en que la distancia es cada vez mayor. Esta apreciación se justifica desde el punto de vista técnico (más allá de especificaciones del fabricante y del estándar) porque la característica pasiva de la tarjeta no permite que su circuito electrónico alcance a almacenar la energía suficiente para transmitir, puesto que para su funcionamiento requiere de la energía emitida por el lector.

Muchos hemos observado funcionar esta tecnología en instalaciones de entidades públicas y privadas en donde nos entregan una tarjeta de este mismo tipo con la cual realizamos el ingreso y la salida acercando la tarjeta al lector ubicado en el punto de acceso y registro de las instalaciones.

La tecnología incorpora técnicas que garantizan la seguridad de la información que se guarda en la tarjeta y se transmite desde ésta, permitiendo que sólo un lector adecuado pueda entender y/o modificar dicha información. Las implementaciones de seguridad están especificadas por el estándar y por el fabricante.

En cuanto a la capacidad de memoria para almacenar información, sólo existen opciones de tarjetas de 1KBytes y 4KBytes; estas capacidades, aunque aparentemente bajas para los avances tecnológicos actuales, son suficientes para implementar múltiples servicios en la tarjeta. A manera de ejemplo, la tarjeta de 1KBytes es la utilizada típicamente para implementar el servicio de pago electrónico en sistemas de transporte público, resaltando que no utiliza el total de la memoria, dejando así la capacidad para implementar nuevos servicios en una misma tarjeta. En la Universidad, dados los servicios que inicialmente se piensan prestar y la expectativa de prestar en un futuro más servicios, la opción de tarjeta de 4KBytes es adecuada para la TIP.

La tecnología de la TIP es aplicable principalmente en sistemas de identificación y en sistemas de pago electrónico. Con la tecnología disponible se pueden implementar servicios como control y registro de acceso, control de préstamo de objetos, control de inventarios y otros, pero siempre considerando la proximidad que debe haber entre la tarjeta y el lector. Tecnológicamente y por razones ya expuestas, no es viable pensar en aplicaciones que impliquen grandes distancias entre tarjeta y lector.

Se debe enfatizar en que las aplicaciones de control y registro de acceso, aunque tienen en común la identificación del portador de la tarjeta, deben considerarse como independientes entre ellas, ya que cada aplicación requiere una implementación particular.

Esta tecnología puede ser considerada confiable desde una perspectiva ambiental y de salud ya que emite niveles muy bajos de energía, por lo tanto no nocivos. En múltiples servicios

conocidos en los cuales esta tecnología ya es usada se evidencia comodidad, agilidad y confiabilidad, como es el caso de servicios relacionados con pacientes en entidades de salud.

Desde un punto de vista tecnológico se puede concluir que la utilización de la TIP y de la tecnología que ésta implica no representa un riesgo para su portador, facilita su identificación como miembro de la comunidad universitaria y además deja abierta para un futuro la posibilidad de mejorar la prestación de servicios ya existentes en diferentes dependencias de la Universidad.”

Metodología

Análisis y Diseño para el prototipo de control de acceso a la Corporación Universitaria Lasallista.

Modelo de dominio

Proceso para el ingreso a la Corporación Universitaria Lasallista

Luego de realizar entrevistas con las personas que están directamente relacionadas con el proceso de ingreso a la universidad, especialmente el área de servicios generales encargada de la seguridad del campus, se pudieron deducir algunos requerimientos. Así mismo, con la entrevista realizada al jefe de sistemas, se pudo tener una mejor noción de las personas que integran la universidad y su jerarquía dentro de ella.

En la Corporación no existía un proceso estricto para el ingreso al Campus pero debido a que se han presentado algunos casos de ingreso de personal extraño, los cuales entran dan vueltas y vuelven a salir y no se dirigen a donde dicen, se ha planteado un protocolo de ingreso a la Corporación Universitaria Lasallista.

La persona que desee ingresar debe presentar el carné que lo acredite como estudiante o funcionario de la universidad de lo contrario deberá dejar un documento diferente a la cédula; si no presenta ningún documento y dice ser perteneciente a la Universidad deberá esperar a que el

vigilante consulte su existencia en las bases de datos que tiene instalada en el computador de la portería.

Si es un visitante deja un documento diferente a la cédula e informa para dónde se dirige, y en la medida de lo posible el personal de la universidad asiste las visitas así: El vigilante que está en turno en la portería anuncia para donde se dirige el visitante y el vigilante móvil lo recibe en la parte de la alameda y hace el acompañamiento hasta el lugar de destino. En otras ocasiones también se anuncia la visita a las personas encargadas del área que se va a visitar y éstas esperan al visitante.

Cómo se desea el funcionamiento

Se desea implementar en la entrada peatonal de la Corporación Universitaria Lasallista un sistema de control de acceso fundamentado en tecnología RFID, la cual se compone de una serie de dispositivos como lo son: Un lector RFID con frecuencia de 13.56 MHZ tarjetas MIFARE compatibles con el lector y un computador. El funcionamiento sería así,

- Al registrar una persona se le debe asociar una tarjeta, la cual será su identificación ante la universidad.
- Una persona es portadora de una tarjeta la cual debe ser leída por el lector al ingresar a la universidad.
- El sistema valida la información de la tarjeta para habilitar el acceso o denegarlo.

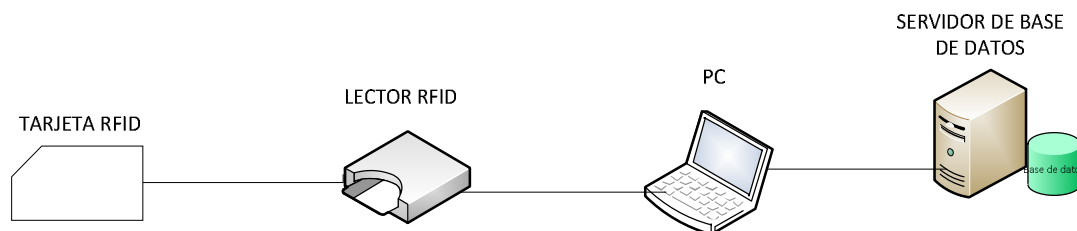
- El sistema registra información de las personas que ingresan a la universidad.

Para llevar a cabo el funcionamiento del sistema el diseño e implementación de este prototipo se enfocará principalmente en el apoyo a la Corporación en la seguridad al ingreso al campus, obteniendo mejores resultados en el registro de usuarios y control de acceso de los mismos.

Para la creación del prototipo se realizó un estudio previo donde se identificó la necesidad básica del sistema, los componentes y desarrollos necesarios para llevar a cabo la construcción de un sistema que nos permitiera a partir de la radio frecuencia, la identificación de las personas al momento de ingresar a la Corporación.

Para lograr llegar al punto de la elaboración debimos realizar un análisis de los componentes que integrarían el sistema. Este análisis se realizó con base en la metodología presentada por Craig Larman⁹ para el análisis y diseño de sistemas por medio de la metodología UML orientada a objetos (Larman, 2004) en la cual surgieron los siguientes diagramas:

⁹ “Informático Canadiense que se especializa en el desarrollo iterativo e incremental de software”, Análisis y diseño mediante objetos y modelado ágil”

Figura 8 Descripción Prototipo control de acceso

El computador es quien siempre comienza las secuencias de comunicación enviándolas al lector con una secuencia de pregunta.

El lector es el encargado de emitir la secuencia de pregunta enviada por el computador por una señal de radio frecuencia.

Las tarjetas reciben el mensaje emitido por el lector y responden a este mensaje emitiendo un código, el lector lo receptiona y lo envía la respuesta al computador.

El computador receptiona la respuesta y ejecuta su lógica de negocio.

y por último valida los datos con el servidor y posteriormente la almacena.

Análisis y diseño del Software

Diagrama Modelo De Dominio

Un modelo de dominio captura los tipos más importantes de objetos en el contexto de un sistema. Los objetos del dominio representan las "cosas" que existen o los eventos que suceden en el entorno en el que trabaja el sistema.

Muchos de los objetos del dominio o clases pueden obtenerse de una especificación de requisitos o mediante la entrevista con los expertos del dominio.

Cabe mencionar que el modelo de dominio de nuestro sistema surge a causa del sistema de control de acceso que opera actualmente en la Corporación Universitaria Lasallista donde un

actor (persona que ingresa), muestra su identificación (carnet), a un segundo actor para lograr un acceso, por tanto en la figura numero 9 presentamos nuestro modelo de dominio final.

