UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE INGENIERIA
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

TÍTULO:

Control de Seguridad Biométrico de Reconocimiento Facial como Caso de Estudio Implementación en el Área Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil.

AUTORES:

Solis Calvopiña, Liliana Nathaly ; Puga Torres, Luiggi Ramiro

Trabajo de Titulación previo a la Obtención del Título de:
INGENIERO EN SISTEMAS COMPUTACIONALES

TUTOR:

Ing. Murillo Bajaña, Eduardo Wenceslao, MSc.

Guayaquil, Ecuador

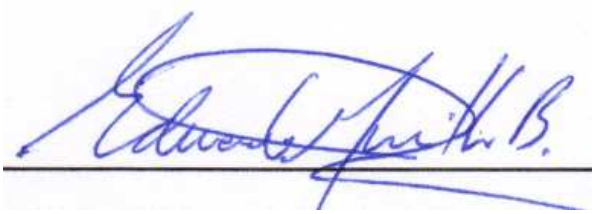
22 de Septiembre del 2016

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE INGENIERIA
CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por **Solis Calvopiña, Liliana Nathaly y Puga Torres, Luiggi Ramiro** como requerimiento parcial para la obtención del Título de **INGENIERO EN SISTEMAS COMPUTACIONALES**

TUTOR



Ing. Murillo Bajaña, Eduardo Wenceslao, MSc.

DIRECTORA DE CARRERA

Ing. Guerrero Yépez, Beatriz del Pilar, Mgs.

Guayaquil, a los 22 días del mes de Septiembre del año 2016

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE INGENIERIA
CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

DECLARACIÓN DE RESPONSABILIDAD

Nosotros,
Solis Calvopiña, Liliana Nathaly y Puga Torres, Luiggi Ramiro

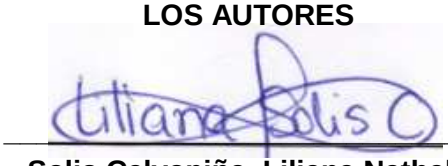
DECLARAMOS QUE:

El Trabajo de Titulación "**Control de Seguridad Biométrico de Reconocimiento Facial como Caso de Estudio Implementación en el Área Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil"** previo a la obtención del Título de **Ingeniero en Sistemas Computacionales**, ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de nuestra total autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del Trabajo de Titulación referido.

Guayaquil, a los 22 días del mes de Septiembre del año 2016

LOS AUTORES



Solis Calvopiña, Liliana Nathaly

Puga Torres, Luiggi Ramiro

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE INGENIERIA
CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

AUTORIZACIÓN

Nosotros,
Solis Calvopiña, Liliana Nathaly y Puga Torres, Luiggi Ramiro

Autorizamos a la Universidad Católica de Santiago de Guayaquil, la **publicación** en la biblioteca de la institución del Trabajo de Titulación: **Control de Seguridad Biométrico de Reconocimiento Facial como Caso de Estudio Implementación en el Área Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil**, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

Guayaquil, a los 22 días del mes de Septiembre del año 2016

LOS AUTORES

Solis Calvopiña, Liliana Nathaly

Puga Torres, Luiggi Ramiro

REPORTE URKUND

URKUND

Urkund Analysis Result

Analysed Document: SOLIS_LILIANA_PUGA_TORRES_FINAL.docx (D21528075)
Submitted: 2016-08-29 01:08:00
Submitted By: eduardo.murillo02@cu.ucsg.edu.ec
Significance: 1 %

Sources included in the report:

http://docplayer.es/14694123-Reconocimiento-de-caras-eigenfaces-y-fisherfaces.html
http://lcsi.umh.es/docs/pfc_sergio/Memoria_Sergio_Rodriguez.pdf

Instances where selected sources appear:

5

AGRADECIMIENTO

Agradezco a Dios por darme el don de sabiduría y de entendimiento, gracias a estos pude desenvolverme de manera correcta a lo largo de mi carrera universitaria y hoy por hoy obtener el Título de Ingeniera en Sistemas Computacionales.

Agradezco a mis padres, por darme un hogar, inculcarme desde siempre valores y por su arduo sacrificio para brindarme los estudios.

Agradezco a mis abuelitos, sus mimos y su dulzura ayudaron a forjarme con un alma sensible.

Agradezco a mis demás familiares, por brindarme sus consejos y estar pendiente siempre de mí.

Agradezco a Paul Legarda, por brindarme su amor y apoyo para no desfallecer en el intento de culminar con éxito mi carrera.

Agradezco a mi tutor Ing. Eduardo Murillo, por brindarnos sus conocimientos y su tiempo con el propósito de llegar a cumplir la meta anhelada.

Agradezco a mi compañero de tesis Luiggi Puga, por dar todo de sí para la creación de este proyecto.

Agradezco a la Universidad Católica de Santiago de Guayaquil por permitirme adquirir mi formación profesional, a mis profesores por brindarme mucho más que sus conocimientos, su experiencia, a mis compañeros de clases por darme su amistad, mientras emprendíamos este camino del estudio universitario, en especial a mi amigo José Plúas.

Solis Calvopiña, Liliana Nathaly

AGRADECIMIENTO

Primero, me gustaría agradecer a la Universidad Católica Santiago de Guayaquil por haberme permitido ser parte de esta prestigiosa institución, así como a sus docentes por habernos brindado su conocimiento.

Agradezco también a mi tutor de tesis Ing. Eduardo Murillo Wenceslao, MSc, quien nos supo guiar en todo el desarrollo de este proyecto.

Agradezco a mi compañera de tesis Liliana Solis, que gracias a su esmero y dedicación han hecho que este proyecto se realice de la mejor forma posible.

A mi familia y seres queridos, por estar siempre allí, apoyándome para que nada salga mal, a sus consejos que han hecho que cumpla con la meta propuesta**.**

Puga Torres, Luiggi Ramiro

DEDICATORIA

Dedico este logro a Dios por permitirme vivirlo y a mi familia; mi padre Olmedo Solis, mi madre Jenny Calvopiña y a mis hermanos Carolina y Fernando Solis, por brindarme siempre su amor y apoyo incondicional.

Solis Calvopiña, Liliana Nathaly

DEDICATORIA

Dedico esta tesis a mi madre que ha sabido guiarme en el trayecto de mi vida, a sus consejos que han hecho de mí la persona que actualmente soy.

De igual forma, dedico la tesis a mis hermanas que han estado siempre apoyándome en mis buenos y malos momentos.

A mi familia en general y a las personas especiales de mi vida, que han sabido complementar mi formación, directa e indirectamente.

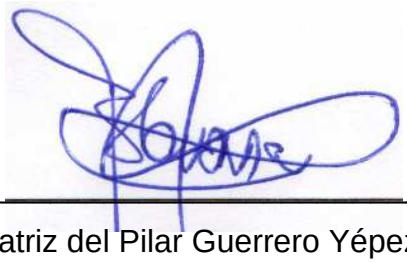
Gracias a todos que han hecho un solo conjunto esencial en mi vida.

Puga Torres, Luiggi Ramiro

TRIBUNAL DE SUSTENTACIÓN

Ing. Eduardo Wenceslao Murillo Bajaña, MSc.

PROFESOR TUTOR



Ing. Beatriz del Pilar Guerrero Yépez, Mgs.

DIRECTORA DE CARRERA

Ing. Lorgia del Pilar Valencia Macías, Mgs.

DOCENTE DELEGADO

Ing. Colón Mario Célleri Mujica, Mgs.

OPONENTE

UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL

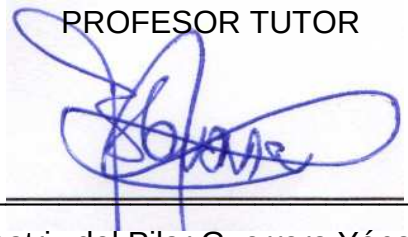
FACULTAD DE INGENIERIA

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

CALIFICACIÓN

Ing. Eduardo Wenceslao Murillo Bajaña, MSc.

