UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Sistema de control de acceso para el laboratorio de Redes y Seguridad – DIE – FI - UNAM

TESIS

Que para obtener el título de

Ingeniero en computación

P R E S E N T A

Miguel Ángel Martínez Sánchez

DIRECTOR DE TESIS

M.C. María Jaquelina López Barrientos

Ciudad Universitaria, Cd. Mx., 2016

ÍNDICE

ÍNDICE DE FIGURAS Y TABLAS

Introducción

Con el continuo crecimiento que han tenido las tecnologías de la información cada día es más notorio que las generaciones van cambiando y que se encuentran más involucradas con el uso y manejo de diversos dispositivos, plataformas, entre otras tecnologías que ayudan a satisfacer las necesidades de la sociedad en cada uno de los aspectos de la vida diaria.

Debido al impacto que han tenido estas tecnologías cada vez existe un mundo donde la comunicación es mucho más fácil y las distancias se ven relativamente pequeñas pero también existen desventajas ya que no se puede asegurar con quién se realizan las comunicaciones o con quién se comparte la información.

La seguridad informática es uno de los aspectos fundamentales en el mundo moderno ya que se ha demostrado que no hay elementos tecnológicos en el mundo que no la requieran, ya que debido a la explosión de las tecnologías de la información se ha visto un incremento significativo en el uso de las mismas pero al mismo tiempo se ha podido observar un crecimiento significativo en los delitos cibernéticos.

Sin embargo es notorio que la tecnología se está volviendo inherente a la seguridad informática puesto que nada ni nadie en ningún ambiente está dispuesto a dejar que su privacidad se vea vulnerada y/o pueda ser engañado por alguna entidad desconocida.

De este modo surgen diversos dispositivos lectores como lo son de huella digital, de retina, de códigos de barras, por proximidad, entre otros. Los cuales existen para asegurar la identidad de los individuos basándose en características físicas únicas o en algún identificador exclusivo que además de verificar y garantizar la identidad del usuario permiten llevar a cabo diversas actividades como el control de acceso a lugares que tienen acceso restringido.

En ese sentido, cabe mencionar que en la Facultad de Ingeniería en la carrera de Ingeniería en Computación se puede cursar el módulo terminal de Redes y Seguridad, en el cual los estudiantes se involucran con temas relacionados a estos ámbitos y como parte complementaria de esas asignaturas deben llevar a cabo diversas actividades a través de la realización de prácticas en el laboratorio de Redes y Seguridad.

Laboratorio en el que es indispensable llevar a cabo un control de acceso, a fin de que solamente los estudiantes y profesores que cursan e imparten clases durante el semestre ingresen a las instalaciones, esto con el fin de preservar los materiales y equipos que ahí se encuentran con el objetivo de brindar un mejor servicio a la comunidad académica.

Actualmente el laboratorio de Redes y Seguridad se utiliza para impartir distintas clases y cursos para alumnos y externos, operando prácticamente todo el año exceptuando los dos periodos de vacaciones administrativas uno a mediados y otro a finales de año, del mismo modo el número de usuarios al semestre escolar es de aproximadamente 500 usuarios y en período inter-semestral de 150 usuarios(en el mayor año de oferta-demanda), por lo que es pertinente considerar que puede alcanzar un promedio de hasta 1300 usuarios al año.

Por lo que los objetivos de este trabajo son:

General:

Diseñar e implementar un sistema de control de acceso para el Laboratorio de Redes y Seguridad.

Particulares:

- Entender el funcionamiento de un sistema de control de acceso.
- Conocer los elementos fundamentales para llevar a cabo un control de acceso efectivo.
- Hacer una comparativa entre las diferentes opciones de dispositivos de control de acceso para evaluar ventajas y desventajas.
- Que el sistema de control sea versátil, esto es, que funcione aun cuando existan circunstancias o eventos que pudieran impedir el funcionamiento.
- Implementar un sistema de vanguardia que permita salvaguardar los activos del laboratorio.

De manera que para alcanzar los objetivos planteados es que en la capítulo 1 se presenta un marco teórico en el que se dan a conocer los principales conceptos que se manejan en el presente trabajo de Tesis.

En el capítulo 2 se presentan diferentes alternativas para solucionar la problemática del laboratorio y se menciona a detalle los elementos para cada una de ellas.

En el capítulo 3 se explica a detalle la solución seleccionada, por lo que se menciona todos los requerimientos y el proceso de desarrollo de la misma.

De manera que al final del documento se dan a conocer las conclusiones y resultados alcanzados a través del presente proyecto

1.Marco Teórico

En este capítulo se analiza a profundidad el estado actual del laboratorio, así como conceptos clave que ayudan a comprender los objetivos que se buscan con este proyecto.

1.1 LABORATORIO DE REDES Y SEGURIDAD DIE- FI – UNAM

El laboratorio se encuentra en el primer piso del edificio Bernardo Quintana Arrioja también conocido como edificio T ubicado en el conjunto sur de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México y cuenta con las siguientes características:

- Instalaciones: Se cuenta con un salón de laboratorio compuesto por un área de docencia (5m x 6m), un área para profesores, tesistas y servicio social (2m x 3 m) y un área administrativa(2m x 3m) (véase figura 1.1)
- Dimensiones: 7.5 m x 6 m aproximadamente.
- Cableado: El cableado del laboratorio está instalado a través de diversas canaletas que permiten la correcta distribución del cableado hacia los diferentes equipos que conforman la red según el área de trabajo correspondiente, principalmente las áreas de: docencia, administración y la de profesores, tesistas y servicio social.
- Equipos: Se cuenta con 11 equipos distribuidos en el área de docencia, 2 para las áreas de profesores, tesistas y servicio social, además de 3 routers, 2 switches, 2 servidores y 1 equipo para el área administrativa.

Figura 1.1 Diagrama del laboratorio de Redes y Seguridad

Instalación eléctrica: el laboratorio cuenta con una instalación eléctrica la cual llega a través de la parte media del área administrativa para posteriormente dividirse en dos, la primera le brinda servicio eléctrico al área administrativa, mientras que la segunda se envía mediante un conducto a nivel de suelo hacia los paneles por los cuales se distribuye hacia todos los equipos del área de docencia. (véase figura 1.2)

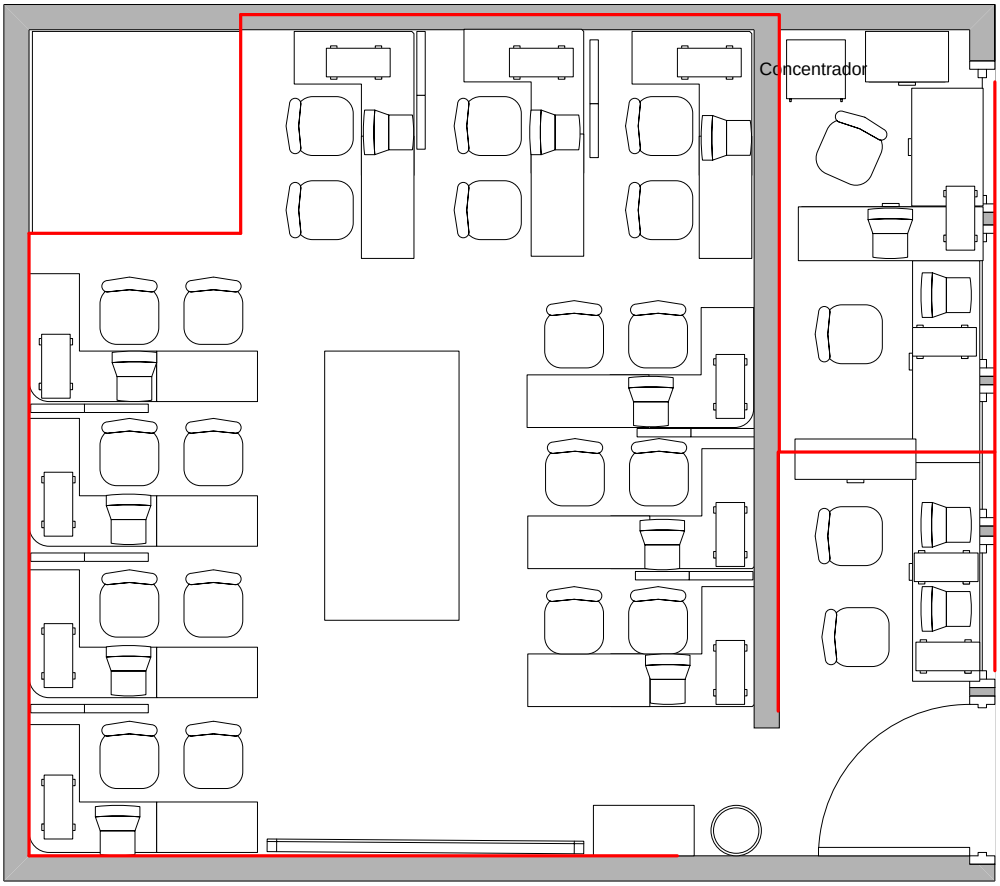

Figura 1.2 Instalación eléctrica en rojo

1.2 PROBLEMÁTICA

La problemática está compuesta por varios puntos a los cuales se debe dar solución ya que son parte esencial para mantener la seguridad e integridad del laboratorio, y estos se detallan a continuación:

- Registro de personal: se registran manuscritamente en una libreta al momento del acceso.

- Diferentes tipos de personal:
  - alumnos,
  - profesores,
  - prestadores de servicio social,
  - ayudantes,
  - invitados o visitantes.
- Tiempo de acceso: al ser un registro manual el tiempo promedio por grupo de 20 alumnos es de 8 minutos.
- Inseguridad en el control de acceso: al ser mediante una libreta, en forma manuscrita, y que no haya personal dedicado a corroborar la veracidad de los datos, no se puede dar veracidad a los nombres ahí anotados.
- Falta de Autenticación: no se puede asegurar que los usuarios sean quienes dicen ser, incluso existe la posibilidad de que algunos no se registren.
- Falta de Rastreabilidad: dada la inseguridad en el control de acceso es difícil confirmar quién, cómo y cuándo hizo algo y en qué equipo ya que el registro pudo ser incompleto (falta de hora de entrada, de salida, de equipo utilizado, y firma).
- Inexistencia del servicio de No repudio: debido a la falta de los controles antes mencionados es factible que alguien pueda negar sus acciones en el laboratorio.
- Bitácora inconfiable: con base en los puntos anteriores la bitácora que se genera carece de confiabilidad.

1.3 CONCEPTOS DE SEGURIDAD

Primordialmente cabe destacar dos conceptos muy diferentes en cuanto a seguridad ya que la seguridad informática es el conjunto de métodos, técnicas y prácticas que

protegen la plataforma tecnológica de cualquier amenaza, mientras que la seguridad de la información se define como el conjunto de métodos, técnicas y prácticas que brindan protección a la infraestructura tecnológica y la información que circula por la misma así como la contenida.

Este documento se enfoca principalmente en la seguridad de la información debido a los elementos que se manejan actualmente en el laboratorio por lo cual entre los principales conceptos que es conveniente manejar y tener presentes a lo largo de la realización del presente proyecto de tesis son lo que a continuación se presentan.

1.3.1 Seguridad Física

Hace referencia a las barreras físicas y mecanismos de control de los sistemas informáticos que protegen el hardware y cualquier elemento físico que maneja información de carácter confidencial de tal manera que se salvaguarde la información de cualquier elemento humano o natural que pueda comprometer o causar pérdida de información

Algunos de los elementos a proteger dentro del laboratorio de seguridad son:

- Computadoras
- Switches, routers y otros dispositivos de telecomunicaciones
- Bitácora
- Cableado
- Sistemas eléctricos
- Mobiliario

Algunos ejemplos de seguridad física son:

- Las llaves o mecanismos de acceso al laboratorio de Redes y Seguridad
- Contar con extintores y barreras que detengan o eviten la propagación de un incendio.
- Contar con sistemas que monitoreen las acciones y o los accesos (cámaras, sistemas de control de acceso, entre otros)
- El encargado del laboratorio cuya tarea es salvaguardar y revisar los elementos que contengan información.

1.3.2 Seguridad lógica

La seguridad lógica hace hincapié en la aplicación de barreras y mecanismos de control que protejan la integridad, confidencialidad y disponibilidad de la información (conocida como la Tríada CIA) dentro de los elementos que contengan o manejen esta información.

Algunos ejemplos de seguridad lógica son:

- Restringir acceso a programas y/o documentos.
- Habilitar sistemas de encriptación de canales y/o documentos
- Definir los privilegios de usuarios
- Controlar el uso de archivos y programas
- Habilitar sistemas de seguridad como firewalls, antivirus, entre otros.

Cabe destacar que la seguridad física y lógica son dos elementos que trabajan juntos, ya que permite establecer un estricto control sobre el laboratorio, el cual ayudará a que exista un mejor desempaño en el mismo

1.3.3 Amenaza

Son aquellas actividades que pueden provocar daños a un sistema computacional cabe mencionar que pueden ser clasificadas en cuatro ramas:

- Humanas intencionales: Como su nombre lo indicada son todas aquellas que provienen de los seres humanos las cuales son realizadas con alevosía y ventajas. Ej: Ingeniería Social.
- Humanas involuntarias: Son acciones que aun cuando provienen de seres humanos son realizadas por error o accidentalmente. Ej: Derramar agua sobre un equipo de cómputo.
- Lógicas: Son las cuales no interactúan con el equipo físicamente pero atacan la información procesada y contenida en el mismo. Ej: Virus, gusanos por mencionar algunos.
- De ambiente naturales: En este punto se abarca todos los desastres naturales los cuales son imprevisibles y no hay manera de controlarlos. Ej: Terremotos, tornados, entre otros.

1.3.4 Vulnerabilidad

Es cualquier debilidad o problema que permite que un sistema sea dañado y puede ser de dos tipos:

- Inherente al sistema: Es una falla o debilidad que es parte del sistema, es decir que lo tiene desde que fue creado. Ej: Los huecos de seguridad en Windows.
- Por falta de un control: Se dan cuando los sistemas no tienen controles de seguridad implementados de manera adecuada o son usados correctamente por lo cual dejan hoyos que pueden ser explotados por alguna amenaza. Ej: Dejar las contraseña en un post it en el monitor.