Figura 9 Diagrama Modelo de Dominio

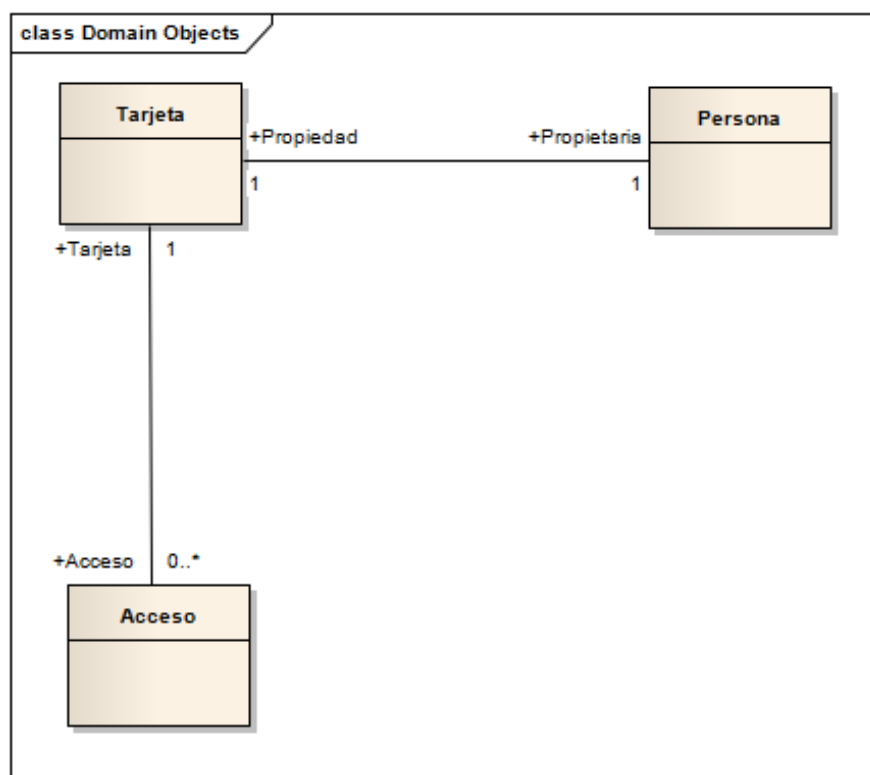
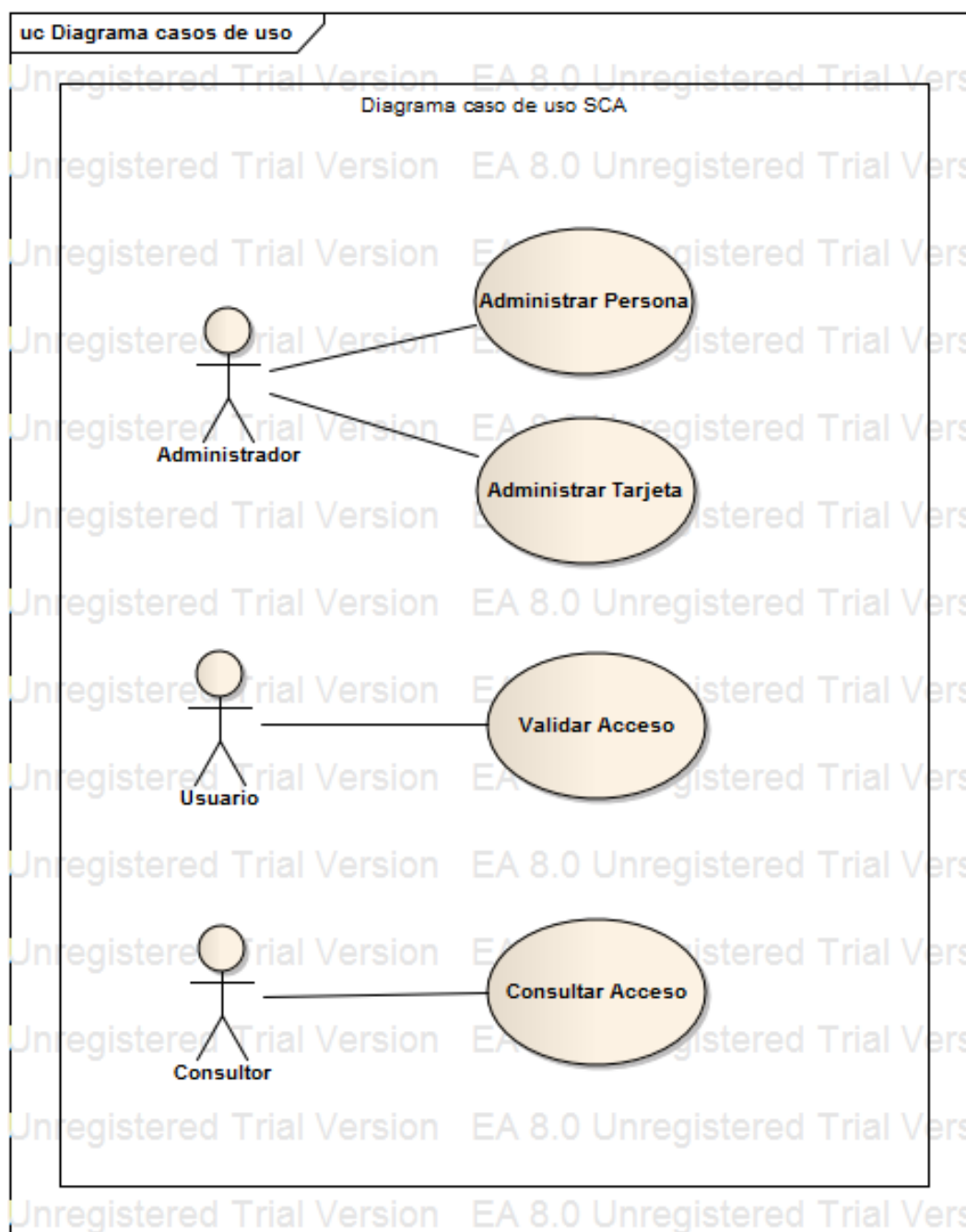


Diagrama caso de uso SCA

Luego de obtener el modelo de dominio debemos identificar cuáles serán los casos de uso que regirán el proceso para lograr el funcionamiento del sistema de control de acceso.

Para esto se deben relacionar las clases del modelo de dominio con una función a realizar, es decir, teniendo en cuenta el actor y el proceso a realizar en una acción, para más comprensión de esta definición mostraremos en la figura 6 el resultado de nuestro análisis.

Figura 10 Diagrama Casos de uso

En la figura 10 observamos que los casos de uso que se definieron para el sistema son:

- ✓ Administración de Personas.
- ✓ Administración de tarjetas.
- ✓ Validación de acceso.
- ✓ Registro de accesos.
- ✓ Consulta de accesos.

Luego de tener claro cuáles son los casos de uso que rigen el sistema debemos analizar qué proceso se llevará a cabo dentro de cada función para lograr su cometido. Para identificar esto recurrimos a utilizar la metodología de Larman para identificar la secuencia que debe realizar cada proceso dependiendo del actor y la función que se desea realizar.

Descripción casos de uso

En la descripción de los casos se encuentra detalladamente el funcionamiento de cada proceso en cuanto a un Rol o agente externo al sistema.

Administrar Tarjeta

CU-001	
Nombre	Administrar Tarjeta(Crear Tarjeta)
Autor	Diana Morales
Fecha	27/11/2011
Descripción	Permitir crear una nueva tarjeta en el sistema
Actores	Administrador
Precondiciones	Debe de existir una nueva persona
Flujo Normal	<p>1. El administrador pulsa el botón crear una nueva tarjeta.</p> <p>2. El sistema muestra el formulario para la creación de una tarjeta.</p> <p>3. El administrador completa los datos del formulario con el número de la tarjeta y el código.</p> <p>4. El sistema almacena los datos de la tarjeta en la base de datos del sistema.</p> <p>5. El sistema notifica los datos de la tarjeta</p> <p>6. El administrador acepta información.</p>

	<p>7. El sistema almacena y notifica la creación de la tarjeta.</p> <p>8. Fin del proceso</p>
<p>Flujo Alternativo</p>	<p>El flujo empieza en el paso 3</p> <p>3. El Administrador recupera la información de la persona de la base de datos de la corporación.</p> <p>4. el flujo continúa en el paso 4.</p>
<p>Pos condiciones</p>	<p>El sistema almacena la información y crea la tarjeta en el sistema</p>

CU-001	
Nombre	Administrar Tarjeta(Eliminar Tarjeta)
Autor	Diana Morales
Fecha	27/11/2011
Descripci	Permitir eliminar una tarjeta del sistema

ón	
Actores	Administrador
Precondiciones	Debe existir la tarjeta en el sistema
Flujo Normal	<p>1. El administrador pulsa el botón eliminar tarjeta.</p> <p>2. El sistema muestra el formulario de búsqueda de tarjetas.</p> <p>3. El administrador busca la tarjeta por medio del código.</p> <p>4. El sistema arroja los resultados de la búsqueda y las opciones que se pueden realizar (update, delete).</p> <p>5. El administrador da clic en la opción delete.</p> <p>6. El sistema muestra advertencia de eliminación.</p> <p>7. El administrador acepta la eliminación.</p> <p>8. El sistema elimina la tarjeta.</p> <p>9. fin del proceso.</p>
Flujo Alternativo	<p>4. A. Los datos ingresados no existen.</p> <p>5. El sistema muestra un mensaje de error en los datos y permite corregirlos y vuelve al paso 3</p>
Pos	El sistema elimina la tarjeta del sistema y

condiciones	notifica al administrador
-------------	---------------------------

CU-001	
Nombre	Administrar Tarjeta(Actualizar Tarjeta)
Autor	Diana Morales
Fecha	27/11/2011
Descripción	Permitir Actualizar la información de una tarjeta del sistema
Actores	Administrador
Precondiciones	Debe existir la tarjeta en el sistema
Flujo Normal	<p>1. El administrador pulsa el botón actualizar información de la tarjeta.</p> <p>2. El sistema muestra el formulario de búsqueda de la tarjeta</p> <p>3. El administrador realiza la búsqueda de la tarjeta por medio del código.</p> <p>4. El sistema muestra el resultado de la búsqueda y las opciones que se pueden realizar (update, delete).</p>

	<p>5. El administrador da clic en la opción update y actualiza los datos.</p> <p>6. El sistema muestra datos a modificar.</p> <p>7. El administrador acepta cambios</p> <p>8. El sistema actualiza los datos de la tarjeta guarda cambios y los almacena en la base de datos.</p> <p>9. Fin del proceso.</p>
Flujo Alternativo	<p>4. El código ingresado no es válido y el sistema muestra un mensaje de error permitiendo su corrección.</p>
Pos condiciones	<p>El sistema actualiza los datos de la tarjeta en el sistema</p>

Administrar Persona

CU-002	
Nombre	Administrar Persona(Crear Persona)
Autor	Diana Morales
Fecha	27/11/2011
Descripción	Permitir crear una Persona en el sistema
Actores	Administrador
Precondiciones	Ingreso de una persona a la corporación
Flujo Normal	<p>1. El administrador pulsa el botón crear una persona.</p> <p>2. El sistema muestra el formulario para la creación de una persona.</p> <p>3. El administrador completa los datos del formulario con la identificación, nombre, apellido, teléfono, email de la persona.</p> <p>4. El sistema almacena los datos de la persona en la base de datos del sistema.</p>

	<p>5. El sistema notifica del registro de la persona en la base de datos y la creación de la misma.</p> <p>6. Fin del proceso</p>
Flujo Alternativo	<p>3. A si el administrador no completa la información el registro el sistema muestra un mensaje de error permitiendo corregirlo en el paso 3.</p>
Pos condiciones	<p>El sistema almacena la información de la persona y la ingresa en el sistema.</p>

CU-002	
Nombre	Administrar Persona(Eliminar Persona)
Autor	Diana Morales
Fecha	27/11/2011
Descripción	Permitir eliminar una persona del sistema
Actores	Administrador
Precondiciones	Debe existir la persona en el sistema