PROFESOR TUTOR



Ing. Beatriz del Pilar Guerrero Yépez, Mgs.

DIRECTORA DE CARRERA

Ing. Lorgia del Pilar Valencia Macías, Mgs.

DOCENTE DELEGADO

Ing. Colón Mario Célleri Mujica, Mgs.

OPONENTE

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

La aplicación de este proyecto está orientada a salvaguardar la seguridad del personal laboral, basado en la detección y reconocimiento facial automático de las personas que ingresan y egresan al Área Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil.

Su diseño se basa en un sistema control de seguridad biométrico de reconocimiento facial. Este cuenta con dos herramientas principales; la librería OpenCV que permite la detección de caras bajo la aplicación de Característicos Haar, y el uso del API Kairos, el cual brinda el servicio de reconocimiento facial a través de la recepción de peticiones con el rostro detectado para identificar si coincide o no con uno de los rostros previamente enrolados.

El administrador podrá enrolar las imágenes de los rostros de las personas autorizadas con sus datos; consultar los registros de detecciones de personas reconocidas y no reconocidas, así como visualizar la lista de las personas enroladas; por último, recibirá diariamente por correo electrónico un informe de las personas no reconocidas.

Para la elaboración de este proyecto se usó el tipo de investigación descriptiva, y para la recolección de datos se aplicaron instrumentos como: encuestas, entrevistas y observaciones. Las encuestas y entrevistas permitieron corroborar la necesidad de la implementación de un sistema control de seguridad y las observaciones directas de las pruebas de funcionamiento del equipo para comprobar la efectividad del proyecto.

Palabras Claves: DETECCIÓN DE CARAS; RECONOCIMIENTO FACIAL; SEGURIDAD DEL PERSONAL LABORAL; LIBRERÍA OPENCV; CARACTERÍSTICAS HAAR; BIOMÉTRICO; API KAIROS.

ABSTRACT

The implementation of this project is aimed at safeguarding the security of the workforce, based on detection and automatic facial recognition of people who enter and leave the Administrative Area of the Faculty of Engineering of the Catholic University of Santiago de Guayaquil.

Its design is based on a biometric control system face recognition security. This has two main tools; the OpenCV library that allows detection of faces under the application of characteristic Haar, and the use of API Kairos, which offers the service of facial recognition through the receipt of requests with the face detected to identify whether or not match one of faces previously enrolled.

The administrator may enlist the images of the faces of those authorized with your data; consult the records of detections recognized and unrecognized people, and to view the list of people enrolled; Finally, you will receive daily email a report of unrecognized people.

For the development of this project the kind of descriptive research was used, and data collection instruments were applied as: surveys, interviews and observations. Surveys and interviews allowed corroborate the need for implementation of a control system security and direct observations of equipment performance testing to verify the effectiveness of the project.

Key Words: FACE DETECTION; FACE RECOGNITION; PERSONAL WORK SAFETY; OPENCV LIBRARY; FEATURES HAAR; BIOMETRICS; KAIROS API.

INTRODUCCIÓN

La Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil UCSG cuenta con dos carreras: Ingeniería en Sistemas Computacionales e Ingeniería Civil. Para su administración la facultad cuenta con 27 personas entre autoridades, personal administrativo y profesores tiempo completo; el horario laboral del área administrativa es de 08h30 a 17h30 muy apartado al de los profesores de tiempo completo y autoridades que empieza desde las 09h00 hasta las 22h00.

En la actualidad el Área Administrativa de la Facultad de Ingeniería de la UCSG es frecuentado a diario por autoridades, profesores, personal administrativo y estudiantes de la Facultad, además de personas ajenas a la facultad. El Área Administrativa cuenta únicamente con un control de video-vigilancia que es monitoreado por el Centro de Investigación de Desarrollo Tecnológico CIDT.

El Área Administrativa de la Facultad de Ingeniería no cuenta con ningún registro de entrada y salida de las personas que transitan a diario en la facultad, que en ocasiones son personas no relacionadas a el área especificada, quienes ingresan por la puerta eléctrica que es operada por el personal de control de cátedra.

El proyecto tecnológico se enfoca en el control automatizado de las personas que acceden al área administrativa de la facultad de ingeniería. Esta herramienta tecnológica, provista de una base de datos de imágenes faciales de las personas autorizadas previamente enroladas, realizará la comparación de las facciones del rostro con las personas que precisen acceder a dicha área para hallar semejanzas. Además, la herramienta está habilitada para generar reportes y alertas que serán accesibles por el administrador de la aplicación.

CAPÍTULO I: EL PROBLEMA

1.1 Problema de Investigación

El proyecto nace de la observación realizada por un docente de tiempo completo de la Facultad de Ingeniería, Ing. Lorgia Valencia, al comentar que en ocasiones se encuentra con personas desconocidas en los pasillos del Área Administrativa de la Facultad.

El Área Administrativa de la Facultad de Ingeniería de la UCSG, no posee un control de seguridad en sus instalaciones, que registre la entrada y salida de las personas que asisten a dicha área, generando inseguridades en el ambiente del personal laboral. En la actualidad solo existe un sistema de control de video-vigilancia monitoreado por el Centro de Investigación de Desarrollo Tecnológico CIDT.

1.2 Objetivo General

Diseñar E Implementar Un Control De Seguridad Biométrico De Reconocimiento Facial Como Caso De Estudio Para La Facultad De Ingeniería De La UCSG.

1.3 Objetivos Específicos

- Diseñar una aplicación de detección facial, para el área administrativa de la Facultad de Ingeniería de la UCSG.
- Diseñar un web service que reciba las peticiones de los dispositivos, registrando las transacciones y procesando las peticiones con los servicios de reconocimiento.
- Diseñar una consola administrativa que permita el monitoreo de la aplicación para la Facultad de Ingeniería de la UCSG.
- Generar reportes de la bitácora del acceso de las personas al área administrativa de la Facultad de Ingeniería de la UCSG.
- Generar notificaciones, correspondiente a las transacciones diarias de personas reconocidas y no reconocidas.

1.4 Justificación

Actualmente en la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil UCSG, el Centro de Investigación de Desarrollo Tecnológico CIDT es el encargado de vigilar mediante un Circuito Cerrado de Televisión CCTV el área administrativa, realizando el control de video-vigilancia.

Para garantizar mayor seguridad del personal que labora y de la información que se genera en la Facultad de Ingeniería de la UCSG, nace el proyecto Control de Seguridad Biométrica de Reconocimiento Facial como Caso de Estudio Implementación en el Área Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil. Para este proyecto se utilizaron técnicas de visión artificial, reconocimiento facial y además se automatizó el proceso de registro de personas que acceden al área, para el control de seguridad de un área específica.

El proyecto proveerá una aplicación que puede ser controlada por un administrador, en la cual se podrá visualizar los rostros detectados de las personas que ingresan y egresan del área administrativa así como acceder a reportes detallados con el reconocimiento de rostros.

1.5 Alcance

El proyecto está enfocado en el reconocimiento facial de las personas que acceden al área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil.

- Se diseñará e implementará una aplicación de detección facial, instalada en una Raspberry Pi (hardware), usando la librería Open Computer Visión (OpenCV) para implementar la función de detección, el algoritmo de Kairos se encargará del reconocimiento facial de personas a través de imágenes, capturadas por la cámara Raspberry Pi.

- Se diseñará e implementará una consola administrativa con *login,* manteniendo las restricciones necesarias para acceder a la aplicación, para permitir el enrolamiento del personal administrativo y visualizar los reportes generados de las transacciones de reconocimiento diarias.

- Se enviarán al personal designado notificaciones de los rostros detectados sin reconocimiento.

CAPÍTULO II: FUNDAMENTACIÓN CONCEPTUAL

2.1 Antecedentes

El reconocimiento facial se remonta a los años sesenta cuando se desarrolló el primer sistema de reconocimiento facial semi-automático, que requería de la interacción del administrador para la localización de rasgos faciales como ojos, nariz, boca y orejas en fotografías antes de que el sistema calculará distancias a puntos de referencia en común, para luego ser comparados con datos de referencia.