1.3.5 Riesgo

Es la posibilidad de que una amenaza encuentre una vulnerabilidad, la explote y esto genere algún daño, por lo cual es importante considerar que los riesgos son lo que se debe reducir, y considerar que mientras se reduzcan las amenazas y/o vulnerabilidades los riesgos serán menores, además una buena mitigación de riesgos ayuda a estar mejor preparado para manejarlos.

Si bien no se debe olvidar los factores negativos de la seguridad hay que considerar la contraparte como los aspectos que se deben tener en cuenta para tener una correcta gestión de la seguridad es decir lo que se desea proteger y como se planea hacerlo.

1.3.6 Ataque

Es la materialización de una amenaza y ocurre cuando se conjuntan varios factores ya que para poder definirlo como ataque se requiere que exista una vulnerabilidad y una amenaza que logre explotar la vulnerabilidad, además es importante considerar que pueden variar en impacto dependiendo del evento de seguridad que haya ocurrido por lo cual los daños pueden variar.

1.3.7 Servicios de seguridad

Son aquellos que permiten mantener la seguridad de la información a través de diferentes controles los cuales se utilizan para salvaguardar los datos, a continuación se describirán estos controles.

1.3.7.1 Confidencialidad

Es el aseguramiento de que la información sólo será accesible para aquellos que tienen autorizado el acceso a la misma (usuarios o procesos) y nada ni nadie más podrá ver información para la cual no tienen privilegios, es decir la información no será revelada sin autorización.

1.3.7.2 Integridad

Indica que la información que se maneja debe ser confiable, completa y protegida de modificaciones no intencionales, no anticipadas y/o no autorizadas por la misma organización y/o dueño de la información que cuente con la autorización correspondiente, por lo cual debe de existir una relación entre los datos y la realidad del mundo exterior manteniendo una consistencia entre ambos.

1.3.7.3 Disponibilidad

Que la información y/o recursos informáticos se encuentren disponibles cuando sean requeridos o en los períodos contemplados para ello por las políticas de la organización, a fin de realizar alguna acción y/o alcanzar un objetivo evitando pérdidas por su ausencia.

1.3.7.4 Control de acceso

El control de acceso se encarga de determinar si el usuario o proceso tiene permitido o no el acceso a los recursos el cual se encuentra compuesto por varios elementos que se deben cumplir para con ello mantener el nivel de seguridad requerido y se enlistan a continuación.

1.3.7.4.1 Autenticación

Se debe comprobar que el usuario sea quien dice ser, por medio de algo que sabe, tiene o es, como por ejemplo: Por medio de un NIP, una credencial o de la huella digital.

1.3.7.4.2 No-repudio

Verifica que un usuario o proceso no pueda negar haber: recibido, enviado, ejecutado, creado, o borrado.

1.3.7.4.3 Cumplimiento

Es una característica que menciona que las personas/organizaciones deben conocer y cumplir con las diferentes disposiciones y/o requerimientos legales a las cuales se ven sometidas al manejar información.

1.3.7.4.4 Identificación

Se refiere a que el usuario o proceso compruebe su identidad para poder ingresar a través del control de acceso.

Ej. Credencial de la UNAM para realizar algún trámite.

1.3.7.4.5 Autorización

Es cuando se verifica que la persona o proceso cuenta con las credenciales que le permitan acceder a los recursos.

Ej. Un alumno no inscrito a alguna materia que se imparte en el laboratorio de Redes y Seguridad no debe poder ingresar a la sección de descarga de prácticas en el portal del laboratorio.

2.Alternativas de Solución

Debido a las características presentadas anteriormente se han desarrollado varias alternativas de solución, las cuales se dividen en tres, la primera abarca el acceso al laboratorio, la segunda abarca el registro y uso del laboratorio, mientras que la tercera menciona algunas recomendaciones para mejorar el desempeño del laboratorio.

2.1 CONTROL DE ACCESO AL LABORATORIO DE REDES Y SEGURIDAD

Al estar trabajando con seguridad es importante considerar cada aspecto y con ello se debe también considerar el acceso al laboratorio no solo al equipo de cómputo por lo cual en este inciso se revisan a detalle las alternativas con las que se cuentan para proteger las instalaciones así como los dispositivos que resguardan.

2.1.1 Llave mecánica de alta seguridad

- Es la que actualmente se tiene en uso (véase figura 2.1), es una cerradura de seguridad que permite tener un estricto control del laboratorio.
- Una gran desventaja es que forzosamente se tienen que repartir gran número de copias entre los profesores para que estos puedan acceder.
- También se corre el riesgo de que alguna copia se extravié y caiga en manos equivocadas.
- Además no permite conocer a quien accede al laboratorio, ni en qué momento.
- La implementación de costo más bajo.

Figura 2.1 Llave mecánica de alta seguridad

2.1.2 Dispositivo biométrico enlazado a cerradura mecánica.

- Este sistema consiste en dos dispositivos que se tienen que enlazar por medio de una interfaz (véase figura 2.2), por lo cual el dispositivo biométrico al detectar a alguien autorizado se enlaza con la cerradura mecánica para brindar acceso.
- Se tiene que adquirir un dispositivo biométrico y dependiendo del modelo será el costo, además depende mucho del modelo para conocer si permite llevar un registro de las entradas o no.
- No se requieren copias de las llaves de acceso, sólo usuarios autorizados podrán entrar lo cual lo convierte en una ventaja.
- Se debe considerar el caso en que no exista energía eléctrica, ya que para mantener funcionando el dispositivo debe adquirirse alguno con baterías y que la interfaz también cuenta con un respaldo eléctrico.
- Se debe adquirir una cerradura mecánica que permita manejar una interfaz y de este modo funcionar junto con el dispositivo.

- Considerar que al ser dos elementos con características especiales se sube el costo de esta implementación.

Figura 2.2 Dispositivo biométrico enlazado a cerradura mecánica

2.1.3: Cerradura biométrica de alta seguridad por huella digital.

- La más segura, ya que sólo usuarios autorizados pueden acceder haciendo uso de su huella digital (véase figura 2.3).
- Se usa con baterías y en caso de falta de energía cuenta con llave mecánica para poder abrir la cerradura.
- Dependiendo del modelo puede contar con conexión a base de datos lo que permite que la información de acceso se centralice y se lleve un registro de las entradas.

- Del mismo modo, dependiendo de la cerradura y sus características sus precios son muy elevados.
- Costo promedio es de $7,500.00 pesos (a noviembre de 2013)

Figura 2.3 Cerradura Biométrica de Alta Seguridad

2.2 REGISTRO DE USO DEL LABORATORIO DE REDES Y SEGURIDAD

Como se menciona al inicio de este trabajo es indispensable para el Laboratorio tener un control de acceso por lo cual de acuerdo a las necesidades que se identificaron se encontraron los siguientes tipos de dispositivos como alternativas de solución.

2.2.1 Dispositivos biométricos

La primera alternativa en ser identificada como una solución viable es el uso de dispositivos biométricos debido a su gran popularidad estos dispositivos han avanzado a pasos agigantados y cada uno tiene sus características únicas dependiendo del uso que se le quiera dar, a continuación se detallan las características de varios de ellos.

2.2.1.1 Lector de huella con enlace a computadora.

- Este dispositivo (véase figura 2.4) se encuentra enlazado a una computadora ya que es dependiente por energía y software Requiere registro previo de los usuarios.

- Acceso de usuarios mediante huella digital.
- Relativamente económico, ya que dependiendo del modelo puede incluir el software o requerir un desarrollo propio.
- Para llevar a cabo el control del uso de equipos sería necesario desarrollar adicionalmente el sistema que lo complemente.

Figura 2.4 Lector de huella con enlace a computadora

2.2.1.2 Controlador de acceso sin enlace a computadora.

- Dispositivos con memoria interna para realizar comparación de huellas (véase figura 2.5).
- Requiere registro previo de los usuarios.
- Acceso de usuarios mediante huella digital.
- Un poco más costoso que la opción 2.1.1, pero la ventaja es que no depende del equipo ni de que exista una conexión.
- De tamaños relativamente compactos.
- No es posible llevar a cabo el control del uso de equipos.
- No tienen conexión directa con base de datos, por lo cual se vuelve más complicado revisar los registros de accesos, sólo cuenta con RS232/ 485 y Tarjeta SD.
- Capacidad para almacenar 500 plantillas y 30,000 registros

- No cuenta con energía auxiliar requiere alimentación.
- Costo aproximado a mediados de febrero de 2014 es de $2,500.00 pesos

Figura 2.5 Controlador de acceso sin enlace a computadora

2.2.1.3 Controlador de acceso con enlace a computadora.

- Dispositivos con memoria interna para realizar comparación de huellas (véase figura 2.6).
- Requiere registro previo de los usuarios.
- Enlace a computadora para acceder a registros de acceso
- Acceso de usuarios mediante huella digital.
- Un poco más costoso que las opciones 2.2.1.1 y 2.2.1.2, pero la ventaja es que no depende de un equipo y permite la transferencia de datos de manera sencilla.
- De tamaños relativamente compactos.
- No es posible llevar a cabo el control del uso de equipos ni combinación de tipos de acceso.
- Cuenta con una conexión TCP/IP lo cual hace práctica la transferencia de datos para revisar los registros de acceso.

- Capacidad de almacenamientos de huellas de hasta 3,000 plantillas (huellas).
- Tiene la capacidad de operar de manera independiente y almacenar hasta 100,000 eventos. Esta información puede ser descargada por el software una vez que el equipo tenga acceso a la red de cómputo de sus instalaciones, a través de una conexión RJ45.
- No cuenta con energía auxiliar requiere alimentación por lo cual sería necesaria adquirir un no-break.
- Costo promedio a mediados de febrero de 2014 es de $6,000.00 pesos.

Figura 2.6 Controlador de acceso con enlace a computadora

2.2.1.3 Controlador de acceso por combinación con enlace a computadora.

- Dispositivo con memoria interna para realizar comparación de huellas (véase figura 2.7).
- Requiere registro previo de los usuarios.
- Acceso de usuarios mediante huella digital y/o contraseña (permite la combinación de tipos de accesos).
- El más costoso de los dispositivos biométricos.
- Mediante la combinación de accesos se busca llevar a cabo el control de equipos.

- Cuenta con una conexión TCP/IP lo cual hace práctica la transferencia de datos para revisar los registros de acceso.
- Memoria para 9000 usuarios y 35,000 registros
- La información puede ser descargada por el software una vez que el equipo tenga acceso a la red de cómputo de sus instalaciones, a través de una conexión RJ45.
- Batería de respaldo de energía de 4 hrs. promedio en caso de fallas de energía eléctrica.
- Costo promedio a mediados de febrero de 2014 es de $21,515.00 pesos

Figura 2.7 Controlador de acceso por combinación con enlace a computadora

2.2.2 Lector de código de barras.

- El dispositivo (véase figura 2.8) aprovecha las credenciales de estudiante de la UNAM para identificar a los alumnos.
- Requiere un registro previo de los alumnos junto con una foto, para identificar que realmente sean ellos y no entre alguien más en su lugar.
- Se necesita del uso de una computadora dedicada, así como un monitor que permita ver la foto del alumno al pasar su credencial.
- Es indispensable tener cierta supervisión por parte del profesor para revisar que los alumnos al autenticarse sean los dueños de la credencial (revisar las fotos en el sistema)

- El costo es relativamente bajo, se tiene que adquirir el lector y dedicar un equipo o de ser necesario adquirir uno.
- Se necesita un desarrollo que permita realizar la comunicación entre el lector y la base de datos, además tiene que permitir la introducción de información extra como es el número de equipo a utilizar. (Revisar Alternativas de solución en el apartado de software).
- Depende completamente de la energía eléctrica proporcionada por el equipo por lo cual para mantener una fuente de respaldo es obligatorio adquirir un no-break
- Su costo a mediados de febrero de 2014 ronda entre $800.00 y $2,500.00 pesos.

Figura 2.8 Lector de código de barras

2.2.3 Tablet Android.

- Esta herramienta (véase figura 2.9) puede aprovechar las credenciales de estudiante de la UNAM para identificar a los alumnos o leer un código QR generado para cada uno de ellos.
- Se requiere un registro previo de los alumnos junto con una foto, para identificar que realmente sean ellos y no entre alguien más en su lugar.
- No requiere más que el uso de la Tablet de manera dedicada para llevar a cabo el registro.
- Requiere cierta supervisión por parte del profesor para revisar que los alumnos al autenticarse sean los dueños de la credencial (revisar las fotos en el sistema).
- Tiene un costo que a mediados de febrero de 2014 ronda entre $1,300 y $7,000 pesos dependiendo de la marca y modelo de la Tablet.
- Se necesita un desarrollo que permita realizar la comunicación entre la cámara y la base de datos, además tiene que permitir la introducción de información extra como es el número de equipo a utilizar. (Revisar Alternativas de solución en el apartado de software).

Figura 2.9 Tablet Android

2.2.4 Software

Para los puntos anteriores se requiere ocupar software, que en la mayoría de las soluciones se maneja de manera independiente a la adquisición del dispositivo, esto es, se debe considerar un gasto adicional.

2.2.4.1 Software de dispositivo biométrico

- Se debe adquirir un software exclusivo del dispositivo, el cual se vende por separado.
- En algunos dispositivos incluye o se adquiere por separado un SDK para el desarrollo de aplicaciones.
- En menor medida y comúnmente para los dispositivos de mayor precio se incluye el software del dispositivo o el de desarrollo.

2.2.4.2 Lector de código de barras

- En cuanto al lector se propone el desarrollo de una solución en java que actúe como aplicación principal y permita la comunicación con una BD en SQL donde se almacene toda la información correspondiente a los grupos.

2.2.4.3 Tablet Android

- En la tablet se propone que se almacene la aplicación principal, la cual tendría que desarrollarse para Android, además de que se buscaría que ésta realizara una conexión vía inalámbrica a una BD SQL al igual que en la solución anterior.

A continuación se presenta en la tabla 2.1 un cuadro comparativo entre las distintas alternativas de solución.