<p>Flujo Normal</p>	<p>1. El administrador pulsa el botón eliminar persona.</p> <p>2. El sistema muestra el formulario de búsqueda de personas.</p> <p>3. El administrador busca la persona por medio de la identificación.</p> <p>4. El sistema arroja los resultados de la búsqueda y las opciones que se pueden realizar (update, delete).</p> <p>5. El administrador da clic en la opción delete.</p> <p>6. El sistema muestra advertencia de eliminación de la persona.</p> <p>7. El administrador acepta la eliminación.</p> <p>8. El sistema elimina la tarjeta.</p> <p>9. Fin del proceso.</p>
<p>Flujo Alternativo</p>	<p>4. A. si los datos ingresados son incorrectos el sistema muestra un mensaje de error y vuelve al paso 3.</p>
<p>Pos condiciones</p>	<p>El sistema elimina la persona del sistema y notifica al administrador</p>

CU-002	
Nombre	Administrar Persona(Actualizar Persona)
Autor	Diana Morales
Fecha	27/11/2011
Descripción	Permitir Actualizar la información de una persona del sistema
Actores	Administrador
Precondiciones	Debe existir la persona en el sistema
Flujo Normal	<p>1. El administrador pulsa el botón actualizar información de personas.</p> <p>2. El sistema muestra el formulario de búsqueda de personas.</p> <p>3. El administrador realiza la búsqueda de la persona por medio de identificación.</p> <p>4. El sistema muestra el resultado de la búsqueda y las opciones que se pueden realizar (update, delete).</p> <p>5. El administrador da clic en la opción update y actualiza los datos.</p> <p>6. El sistema muestra mensaje de cambios</p>

	<p>guardados y los almacena en la base de datos.</p> <p>7. El administrador acepta.</p> <p>8. El sistema actualiza los datos de la persona.</p> <p>9. Fin del proceso.</p>
Flujo Alternativo	
Pos condiciones	El sistema actualiza los datos de la persona en el sistema

Consultar Información de acceso

CU-003	
Nombre	Consultar Acceso del sistema
Autor	Diana Morales
Fecha	27/11/2011
Descripción	Permitir a usuarios externos consultar la base de datos del acceso
Actores	Administrador/ personal de seguridad
Precondic	Debe existir previos registros de acceso en el

iones	sistema
<p>Flujo</p> <p>Normal</p>	<p>1. El actor ingresa en el formulario de accesos.</p> <p>2. El sistema muestra el formulario de búsqueda de accesos.</p> <p>3. El actor selecciona los parámetros de búsqueda.</p> <p>4. El sistema realiza la búsqueda de acuerdo a los parámetros selecciones</p> <p>5. El sistema muestra el resultado de la búsqueda.</p> <p>6. Fin del proceso.</p>
<p>Flujo</p> <p>Alternativo</p>	<p>6. A. El actor desea imprimir los resultados.</p> <p>7. El sistema acepta la solicitud e imprime los resultados.</p> <p>8. fin del proceso.</p>
<p>Pos</p> <p>condiciones</p>	<p>El sistema provee la información</p>

Validar Acceso

CU-004	
Nombre	Validar Acceso
Autor	Diana Morales
Fecha	27/11/2011
Descripción	Validar la existencia en la corporación de la persona que ingrese a la universidad
Actores	Usuario
Precondiciones	Generar contacto entre la tarjeta y el lector
Flujo Normal	1. Acercar la tarjeta al lector RFID 2. Usuario Válido 3. Permitir Ingreso
Flujo Alternativo	2. Usuario Inválido 3. Rectificar usuario en admisiones 4. Permitir o denegar Acceso

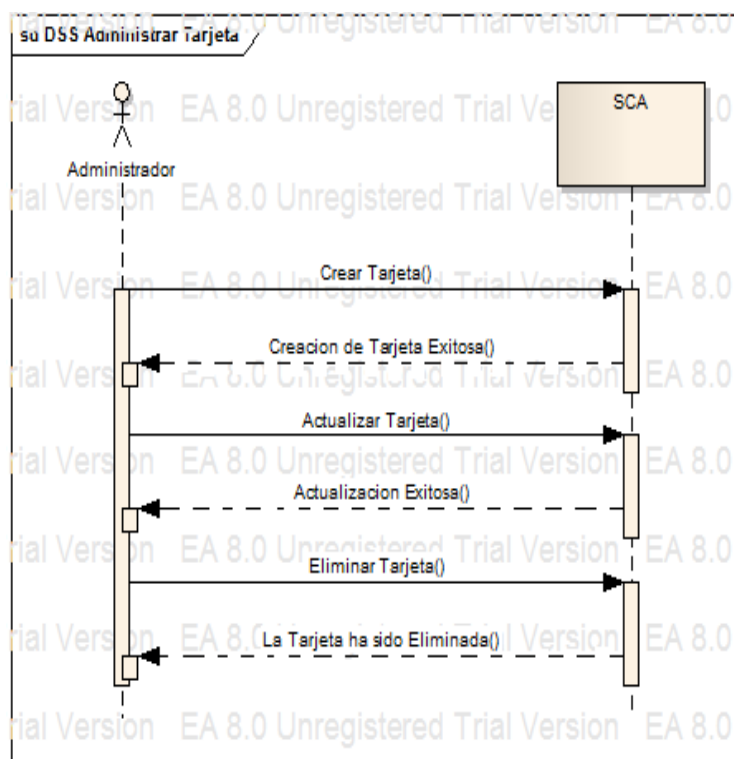
Pos	El sistema le permite el ingreso a la persona
Condiciones	exitosamente

Diagramas de secuencia del sistema (DSS)

Como mencionábamos anterior mente necesitamos una funcionalidad que nos permita administrar las personas y las tarjetas que integrarán el sistema, por tanto necesitamos una secuencia paso a paso de lo que se debe realizar para lograr estos dos fines. Por eso las figuras número 11 y 12 nos describen claramente como se deben ejecutar estas secuencias.