Según el Consejo Nacional de Ciencia y Tecnología (2006) en la década de los setenta, Goldstein, Harmon & Lesk utilizaron su propio método basado en 21 marcadores subjetivos, como el color del pelo o el grosor de los labios; sin embargo todos los marcadores se calculaban manualmente. En 1988 Kirby & Sirobich aplicaron el análisis de componentes principales, una técnica estándar del álgebra lineal, al problema del reconocimiento facial y mostraron que necesitaban menos de cien valores para cifrar acertadamente la imagen de una cara convenientemente alineada y normalizada.

Además el Consejo Nacional de Ciencia y Tecnología (2006) menciona que, en 1991 Turk & Pentland, utilizaron las técnicas Eigenfaces; las cuales extraen los rasgos característicos de la cara como ojos, nariz, boca de las imágenes capturadas; discriminando señales de entrada que impidan realizar esta acción como las diferentes condiciones de iluminación que se presentan en el ambiente. Mediante estas herramientas se pudo detectar caras en las imágenes, permitiendo automatizar sistemas de reconocimiento facial en tiempo real.

2.2 Biometría

Según la apreciación de Mou Dengpan en su libro Machine-based Intelligent Face Recognition (2010) El término "biometría" proviene de las palabras griegas "bio" (significa vida) y "métrica" (significa medida). Mide y analiza las características biológicas únicas del humano, ya sea física o de comportamiento, en el propósito de reconocimiento (autenticación). A su vez Misfud (2012) se refiere a Biometría como,

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.

Entre las biometrías para la identificación de las personas tenemos:

2.2.1 Huella Dactilar

De acuerdo a Valdés (2015), una huella dactilar es el patrón de valles y crestas en la superficie de un dedo, que se forma durante los primeros siete meses de desarrollo fetal. Se trata de una característica única, que no se repite inclusive entre mellizos idénticos.

Dentro de las ventajas de utilizar la biometría dactilar para implementarla en un sistema biométrico de detección y reconocimiento son el bajo costo de la arquitectura de hardware y la exactitud obtenida del reconocimiento de la huella dactilar del usuario, entre sus desventajas existen la pérdida o desgaste de las huellas dactilares del usuario por lo cual dejaría de ser efectivo el sistema biométrico; comúnmente es utilizada para el control de acceso lo cual requiere de una interacción directa con el dispositivo biométrico.

2.2.2 Facial

Según lo que expresa en su tesis Valdés (2015), la biometría facial se basa en la localización y sus atributos faciales distinguibles como ojos, cejas, nariz, labios y mentón; y sus relaciones espaciales, elementos que pueden ser medidos y asociarlos a un solo individuo.

Esta biometría tiene como ventaja la baja participación del usuario para la detección de su rostro, sin embargo se ve afectada por los diferentes ambientes de iluminación que puede darse según el lugar y la ubicación del equipo biométrico.

2.2.3 Iris

La biometría de iris, “es la región anular del ojo limitada por la pupila y la esclera. Su textura compleja, formada durante el desarrollo fetal, resulta muy distintiva y, por ende, útil para el reconocimiento de personas, pues no hay dos que posean idéntico iris.” (Valdés, 2015)

La ventaja de esta biometría es que el músculo utilizado para la detección es interno y se encuentra protegido, con menor probabilidad a lesiones; mientras que su desventaja es que la captura de la imagen de iris del usuario requiere alto grado de atención y participación con el dispositivo biométrico.

2.2.4 Retina

Se basa en la estructura de la vasculatura de la retina que es característica de cada ojo del individuo, y, debido a la dificultad para cambiarla o replicarla, podría ser considerada la medida biométrica más segura.

La ventaja de usar la retina para la detección es que se utilizan los vasos sanguíneos del usuario para su detección y reconocimiento, los cuales se mantienen a lo largo de la vida humana, también son difíciles de ser imitados, su desventaja radica en un mayor esfuerzo realizado por el usuario lo cual causa impaciencia y por ende sea este el rechazo a este tipo de biometría

2.3 Herramientas de Visión Artificial

Según Grimson & Mundy (1994) su definición de visión artificial “se deriva de la “Inteligencia Artificial” que, mediante el uso de técnicas adecuadas, se puede obtener el procesamiento y análisis de cualquier tipo de información en base a las imágenes digitales capturadas mediante las entradas sensoriales”.

Entre algunas librerías de visión artificial tenemos:

2.3.1 Torch3vision

Marcel y Rodríguez (2016) expresan en la página web del Instituto de Investigación IDIAP qué, torch3vision es una “biblioteca de software común para la visión artificial con algoritmos de aprendizaje automático. Escrito en C++ sencilla, esta biblioteca se basa en Torch y se distribuye bajo una licencia BSD.” Su última versión es la 2.1 y fue actualizada el 2 de abril del 2007.

2.3.2 VXL

Según determina la página web VXL (2016), VXL (the vision something - libraries) (2016) es una colección de bibliotecas de C++ diseñado para la investigación y la aplicación de visión por ordenador. Fue creado a partir TargetJr y el IUE con el objetivo de hacer una luz sistema, rápido y consistente. VXL está escrito en ANSI / ISO C++ y está diseñado para ser portátil sobre muchas plataformas.

2.3.3 OpenCV

OpenCV es una biblioteca de código abierto de visión por computadora desarrollado por Intel, es multiplataforma para sistemas operativos como Windows, Linux y Mac OX; también es multilenguaje para ser implementado en lenguajes de programación como Java, Python, C++ y C#; sirve para extraer y procesar datos significativos a partir de imágenes mediante el algoritmo de Viola-Jones con las características Haar, las cuales se explicarán posteriormente.

OpenCV utiliza en su librería un objeto principal de tipo Mat(tipo matriz), básicamente es una clase dividida en dos miembros:

- Cabecera de matriz con un tamaño constante. Contiene el tamaño de la matriz, el método utilizado para almacenar, en la que la dirección es la matriz almacenada, el tamaño de la matriz varía dependiendo de la imagen según su calidad.

- Puntero a la matriz que contiene el valor de los pixeles, el tamaño de la propia matriz puede variar de imagen a imagen y por lo general es mayor en varios órdenes de magnitud.

2.4 Herramienta de Reconocimiento Facial

Según el Grupo de Trabajo Sobre Protección de Datos (2012), el reconocimiento facial es el tratamiento automático de imágenes digitales que contienen las caras de personas a fines de identificación, autenticación/verificación o categorización de dichas personas.

2.4.1 Kairos

Kairos es una plataforma de análisis humano, que desarrolla herramientas de visión por computadora pagadas, creadas para el reconocimiento facial, en donde busca, encuentra y reconoce de entre las personas enroladas la imagen capturada; análisis de emociones, la cual analiza la expresiones y comprende los sentimiento del usuario mediante el video capturado y demografía de multitudes, el algoritmo que mide la cantidad y características de las personas como su atención, edad y género de multitudes, mediante la captura de videos, imágenes o en tiempo real.

2.4.2 OpenFace

OpenFace es un software libre, desarrollado por un grupo de investigadores de la Universidad Carnegie Mellon de Pensilvania “basado, en FaceNet, el proyecto de investigación de Google que es capaz de captar e identificar los rostros en tiempo real.” (Llorca, 2015)

2.4.3 OpenBR

Es un proyecto originario de la Corporación MITRE, publicado como software de código abierto bajo la licencia Apache 2, desarrollado en C++ activo en los sistemas operativos Windows, Mac y Linux, con los puertos a Android, iOS; su

marco de referencia se inclina al reconocimiento facial de imágenes fijas, evaluando su rendimiento sobre la cara frontal.