Tabla 2.1 Comparativa entre los dispositivos de control de acceso

	Lector de huella digital	Lector de código de barras o QR	Acceso combinado	Registro De Equipo	Batería Interna	Conexión a servidor	No. Usuarios	Software	Costo aproximado en pesos (a mediados de febrero 2014)
Lector de huella con enlace a computadora	X					X	Indefinido	Depende del dispositivo puede incluirlo	$1,300.00
Controlador de acceso sin enlace a computadora	X						500	Incluido/ Debe programarse	$2,500.00
Controlador de acceso con enlace a computadora	X		X			X	3000	Incluido	$6,000.00
Controlador de acceso por combinación con enlace a computadora	X	X	X	X	X	X	9000	Incluido	$21,515.00
Lector de código de barras		X	X	X		X	Indefinido	Debe programarse	Entre $800.00 y $2,500.00
Tablet Android		X	X	X	X	X	Indefinido	Debe programarse	Entre $1,300.00 y $7,000.00

Con base en la tabla 2.1, los costos que aquí se presentan, así como las características consideradas y la problemática analizada anteriormente, se consideran como alternativas viables dos opciones las cuales serán revisadas con mayor detalle a continuación

Lector de código de barras.

- Es una solución idónea debido a las siguientes razones.
  - Costo – Tiene un costo que varía entre los $800 y $2500 pesos dependiendo del modelo, desde lo más básicos nos funcionan adecuadamente y el costo por software no tendría problemas ya que lo incluye o no lo requiere.
  - Implementación – No existe este problema ya que aun cuando se requieren más elementos para su uso como lo es una computadora, existen elementos disponibles en el laboratorio que podrían desempeñar esa labor.
  - Software – Permite desarrollar en una variedad de lenguajes entre ellos C y Java los cuales son lenguajes muy populares y fáciles de ocupar lo cual da opción a crear un desarrollo de gran funcionalidad.
  - Dependencia – El lector tiene una dependencia a otros dispositivos, ya que para manejarlo adecuadamente y con las medidas de seguridad deseadas se requiere que haya una computadora dedicada al acceso de los alumnos, además se debe verificar la conexión al servidor de BD.
  - Riesgos - En caso de falla habría que revisar dónde está ocurriendo y verificar cada uno de los dispositivos de los cuales depende (CPU, Monitor, Teclado, etc.) por lo que requiere dar mantenimiento a todos los dispositivos.
  - Energía – En caso de falla eléctrica si la computadora, el router/switch y el servidor no cuentan con un No-break el sistema no funciona.

- Tablet Android

o Es una solución idónea debido a las siguientes razones.

▪ Costo – Tiene un costo que ronda entre los $1,300 y $7,000 pesos considerando que solo va a ocuparse exclusivamente para el registro de usuarios se pueden ocupar los modelos básicos, mientras que la protección para fijar la misma tiene un costos aproximado de $400 pesos.

▪ Implementación – No existe problema solo debe de revisarse la conectividad de la red entre la Tablet y el servidor para mantener una comunicación constante con la BD.

▪ Software – Permite desarrollar en una variedad de lenguajes entre ellos C y Java los cuales son lenguajes muy populares y fáciles de ocupar lo cual da opción a crear un desarrollo de gran funcionalidad.

▪ Dependencia – No depende de otros dispositivos para su funcionamiento el único punto importante a considerar es que debe mantener conexión al servidor de BD para actualizar correctamente la información.

▪ Riesgos – En caso de alguna falla depende totalmente de la Tablet y tendría que ser reemplazada, pero puede sustituirse temporalmente con algún dispositivo Android.

• Energía – En caso de falla eléctrica es necesario que el servidor y el router/switch inalámbrico cuenten con un No-Break ya que la Tablet puede estar operando con su batería interna.

A continuación se presenta en la tabla 2.2 un cuadro comparativo entre las dos alternativas de solución más viables.

Tabla 2.2 Comparativa entre Tablet y Lector

	Tablet Android	Lector de código de barras
Características	Procesador a 1.3 GHz 1 GB RAM Tarjeta de red inalámbrica Memoria ROM: 4GB	Depende de una PC la cual debe tener las siguiente características mínimas: • Procesador a 1.8 Ghz • 2 GB RAM • Espacio disponible en HD de 150 MB • Tarjeta de red alámbrica o inalámbrica
Dependencia	Conexión activa al servidor	• Conexión activa al servidor • PC
Costo	Dependiendo del modelo de tablet y considerando la protección entre $1,700 a $ 7,400 pesos	Considerando únicamente el lector entre $800 y $2500 pesos
Espacio	La Tablet ocupará un espacio de unos 25 X 30 cm.	El lector ocupará un espacio de 1 X .5 m debido a la PC de la cual depende
Energía	Contar con un respaldo eléctrico para el servidor y el router/switch inalámbrico	Contar con un respaldo eléctrico para el servidor,el router/switch y la PC
Fallas	Es un solo elemento si existe una falla es más fácil aislar el problema	Debido a que depende de una PC es necesario analizar la PC y cada uno de los dispositivos para que funcione en óptimas condiciones
Software(Lenguajes)	Se recomienda C o Java	Se recomienda C o Java
Comunicación	Inalámbrica	Alámbrica

Con base en la tabla 2.2, los costos, las características consideradas y la problemática que aquí se presenta, se considera que la solución idónea es la Tablet Android debido a su versatilidad y múltiples funciones que permiten la implementación de un sistema más completo y efectivo.

2.3 PORTAL DE REGISTRO DE ALUMNOS PARA EL ACCESO AL LABORATORIO DE REDES Y SEGURIDAD

Aun cuando ya se cuenta con una solución para el registro de acceso al laboratorio es importante considerar una solución para el registro de los alumnos en la base de datos, ya que de realizarse de manera manual podría llevarle a los profesores y/o administrador del mismo un tiempo considerable de acuerdo a la cantidad de usuarios que existirían.

Adicionalmente al momento de realizar el registro manual se vuelve complicado debido al alto volumen de información por lo cual pueden existir errores que compliquen el seguimiento de asistencia del alumno por parte de los profesores como podría ser el caso de un número de cuenta incorrecto.

Como parte de la búsqueda de esta solución se determinó no utilizar las credenciales y de esta manera evitar algún uso indebido de las mismas así como evitar conflictos al leerlas debido al desgaste que pueden sufrir por lo cual se concluyó que una solución óptima es asignar un código QR para cada alumno, el cual se elaborará en base a su número de cuenta lo cual lo hará único y también permitirá que el usuario lo pueda portar como una

imagen en formato físico o electrónico e incluso ambas mientras mantenga guardado el código proporcionado, de modo que se debe considerar que la herramienta debe generar y entregar este código.

Considerando lo mencionado anteriormente se encontró como solución idónea el uso de un portal web el cual permitirá a los usuarios registrarse de manera similar a como lo hacen actualmente para la descarga de prácticas de laboratorio y conforme a esta visualización se obtuvieron las siguientes alternativas.

2.3.1 Desarrollo en JAVA y Tomcat

De acuerdo a la solución mencionada para el registro la primera alternativa fue desarrollar una solución que fuese basada en la misma plataforma adicionalmente para poder desarrollar esta aplicación se requiere del software Tomcat de Apache como una herramienta adicional, a continuación se enumeran sus características:

- Mismo lenguaje que la solución para el registro de uso del laboratorio.
- Trabaja adecuadamente con el SQL Server Express 2008 mientras se tengan las librerias.
- Complejidad en una implementación para ambientes WEB y depende de que trabaje adecuadamente el servicio de Apache Tomcat.
- No se puede trabajar directamente en vía web, por lo cual se debe realizar una aplicación que pueda montarse sobre el Tomcat.
- Configuración compleja puesto que de modo estándar se corren graves riesgos de seguridad.
- Permite regresar al momento del registro una imagen con el QR del alumno.

2.3.2 Desarrollo en C#

Otra alternativa que se obtuvo de la investigación para solucionar este punto fue una aplicación en C# que además trabaja en conjunto con SSL como herramienta adicional para montarse vía web, a continuación se mencionan sus características:

- Diferente lenguaje
- Trabaja adecuadamente con SQL Server Express 2008 puesto que al tratarse también de una herramienta de Windows son compatibles al igual que el SSL.
- El SSL normalmente viene incluido como una característica nativa de Windows 7 en adelante y solo hace falta activarlo, por lo cual su complejidad se reduce en gran medida.
- Del mismo modo que Java no puede trabajarse vía web directamente requiere en este caso el SSL.
- Automáticamente contiene ciertos esquemas de seguridad y solo se debe considerar la programación para evitar un SQL Injection.
- Realizar conexiones a la BD SQL es una característica incluida en el sistema.
- Permite regresar al momento del registro una imagen con el QR del alumno.

2.3.3 Selección del desarrollo idóneo

Debido a las características de ambos lenguajes mencionadas anteriormente se determinó usar el C# puesto que debido a las razones de seguridad y simplicidad del proceso es mucho más fácil de ocupar y adicionalmente considerando el entorno en el cual estará funcionando esta aplicación es totalmente externo al de la aplicación del

registro de uso del laboratorio por lo cual no importará si las aplicaciones no están basadas en el mismo lenguaje.

También fue importante para la selección considerar a cada uno de los intermediarios puesto que estos son los que nos permiten trabajar adecuadamente con los sitios programados, un detalle de importancia es mencionar que si se utilizará Java debería de añadirse un Software más como lo es Apache Tomcat y el sistema estaría dependiendo de esta aplicación y que el servicio estuviera conectado correcamente, mientras que el SSL al tratarse de una herramienta nativa de Windows simplifica mucho esta labor.

Cabe mencionar que esta solución solo se ocupará para realizar el registro de los alumnos por lo cual una vez concretadas las fechas para el mismo, este deberá ser desactivado por la administración del laboratorio para controlar la información y el registro de los usuarios.

2.4 RECOMENDACIONES PARA EL BUEN FUNCIONAMIENTO DE LAS INSTALACIONES

Este trabajo tiene como objetivo el control de accesos pero debido al análisis que fue llevado a cabo surgieron varios puntos importantes que se deben tener en cuenta para el laboratorio ya que ayudarían a mejorar y asegurar el desempeño de todos y cada uno de los elementos que lo componen.

2.4.1 Protección Eléctrica

Uno de los puntos más importantes a considerar al trabajar con el equipo de cómputo es la protección eléctrica ya que es común que la mayoría de los equipos se

dañen por no contar con un regulados y un no-break por lo que las fluctuaciones de energía o apagones pueden llegar a dañar algún componente, dañar alguna librería de algún programa o incluso llegar a generar un error de integridad en la base de datos por lo que siempre es importante contar con un dispositivo que permita apagar lo equipo de manera adecuada y que impida que los altibajos de energía afecten en cualquier aspecto.

2.4.2 Instalaciones no seguras

Un punto relevante son las instalaciones en las que se encuentra el laboratorio ya que se encuentra en un espacio donde se cuentan con cristales de media pared por lo cual se vuelve un gran riesgo el que se encuentre el laboratorio en este espacio ya que las características del mismo se podrían considerar una vulnerabilidad.

2.4.3 Condiciones de los equipos

El laboratorio actualmente no cuenta con un sistema de ventilación para mantener los equipos con ciertas condiciones ambientales que los mantengan en su estado óptimo y esto puede actuar como un factor importante para reducir el tiempo de vida de los dispositivos, además se tienen dos servidores uno de ellos de torre y el otro en rack y es importante mencionar que además de que se encuentran en un espacio reducido con problemas de ventilación no se tienen los elementos necesarios para estos equipos ya que el ejemplo más claro es que no hay un rack en el cual se pueda montar el servidor.

2.4.4 Prevención de accidentes

Se debe de considerar contar con un botiquín de primeros auxilios ya que como acceden muchos usuarios que manejan pinzas de corte y ponchadoras por primera vez puede llegar a suceder un accidente y es importante contar con las medidas básicas para ayudar al usuario mientras se le transporta a las instalaciones médicas correspondientes.

Por otra parte se debe contar con un extintor ya que según la Norma Mexicana de Seguridad y Prevención debe de contarse con un extintor por cada 200 metros cuadrados además debe colocarse en un lugar estratégico en caso de que hubiera cualquier tipo de incendio y es relevante se tomen todas las medidas precautorias como lo son el estar revisando y dándole mantenimiento a los mismos para que siempre se encuentren en un estado óptimo si llegasen a ser requeridos.

3 Desarrollo de la Solución

De acuerdo a lo analizado en el capítulo anterior en éste se analiza y explica a detalle el desarrollo de la solución en la tablet Android la cual tiene como base el lenguaje de programación Java de Oracle y la conexión se realiza con una base de datos SQL Server Express 2008 como parte de la solución idónea, también se presenta la elaboración del portal de registro de usuarios en C# para el uso del laboratorio ambos conforme a los requisitos de seguridad que se explican a mayor detalle dentro de esta sección.

3.1 ESPECIFICACIONES DE LA SOLUCIÓN

En este punto se analiza a detalle cada uno de los elementos que compondrán la solución y posteriormente se presenta una relación entre los servicios de seguridad y las estrategias utilizadas para cubrirlos.

3.1.1 Hardware (Tablet Android)

Se eligió esta opción ya que es la más factible de acuerdo a las necesidades del laboratorio de redes y seguridad debido a los siguientes factores:

- Debido al espacio es más fácil colocar e implementar la Tablet por medio de una protección que permita fijarla a un escritorio o pared.
- La comunicación será vía inalámbrica por lo cual se evita instalación y mantenimiento de cableado.
- Por otra parte el que toda la implementación sea a través de una Tablet y no dependa de otros elementos lo hace más sencillo para dar mantenimiento, ya que en la otra opción se tienen varios elementos de los cuales depende el funcionamiento.
- Del mismo modo al ser menos elementos reduce los costos.
- En caso de que un mal funcionamiento del equipo basta con reemplazarlo e incluso temporalmente podría darse una comunicación desde otro dispositivo Android.
- En cuestión de protección eléctrica también permite reducir costos ya que no se debe invertir tanto en protección eléctrica y en caso de falla eléctrica cuenta con su batería de respaldo por lo cual no requiere de un no-break.
- En cuanto a la seguridad es también un buen elemento ya que como cualquier unidad física inicialmente se puede proteger montando el dispositivo en un lugar fijo en el cual no pueda ser desplazado lo cual impida que la sustraigan o trasladen de lugar,

adicionalmente en cuanto a seguridad de la información al tratarse solo del contenedor de la interfaz gráfica lo vuelve muy seguro puesto que no hay forma de acceder a la información desde la misma.