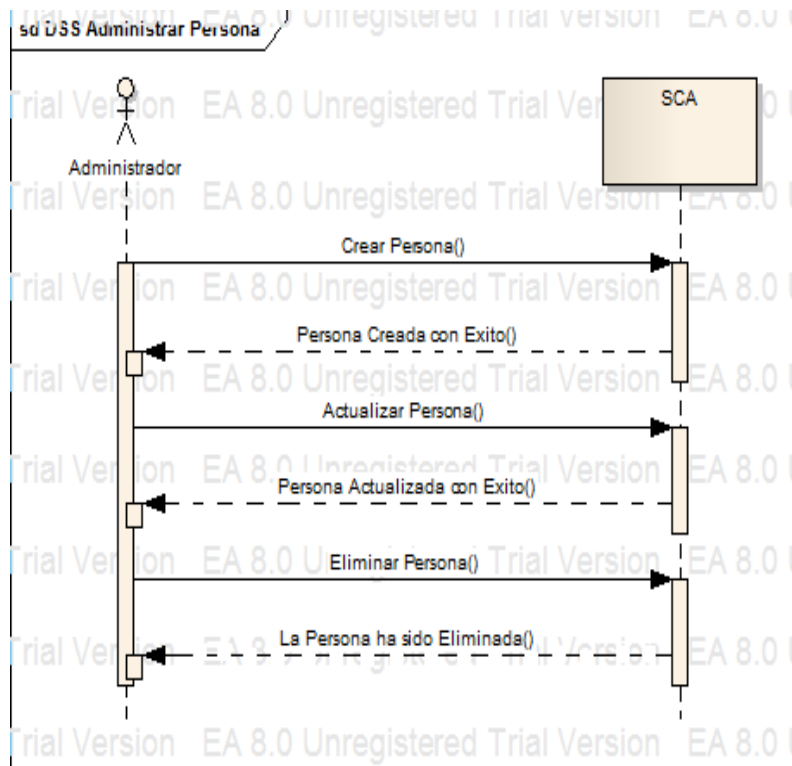
Administrar Tarjeta

Figura 11 Diagrama de Secuencia Administrar Tarjeta



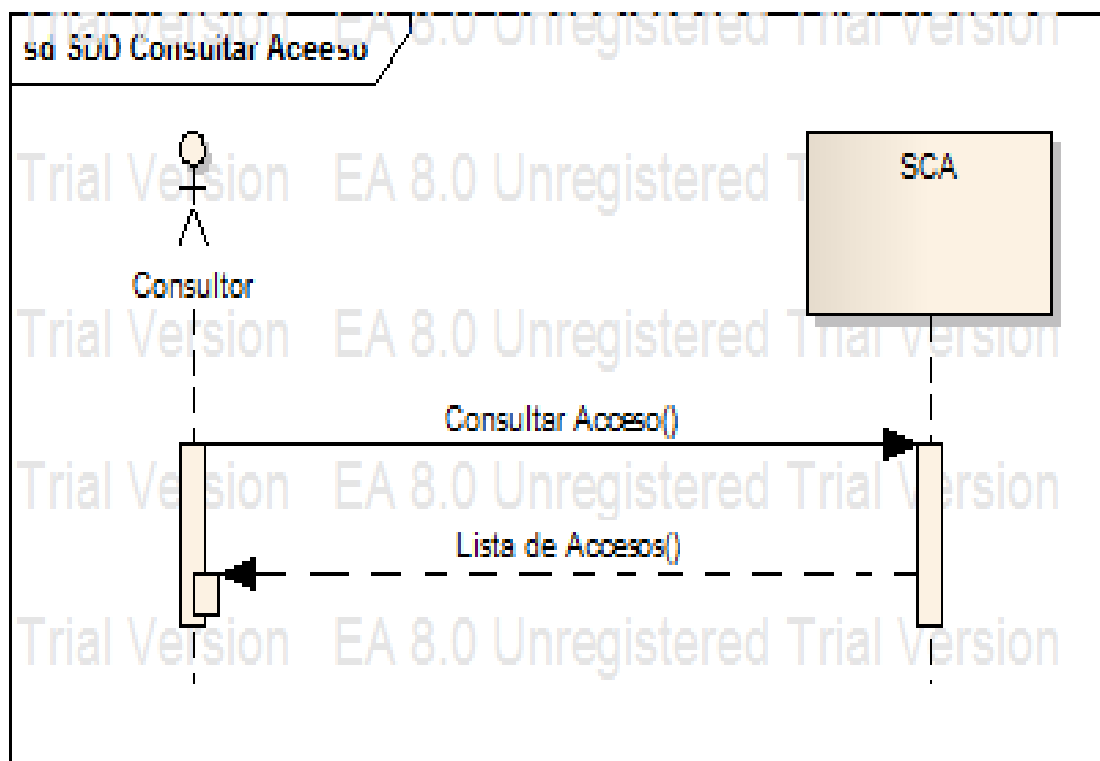
Administrar persona

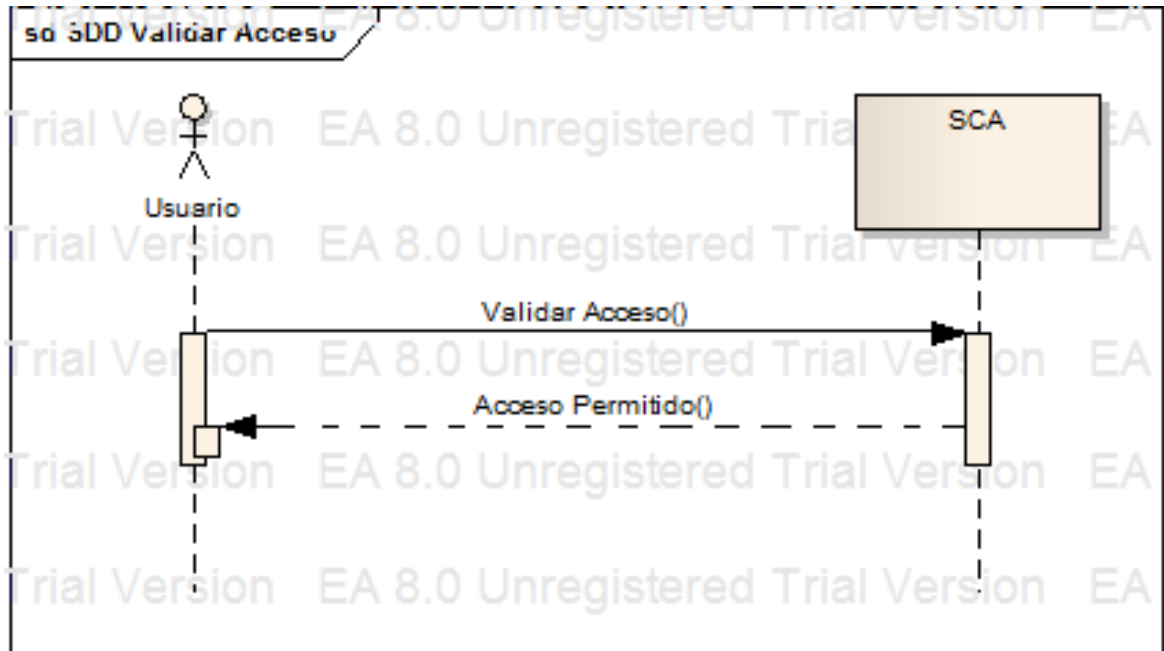
Figura 12 Diagrama de Secuencia Administrar Persona



Consultar Accesos

Figura 13 Diagrama de Secuencias Consultar Acceso



Validar Acceso**Figura 14** Diagrama de Secuencia Validar Acceso

Diagramas de colaboración

Los diagramas de colaboración permiten describir como un sistema implementa su funcionalidad, modelando el comportamiento dinámico de un procedimiento, transacción o caso de uso, haciendo énfasis en el proceso que se desea llevar a cabo; muestran interacciones organizadas alrededor de los roles (Larman, 2004).

Los diagramas de colaboración a diferencia de los diagramas de secuencia, muestran explícitamente las relaciones de los roles.

En las siguientes figuras se muestran los diagramas de colaboración diseñados para la implementación del Prototipo para el control de acceso a la Corporación Universitaria Lasallista.

Continuando con el análisis de nuestro sistema tenemos los diagramas de colaboración que son los que nos ayudan a identificar cuáles son las clases faltantes para lograr una comunicación de todo el sistema, es decir, aquellas clases que me permiten comunicación con el motor de base de datos, los controladores de las clases, las funciones creadoras y las clases principales, es decir, las que pertenecen al diagrama de dominio.

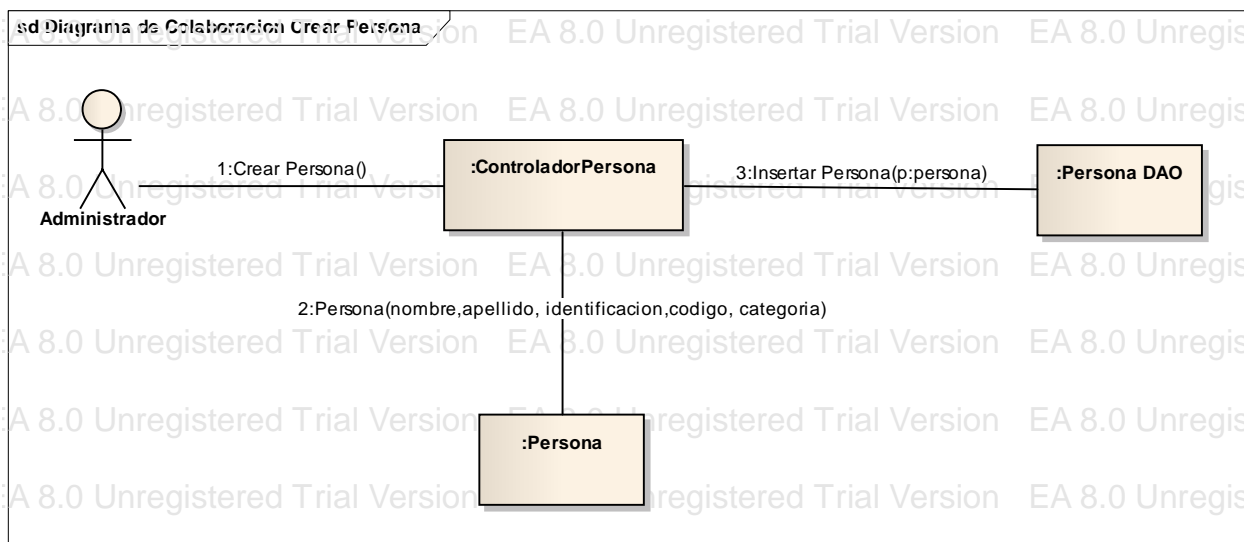
Dentro de los diagramas de colaboración que tenemos se encuentran los siguientes:

➤ Para el caso de uso de Administrar Persona tenemos :

Para la creación de una persona tenemos el diagrama de colaboración plasmado en la figura 15 que consta de un controlador de Persona, un controlador de ingreso a la base de datos DAO y un constructor persona, esto para lograr la creación exitosa de una persona; cabe decir que este mismo proceso se debe llevar a cabo para la creación de una tarjeta como lo muestra la figura número 18

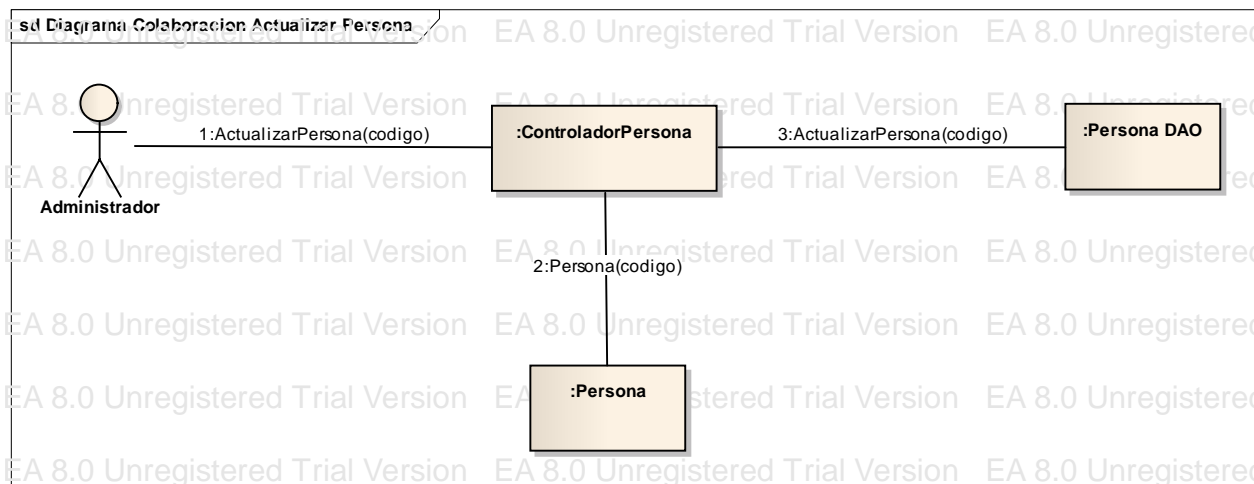
Crear Persona

Figura 15 Diagrama de Colaboración Crear Persona



Actualizar Persona

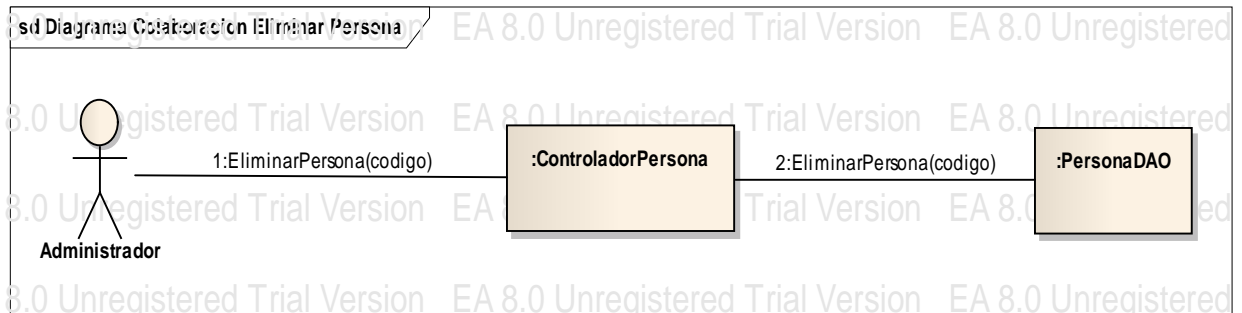
Figura 16 Diagrama de Colaboración Actualizar Persona



En la figura 16 podemos identificar las clase que necesita el sistema para lograr una comunicación entre la base de datos y el controlador persona para así llevar a cabo la actualización exitosa de una persona dentro del sistema. Es necesario decir que este mismo proceso al igual que en el de crear personas y tarjetas, también se genera el mismo proceso para la actualización de una tarjeta como lo muestra la figura número 19.