2.5 Explicación del Algoritmo de Detección Facial Viola – Jones

Este algoritmo fue creado por Pablo Viola y Michael Jones en el año 2001, basado en la detección de objetos visuales en tiempo real, propone un modelo clasificador en cascada con características en vez de pixel a pixel, reduciendo tiempo mediante la abstracción del algoritmo.

2.5.1 Integral de la Imagen

Viola-Jones utiliza esta integral para calcular aceleradamente el valor escalar de un grupo.

Gráfico 1: Integral de la Imagen

$$ii(x, y) = \sum_{x' \leq x, y' \leq y} i(x', y'),$$

Fuente: (Viola & Jones, 2001)

Para realizar el cálculo se determina un punto x,y; que se establece su valor en la suma de los pixeles ubicados por encima y a su izquierda de dicho punto incluyéndose, convirtiendo la imagen original en una imagen integral.

Gráfico 2: Imagen Original y su transformación a Imagen Integral aplicando la fórmula Integral de la Imagen

1	1	1
1	1	1
1	1	1

1	2	3
2	4	6
3	6	9

Fuente: (Hernández, Cabrera, Sánchez, & Cabrera, 2012)

En el Grafico 2, la primera tabla es la Imagen Original y la segunda es la Imagen Integral, resultado de la aplicación de la Integral de la imagen mostrada en el Gráfico 1. Obtenida la imagen integral se pueden aplicar las diferentes

características (filtros) de Haar y lograr así una mejor identificación de rostro sobre la imagen.

2.5.2 Características Haar

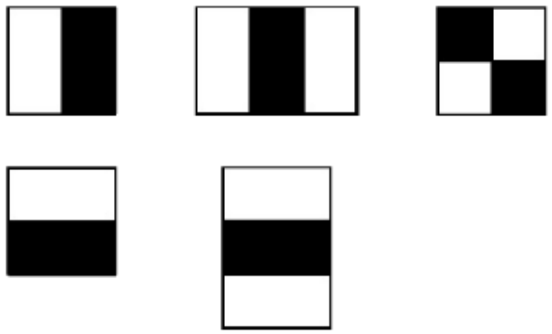
Según Joaquín Planells (2009) las características tipo Haar se definen sobre regiones rectangulares de una imagen en escala de grises, permitiendo evaluar y obtener información de zonas específicas que puedan contener partes de un rostro, mediante formas geométricas asignadas para realizar operaciones matemáticas simples.

Está compuesta por tres características Haar:

- Dos rectángulos (horizontal - vertical)
- Tres rectángulos (horizontal - vertical)
- Cuatro rectángulos

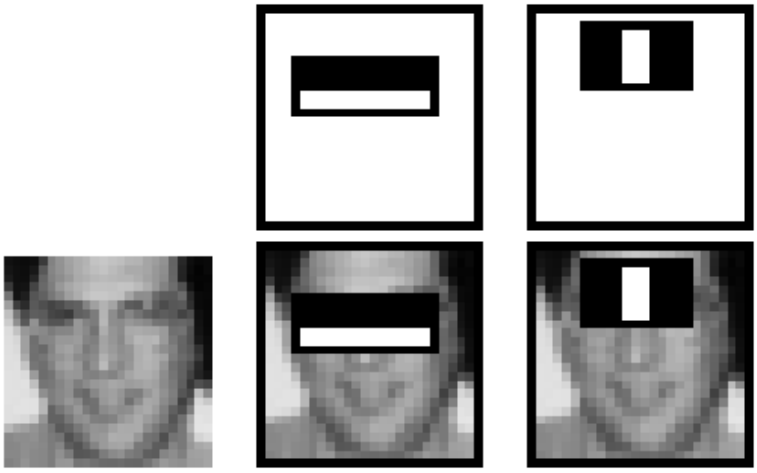
Se pueden visualizar en el Gráfico 3.

Gráfico 3: Características tipo Haar de 2, 3 y 4 rectángulos definidas por Viola y Jones. Debajo se muestran las características rotadas



Fuente: Implementación del algoritmo de detección facial de Viola-Jones

Gráfico 4: Aplicación de Características Haar a un Rostro



Fuente: (Viola & Jones, 2001)

En el Gráfico 4 se muestra dos de las características Haar aplicadas a una cara, la primera es de dos rectángulos sobrepuesta en la región de los ojos y la región superior de las mejillas, comparando la intensidad de las regiones la característica centraliza la observación en la de los ojos ya que a menudo es más oscura que la región de las mejillas. Así mismo pasa con la segunda característica aplicada que es la de tres rectángulos su intensidad se fija en la región los ojos a comparación con la región del puente de la nariz.

El valor escalar de las características Haar se lo obtiene, de la diferencia entre la suma de píxeles de rectángulos blancos de la suma de píxeles de rectángulos negros dentro de la zona asignada.

Gráfico 5: Aplicación de Característica Haar Dos Rectángulos a la Matriz Integral

200	200	100	100	200	200	100	100
250	250	50	50	250	250	50	50
255	255	255	255	100	100	100	100
255	255	255	255	100	100	100	100
200	200	100	100	200	200	100	100
250	250	50	50	250	250	50	50
255	255	255	255	100	100	200	200
255	255	255	255	100	100	250	250

Fuente: (Valveny, 2016)

El Gráfico 5 muestra una matriz de pixeles en la que se sobrepone la característica Haar de dos rectángulos, a continuación se realizará el cálculo del valor escalar.

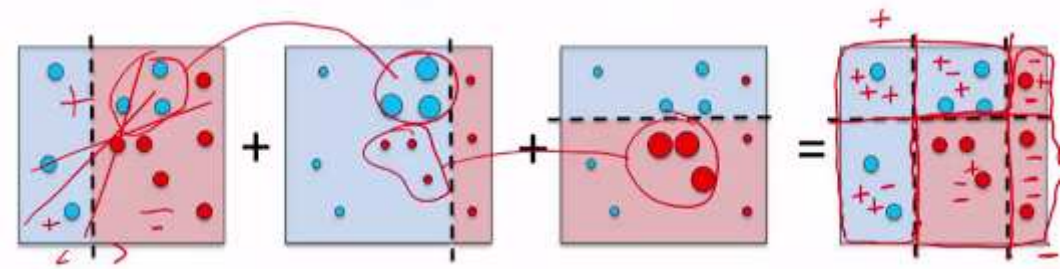
Valores de rectángulos negros: 200, 200, 250, 250
Valores de rectángulos blancos: 100, 100, 50, 50
Valor escalar: 200 + 200 + 250 + 250 + 100 + 100 + 50 + 50
Valor escalar: 550

Obteniendo un valor positivo como resultado, debido a que el rectángulo negro contiene mayor intensidad dentro de la característica, donde posiblemente se encuentre parte de un rostro.

2.5.3 Adaboost

Es un algoritmo entrenador de clasificadores que permite obtener un nuevo más robusto, que acelere la detección de rostros en la imagen. Se crea a base de la aplicación de filtros simples seleccionando las características más relevantes de una imagen para identificar zonas que contengan rostro.

Gráfico 6: Iteraciones del Algoritmo Adaboost.