3.1.2 Software

El software es uno de los elementos más importantes para esta solución puesto que va a brindarle la interfaz amigable, la seguridad, la portabilidad y el desempeño por lo cual se ocupan dos softwares importantes y que cuentan con licencia gratuita, además de un importante desarrollo y sets de herramientas para realizar a través de Java una aplicación que permita llevar el control adecuado de los equipos y su uso además de mantener un registro inalterable, seguro y eficiente de quien accede al laboratorio.

3.1.2.1 Lenguaje de programación de la aplicación (JAVA)

Para la realizar la aplicación se utiliza el lenguaje Java debido a su compatibilidad con el sistema operativo Android, adicionalmente cuenta con importantes características como lo son la portabilidad y el desempeño, además de lo mencionado anteriormente hay una razón extra por la cual es muy importante ocupar este lenguaje de programación y es debido a la conexión con la base de datos, ya que Java cuenta con librerías tanto de Microsoft como las del proyecto jTDS que nos permiten establecer una conexión entre Android y la BD.

3.1.2.2 Base de datos (SQL Server Express 2008)

En cuanto a la base de datos se ocupa SQL Server Express 2008 por tratarse de una herramienta robusta, la cual adicionalmente puede trabajarse fácilmente y lograr un desarrollo importante y que permita tener mayor número de posibilidad en

cuanto al manejo, almacenamiento y resguardo de la información, por otra parte es importante mencionar que al momento del registro de los alumnos no es posible conocer el número de peticiones simultaneas que puede experimentar el servidor por lo cual SQL Express tiene las características para poder soportar este tipo de carga sin verse afectado.

3.1.2.3 Lector de códigos de barras (Barcode Scanner by Zxing)

Es una aplicación de lector de códigos de barras desarrollada por Zxing la cual además de ser gratuita cuenta con la opción de ser invocada desde cualquier aplicación y regresar el resultado del código escaneado a alguna variable dentro del código, por estas razones esta aplicación se utiliza para leer el código QR que se le asigne a cada uno de los alumnos y con ello cumplir con parte de la autenticación establecida.

3.1.2.4 Lenguaje de programación del portal de registro de usuarios(C#)

Para el desarrollo del portal se utiliza el lenguaje C# en conjunto con IIS lo que permite montar un servidor con conexión a la BD SQL lo cual se ocupa para realizar el registro de los usuarios y el almacenamiento del mismo, poder cotejarlo al momento del acceso al laboratorio, adicionalmente en este mismo portal se realiza una consulta al momento del registro para que la BD nos regrese el valor del código QR el cual se genera internamente desde SQL de modos que podamos mostrarlo al alumno y tenga la posibilidad de guardar la imagen para conservarla y llevarla al laboratorio en formato físico o digital.

3.1.3 Servicios de Seguridad

Los servicios de seguridad son una de las partes más importantes de este proyecto, ya que como se encuentra definido en el marco teórico y en la solución deseada, se busca un control de acceso el cual es parte de los servicios de seguridad y cuenta con sus propios elementos , además se trata de un sistema el cual debe contar con la protección necesaria para brindar confianza y validez a los registros almacenados en la BD, para lograr esto se deben de considerar todos los aspectos de los servicios de seguridad por lo cual a continuación se menciona como es que se están cubriendo cada uno de ellos. .

3.1.3.1 Confidencialidad

Para cumplir con el servicio de confidencialidad la BD el almacenamiento se realiza en el servidor dedicado del laboratorio y está protegido al solo permitir conexión a través de la red interna, adicionalmente se considera que la información viaja a través del wi-fi por lo cual para evitar el que la información pueda ser capturada con fines mal intencionados se la aplicará un hashing al QR, lo cual permite que la información viaje segura por el medio sin correr el riesgo de comprometer la información

3.1.3.2 Integridad

Para mantener la integridad se está ocupando una BD segura que nos permita brindar este servicio de integridad y adicionalmente un script se encuentra programado para correr de manera automatizada en el servidor y que se genere un respaldo periódico de la información.

3.1.3.3 Disponibilidad

La disponibilidad es uno de los servicios más importantes y como se comenta en puntos anteriores la selección de la base de datos se debe en parte a este punto, ya que se busca mantener la disponibilidad del servicio aun cuando pueda existir una alta demanda al momento del registro, así como un buen desempeño que le permita a la aplicación funcionar sin inconvenientes.

En el caso del portal de registro es importante mencionar que la disponibilidad depende de las políticas del laboratorio así como de lo que determine la administración del mismo.

3.1.3.4 Autenticación

La autenticación es uno de los puntos más importantes para el control de acceso, ya que debemos verificar que el usuario se identifique y se determine su identidad con la mayor seguridad posible por lo cual se maneja un sistema de autenticación de doble factor el cual requiere que los alumnos porten un código QR el cual es asignado al momento de realizar su registro en el laboratorio, además se procesa de manera inicial por un hashing para una mayor seguridad y además el usuario es responsable de definir un NIP numérico de 4 dígitos el cual debe ingresar cada vez que requiera acceder al laboratorio

3.1.3.5 No Repudio

No repudio se encuentra estrechamente enlazado con el punto anterior, ya que como el QR es generado con información del usuario al momento del registro automáticamente se crea un registro en la BD de quien y en que horario

accedió al laboratorio, por lo cual no hay manera de que el usuario niegue su presencia en el mismo.

3.1.3.6 Cumplimiento

El cumplimiento es uno de los puntos principales en la seguridad informática ya que como se menciona es necesario cumplir con las disposiciones legales del país en el cual el sistema está localizado, cabe mencionar que la UNAM cuenta con un documento propio en cuanto a la protección de datos personales pero del mismo modo es importante mencionar que en nuestro caso no se utiliza información sensible del usuario, ya que no se ocupa ningún dato personal a excepción del número de cuenta proporcionado por la universidad.

3.1.3.7 Identificación

Se confirma la identidad del usuario al ingresar sus códigos tanto el QR como el NIP privado, el cual se es cotejado con la base de datos para brindarle acceso, la información está sujeta a ser mal utilizada por los usuarios por lo cual se debe agregar una norma de seguridad indicando que ellos son responsables de su información y cualquier mal versación o compartición de la misma los responsabiliza de los actos que puedan cometer otros en su lugar.

3.1.3.8 Autorización

Este punto se es cubierto de manera relativamente simple ya que los usuarios no pueden acceder al laboratorio si no cuentan con un código QR por lo cual tienen que ser alumnos inscritos y deben cumplir con el registro correspondiendo por medio del portal para que les sea entregado.

3.2 PROCESO DE DESARROLLO DE LA SOLUCIÓN

En este apartado se reporta todo el proceso de la solución así como los problemas que se han sido encontrados en cada uno de los puntos de la construcción de la aplicación denominada (“Labred”) y como dar solución a los mismo y la estructura con la cual se desarrolló.

3.2.1 Diagrama básico de la aplicación Android.

En el diagrama básico de la aplicación (véase figura 3.1) se muestra el flujo del proceso que debe llevar la aplicación así como las rutas y condiciones a seguir en cada uno de los pasos del proceso de tal manera que siempre regrese al estado inicial que se basa directamente en la interfaz gráfica puesto que este es el punto central de la aplicación y en torno a ella giran todas las demás actividades.

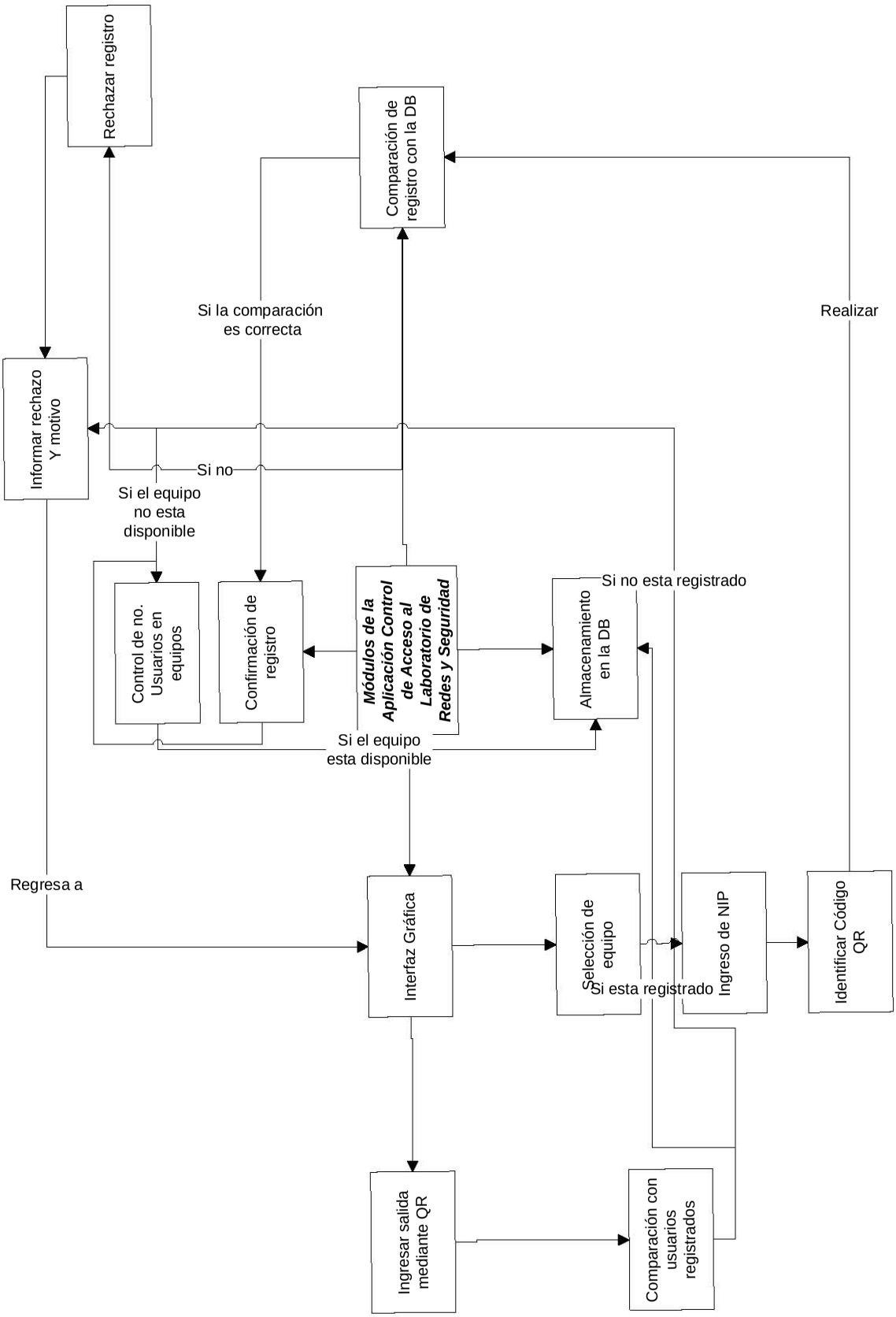

Figura 3.1 Diagrama básico de la aplicación Android

3.2.2 Interfaz gráfica

- En la interfaz (véase figura 3.2) es importante considerar la colocación de los botones así como las leyendas, un aspecto significativo a tomar en cuenta es que cuando un objeto es agregado (leyenda, botón, botón gráfico) éste se vuelve dependiente de los objetos que lo rodean, es decir, adquiere su posición con base en las posiciones que ocupan los demás, esto dificulta la actualización e integración de más elementos, ya que cuando se busca reorganizar el espacio todo se mueve de lugar debido a la interrelación de los elementos.
- En cuanto a las leyendas, es decir los textos, es importante considerar que no son simples etiquetas, estas etiquetas están definidas dentro de la parte de res/values/Strings.xml ya que de ahí un enlace a la etiqueta es creado y es como se relaciona el texto con su respectiva etiqueta.
- Otro detalle importante es que cada pantalla en Android es un archivo .xml en este caso para la interfaz gráfica se ocupan dos pantallas ya que contamos con la principal la cual tiene como propósito llevar a cabo el registro de alumnos y la pantalla secundaria la cual solicita una contraseña cuando un profesor tiene que marcar su salida.

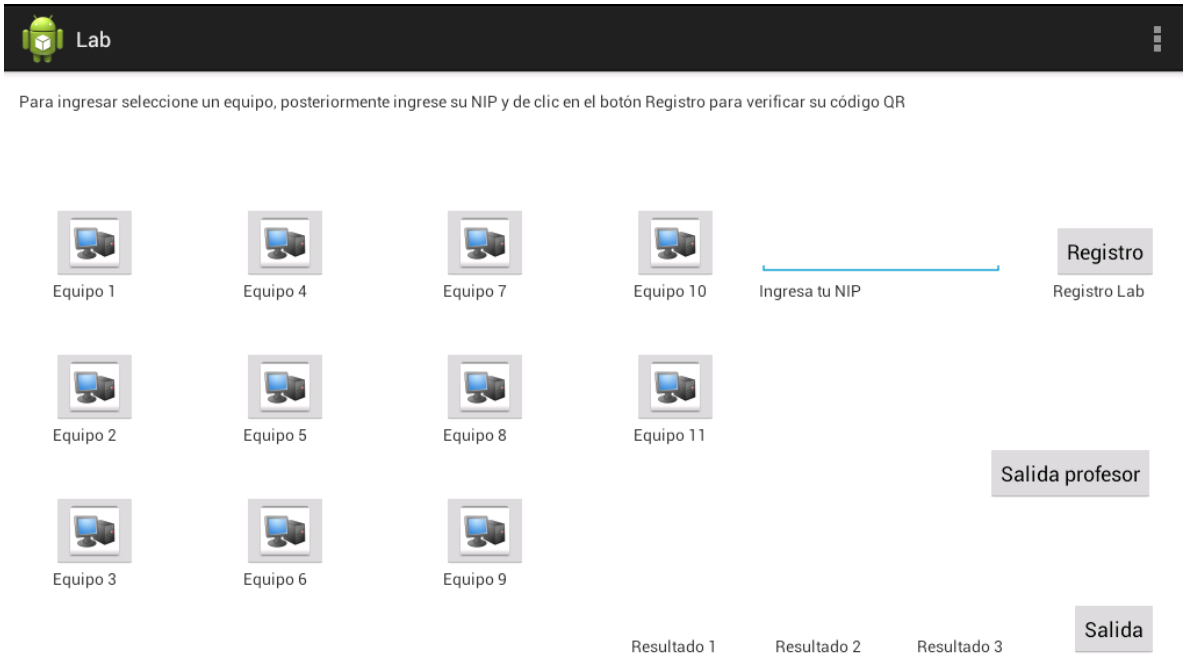

Figura 3.2 Interfaz gráfica de la aplicación

3.2.3 Lector de códigos

- No es un desarrollo para este proyecto, si no es un lector que permite ser usado por aplicaciones externas por lo cual se requiere la instalación del programa que se encarga de leer los diferentes códigos.
- Consta de 3 partes: a) la definición del botón en main que llama al lector, posteriormente b) la acción que ejecuta el evento, y por último c) lo que se realiza una vez ocurra la acción.
- El problema surge cuando se busca utilizar el lector con dos botones para dos acciones diferentes, esto debido a que trabaja bien hasta que se intenta ocupar el segundo botón con el cual el programa termina inesperadamente aunque esta parte ya se encuentra solucionada dentro de la aplicación.