Eliminar Persona

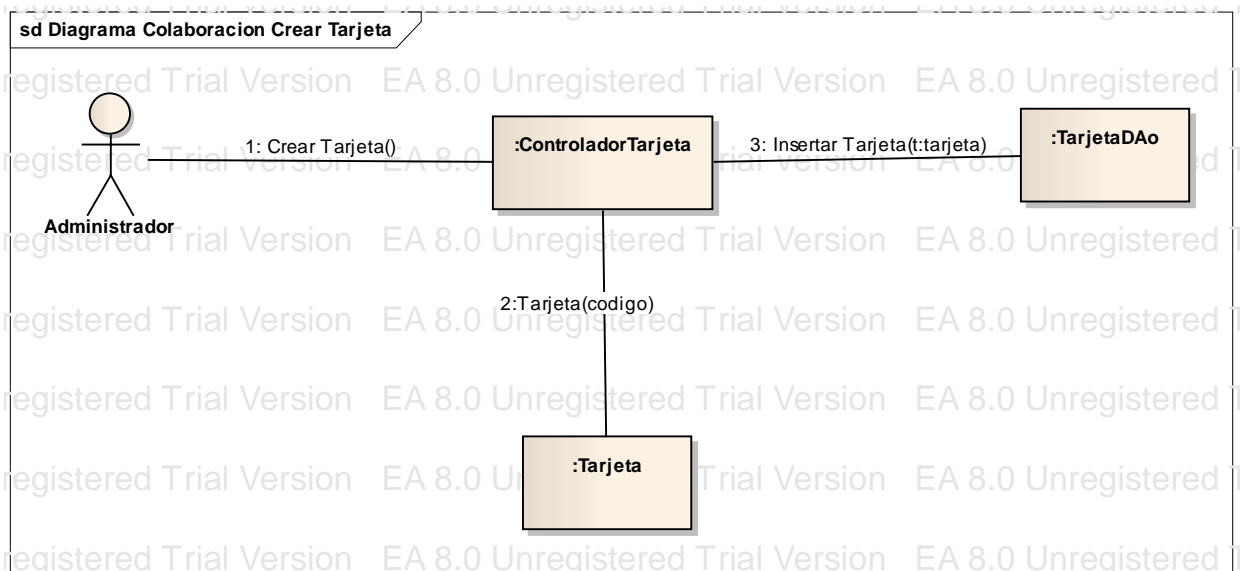
Figura 17 Diagrama de Secuencia Eliminar Persona



Las figuras número 17 y 20 me exponen el proceso que se debe generar para que tanto una persona como una tarjeta sean eliminadas del sistema.

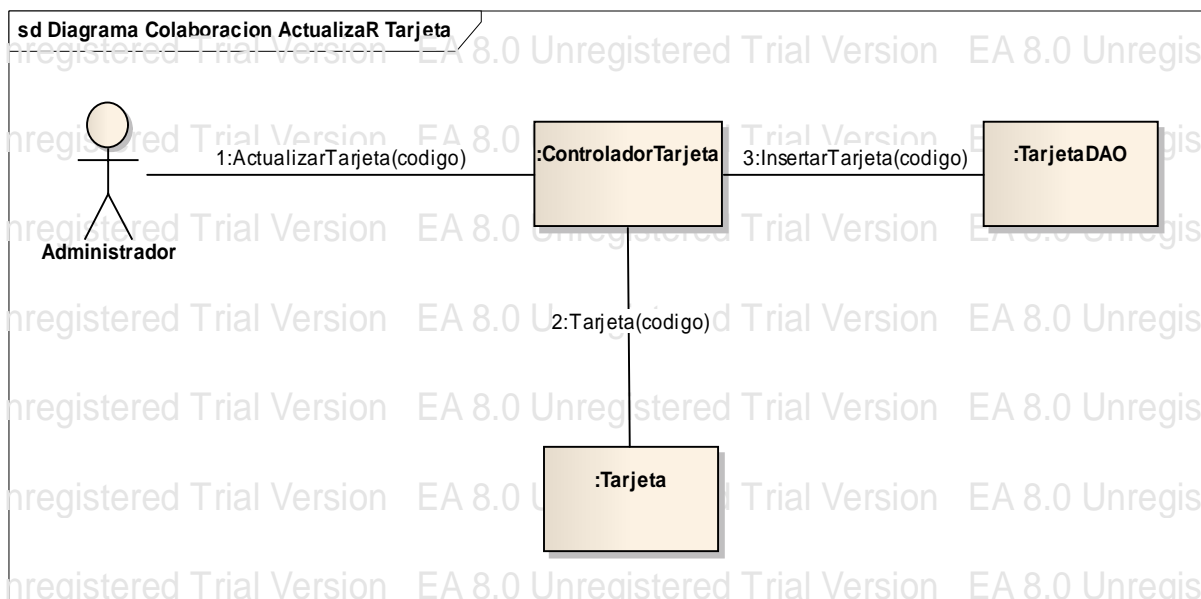
Crear Tarjeta

Figura 18 Diagrama de Colaboración Crear Tarjeta



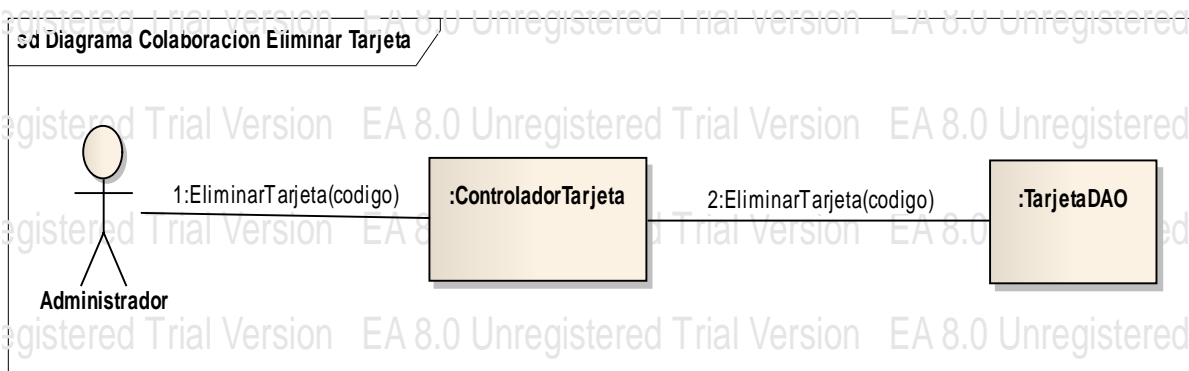
Actualizar Tarjeta

Figura 19 Actualizar Tarjeta Diagrama de Colaboración



Eliminar Tarjeta

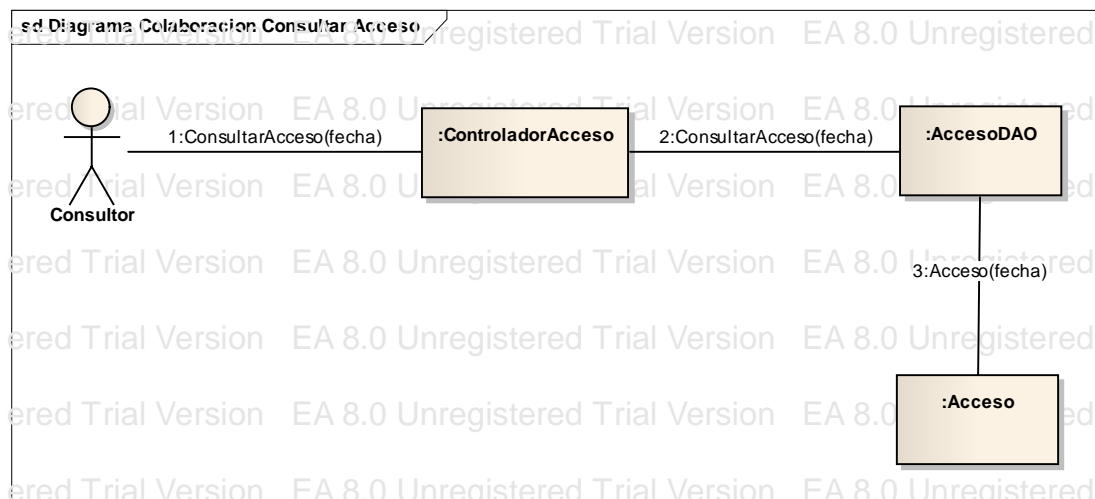
Figura 20 Diagrama de Colaboración Eliminar Tarjeta



Por último tenemos los diagramas de colaboración para las funciones de consultar acceso y validar acceso.