Fuente: (Valveny, 2016)

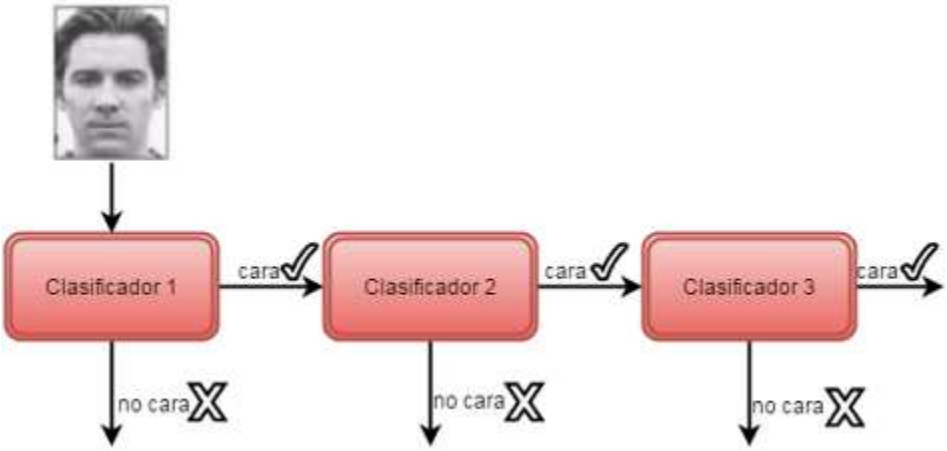
El Gráfico 6 muestra mediante 3 pasos como actúa el algoritmo de entrenamiento Adaboost. En el primer conjunto de muestras se aplica un clasificador simple basado en una sola característica, el cual separa las muestras positivas y negativas, en la siguientes aplicaciones las muestras mal clasificadas

aumentan su peso para que el próximo clasificador le dé mayor importancia; en el segundo conjunto se aplica un nuevo clasificador el cual se centra en separar aquella muestras que no se han clasificado correctamente y así mismo sucede en el tercer conjunto de muestras, habiendo identificado cuáles son las muestras positivas y cuáles son las negativas; finalmente en el último conjunto de muestras se combinan todos los clasificadores obteniendo un nuevo clasificador, determinando con la mayoría de clasificaciones positivas la zona óptima.

2.5.4 Cascada de Clasificadores

Es una aplicación secuencial de clasificadores entrenados con adaboost, una imagen será únicamente detectada como cara solo si, fue aceptada por todos los clasificadores, caso contrario si al menos un clasificador no la reconoció es automáticamente eliminada.

Gráfico 7: Funcionamiento de Clasificador de Cascadas.



Fuente: (Valveny, 2016)
Elaborado por: Los autores

Como lo expone el Gráfico 7. El objetivo de cada etapa es discriminar determinantemente los falsos positivos (imágenes sin cara), aplicando diferentes clasificadores en cada una sumando el resultado de los mismos, se descarta la imagen si este es inferior al umbral de la etapa; y así secuencialmente se

aplicara para cada una. Obteniendo una mejor efectividad de detección al haber atravesado todas las etapas.

Para finalizar se explica brevemente las etapas del algoritmo Viola-Jones.

Gráfico 8: Etapas del Algoritmo Viola-Jones

Fuente: (Viola & Jones, 2001)
Elaborado por: Los autores

- Imagen integral: Ayuda de mejor manera a computarizar los rectángulos brindando una rápida evaluación de las características, se la obtiene realizando operaciones por pixel aplicada a la imagen original.
- Características Haar: Obtiene información de una zona específica aplicando un filtro de Haar, mediante una operación aritmética obteniendo su valor mediante la resta de la suma de los rectángulos blancos de la suma de los rectángulos negros de la imagen.
- Adaboost: Algoritmo clasificador de características entre un gran conjunto de filtros simples, aplicando de mejor forma los clasificadores para una detección correcta.
- Cascada de clasificadores: Conjunto de clasificadores, cada etapa aplica un clasificador con varias características; entrenadas por el algoritmo adaboost. Se empieza a descartar las sub-imágenes que no contienen rostros desde la primera etapa y en la última etapa objetos más complejos(pelotas), obteniendo efectivamente una imagen con rostro detectado quien haya pasado por todos los clasificadores.
- Detección: Procesamiento de la imagen con la localización del rostro detectado.

2.6 Explicación de Algoritmo de Reconocimiento de Rostro Eigenfaces

Es un algoritmo matemático desarrollado en 1987, usado en sistemas de visión por computador para el reconocimiento facial, según Guillermo Ottado (2010) Eigenfaces realiza una proyección lineal del espacio de imágenes a un espacio de características de menor dimensión, esta reducción se realiza utilizando la técnica PCA(Análisis de Componente Principales) que consiste en identificar patrones principales finitos en problemas de dimensión infinita.

Para Rodríguez, (2010) el reconocimiento se realiza proyectando una nueva imagen sobre el espacio formado por las “eigenfaces”, mediante la clasificación de los componentes principales para luego comparar su posición en ese espacio con las posiciones de los individuos ya conocidos.

Además Ottado (2010) describe el método de la siguiente manera, El proceso de reconocimiento de caras consiste en tomar una imagen de dos dimensiones, a filas y b columnas, a la que se transforma en un vector unitario contenido en un espacio de imágenes n-dimensional (n = a×b). Luego se le substrae la imagen promedio y se proyecta el vector resultante en un sub-espacio de menor dimensión utilizando uno de los métodos de reducción de dimensión (extracción de características). Esta proyección es comparada con la proyección de un conjunto de imágenes de una base. La clase del vector más similar, utilizando algún criterio de similitud, es el resultado del proceso de reconocimiento.

2.7 Ordenadores de Placa Reducida

Es una computadora completa en un sólo circuito. El diseño se centra en un solo microprocesador con la RAM, E/S y todas las demás características de un computador funcional en una sola tarjeta que suele ser de tamaño reducido, y que tiene todo lo que necesita en la placa base.

2.7.1 Raspberry Pi

Raspberry es una pequeña placa con varios componentes que puede ejecutar un sistema operativo a través de una microSD, posee un hardware de bajo costo pero potente para algunos proyectos, además puede manejar varios sistemas operativos.

Raspberry Pi cuenta con varios modelos; entre ellos el más destacado es el Raspberry Pi 3 debido a su acrecentamiento en velocidad y mejoras en su modelo arquitectónico, su precio actual es de $35.00 dólares americanos.

Tabla 1: Especificaciones Técnicas Raspberry Pi 3

Especificación	Detalle
CPU	Un 1,2 GHz de 64 bits de cuatro núcleos ARMv8
GPU	Broadcom VideoCore IV 3D núcleo de gráficos, OpenGL ES 2.0, MPEG-2 y VC-1 (con licencia), 1080p30 H.264/MPEG-4 AVC3
Memoria (SDRAM)	1 GB (compartidos con la GPU)
Almacenamiento integrado	Micro SD push-pull
Conectividad Red	10/100 Ethernet (RJ-45) vía hub USB
Conectividad WIFI	802.11n Wireless LAN
Conectividad Bluetooh	Bluetooth 4.1 Classic, Bluetooth Low Energy
Entrada de video	Conector MIPI CSI que permite instalar un módulo de cámara desarrollado por la RPF.
Salidas de video	Conector RCA (PAL y NTSC), HDMI (rev1.3 y 1.4), Interfaz DSI para panel LCD.
Salidas de audio	Conector de 3.5 mm, HDMI
Puertos USB 2.0	4 puertos USB
GPIO	40 pines de cabecera
Sistemas Operativos Soportados	GNU/Linux: Debian (Raspbian), Fedora (Pidora), Arch Linux (Arch Linux ARM), Slackware Linux. RISC OS2

Fuente: Sitio web Raspberry Pi
Elaborada por: Los autores

2.7.2 Orange Pi

Es un ordenador de placa reducida de código abierto, que llegó al mercado para competir con la Raspberry Pi, es capaz de ejecutar los sistemas operativos Android, Ubuntu, Raspbian y Debian; utiliza el procesador AllWinner.

Orange Pi cuenta con algunos modelos de ordenadores el que analizaremos a continuación Orange Pi Plus 2, con un valor en el mercado de $39.00 dólares americanos.