- El lector está definido como el trigger para las acciones de registro por lo cual una vez seleccionado el botón de registro, se ejecutan diversas acciones. Al momento de leer el código QR la información requerida es extraída, el lector procede a validar e ingresar los datos a la BD, es importante el orden y la información a tomar en cuenta para poder confirmar el registro de manera correcta.
- Dentro de la estructura se encuentra definido un arreglo que permita llevar el control de los usuarios que entran al laboratorio, esto tiene como objetivo registrar la asistencia de los usuarios a las instalaciones y con ella generar un registro de acceso que es proporcionado al profesor que concede el acceso, este arreglo trabaja en conjunto con el lector de códigos, el cual se va a actualizando conforme los usuarios presentan su código QR, es importante mencionar que del mismo modo para actualizar el arreglo e identificar la liberación de equipos se solicita el QR al presión el botón de salida.

3.2.3 Campo para ingreso de clave.

Este campo se ocupa para ingresar el NIP (véase figura 3.3) con el cual los alumnos verifican su identidad, se debe considerar que solo es numérico y que se debe capturar el valor en el momento exacto como se comentó en el punto anterior, ya que requiere de un trigger dentro de la aplicación que permita guardar el valor una vez haya sido ingresado, ya que si no se corre el riesgo de guardar el valor antes de que el usuario pueda ingresar su clave.

3.2.4 Botones gráficos.

- Estos botones son los que se ocupan para representar los equipos ya que permiten agregar una imagen dentro del mismo (véase figura 3.3).

▪ En este punto se debe considerar que es complicado definir como trabajan las acciones sin un conocimiento previo, ya que es muy relevante realizar el proceso con el orden requerido para ocupar estos objetos de manera adecuada, como solución a este caso al momento de realizar una acción (presionar el botón) se identifica por medio de un id cual es el proceso a ejecutar y se guarda el valor en un campo dinámico.

▪ Posteriormente y como se menciona en la sección anterior se implementa un arreglo que permite llevar el control del número de usuarios por equipo así como el acceso a los mismos, ya que como se encuentra definido en el planteamiento del problema sólo pueden existir dos usuarios para un mismo equipo en un mismo período de tiempo.

Figura 3.3 Botón gráfico y campo de ingreso de clave

3.2.5 Preparación de la BD

• Regularmente se utiliza para las diferentes aplicaciones de Android una base de datos SQLite pero en la búsqueda de implementar un sistema con mayor seguridad e integridad se opta por ocupar una BD SQL Server 2008 Express, lo cual requiere de un proceso diferente y no cuenta con la misma documentación y esto desencadena algunas complicaciones las que se detallan a continuación junto con los pasos a seguir para darle solución:

• El primer paso es instalar el SQL Server Express 2008, es relevante y un paso fundamental realizar la instalación con modo de autenticación de mixto, ya que es uno

de los requisitos tener configurada la conexión adecuadamente puesto se lleva a cabo por medio del usuario “sa” de SQL, aquí pueden existir algunos detalles ya que el instalador de SQL tiene dependencia con algunos otros programas como lo son Windows Installer, .NET Framework y también Visual Studio. Al tener este último en el equipo donde se instala la aplicación se generan una serie de conflictos, los que se solucionaron desinstalado el Visual Studio.

- Una vez que la instalación esta completa se procede a configurar los protocolos y puertos por medio del SQL Management, ya que se requiere se necesita tener activos tanto el protocolo TCP/IP como el Named Pipes y en ambos configurar el puerto por el cual se realiza la conexión, además de activar y/o habilitar el servicio de SQL Server Browser el que se requiere para realizar una conexión adecuada por medio de la red, una vez finalizada esta configuración se reinician los servicios y queda funcional la aplicación.

3.2.6 Conexión a la BD

- Otra cuestión importante que surgió fue la conexión a la BD por que requiere investigar mediante que librerías se puede realizar la conexión, el problema se da cuando al intentar realizar la conexión la aplicación arroja un error debido a la construcción de la cadena de conexión por lo que para encontrar e identificar la raíz del error se realiza una copia de la aplicación y se corre de manera individual para verificar paso a paso la información y una vez que se logra identificar el problema se modifica hasta que el funcionamiento es el adecuado, una vez finalizada esta parte se devuelve a la aplicación con las modificaciones pertinentes, al realizar las pruebas sigue sin funcionar la misma por lo cual se procede a elaborar de nueva cuenta una investigación

que arroja como resultado que las librerías que son descargadas e importadas de Microsoft tienen problemas de compatibilidad con aplicaciones Android.

- Esto genera una nueva investigación la cual permite encontrar ciertas librerías desarrolladas por "The jTDS Project" las cuales mediante los mismos comandos y algunos cadenas de conexión bastante similares permite realizar la conexión a la BD SQL Express 2008, sin embargo al momento de aplicar estas librerías se generan una serie de errores que se surgen por la diferencias en las cadenas de conexión y diferencias de versiones, las cuales son ser verificadas y adaptadas a las nuevas librerías.

3.2.7 Elaboración de la BD

- Una parte trascendental en el desarrollo fue el diseño de la base de datos(véase figura 3.4), ya que como es bien conocido este elemento fundamental dentro de muchas aplicaciones es la que permite almacenar y realizar un correcto procesamiento de la información, el diseño inicial consistía en dos tablas las cuales posteriormente fueron reemplazadas por tres que manejan diversos tipos de datos además de permitir segmentar la información adecuadamente pues de realizando de otra manera podría sobrecargar las tabla de información lo cual afectaría el desempeño de las consultas realizadas, a continuación se presentará a detalle la información contenida en las tres tablas.

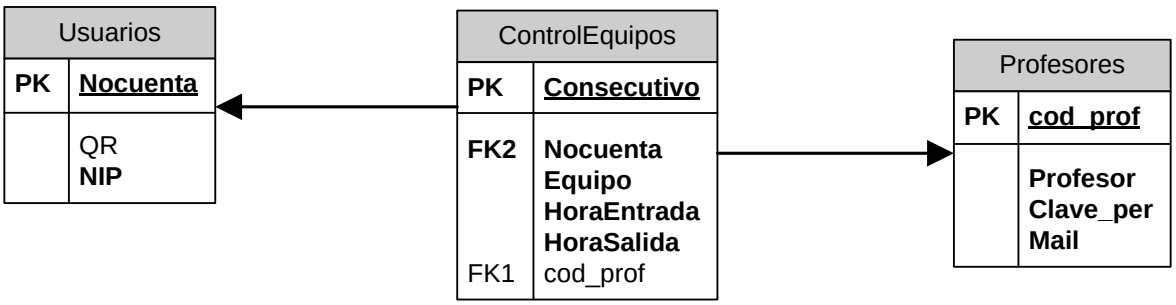

Figura 3.4 Diagrama relacional

3.2.7.1 Tabla Profesores

- Esta tabla contiene cuatro campos que son indispensables para el manejo de los profesores los cuales son los siguientes:
  - Profesor
    - En este campo se encuentra contenido el nombre del profesor
  - Clave_per
    - A cada profesor se le asignará una clave personal la cual se encontrará contenida en este registro.
  - Mail
    - Adicionalmente y como medio para enviar la información de los asistentes a las clases se guardará un correo electrónico.
  - cod_prof
    - Este campo es una clave la cual servirá para identificar a que profesor se deberá enviar el resultado de los alumnos de esa clase.

3.2.7.2 Tabla Usuarios

- Esta tabla contiene cuatro campos que son indispensables para el manejo de los profesores los cuales son los siguientes:
  - Nocuenta
    - En este registro se almacena el número de cuenta del usuario
  - QR
    - Al momento del registro en este campo se almacena la cadena contenida en el QR de cada usuario.
  - NIP
    - Finalmente cada usuario registra un NIP de cuatro dígitos como medida extra de seguridad los cuales se almacenan en esta columna.

3.2.7.3 Tabla ControlEquipos

- Esta tabla contiene cuatro campos que son indispensables para el manejo de los profesores los cuales son los siguientes:
  - Nocuenta
    - En este registro se almacena el número de cuenta del usuario.
  - Equipo
    - Campo el cual indica el equipo ocupado por cada uno de los usuarios.
  - HoraEntrada
    - Registro que guarda la hora de entrada del alumno.
  - HoraSalida
    - Registro que guarda la hora de salida del alumno.
  - cod_prof

- Este campo es una clave la cual se identifica a que profesor se debe enviar el resultado de los alumnos de esa clase.

- Consecutivo
  - Campo de control para tener identificador único y se incrementa en uno por cada inserción de registro de acuerdo a su configuración.

3.2.8 Registro y salida de usuarios

- Para realizar las actividades del registro y la salida se genera la programación correspondiente pero es importante mencionar que está compuesta de dos secciones principales la cual es la interfaz gráfica y en la cual el código de la aplicación se encuentra en un archivo java y un segundo archivo ".java" el cual realiza todos los procesos de conexión a la BD así como cualquier clase de consulta como lo son las inserciones y actualizaciones a la misma, debido a esta correlación el seguimiento de errores se vuelve complicado porque hay que revisar constantemente donde se encuentran los detalles y verificar que se trabaje sobre el verdadero problema.
- Una de las complicaciones más importantes se encuentra al realizar los update a la BD ya que la instrucción que se estaba utilizando(executeUpdate) se ejecuta dentro de un ciclo que se realiza las actualizaciones a todos los registros que cumplen la condición y el error ocurre al momento de actualizar registros y solo realiza uno solo, revisando el API se identifica que la instrucción tiene un detalle y al momento de ejecutar la misma cierra el conjunto de resultados sobre los cuales se está trabajando, por lo cual para solucionar este comportamiento se modifica la lógica y las condiciones para ejecutar el update para todos los registros que cumplan la condición.

- Otro de los errores que surgen a lo largo del desarrollo y que en realidad no tiene justificación en cuanto a programación es que solo se permite realizar un registro, ya que los posteriores arrojan una falla, para encontrar solución a este detalle se realiza un debug de la aplicación de forma intensiva sin encontrar falla alguna que pudiera indicar el origen del problema, sin embargo se verifica y encuentra una solución alternativa la cual consiste en que antes de realizar cualquier inserción se le solicita al sistema devuelva la columna sobre la cual está apuntando y esto refresca la memoria evitando que se genere el error antes mencionado, por lo cual parece ser una falla en las librerías o en el SQL.
- En cuanto al registro existe una complicación en el desarrollo para poder generar adecuadamente la fecha, ya que la fecha en SQL tiene un formato diferente al que normalmente se maneja el cual incluye fecha y hora por lo cual se busca encontrar la manera de enviar la fecha en el formato indicado desde Java lo cual fue se soluciona ocupando objetos de tipo Calendario y SimpleDateFormat lo cuales permiten definir un formato al momento de la declaración, aun así esto devuelve más datos de los que son necesarios por lo cual se le realiza en la parte final un substring para extraer solamente la información requerida.
- En cuanto al QR al momento de leer la información se realiza una separación entre el número de cuenta en claro y la cadena hasheada, de modo que se solicita a SQL realice el Hasheo del no. De cuenta para compararlo con él se recibe a través del código y en caso de coincidir realiza una búsqueda en la BD de ese QR junto con el NIP el cual devuelve un número de cuenta, en caso contrario se comprueba que el usuario no se

encuentra registrado, en caso de que la comparación de los hasheos no sea satisfactoria automáticamente rechaza el ingreso.

- En todo el proceso de desarrollo es muy importante realizar diversas pruebas para asegurar el funcionamiento del sistema, así como los resultados de las diversas consultas a la base de datos para evitar algún malfuncionamiento que genere un error y por lo mismo un cierre forzado del sistema o un problema de integridad en la información contenida dentro de la BD.

3.2.9 Elaboración del código QR

- El código QR es un elemento fundamental para el control de acceso de los alumnos ya que tiene que ser un identificador único que permita al alumno demostrar su identidad por lo cual se genera un código compuesto, el cual proporciona seguridad al estar conformado en primera instancia está por el número de cuenta del usuario y posteriormente se hashea por el algoritmo SHA1, la concatenación de ambos elementos forma el código QR, es importante mencionar que SQL Server Express 2008 es el que realiza el proceso de hash con SHA1 y la concatenación reenviando este código al portal para la generar la imagen correspondiente de manera que pueda ser mostrada al alumno (véase figura 3.5).

Adicionalmente para la correcta elaboración de este QR se realizar un trigger dentro de la tabla de Usuarios por lo cual al momento de crear cualquier registro en la misma este proceso se dispara creando el código de la manera mencionada anteriormente. Esto es una parte importante ya que la codificación del QR se elabora de manera interna sin que tenga que pasar información por la página web para evitar que se utilice información sensible en el portal.