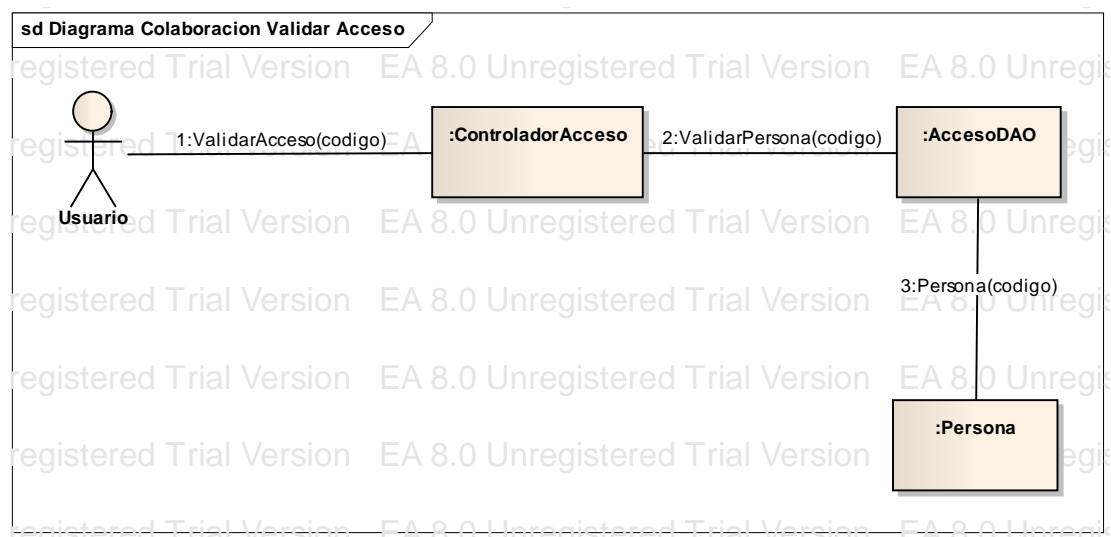
Consultar Acceso

Figura 21 Diagrama de Colaboración Consultar Acceso



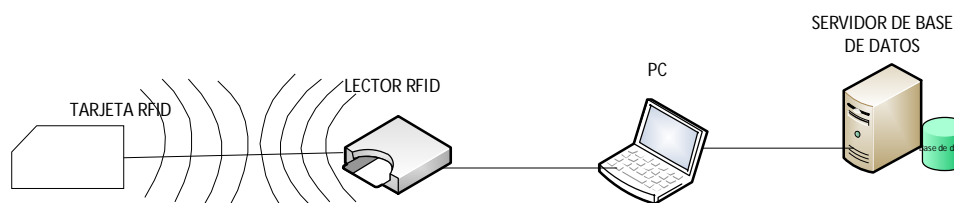
Validar Acceso

Figura 22 Diagrama de Colaboración Validar Acceso



Luego de finalizar el análisis para el diseño del prototipo llegamos a la conclusión de que el funcionamiento del sistema será acorde o similar a lo que se describe en la figura 23.

Figura 23 Funcionamiento Sistema Control de Acceso



El computador es quien siempre comienza las secuencias de comunicación enviándolas al lector con una secuencia de pregunta.

El lector es el encargado de emitir la secuencia de pregunta enviada por el computador por una señal de radio frecuencia.

Las tarjetas reciben el mensaje emitido por el lector y responden a este mensaje emitiendo un código, el lector lo recibe y lo envía la respuesta al computador.

El computador recibe la respuesta y ejecuta su lógica de negocio.

y por último valida los datos con el servidor y posteriormente la almacena.

Detalles de la metodología Utilizada en el análisis para el desarrollo del sistema

La metodología utilizada para el desarrollo de cada uno de los módulos que componen el sistema se basó principalmente en metodologías de análisis y diseño de software orientado a objetos, ya que es una metodología tan completa que solo se necesita de los mismos conceptos tanto para el análisis y la implementación de aplicaciones que desean satisfacer en su totalidad la necesidad del cliente de una forma más completa y usable en posteriores fases del producto.

Para conocer más a fondo el proceso que se llevó a cabo para la implementación del prototipo de control de acceso a la Corporación Universitaria Lasallista, comenzaremos diciendo que para el desarrollo de un software primero se debe iniciar con un análisis de las necesidades del sistema, de donde apoyándonos en la metodología de Craig Larman para el análisis y diseño de software se pudo encontrar el sistema base que rige el producto, es decir, se diseñaron diagramas como por ejemplo el Diagrama de dominio donde especificamos las clases madres del software, Diagrama de clases donde visualizamos la interacción de todas las clases entre sí para

logar un funcionamiento adecuado para suplir la necesidad del cliente; esto por la parte de análisis y diseño de software.

Pasando a la implementación se realizaron algunos controles de cambio al sistema inicial ya que a medida que se iba desarrollando se fueron aclarando procesos que mostraban un mejor y eficiente funcionamiento del sistema, uno de los controles de cambio fue cambiar la metodología de desarrollo de RUP a metodología de desarrollo ágil, este cambio se dio ya que al mercado ingreso una herramienta de desarrollo con metodología ágil y fácil de implementación llamada LightSwitch.

A continuación detallaremos cada modulo y hardware que integran el sistema.

Componentes de Hardware

- ✓ Lector **USB TCR-501** el cual trabaja a una frecuencia de 13.56 MHZ.
- ✓ Tarjetas MIFARE con un protocolo universal estándar ISO/IEC 15693 (TAG-IT HFI).
- ✓ Equipo Servidor.

Componentes Software

Software de administración

Con este software se realiza la administración de usuarios (figura 24) y tarjetas (figura 25), consulta y reporte de accesos (figura 26). Este software es una aplicación Web

desarrollada con la herramienta Visual Studio LightSwitch 2011 conectada con la base de datos desarrollada en SQL Server 2008 R2.

Figura 24 Administración de Personas

Inicio

Administrar Personas X

Personas

	Identificación	Nombre	Apellido	Categoría
▶	71396619	Cesar Augusto	Ruiz Jaramillo	Empleado ▼
	70563830	Álvaro de Jesús	Arango Ruiz	Empleado ▼
	43742630	Angélica María	Hernández	Empleado ▼
	76319129	Carlos Arturo	David Ruales	Empleado ▼
	1026137285	Édison	Rivera Aroyave	Empleado ▼
	75080683	Francisco Javier	Arias Vargas	Empleado ▼
	79338924	Jairo Augusto	Alvarado Sánchez	Empleado ▼
	79953370	Juan Carlos	Restrepo Botero	Empleado ▼
	71366023	Juan Fernando	Montoya Carvajal	Empleado ▼
	43208208	Lina María	Varón Jiménez	Empleado ▼
	98566561	Luis Felipe	Londoño Ardila	Empleado ▼
	42894495	María Encarnación	Ramírez Escobar	Empleado ▼
	42982619	Silvia Stella	Moreno Rodas	Empleado ▼

Figura 25 Administración de Tarjetas

Inicio

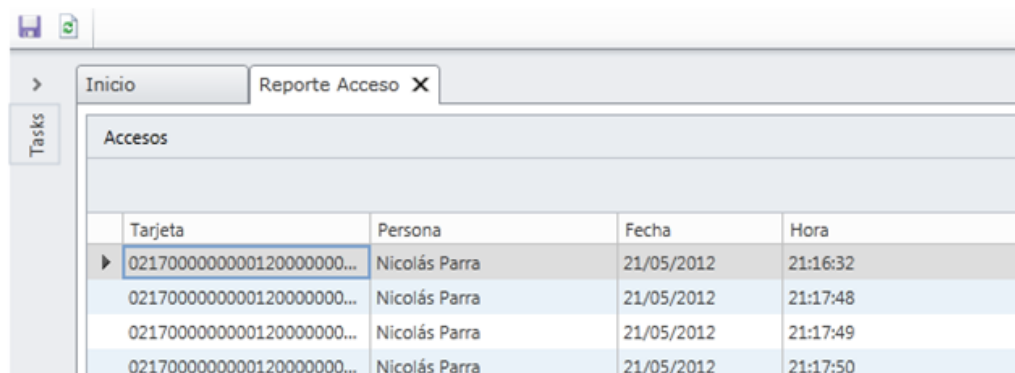
Administrar Tarjetas X

Tarjetas

+

X

	Código tarjeta	Estado	Persona
▶	020004305C71F1E803	Activa	▼ Álvaro de Jesús Arango Ruiz ▼
	020004408E73F17803	Activa	▼ Angélica María Hernández ▼
	020004908474F19503	Activa	▼ Carlos Arturo David Ruales ▼
	020004F03173F14703	Activa	▼ Édison Rivera Aroyave ▼
	020004908D72F19A03	Activa	▼ Francisco Javier Arias Vargas ▼
	020004B0CF71F1FB03	Activa	▼ Jairo Augusto Alvarado Sánchez ▼
	020004302175F19103	Activa	▼ Juan Carlos Restrepo Botero ▼
	020004B07E74F14F03	Activa	▼ Juan Fernando Montoya Carvajal ▼
	020004806F76F16C03	Activa	▼ Lina María Varón Jiménez ▼
	020004504073F19603	Activa	▼ Luis Felipe Londoño Ardila ▼

Figura 26 Reporte de Accesos


Tarjeta	Persona	Fecha	Hora
0217000000000120000000...	Nicolás Parra	21/05/2012	21:16:32
0217000000000120000000...	Nicolás Parra	21/05/2012	21:17:48
0217000000000120000000...	Nicolás Parra	21/05/2012	21:17:49
0217000000000120000000...	Nicolás Parra	21/05/2012	21:17:50

Software de validación y registro de acceso.

Es una aplicación de escritorio desarrollada con Visual C# 2010 que interactúa con la base de datos y el lector RFID, cuya responsabilidad es recibir los datos obtenidos por el lector desde el Tag y realizar las validaciones sobre la base de datos para autorizar o no autorizar el acceso como se muestra en las figuras 27 y 28, si el acceso es autorizado se registra en la base de datos la persona que accede, fecha y hora.

Con esta aplicación también se tiene, la posibilidad de registrar el ingreso de los visitantes como lo registra la figura número 29, los cuales no poseen tarjetas de acceso por tanto con esta aplicación se registran los datos Identificación, nombre, apellidos, fecha y hora.