Tabla 2: Especificaciones Técnicas Orange Pi Plus 2

Especificación	Detalle
CPU	H3 de cuatro núcleos Cortex-A7 H.265 / HEVC 4K
GPU	Mali400MP2 GPU @ 600 MHz, OpenGL ES 2.0
Memoria (SDRAM)	2 GB DDR3 (compartido con GPU)
Almacenamiento integrado	TF tarjeta (máx. 64 GB)/ranura para tarjetas MMC, hasta 2T en 2,5 disco SATA de 16 GB flash EMMC
Conectividad Red	10/100/1000M Ethernet RJ45
Conectividad WIFI	Realtek RTL8189ETV, IEEE 802.11 b / g / n
Entrada de video	CSI conector de entrada de la cámara Soporta interfaz de sensor CMOS YUV422 de 8 bits Soporta protocolo CCIR656 para NTSC y PAL Soporta sensor de píxeles de la cámara SM Soporta resolución de captura de vídeo de hasta 1080p@30fps
Salidas de video	Soporta salida HDMI con HDCP, CEC CVBS integrada Soporta salida simultánea de HDMI y CVBS
Salidas de audio	Conector de 3.5 mm, HDMI
Puertos USB 2.0	2.0 HOST, un 2.0 OTG USB Cuatro puertos USB
GPIO (1x3) pin	UART, suelo.
Sistemas Operativos Soportados	Android, Ubuntu, Debian, Raspberry Pi Image

Fuente: Sitio web Orange Pi
Elaborada por: Los autores

2.7.3 Arduino

Es una placa microcontroladora de código abierto que nació como herramienta de enseñanza para estudiantes, el cual sirve como componente de una computadora; con un entorno de desarrollo para poder programarlas en plataformas como Windows, Linux y Mac. Diseñado para aplicaciones pequeñas y sencillas desarrolladas en lenguaje de programación Processing; Arduino no puede ejecutar un sistema operativo completo.

Tabla 3: Especificaciones Técnicas Arduino UNO

Especificación	Detalle
CPU	ATMega320 de 8bits a 16 Mhz
GPU	N/A
Memoria (SRAM)	2Kb
Almacenamiento integrado	N/A
Conectividad Red	N/A
Conectividad WIFI	N/A
Conectividad Bluetooh	N/A
Entrada de video	N/A
Salidas de video	N/A
Salidas de audio	N/A
Puertos USB 2.0	1 puerto USB
GPIO	16 pines digitales
Sistemas Operativos Soportados	N/A

Fuente: Sitio web Arduino
Elaborada por: Los autores

2.8 Cámaras

La cámara es un factor esencial en el proyecto, porque es el sensor visual que capturará las imágenes de los rostros que serán almacenadas en la base de datos para luego ser reconocidas, se debe usar una cámara de cualidades medianamente aceptables, de lo cual lo más importante es la resolución de imágenes que pueda brindar este dispositivo.

Existen varios tipos de cámaras:

2.8.1 Webcam USB

Compatible con el sistema operativo de Raspberry Pi, se puede tomar fotos y grabar vídeo.

Su desventaja radica en que la calidad y capacidad de la cámara web, es inferior a la que brinda la cámara Raspberry Pi.

Tabla 4: Especificaciones Técnicas Genius FaceCam 321

Especificación	Detalle
Tipo	Cámara Web VG
Modelo	Genius FaceCam 321
Dimensiones	45 x 40 x 60 mm
Resolución:	8 MP
Resolución de imágenes:	640 x 480 píxeles
Máxima frecuencia de captura de imagen:	30 fps
Resolución de video:	640 x 480 píxeles
Conexión	USB

Fuente: Sitio web Genius
Elaborada por: Los autores

2.8.2 Camera Raspberry Pi

Desarrollada por los creadores del Raspberry Pi, es compatible con los modelos A y B de la Raspberry. Capaz de capturar imágenes en alta resolución, así como videos en alta definición; se enchufa directamente en el conector de CSI en la Raspberry Pi.

Tabla 5: Especificaciones Técnicas Cámara Raspberry Pi

Especificación	Detalle
Tipo	Cámara Módulo
Modelo	Cámara Raspberry Pi
Dimensiones	8.5 x 8.5 x 5mm
Resolución:	5 MP
Resolución de imágene:	2592 x 1944
Frecuencia captura imagen:	30 fps
Resolución de video:	1080p 30fps y 60/90 de grabación
Conexión	Cable plano de 15 pines MIPI con protocolo de interface serial de camera

Fuente: Sitio web Raspberry Pi
Elaborada por: Los autores

2.8.3 Cámara IP - Domo

Cámara de pequeño tamaño, con diseño compacto que se encuentra protegida por una carcasa de forma circular. Una de sus ventajas es su diseño, debido a este realiza vigilancia discreta, ya que dificulta distinguir hacia qué dirección apunta la cámara. Además, su carcasa circular la protegen de manipulaciones y desenfoque.

Tabla 6: Especificaciones Técnicas Camara IP Domo Hikvision DS2CD2110I

Especificación	Detalle
Tipo	Domo
Modelo	DS2CD2110I
Dimensiones	111 x 82 mm.
Resolución:	1.3 MP
Resolución de imágenes:	1280 x 960
Máxima frecuencia de captura de imagen:	30 fps
Resolución de video:	1280 x 960
Conexión	Ethernet por RJ45

Fuente: Sitio web Hikvision
Elaborada por: Los autores

CAPÍTULO III: METODOLOGÍA DE INVESTIGACIÓN

3.1 Tipo de investigación

El propósito de utilizar un tipo de investigación es guiar el estudio del proyecto, mediante un método seleccionado a obtener información relevante, que servirá de base para cumplir con el objetivo. Según lo que expone Dankhe (1986), propone cuatro tipos de estudios: exploratorios, descriptivos, correlacionales y experimentales.

Habiendo analizado los tipos de investigación antes mencionados la metodología de investigación que se emplea es la descriptiva, según Fidias G. Arias (2012), define: la investigación descriptiva consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento. Los resultados de este tipo de investigación se ubican en un nivel intermedio en cuanto a la profundidad de los conocimientos se refiere. (pág.24)

Este método de investigación permite analizar e identificar las características del suceso que estamos investigando, adicionalmente Sabino (1986) explica que, la investigación de tipo descriptiva trabaja sobre realidades de hechos, y su característica fundamental es presentar una interpretación correcta. Para la investigación descriptiva, su preocupación primordial radica en descubrir algunas características fundamentales de conjuntos homogéneos de fenómenos, utilizando criterios sistemáticos que permitan poner de manifiesto su estructura o comportamiento. De esta forma se pueden obtener las notas que caracterizan a la realidad estudiada. (pág. 51)

3.2 Enfoque Metodológico

Este proyecto utilizará el enfoque metodológico mixto (cuantitativo-cualitativo), a continuación una breve explicación:

Según el autor Fidias G. Arias (2012), enfoque cuantitativo, cuando el objetivo es recolectar datos mediante la métrica, confiando en el uso estadístico para conocer y medir los patrones de comportamiento en una población en base a la aplicación de cuestionarios y encuestas.

De la misma manera el autor Fidias G. Arias (2012) se refiere al enfoque cualitativo, que está basado en utilizar la recolección de datos sin medición numérica tales como las entrevistas en profundidad, donde se identifican categorías o grupos de conceptos relevantes para la investigación, con la finalidad de comprender, interpretar, reconstruir y reflexionar acerca de las experiencias e historias de los informantes.

En cuanto a lo que se refiere a enfoque mixto según Tashakkori y Teddlie (2003), este es un proceso que recolecta, analiza y relaciona datos cuantitativos y cualitativos integrados en un mismo estudio, en una serie de investigaciones para responder a un planteamiento del problema, o para preguntas de investigación, obteniendo mejores resultados para la investigación.

3.3 Población y Muestra

De acuerdo a Levin & Rubin (1999), una población “es el conjunto de todos los elementos que se estudian y acerca de los cuales se intenta sacar conclusiones”. El concepto de población en estadística, se precisa como un conjunto finito o infinito de personas u objetos que presentan características comunes. (pág. 135). Para esta investigación, se establece como población el personal administrativo, autoridades y profesores tiempo completo; que laboran en el área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil para recolectar los datos necesarios.

Según Fidias G. Arias (2012) la muestra es un subconjunto representativo y finito que se extrae de la población accesible. Para este proyecto se toma como muestra a un grupo seleccionado aleatoriamente de personas de la población objetivo, según el instrumento que se aplique. Se detalla la muestra a continuación:

- Para la Encuesta, la muestra fue 15 personas.
- Para la Entrevista, la muestra fue 2 personas.