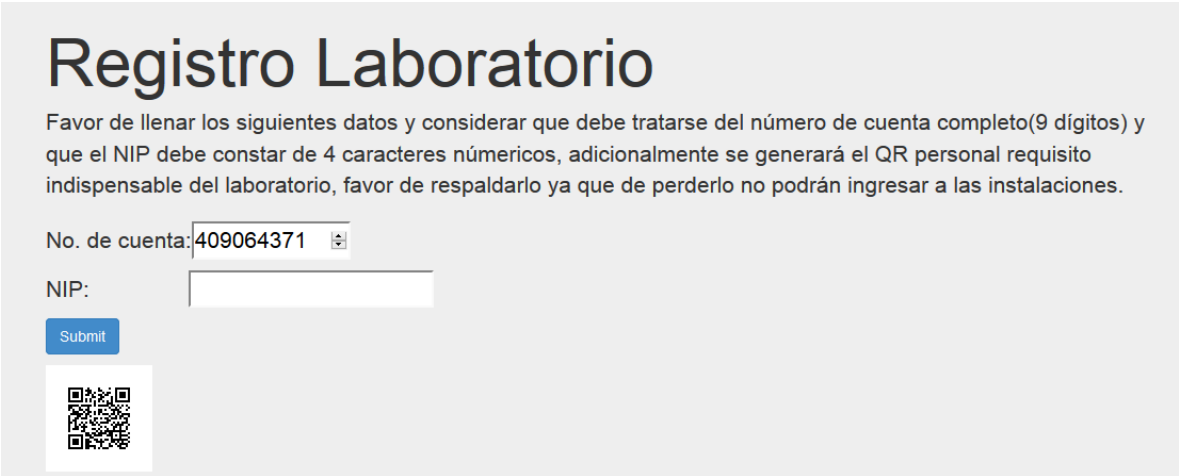

Figura 3.5 Ejemplo de entrega de código QR al alumno

3.2.10 Módulo de profesores

- Dentro de la programación de la aplicación se encuentra un apartado donde cada profesor marca su salida por medio de una contraseña (véase figura 3.6) de manera que exista un registro de los profesores y adicionalmente para evitar que algún usuario se mantenga en el salón puesto que al momento en el cual el profesor marca su salida automáticamente se marcan las salidas de todos los usuarios que no hayan cerrado su sesión y se asigna un identificador único del profesor que cerró ese grupo.
- Además de lo mencionado anteriormente el módulo de profesores tiene una segunda función ya que al marcar su salida genera una la lista de los usuarios que han ingresado desde la última salida de profesor y por medio de una consulta envía la lista al profesor para que pueda contar con su propia lista de asistencia (véase figura 3.7), esta lista se manda a un correo definido por el profesor al momento de su registro, este registro se encuentra a cargo de la administración del laboratorio por motivos de seguridad.
- El registro de los profesores se realiza por la administración del laboratorio ya que debe realizarse mediante inserciones directamente en la base de datos lo cual evita que

un tercero tenga capacidad para modificar/alterar las cuentas y adicionalmente que la administración en el momento que lo requiera pueda crear o inhabilitar cualquier cuenta.

- El problema presentado en este punto lo presenta SQL Server Express dentro de sus características, esto debido a un problema de compatibilidad con el envío por correo, por lo cual se realiza una investigación y se encuentra que por medio de codificación es posible configurar esta característica para habilitar un envío de correo desde una cuenta que nosotros designemos.

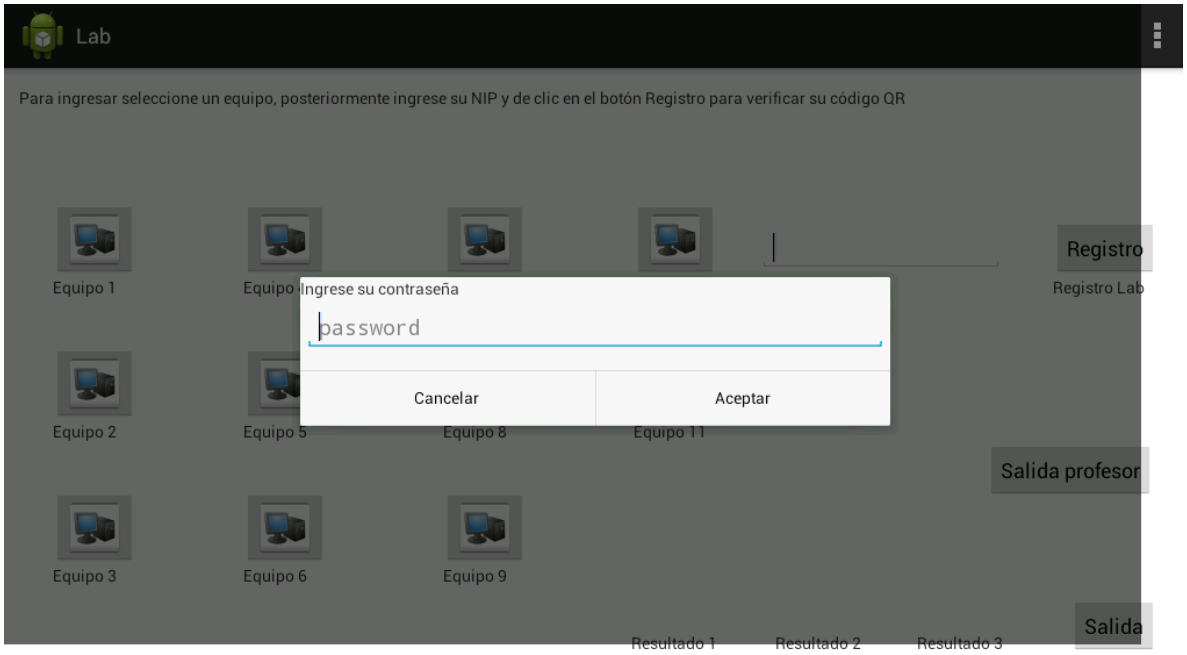

Figura 3.6 Módulo de profesores

```
Se cambió el contexto de la base de datos a 'Tesis'.
Nocuenta             Equipo
-------------------- ------
           409064380 1
           293642454 1

(2 filas afectadas)
```

Figura 3.7 Ejemplo de envío del resultado de asistencia

3.2.11 Portal de registro de usuarios

- En el portal de registro de usuarios (véase figura 3.8) dentro de la fase de desarrollo se realiza la programación correspondiente y conforme a lo establecido para evitar SQL injection se realiza una conversión de los datos recibidos a valores enteros para evitar inyección de algún otro código, el detalle en esta parte surge al devolver el QR del alumno puesto que no es posible colocar simplemente imágenes dentro del desarrollo WEB puesto que son objetos no aceptados y es complicado transformarlos a un formato soportado, por lo cual se optó por generar la imagen para después desplegarla, de manera que el proceso genera la imagen al vuelo y la despliega quedando un respaldo de la misma en el servidor.
- Un inconveniente importante que se presenta en esta parte es que al realizar la conexión a la BD no se obtiene el resultado esperado y arroja un error debido a que en la consulta no se ingresa los tipos de valores correctamente, una vez ajustados los parámetro de entrada se le da solución al problema.

• Adicionalmente es necesario mencionar que en el desarrollo de C# el botón Submit es aquel que dispara las acciones en la base de datos, tanto la inserción como la consulta las cuales ya se encuentran predefinidas en la programación del mismo.

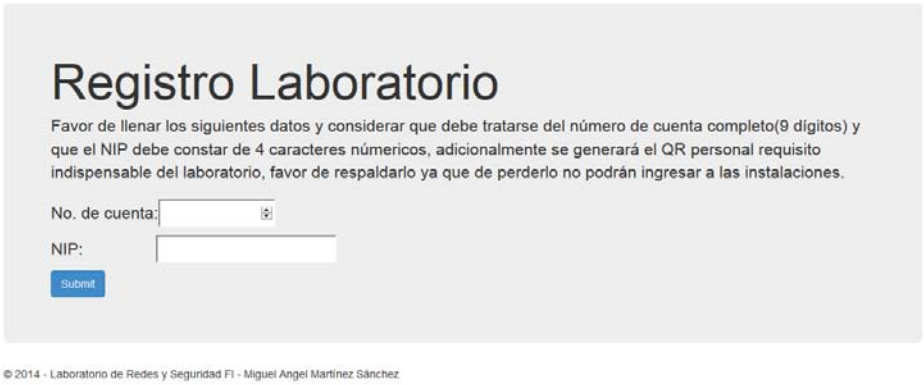

Figura 3.8 Portal de registro de usuarios

4 Pruebas y Resultados

En este capítulo se muestran los resultados del desarrollo de la aplicación, así como las pruebas que se realizaron a la misma.

4.1 PRODUCTO FINAL

La aplicación se encuentra instalada en una Tablet a la entrada del Laboratorio de Redes y Seguridad, mientras que el portal de registro se encuentra instalado en el servidor.

4.1.2 El portal de registro

La pantalla inicial del portal de registro puede visualizarse como se muestra en la figura 4.1 al acceder a la liga:

Figura 4.1 Portal de registro de usuarios en pruebas

El funcionamiento del portal es muy sencillo, ya que la información relevante para se efectúe el registro se le indica al usuario a través de las instrucciones en el portal el cual requiere el número de cuenta y que el usuario defina su NIP, existen algunas restricciones para el mismo las cuales son indicadas explícitamente dentro de las instrucciones.

Una vez realizado esto el usuario deberá esperar a que el portal les devuelva su código QR como se puede visualizar en la figura 4.2 el cual deberán almacenar a su discreción.

Figura 4.2 QR desplegado por el portal de usuarios

4.1.2 La aplicación

La pantalla inicial de la aplicación puede visualizarse como se muestra en la figura 4.3

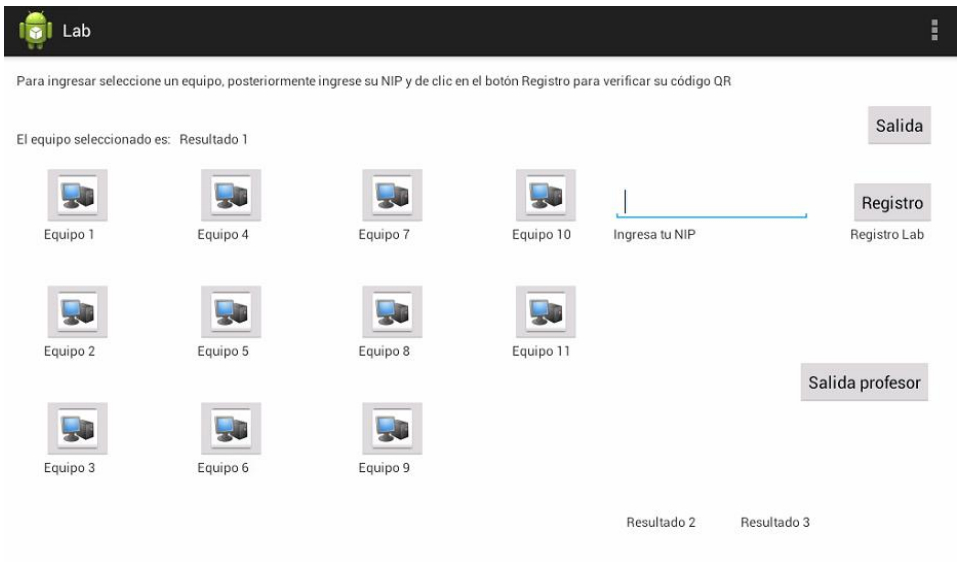

Figura 4.3 Pantalla inicial de la aplicación

Al ingresar a la aplicación se pueden ver a la izquierda los equipos en la parte media un campo para ingresar el NIP y en la parte derecha se encuentra el botón de ingreso, el cual al darle clic desplegará la cámara para poder leer el código QR del usuario.

En la parte inferior izquierda se muestra un mensaje el cual indica el resultado de la operación con una leyenda en letras rojas para que el usuario pueda confirmar si su registro fue exitoso o no como se puede observar en la figura 4.4.

Figura 4.4 Leyenda de registro exitoso

En la parte inferior derecha se localizan los botones de salida, en el caso del botón de salida se despliega la cámara al darle clic para que se le proporcione el código QR y de esta forma confirme la salida del usuario correspondiente, mientras que al dar clic en el botón de salida profesor la aplicación despliega un campo para ingresar una contraseña, la cual debe coincidir con alguna de las que se encuentran almacenadas en la base de datos, lo cual permite que el profesor sea identificado y automáticamente marque la salida de cualquier alumno que todavía permanezca registrado en el laboratorio y le notifique con un mensaje como se muestra en la figura 4.5.

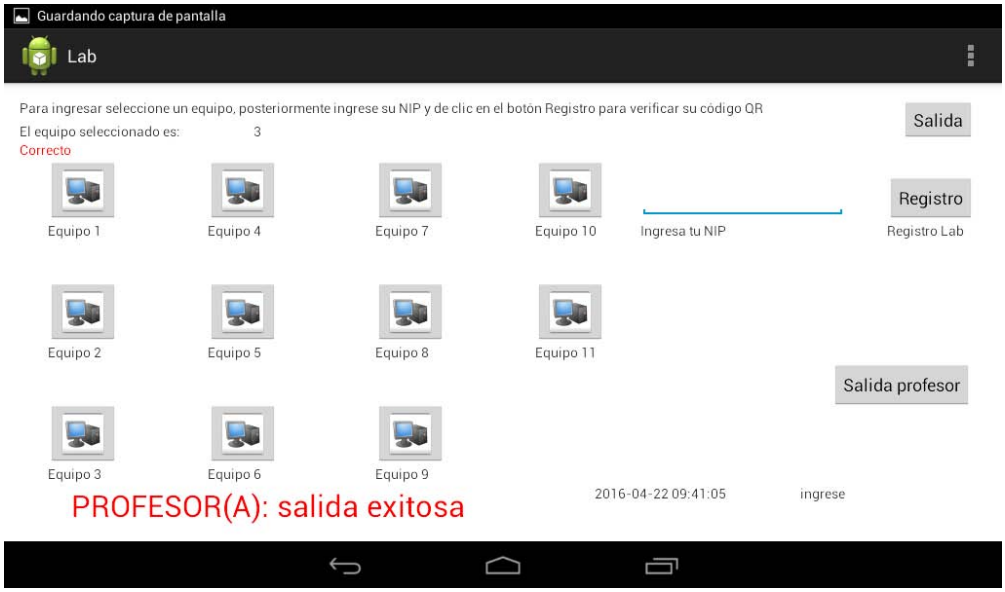

Figura 4.5 Leyenda salida de profesor

4.2 PRUEBAS DE FUNCIONALIDAD DEL SISTEMA

A continuación se mencionan varias de las pruebas que se han realizado a la aplicación y al portal para verificar su funcionamiento, es importante mencionar que para las mismas se tomaron como piloto algunos grupos del Laboratorio de Redes y Seguridad.