Figura 27 Aplicación de Escritorio (Acceso Autorizado)

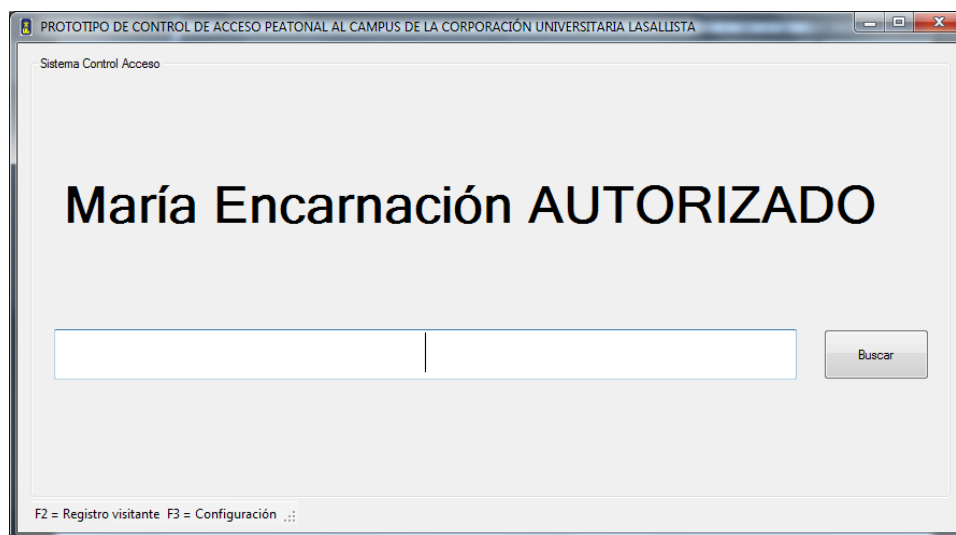


Figura 28 Aplicación de Escritorio (Acceso No Autorizado)

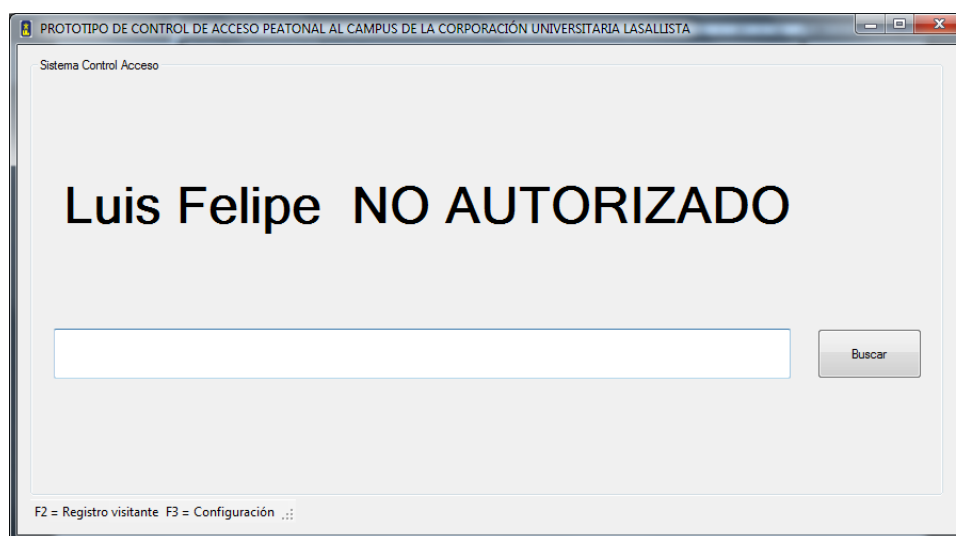
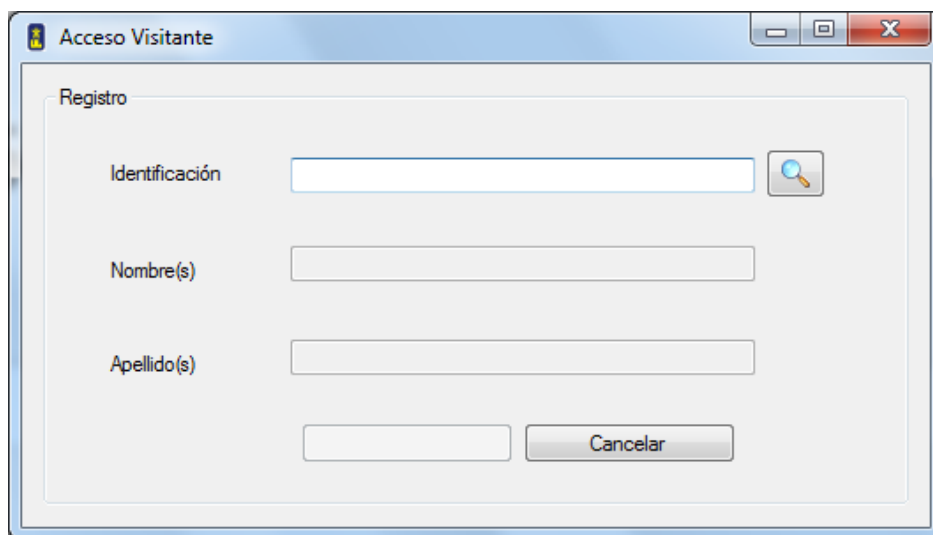


Figura 29 Registro Acceso Visitantes

Acceso Visitante

Registro

Identificación

Nombre(s)

Apellido(s)

Cancelar

Software Recolector de Datos

Es un software instalado en el lector desde fábrica, que tiene como función escribir y leer información desde y en los tag, y responde a las señales enviadas por el computador.

Resultados

Para llevar a cabo la ejecución de las pruebas del sistema De control de acceso para la corporación Universitaria lasallista se implemento un prototipo que simulara el funcionamiento del sistema al ingreso del campus; para el desarrollo de las prueba se realizara la siguiente estrategia.

Se instalara en el lugar correspondiente (portería principal de la Corporación), el prototipo que consta de elementos tales como un computador portátil que cumple la función de “Servidor” y cliente en él estarán instaladas las últimas versiones del desarrollo de cada uno de los módulos que fueron implementados a lo largo del desarrollo de todo el proceso de investigación, también tendrá instalado el motor de base de datos donde se guardaran los registros de los ingresos que se capturen desde el sistema.

Se instalara también el lector RFID que junto con el ordenador y sus aplicaciones constituyen el 90% del total del sistema, este lector será el encargado de leer las tarjetas, las cuales contienen la información de las personas que las porten, con esto último (Tarjeta) podemos decir que se tiene el otro 10% faltante de los componentes que integran y completan el proceso de control de acceso.

Para que el sistema funcionará correctamente fue necesario dictar una corta capacitación al personal de vigilancia, los cuales cumplieron el rol de agente supervisor para vigilar el buen uso y funcionamiento del proceso; se les explicó detalladamente las funcionalidades de cada módulo que integra el sistema.

Se les explicó con más detalle el módulo que registra los accesos de personas externas a la corporación, es decir, los ingresos que se presentaran como visitantes.

Para lograr que el proceso de captura de información por medio del prototipo se llevara a cabo, fue necesario contar con personal administrativo de la Corporación, los cuales entraron a ser parte de la muestra en cuestión de estas pruebas, en la figura 30 se muestra el registro de las personas que hicieron parte de estas pruebas.

Figura 30 Muestra para la ejecución de las pruebas.

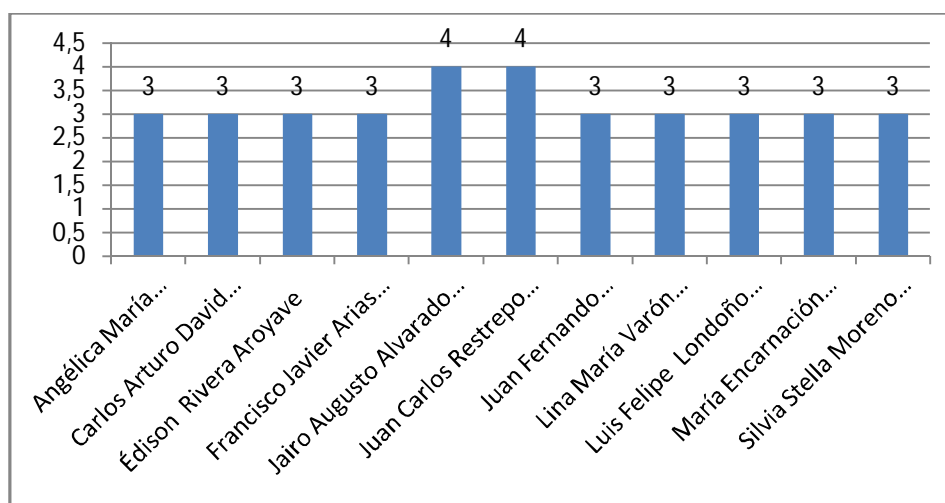
Estado	Persona
Activa	Álvaro de Jesús Arango Ruiz
Activa	Angélica María Hernández
Activa	Carlos Arturo David Ruales
Activa	Édison Rivera Aroyave
Activa	Francisco Javier Arias Vargas
Activa	Jairo Augusto Alvarado Sánchez
Activa	Juan Carlos Restrepo Botero
Activa	Juan Fernando Montoya Carvajal
Activa	Lina María Varón Jiménez
Activa	Luis Felipe Londoño Ardila
Activa	María Encarnación Ramírez Escobar
Activa	Silvia Stella Moreno Rodas

El sistema estuvo instalado en la portería por un periodo de 4 días de los cuales se obtuvieron los siguientes resultados en el ambiente real del proceso.

Se realiza una depuración de los registros encontrados en el sistema y se concluye que las personas que integraron la muestra mostraron total disposición para lograr observar el funcionamiento real del sistema, también podemos decir que ellos sin falta pasaron día a día sus tarjetas para lograr un ingreso exitoso en el sistema.

En la figura 31 tenemos la estadística del funcionamiento del sistema durante los 4 días de funcionamiento del piloto, hay que tener presente que el rango de fechas fueron del 03/07/2012 al 06/07/2012, más detalladamente en esta grafica tenemos la cantidad de accesos por empleado durante el rango de fechas anteriormente mencionadas.