3.4 Instrumentos

Métodos, técnicas o herramientas mediante las cuales recolectamos la información necesaria, para luego ser analizada. Para este proyecto se utilizara los siguientes instrumentos:

Encuesta

Cuestionario de preguntas cerradas, diseñado para el personal administrativo, autoridades y profesores a tiempo completo seleccionados aleatoriamente; con el objetivo de investigar e identificar la importancia de la existencia de un control de seguridad en el área administrativa, para mantenerse en un ambiente laboral seguro. El formato de la encuesta se encuentra en la sección de Anexos como Anexo 1.

Entrevista

Con el objetivo de que el entrevistador obtenga la información requerida en base al tema planteado se inicia un diálogo guiado con preguntas abiertas. La entrevista fue dirigida a la Ing. Beatriz Guerrero (Directora de la Carrera) y a la Ing. Lorgia Valencia (Profesora Tiempo completo) de la Carrera de Ingeniería en Sistemas Computacionales de la Facultad de Ingeniería. El formato de la entrevista se encuentra en la sección de Anexos como Anexo 2.

Observación

Técnica, la cual se basa en la visualización directa de las situaciones que se presentan en el espacio delimitado (Área Administrativa), en función del siguiente

objetivo: verificar el proceso de adecuación y adaptación del equipo biométrico de reconocimiento facial en el Área Administrativa de la Facultad de Ingeniería. Así como de las diferentes pruebas realizadas.

3.5 Procesamiento y Análisis de resultados

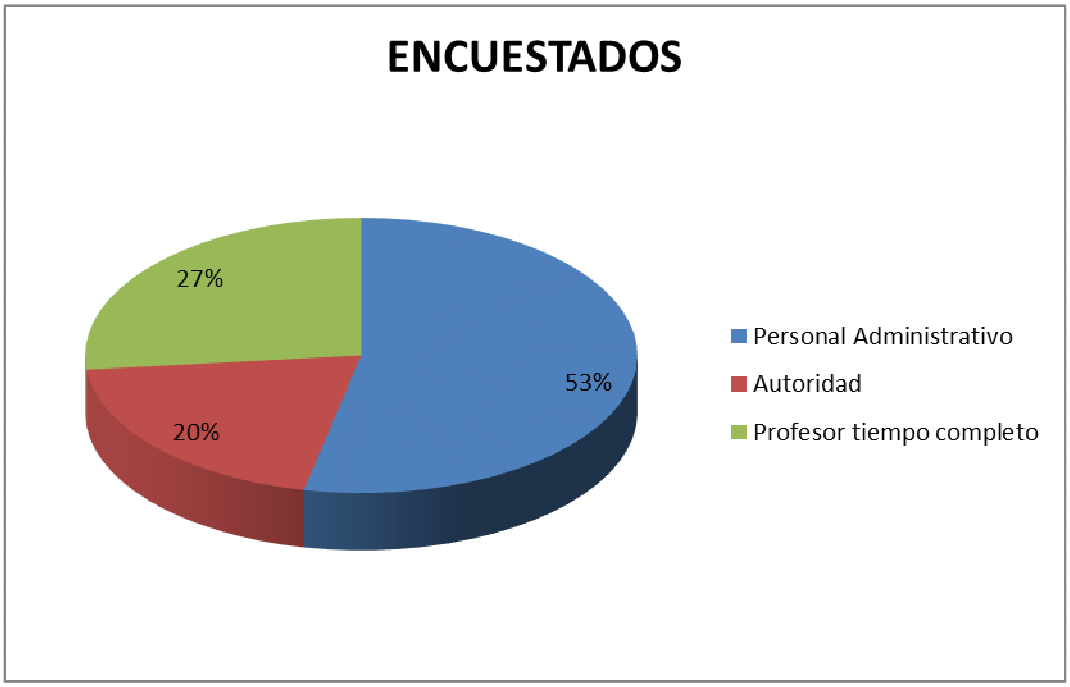
Aplicados los instrumentos de recolección de datos, se obtuvo el siguiente análisis.

Encuesta

La pregunta 1 describe, que de las personas que laboran en el Área Administrativa de la Facultad de Ingeniería de la UCSG, el 53% de las personas encuestadas fueron personal administrativo, un 27% profesores tiempo completo y un 20% concerniente a las autoridades.

1. Persona encuestada

Gráfico 9: Encuesta - Pregunta 1

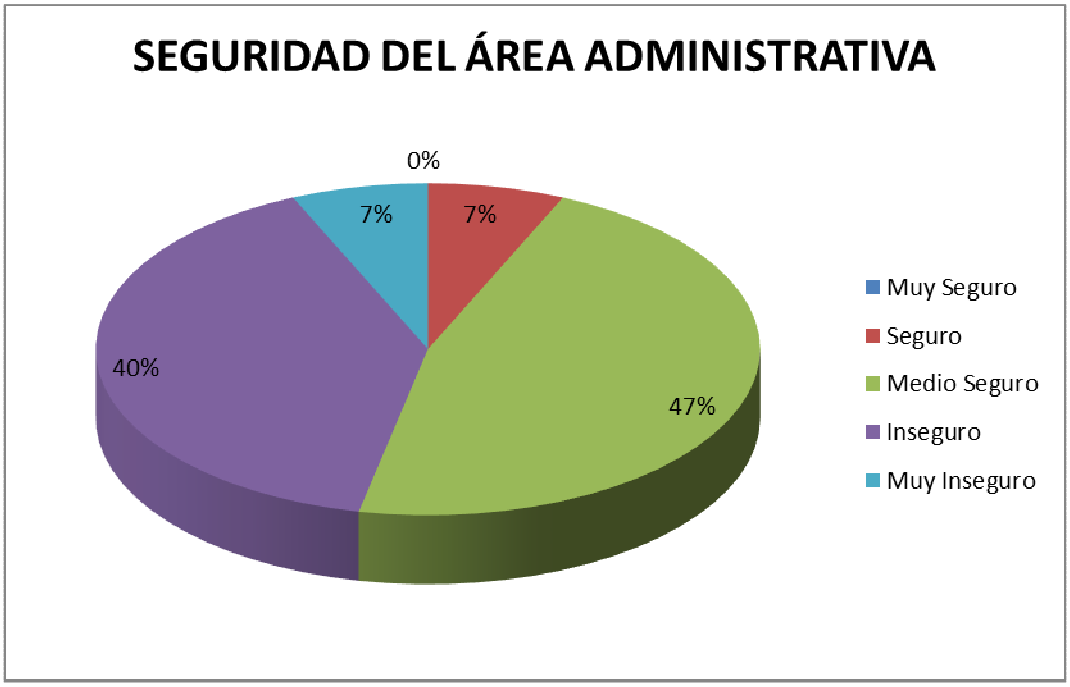


Elaborada por: Los autores

La pregunta 2, determinando un cierto grado de preocupación entre los encuestados, indica, un 47% de las personas encuestadas aseguran que el Área Administrativa es medio seguro, el 40% se sienten inseguros, un 7% muy inseguro y otro 7% seguro, ninguno de los encuestados manifiestan un grado de total seguridad.