4.2.1 Prueba de registro de usuarios

Se realizaron diversos registros de usuario dentro del portal de los cuales se aproximadamente el 90% de los casos fue realizado de manera satisfactoria, mientras que el porcentaje restante se identificó como errores fuera del control de la aplicación, ya que el factor para desencadenar estos fueron humanos.

El primer caso que se identifico es que algunos usuarios no permitían al portal devolverles el código QR y volvían a ingresar la información dando un segundo clic, por lo cual en vez de devolverles el QR les aparecía la leyenda de una violación de llave primaria de SQL indicando que ya estaban registrados como se muestra en la figura 4.6.

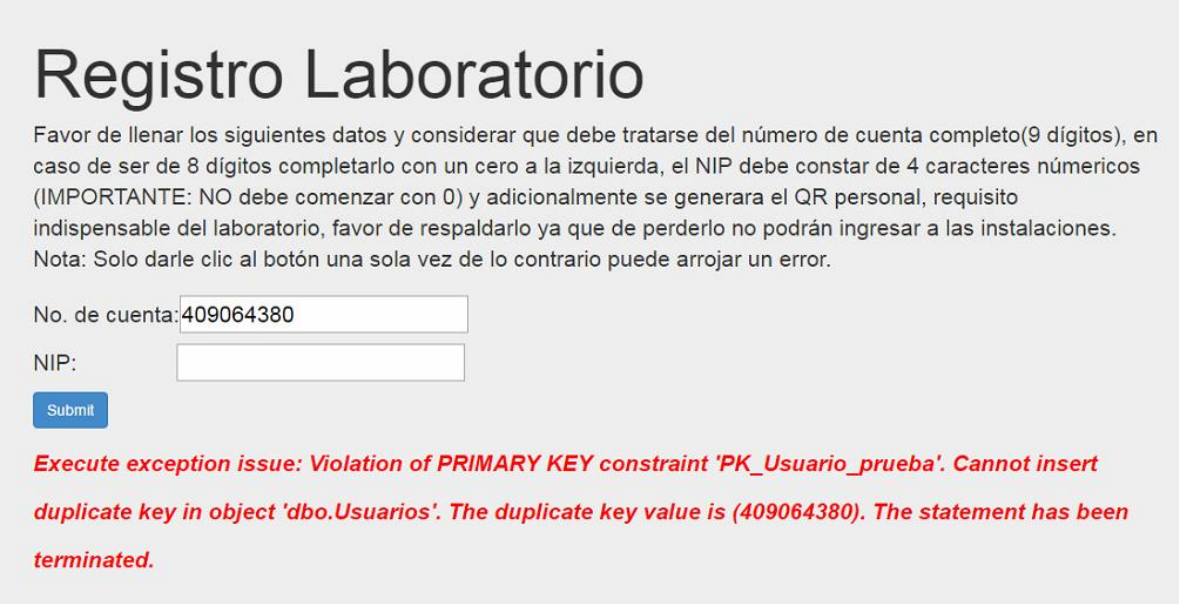

Figura 4.6 Leyenda de violación de llave privada

El segundo caso se dio principalmente por que los usuarios no leyeron las instrucciones de registro que se indican en el portal por lo cual ingresaron información errónea, como puede ser letras en vez de números en el campo del NIP.

4.2.2 Prueba de ingreso de usuarios

Una vez completado el registro de los usuarios se procedió a verificar el ingreso de los mismos, el cual nos permitió identificar algunos puntos a mejorar dentro de la aplicación.

El registro de usuarios es exitoso pero se identificaron ciertas variables que hacían que el tiempo invertido para el ingreso fuese mayor, ya que algunos de los usuarios no sabían que equipo habían seleccionado o no borraban el NIP anterior antes de presionar el botón de registro, por lo cual se agregó una leyenda en la parte superior de los equipos para que muestre el equipo seleccionado, del mismo modo se configuro la aplicación para que el campo del NIP sea borrado automáticamente después de cada registro.

Es importante mencionar que dentro de las pruebas realizada se encontró una situación en la cual el registro de usuarios quedo obsoleto y después de realizar el troubleshooting para la aplicación se identificó que el problema es la red inalámbrica del laboratorio ya que no estaba funcionando, como se menciona previamente esta parte es indispensable para que la aplicación pueda realizar correctamente la conexión con la base de datos y de esta manera llevar a cabo todo el proceso de registro de usuarios y control de equipos.

4.2.3 Prueba de salida de usuarios

La prueba de salida de usuarios fue exitosa y no presentó inconvenientes.

4.2.4 Prueba de salida de profesores

Esta prueba es importante ya que la salida de un profesor conlleva para la aplicación y la base de datos varias tareas en específico, entre las cuales se encuentran la salida de los usuarios restantes, el registro de los alumnos del profesor y el envío de la lista de asistencia para el profesor.

Estas pruebas fueron exitosas en los tres sentidos mencionados ya que se ejecutó la salida de los usuarios restantes, se identificaron como alumnos del profesor que marco la salida y las listas fueron enviadas por correo electrónico a cada uno de los profesores.

Nota: Es importante tener en cuenta que los profesores deben de pedir al administrador que actualice su dirección de correo en caso de ser necesario.

Conclusiones

El principal objetivo de este trabajo fue desarrollar una aplicación que fungiera como sistema de control de acceso para el Laboratorio de Redes y Seguridad, para lo cual se tuvo que realizar una extensa investigación para entender los elementos que conforman un sistema de control de acceso, así como las medidas de seguridad y todos los factores que deben ser considerados al elaborar uno de estos sistemas, ya que el generar una aplicación con este enfoque son muchos detalles los que deben de tomarse en cuenta para que brinde el servicio adecuadamente.

Es relevante mencionar que un sistema de control de acceso conlleva manejar elementos de desarrollo de software, análisis de hardware, implementación y creación de bases de datos además de conocimiento y la habilidad de realizar troubleshooting a las redes, adicionalmente en cada una de estas ramas se debe considerar la seguridad puesto que varía para cada una de ellas.

Una vez que se tienen todos los elementos a considerar es importante comunicarse con las personas que ocupan la aplicación, para poder encontrar la mejor solución que se adapte a los requisitos y necesidades del laboratorio, pero también que sea funcional para los usuarios y administradores de manera que sea un sistema de control de acceso en vez de una simple aplicación.

El crear o implementar un sistema de control de acceso permite verificar e investigar sobre todas las opciones existentes para poder cumplir los objetivos, puesto que en el mercado existen gran cantidad de dispositivos que se ocupan para este fin y siempre es importante verificar con el solicitante de la solución cual es el que mejor se adapta a sus necesidades y posibilidades, las cuales pueden ser muy variantes desde un registro simple para llevar una lista, hasta poder brindar un servicio de calidad el cual cumpla con ciertas normas que resguarden la información y aseguren el servicio.

A lo largo de este documentos se presentan varias opciones para generar el sistema de acceso, sin embargo se aprovecharon todas las tecnologías con las que se cuentan actualmente y de acuerdo al análisis de las características de seguridad con las que se debe contar se logró desarrollar una herramienta a la medida que brinde seguridad y versatilidad al acceso de los usuarios del laboratorio.

Es importante mencionar que adicionalmente a los objetivos inicialmente planteados se logró que el sistema cumpliera con un par de objetivos adicionales como lo son el registro de profesores, ya que con el sistema queda una evidencia con la que se puede determinar la hora en la que se permitió acceso a los usuarios y si el profesor no marca su salida automáticamente se tendrá evidencia de que no estuvo presente o el envío de la lista de asistencia la cual permite y simplifica el trabajo de los profesores, ya que ellos evitan perder

tiempo en esta parte y también impiden que un usuario tenga la posibilidad de argumentar falsedades en cuanto a su ingreso al laboratorio.

Es importante mencionar que aunque la aplicación se encuentra completa para cumplir con el objetivo principal de este proyecto, tiene un gran ventaja ya que el desarrollo realizado para el sistema de control de acceso ocupa herramientas de amplio uso hoy en día, esto permite que las opciones de crecimiento a futuro sean ilimitadas, porque se pueden generar diversos módulos y herramientas que puedas interconectarse a lo ya establecido de manera que pueda cumplir con otras funciones, como puede ser un módulo de consulta para la administración o profesores o incluso desarrollar un sistema automatizado de calificaciones que pueda interconectarse con el de acceso para verificar la asistencia de los alumnos.

En gran medida lo que se realice a futuro con el sistema depende de la imaginación y creatividad que se tenga por parte de la administración y los usuarios para ayudar a mejorar y/o actualizar con las últimas necesidades el sistema de control de acceso o para los nuevos desarrollos que puedan reutilizar partes del mismo para simplificar los procesos del laboratorio.

Actualmente la aplicación se encuentra en el ambiente productivo después de haber pasado una fase beta durante un semestre, es importante mencionar que para un funcionamiento óptimo los profesores, alumnos y la administración del laboratorio deben comprender/implementar las nuevas políticas para el acceso al Laboratorio de Redes y Seguridad, así como estar al pendiente de seguir las mejores prácticas y recomendaciones para mantener en optimo estado el sistema.

Anexos

GLOSARIO DE TERMINOS

- .NET Framework: .NET Framework 4.5 incluye mejoras importantes en el lenguaje y en la plataforma para C#, Visual Basic y F# que simplifican la escritura de código asincrónico y le permiten combinar flujo de control en el código sincrónico, además de proporcionar una interfaz de usuario con gran capacidad de respuesta y escalabilidad de las aplicaciones web. (Microsoft.com, 2016)
- Algoritmo SHA1 (Secure Hash Algorithm 1): El popular algoritmo de cifrado de una vía utilizada para crear firmas digitales. SHA fue desarrollado por el NIST, y SHA-1 es una revisión de la norma publicado en 1994. (TheFreeDictionary.com, 2016)
- Antivirus: Un programa de computadora que escanea la memoria de una computadora y el almacenamiento masivo para identificar, aislar y eliminar viruses, y examina si los archivos entrantes contienen virus conforme van llegando. (Microsoft Press, 2002, p. 36)
- Base de datos: Un archivo compuesto de registros, cada uno contiene campos que cuentan con una serie de operaciones que permiten buscar, ordenar, recombinar y otras funciones. (Microsoft Press, 2002, p. 177)
- C: Un lenguaje de programación desarrollado por Dennis Ritchie en 1972 en los laboratorios Bell. (Microsoft Press, 2002, p. 99)
- C#: C# es un lenguaje de programación que se ha diseñado para compilar diversas aplicaciones que se ejecutan en .NET Framework. C# es simple, eficaz, con seguridad de tipos y orientado a objetos. (Microsoft.com, 2016)
- Ciclo (bucle): Las estructuras de bucles de Visual Basic permiten ejecutar una o varias líneas de código de forma repetitiva. (Microsoft.com, 2016)
- Código QR: Los códigos QR son códigos de barra bidimensionales que contienen un vínculo directo a la página web de un producto o servicio.
- Debug: Es una herramienta que permite detectar, localizar y corregir error sintácticos o lógicos en un programa o malfuncionamientos de hardware.(Microsoft Press, 2002, p. 187)
- Dispositivo biométrico: La Biometría es una serie de medidas de características específicas que permiten la identificación de personas utilizando dispositivos electrónicos que las almacena. Esta identificación consiste en comparar esas características físicas específicas de cada persona con un patrón conocido y almacenado en una base de datos. (Elvira Misfud-k idatzia, 2012)
- Dispositivos lectores: Los Lectores son los dispositivos que interactúan con el usuario y que permiten su identificación informando de este hecho a la Placa Controladora o al Equipo de Control de Acceso. (Lealsistemas.com.ar, 2016)

- Firewall: Un sistema de seguridad cuyo objetivo es proteger la red de una organización contra amenazas externas como lo son hackers. (Microsoft Press, 2002, p. 270)
- Gusano: Un programa que se propaga a si mismo a través de las computadoras, usualmente creando copias de si mismo en la memoria de las computadoras. (Microsoft Press, 2002, p. 722)
- Hardware: Los componentes físicos de un sistema de cómputo, incluyendo cualquier dispositivo periférico como lo son impresoras, módems y ratones. (Microsoft Press, 2002, p. 311)
- Hash: Un hash es un número que se genera mediante la lectura de los contenidos de un documento o mensaje. Diferentes mensajes deben generar distintos valores de hash, pero el mismo mensaje hace que el algoritmo para generar el mismo valor hash.(Microsoft.com, 2016)
- Hashing: Es el proceso de aplicarle un hash a un documento o mensaje.
- IIS (Internet Information Server): Es la marca de servidor de web de Microsoft. (Microsoft Press, 2002, p. 358)
- Inserción (insert) (BD): Agrega una o varias filas a una tabla o una vista en SQL Server.(Microsoft.com, 2016)
- Interfaz gráfica: Un ambiente visual en las computadoras que representa programas, archivos y opciones con imágenes gráficas, como iconos, menús y cajas de dialogo. (Microsoft Press, 2002, p. 302)
- Java: Un lenguaje de programación en base a objetos desarrollado por Sun Microsystems. (Microsoft Press, 2002, p. 371)
- Leyendas: Text que describe o explica una gráfica. (Microsoft Press, 2002, p. 390)
- Librería: En programación, una colección de rutinas almacenadas en un archivo. cada conjunto de instrucciones tiene un nombre y cada uno realizar una tarea diferente. (Microsoft Press, 2002, p. 99)
- Modo de autenticación de doble factor: Es un modo de autenticación que requiere que para la verificación de identidad el usuario existen dos requisitos el tener "algo" y saber "algo". (Cisco Press, 2015)
- Named Pipes: En programación, son conexiones de una o dos vías usadas para transferir datos entre procesos. Los named pipes son porciones de memoria reservada temporalmente para almacenamiento de datos. (Microsoft Press, 2002, p. 449)
- No repudio: El no repudio es el proceso que garantiza que el emisor no pueda negar lo que hizo. No repudio equivale al término de "Aceptación" y es una de las características más difíciles de garantizar. (Datateca.unad.edu.co, 2016)
- No-break (UPS): Dispositivo que proporciona un respaldo de batería cuando la potencia eléctrica falla o existe una caída a un nivel de voltaje inaceptable. (Pcmag.com, 2016)