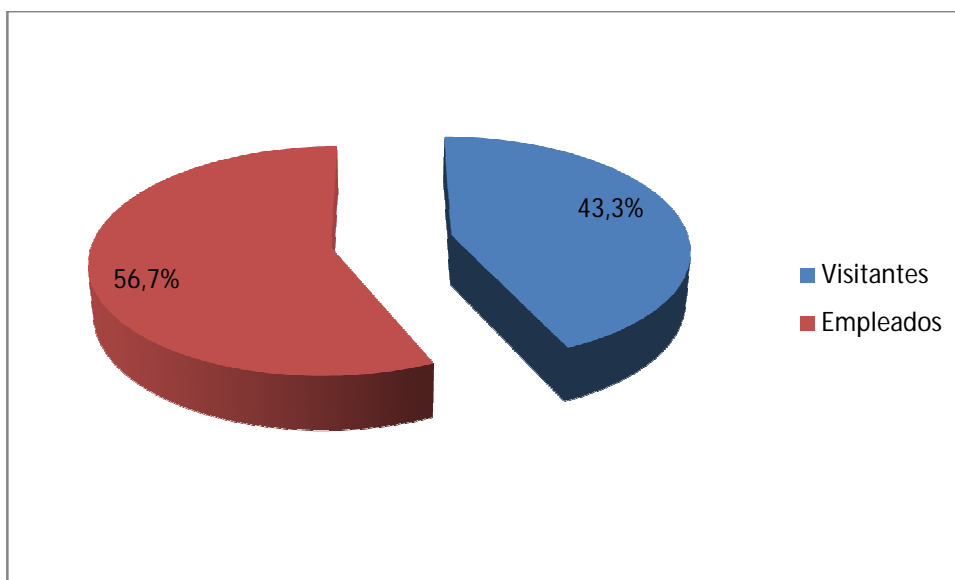
Figura 31 Cantidad de accesos por persona



Por parte del módulo de registro de visitantes se obtuvieron resultados muy favorables especialmente para este módulo ya que al personal de vigilancia se les hizo más rápido, fácil y practico el registro de terceros por medio de este entorno, en la figura 32 se muestra una estadística en cuanto a ingresos de empleados y visitantes en términos de porcentaje , en total se registraron 67 acceso donde el 56,7% registran el ingreso de empleados y el 43,3% los registros generados por los visitantes; aun que las sugerencias por parte de este personal es tener en cuenta en la implementación final de proyecto el formato actual que ellos utilizan para tal registro, nos informan que es bueno que se

tengan en cuenta campos como: con qué fin visita la universidad y para donde se dirige.

Figura 32 Estadísticas de ingresos entre empleados y visitantes.



A continuación en la figura 33 se muestran algunos ingresos que fueron registrados por el personal de vigilancia en el modulo correspondiente y del cual merecieron sus opiniones.

Figura 33 Registro de visitantes.

Identificación	Nombre	Apellido	Categoría
1026136327	Nicolas Giovany	Parra Morales	Visitante ▼
1026138244	Diana	Morales	Visitante ▼
12345	fsdfs	sdfasdf	Visitante ▼
1037615272	John	londoño	Visitante ▼
3493214	gildardo	giraldo	Visitante ▼
15347840	Juvenal	herrera restrepo	Visitante ▼
71640226	Jose Enrique	gutierrez	Visitante ▼
95092328547	brayan alexander	prosaco caribe	Visitante ▼
43722583	adriana	moncada	Visitante ▼
15259024	rodrigo	tamayo	Visitante ▼
1152193744	emanuela	calle	Visitante ▼
41947578	paula	trejos	Visitante ▼
71876969	luis	palacios	Visitante ▼
70087486	luis fernando	fernandez	Visitante ▼
43578088	luiza fernanda	sierra gallon	Visitante ▼
42781216	sandra yannet	medina pierotti	Visitante ▼
43626344	paula andrea	moreno angel	Visitante ▼
70555654	julio hernando	buritica	Visitante ▼
89040469029	fredy	muñoz escalante	Visitante ▼
1040732930	eliana	artuanga	Visitante ▼

Otros resultados obtenidos en la entrevista realizada al personal de vigilancia a cargo del proceso durante la semana en que estuvo el piloto en funcionamiento, el vigilante Adrian Ignacio Torres Marín, opina que el sistema le parece demasiado bueno ya que les permitiría cumplir con la verdadera función que tienen como personal de vigilancia que es velar por la seguridad y el control de personal al ingreso de la Universidad; “poder ofrecer un mejor servicio a los visitantes, y no tener que estar centrados en la recepción de todas y cada una de las personas que ingresan al campus.”

“Principalmente con la implementación del sistema el servicio de vigilancia estaría más tranquilo porque todas las personas que ingresen o deseen ingresar deberán portar un carnet de identificación que pasaran por el lector y este les permite el ingreso por medio de validaciones reales dentro del sistema de la universidad, es decir, contra registros reales de pertenencia a la universidad y no con el proceso normal donde se nos muestra un carnet como identificación pero no sabemos qué tan verídico sea y la otra

ventaja para el servicio de vigilancia seria poder mejorar el control de las personas visitantes ya que podremos ofrecer un mejor servicio(más amables y entregados al servicio a terceros) sin tener que estar pendiente de que van a ingresar personas ajenas a la corporación mientras estamos atendiendo una visita”.

¿Qué sugerencias nos pueden aportar al sistema?

Para la implementación se debe tener en cuenta los sistemas que actualmente funcionan en otras instituciones, es decir, para que el sistema sea totalmente automático debe contener un torniquete ya que este cumpliría nuestra función de vigilancia mientras estamos atendiendo las personas que no tiene tarjeta de acceso y así el personal de vigilancia identifique más fácil la validación de los ingresos, y que las personas sean las que deban acercar la tarjeta al lector y así disminuir el tiempo de ingreso de ellas.

Teniendo en cuenta todos los aportes por parte del personal de vigilancia, podemos concluir que el éxito del sistema está en el buen control, administración y correcto uso de los módulos y materiales que conforman o lleguen a integrar el sistema y así poder incrementar día a día la seguridad y la confianza al pertenecer a la Corporación Universitaria Lasallista.

Conclusiones

Después de analizar todas las tecnologías disponibles para el control de acceso; por su agilidad, confiabilidad y seguridad la RFID es la más apropiada para la implementación del prototipo en la Corporación.

Los software desarrollados nos permitirán agilizar el acceso al campus ya que este va a ser el encargado de realizar esta tarea de forma más rápida y segura.

RFID es una tecnología que aparte de permitir crear aplicaciones de control de acceso también nos permite crear aplicaciones para monitoreo y seguimiento de personas, automatización de plantas industriales, manejo de inventario en bodegas, entre otra infinidad de funcionalidades.

Se tiene la posibilidad de implementar gran cantidad de aplicaciones que aporten a un mayor crecimiento integral del campus de la corporación mejorando así la calidad de las personas que pertenecen y asisten día a día a este espacio educativo.

Recomendaciones

A lo largo de la investigación nos dimos cuenta que la tecnología por radio frecuencia nos arroja ventajas tanto de costo como de funcionalidad por lo cual nos lleva a pensar que esta tecnología por su facilidad de manejo y control es la más indicada para crear grandes proyectos dentro del campus de la universidad de los cuales se pueden resaltar para próximos proyectos los siguientes:

- Sistema de control de acceso a las aulas de informática.
- Reserva controladas por RFID de las aulas de informáticas y salones tecnológicos como los del Bloque C y Bloque B
- Control de personal en el ingreso de la biblioteca
- Reservas, Préstamos y devoluciones del material bibliográfica y digital de la biblioteca.
- Control de acceso a los diferentes laboratorios con los que cuenta la Corporación.

Entre otros proyectos que con la dedicación y disponibilidad de los alumnos se pueden llevar a cabo dentro de los grupos de investigación que hasta hoy existen en la Universidad.

También se le recomienda a las personas (docentes) que hacen parte de estos grupos de investigación y que son los guías de estos grupos de trabajo, que acompañen con más dedicación y entrega a los alumnos que quieren hacer de la Institución un lugar más competitivo en la parte de la investigación de proyectos tecnológicos a nivel nacional e internacional y así poder obtener más nivel educativo y profesional para enfrentar el desarrollo y avance del mundo.

Para el presente trabajo de investigación los resultados fueron favorables en cuanto acogida, disposición y agrado por parte de las personas que formaron parte de la muestra, Por tanto la recomendación que se le deja a la administración de los proyectos, es que los estudiantes también tiene ideas brillantes para lograr soluciones a un problema y lo único que se necesita es que la Corporación apoye los proyectos que realmente aportan un avance y mejora del campus, incremento en él, el análisis y desarrollo de proyectos y al desarrollo integral de la persona.

Bibliografía

Almeida, Daniel. (2008) *Diseño e implementación de un prototipo para un sistema de monitoreo de personal basado en RFID*. Recuperado de: <http://bibdigital.epn.edu.ec/handle/15000/4198>

Cervantes Najera, Alejandro. (2006) *Sistema de información y control de acceso basado en tecnología RFID*. Recuperado de <http://itzamna.bnct.ipn.mx:8080/dspace/bitstream/123456789/5473/1/SISTEMADEINFORM.pdf>

Competitivo de la cadena de carne bovina en la región del MERCOSUR. Recuperado de: http://www.produccion-animal.com.ar/produccion_organica_y_trazabilidad/41-sistemas.pdf

CVNE, Centro Virtual de noticias de la educación, (2012). *Tarjeta Integrada Personal en la UdeA*. Recuperado de: <http://www.mineduacion.gov.co/cvn/1665/w3-article-235236.html>

ERICEL & DETEC INGENIERÍA. Documentación: Lector RFID DTR10-232[en línea]. <http://www.ericel.com/>.

Green, Raúl. (2007). *Plataforma Tecnológica Regional, hacia el fortalecimiento*

Herrera, José María. *Estudio, Diseño y simulación de un sistema de RFID Basado en EPC*. Recuperado de: <http://upcommons.upc.edu/pfc/bitstream/2099.1/3552/2/40883-2.pdf>

Herrera, Juan. (2011). *Tecnología RFID aplicada al control de accesos*. Recuperado de: http://polibits.gelbukh.com/2009_40/40_08.pdf.

Jaramillo, Diana. (2009). *Sistema de Control de Personal*. Ingeniero en Electrónica y Telecomunicaciones. Guayaquil: Escuela Superior Politécnica del Litoral.

Larman, Craig (2004). *Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design*. Westford : Pearson Education.

Placencia, Diego. (2007). *Diseño y construcción de un prototipo de RED para el control de ingreso a sitios de acceso masivo utilizando la tecnología de identificación por radio frecuencia (RFID)*. Recuperado de: <http://bibdigital.epn.edu.ec/handle/15000/778>.

Pupiales, Pablo. *Diseño de un sistema de control de acceso utilizando la tecnología RFID para la empresa Soluciones G cuatro del Ecuador CIA. LTDA*. Recuperado de: <http://biblioteca.cenace.org.ec>

Rodríguez, Marco. (2007). *Sistema de Gestión de acceso mediante RFID*. Catalunya: Universidad Politécnica de Catalunya.

Servicios informáticos kiffer: *Introducción a los sistemas RFID*. Recuperado de <http://www.kifer.es/Recursos/Pdf/RFID.pdf>