- Página web: Conjunto de informaciones de un sitio web que se muestran en una pantalla y que puede incluir textos, contenidos audiovisuales y enlaces con otras páginas. (Diccionario de la lengua española, 2016)
- Privilegios de usuarios: Los privilegios de usuario son aplicados localmente y permiten a los usuarios realizar ciertas tareas. (Microsoft.com, 2016)
- Rack: Marco o estante, a menudo se forma de barras, Que se utiliza para mantener las cosas. (Dictionary.cambridge.org, 2016)
- RJ45: An eight-wire connector used to attach devices to cables. The eight wires are encased in a plastic sheath and color-coded to match corresponding slots in jacks. RJ-45 jacks are used to connect computers to LANs (local area networks) and to link ISDN (Integrated Services Digital Network) devices to NT-1 (Network Terminator 1) devices. (Microsoft Press, 2002, p. 572)
- Router: Los routers se utilizan para conectar varias redes. Los routers analizan los datos que se van a enviar a través de una red, los empaquetan de forma diferente y los envían a otra red o a través de un tipo de red distinto. (Cisco, 2012, p. 2)
- RS232: Un estándar aceptado por la industria para las conexiones de comunicaciones serie. (Microsoft Press, 2002, p. 576)
- RS485: Es una especificación para la capa física de la red que utiliza la diferencia de voltajes entre dos cables. (Chipkin.com, 2016)
- SDK (Software Development Kit): Acrónimo de software de desarrollo de la misma. Un conjunto de rutinas (Por lo general, en una o más bibliotecas) diseñados para permitir a los desarrolladores escribir más fácilmente programas para un equipo determinado, sistema operativo, o de la interfaz de usuario. Ver también la biblioteca (definición 1), caja de herramientas. (Microsoft Press, 2002, p. 195)
- Servidor de BD: Un nodo de red, o estación, dedicados a almacenar y proporcionar acceso a una base de datos compartida. (Microsoft Press, 2002, p. 177)
- Servidor web: Es un servidor de software que principalmente utiliza HTTP para proporcionar documentos HTML, así como archivos asociados y scripts cuando sean solicitados por un cliente, como lo sería un navegador web. (chipkin.com, 2016)
- SimpleDateFormat: Es una clase concreta para formatear y analizar las fechas de una manera sensible a la localidad. (Docs.oracle.com, 2016)
- Software: Son una serie de instrucciones que permiten que el hardware realice diversas funciones. Dos tipos principales de software son software del sistema (sistemas operativos), que controla el funcionamiento de la computadora, y aplicaciones, tales como programas de procesamiento de texto, hojas de cálculo y bases de datos, que realizan las tareas para los cuales la gente usa los ordenadores. (Microsoft Press, 2002, p. 615)

- SQL injection: La inyección de código SQL es un ataque en el cual se inserta código malicioso en las cadenas que posteriormente se pasan a una instancia de SQL Server para su análisis y ejecución.(Microsoft.com, 2016)
- SQL Management Studio: Microsoft SQL Server 2008 Management Studio Express es un entorno gratuito e integrado para obtener acceso, configurar, administrar y desarrollar todos los componentes de SQL Server, así como para combinar un amplio grupo de herramientas gráficas y enriquecidos editores de scripts que proporcionan acceso a SQL Server para programadores y administradores de todos los niveles. (Microsoft.com, 2016)
- SQL Server Browser: El programa SQL Server Browser se ejecuta como un servicio de Windows. SQL Server Browser escucha las solicitudes entrantes de recursos de Microsoft SQL Server y proporciona información acerca de las instancias de SQL Server instaladas en el equipo. (Microsoft.com, 2016)
- SQL Server Express 2008: Microsoft SQL Server 2008 Express es un sistema de administración de datos eficaz y confiable que ofrece un variado conjunto de características, protección de datos y rendimiento para clientes de aplicaciones incrustadas, aplicaciones web ligeras y almacenes de datos locales. (Microsoft.com, 2016)
- SQLite: Es una librería que implementa un motor de base de datos. (Sqlite.org, 2016)
- SSL: Es un protocolo que autentica servidores y clientes que posteriormente se usa para cifrar los mensajes entre las partes autenticadas. (Microsoft.com, 2016)
- Substring: Función que devuelve parte de una expresión de caracteres, binaria, de texto o de imagen en SQL Server. (Microsoft.com, 2016)
- Switch: Son equipos que se utilizan para conectar varios dispositivos a través de la misma red dentro de un edificio u oficina. (Cisco, 2012, p. 2)
- Tablet: Dispositivo electrónico portátil con pantalla táctil y con múltiples prestaciones. (Diccionario de la lengua española, 2016)
- Tarjeta SD (tarjeta de memoria): Las tarjetas de memoria flash almacenan información del equipo, como texto, imágenes y música. Puede borrar y volver a usar las tarjetas de memoria una y otra vez. (Microsoft.com, 2016)
- TCP: TCP es un protocolo de transporte orientado a la conexión que envía los datos no estructurados como una corriente de bytes. (Cisco.com, 2016)
- IP: IP es el protocolo primario de Capa 3 en la suite de Internet. Además de enrutamiento entre redes, IP proporciona informes de errores y la fragmentación y el montaje de unidades de información llamados datagramas para la transmisión a través de redes con diferentes tamaños máximos de unidades de datos. IP representa el corazón de la suite de protocolo de Internet. (Cisco.com, 2016)
- The jTDS Project: Es una librería para desarrollada para Java la cual permite la comunicación con Microsoft SQL Server. (Jtds.sourceforge.net, 2106)

- Tomcat de Apache: Es una implementación abierta de Java Servlet, JavaServer Pages, Expresiones de Java y las tecnologías de Java WebSocket. (tomcat.apache.org, 2016)
- Trigger (Disparadores): Un disparador es una clase especial de procedimiento almacenado que se ejecuta automáticamente cuando se produce un evento en el servidor de bases de datos. (Microsoft.com, 2016)
- Troubleshooting: Detectar, localizar y corregir error sintácticos o lógicos en un programa o malfuncionamientos de hardware.
- Update (BD): Cambia los datos de una tabla o vista. (Microsoft.com, 2016)
- Virus: Un programa intrusivo que infecta ficheros informáticos mediante la inserción en esos archivos de copias de sí mismo. (Microsoft Press, 2002, p. 699)
- Visual Studio: Un completo entorno de desarrollo integrado para crear aplicaciones espectaculares para Windows, Android e iOS, además de aplicaciones web y servicios de nube innovadores.(Visualstudio.com, 2016)
- Windows Installer: Microsoft Windows Installer es un componente del sistema operativo Windows. Windows Installer proporciona una base estándar para la instalación y la desinstalación de software. (Microsoft.com, 2016)

GUIA DE INSTALACION DE SQL SERVER

Para realizar la instalación de SQL Server Express 2008 se pueden encontrar múltiples guías en internet, pero es recomendable utilizar la del sitio del desarrollador en este caso Microsoft para obtener la información exacta para este sistema, a continuación se encuentra el link donde es posible encontrar la información:

https://msdn.microsoft.com/es-mx/library/gg512108(v=vs.91).aspx

Sobre la guía anterior en caso de querer manejar el modo de autenticación mixto se debe ignorar el paso no.9 y para mayor detalle e información se puede consultar el siguiente enlace:

https://technet.microsoft.com/es-es/library/ms143705(v=sql.90).aspx

Fuentes de Información

(2016). *Support.microsoft.com*. Retrieved 5 June 2016, from https://support.microsoft.com/es-mx/kb/942288

Brochure_redes. (2016) (1st ed.). Retrieved from http://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectadosanonimos/routing/pdfs/brochure_redes.pdf

C#. (2016). *Msdn.microsoft.com*. Retrieved 5 June 2016, from https://msdn.microsoft.com/es-mx/library/kx37x362.aspx

Código QR | ESAN. (2016). *Esan.edu.pe*. Retrieved 5 June 2016, from http://www.esan.edu.pe/qr/

design, D. (2016). *Control de accesos | Leal sistemas*. *Lealsistemas.com.ar*. Retrieved 5 June 2016, from http://www.lealsistemas.com.ar/control-de-acceso.html

CREATE TRIGGER (Transact-SQL). (2016). *Msdn.microsoft.com*. Retrieved 5 June 2016, from https://msdn.microsoft.com/es-es/library/ms189799(v=sql.120).aspx

Data Hashing in SQL Server. (2011). *Blogs.msdn.microsoft.com*. Retrieved 5 June 2016, from https://blogs.msdn.microsoft.com/sqlsecurity/2011/08/26/data-hashing-in-sql-server/

Dictionary, r. (2016). *rack Meaning in the Cambridge English Dictionary*. *Dictionary.cambridge.org*. Retrieved 5 June 2016, from http://dictionary.cambridge.org/dictionary/english/rack

Download Microsoft .NET Framework 4.5 from Official Microsoft Download Center. (2016). *Microsoft.com*. Retrieved 5 June 2016, from https://www.microsoft.com/es-mx/download/details.aspx?id=30653

Download Microsoft® SQL Server® 2008 Express from Official Microsoft Download Center. (2016). *Microsoft.com*. Retrieved 5 June 2016, from https://www.microsoft.com/es-mx/download/details.aspx?id=1695

Download Microsoft® SQL Server® 2008 Management Studio Express from Official Microsoft Download Center. (2016). *Microsoft.com*. Retrieved 5 June 2016, from https://www.microsoft.com/es-mx/download/details.aspx?id=7593

Estructuras de bucles (Visual Basic). (2016). *Msdn.microsoft.com*. Retrieved 5 June 2016, from https://msdn.microsoft.com/es-MX/library/ezk76t25.aspx

INSERT (Transact-SQL). (2016). *Msdn.microsoft.com*. Retrieved 5 June 2016, from https://msdn.microsoft.com/es-es/ms174335

Instrumentos de Medicion industrial y Cerraduras biometricas. (2016). *Bluemetric.mx*. Retrieved 5 June 2016, from http://www.bluemetric.mx/

Inyección de código SQL. (2016). *Technet.microsoft.com*. Retrieved 5 June 2016, from https://technet.microsoft.com/es-es/en-es/library/ms161953(v=sql.105).aspx

jTDS JDBC Driver. (2016). *Jtds.sourceforge.net*. Retrieved 5 June 2016, from http://jtds.sourceforge.net/

Lección 14: No repudio. (2016). *Datateca.unad.edu.co*. Retrieved 5 June 2016, from http://datateca.unad.edu.co/contenidos/233011/233011Exe/leccin_14_no_repudio.html

Memoria y almacenamiento. (2016). *windows.microsoft.com*. Retrieved 5 June 2016, from http://windows.microsoft.com/es-MX/windows7/memory-and-storage

MercadoLibre México. (2016). *Mercadolibre.com.mx*. Retrieved 5 June 2016, from http://www.mercadolibre.com.mx/

Microsoft Press. (2002). Microsoft® Computer Dictionary. Redmond, Wash.: Microsoft Press.

Modo de autenticación (SQL Server Express). (2016). *Technet.microsoft.com*. Retrieved 5 June 2016, from https://technet.microsoft.com/es-es/library/ms143705(v=sql.90).aspx

página. (2016). *Diccionario de la lengua española*. Retrieved 5 June 2016, from http://dle.rae.es/?id=RRvUbbP

Project, A. (2016). *Apache Tomcat® - Welcome!*. *Tomcat.apache.org*. Retrieved 5 June 2016, from http://tomcat.apache.org/

Servicio SQL Server Browser. (2016). *Technet.microsoft.com*. Retrieved 5 June 2016, from https://technet.microsoft.com/es-es/library/ms181087(v=sql.105).aspx

SHA-1. (2016). *TheFreeDictionary.com*. Retrieved 5 June 2016, from http://encyclopedia2.thefreedictionary.com/SHA-1

SimpleDateFormat (Java Platform SE 7). (2016). *Docs.oracle.com*. Retrieved 5 June 2016, from https://docs.oracle.com/javase/7/docs/api/java/text/SimpleDateFormat.html

SISTEMAS DE CONTROL DE ACCESO Y ASISTENCIA. (2016). *Altecmex.com.mx*. Retrieved 5 June 2016, from http://www.altecmex.com.mx

SL, M. (2016). *Kimaldi | Control de acceso, Control de presencia, Biometría, RFID, Lectores e Impresoras de tarjetas - kimaldi*. *Kimaldi.com*. Retrieved 5 June 2016, from http://www.kimaldi.com

SQLite Home Page. (2016). *Sqlite.org*. Retrieved 5 June 2016, from https://www.sqlite.org/

SUBSTRING (Transact-SQL). (2016). *Msdn.microsoft.com*. Retrieved 5 June 2016, from https://msdn.microsoft.com/es-es/library/ms187748(v=sql.120).aspx

tableta. (2016). *Diccionario de la lengua española*. Retrieved 5 June 2016, from http://dle.rae.es/?id=YtKUrYg

TCP/IP Overview. (2016). *Cisco*. Retrieved 5 June 2016, from http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13769-5.html

Tutorial: instalar y configurar SQL Server 2008 R2 Express con Advanced Services. (2016). *Msdn.microsoft.com*. Retrieved 5 June 2016, from https://msdn.microsoft.com/es-mx/library/gg512108(v=vs.91).aspx

UPDATE (Transact-SQL). (2016). *Msdn.microsoft.com*. Retrieved 5 June 2016, from https://msdn.microsoft.com/es-es/en-es/library/ms177523.aspx

User Rights. (2016). *Technet.microsoft.com*. Retrieved 5 June 2016, from https://technet.microsoft.com/en-us/library/dd349804%28v=ws.10%29.aspx

Vallejo, C. (2016). *Sistemas físicos y biométricos de seguridad | Observatorio Tecnológico.Recursostic.educacion.es*. Retrieved 5 June 2016, from http://recursostic.educacion.es/observatorio/web/eu/cajon-de-sastre/38-cajon-de-sastre/1045-sistemas-fisicos-y-biometricos-de-seguridad

Visual Studio - Microsoft Developer Tools. (2016). *Visualstudio.com*. Retrieved 5 June 2016, from https://www.visualstudio.com/

What is TLS/SSL?: Logon and Authentication. (2016). *Technet.microsoft.com*. Retrieved 5 June 2016, from https://technet.microsoft.com/es-us/library/cc784450(v=ws.10).aspx

Woland, A. & Redmon, K. (2015). *CCNP Security SISAS 300-208 Official Cert Guide* (1st ed.). Indianapolis: Cisco Press. Retrieved from http://safaribooksonline.com