2. **¿Qué tan seguro cree usted que es el Área de Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil?**

Gráfico 10: Encuesta - Pregunta 2

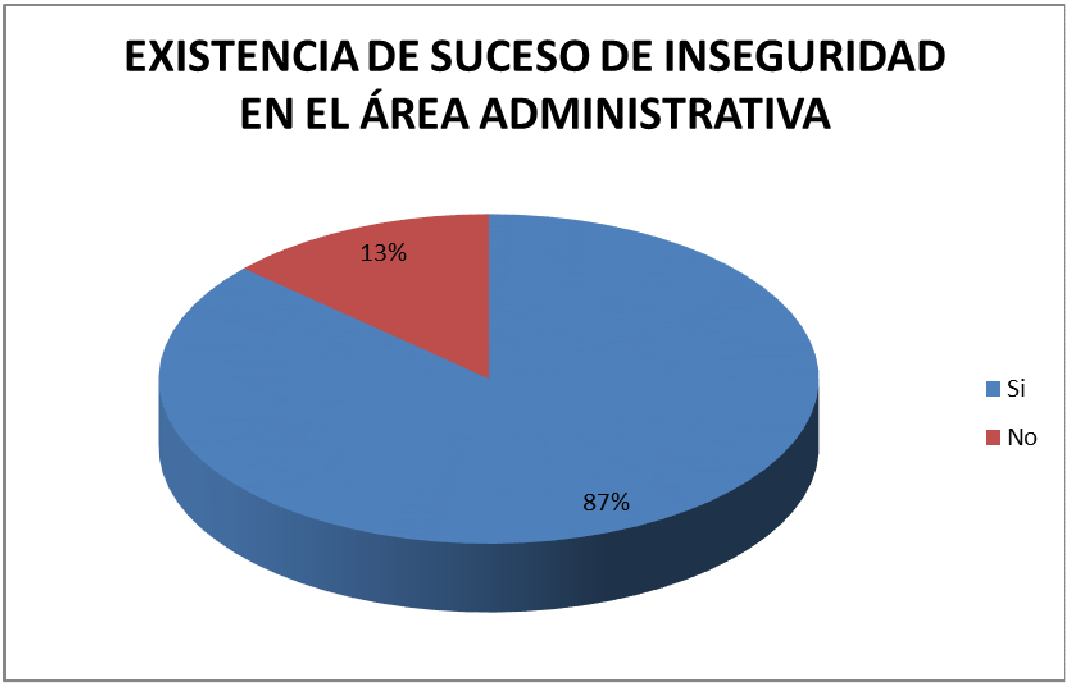


Elaborada por: Los autores

La pregunta 3 muestra, que ha existido algún suceso de inseguridad en el Área Administrativa confirmándolo con un Si un 87% de las personas encuestadas y el 13% restante indica que No.

3. **¿Ha sucedido algún suceso de inseguridad en el área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil?**

Gráfico 11: Encuesta - Pregunta 3

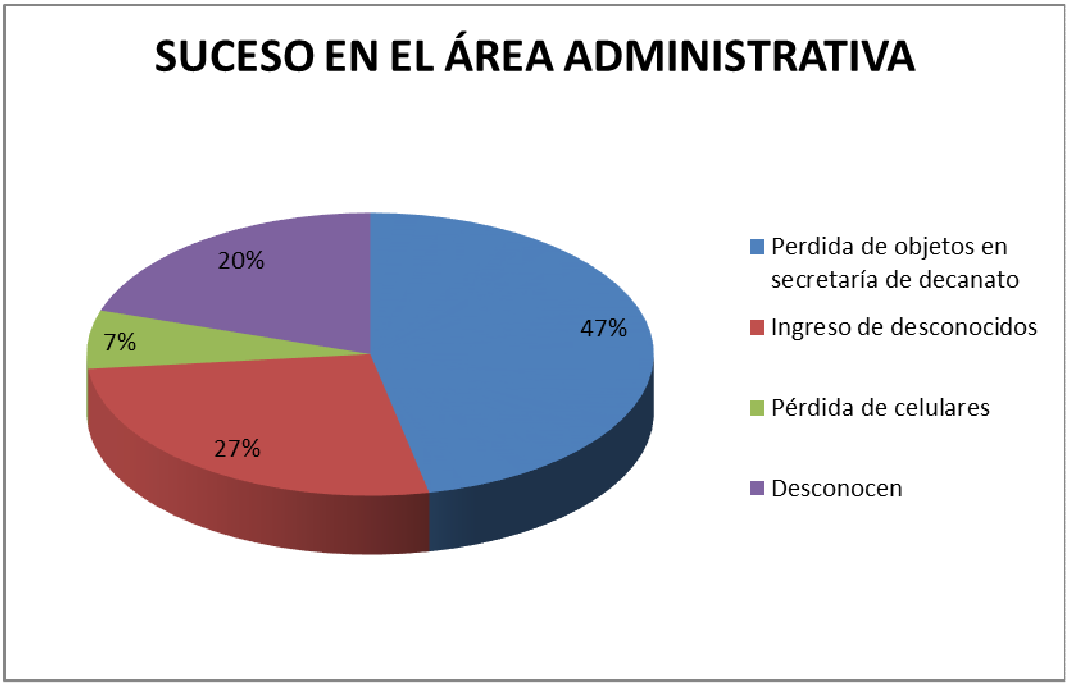


Elaborada por: Los autores

La pregunta 4 respalda a la pregunta 3, sustentando que un 47% de los encuestados indicaron que han existido perdidas de objetos en Secretaria de Decanato del Área Administrativa, un 27% asegura que personas desconocidas ingresan al Área, un 20% desconoce de algún suceso y el 7% notifica perdida de celulares.

4. Si su respuesta anterior fue si, ¿Cuál fue el suceso que ocurrió?

Gráfico 12: Encuesta - Pregunta 4

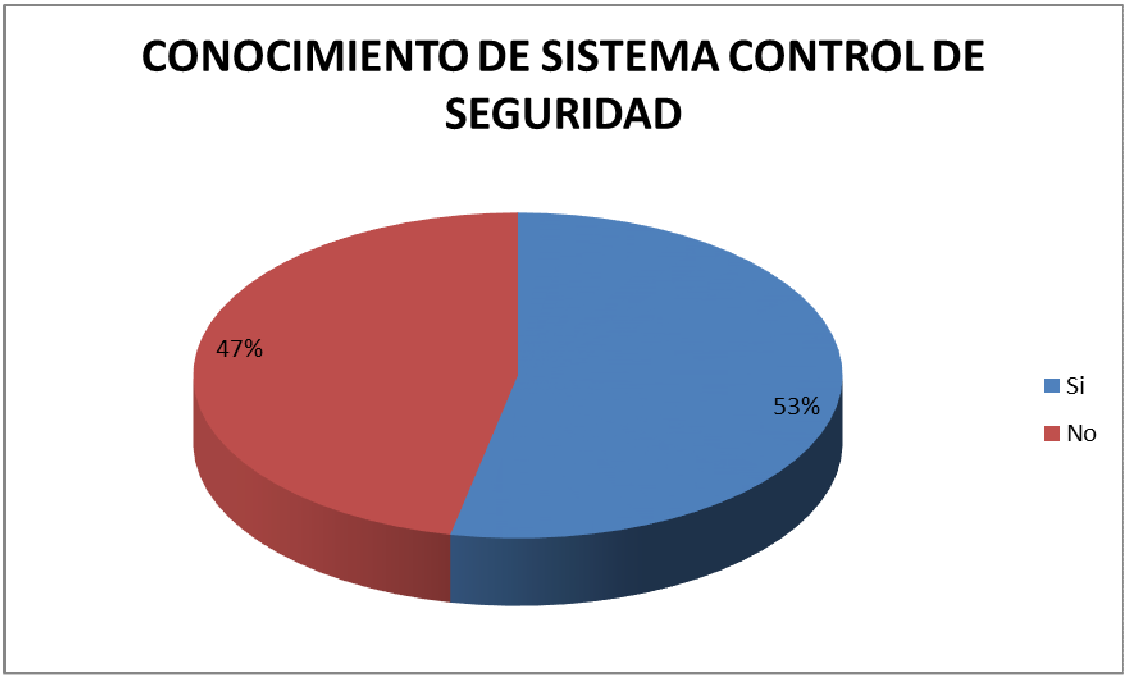


Elaborada por: Los autores

La pregunta 5 determina que, el 53% de las personas encuestadas tienen conocimiento de algún sistema de control de seguridad.

5. **¿Conoce usted de algún sistema de control de seguridad existente en el Área Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil?**

Gráfico 13: Encuesta - Pregunta 5

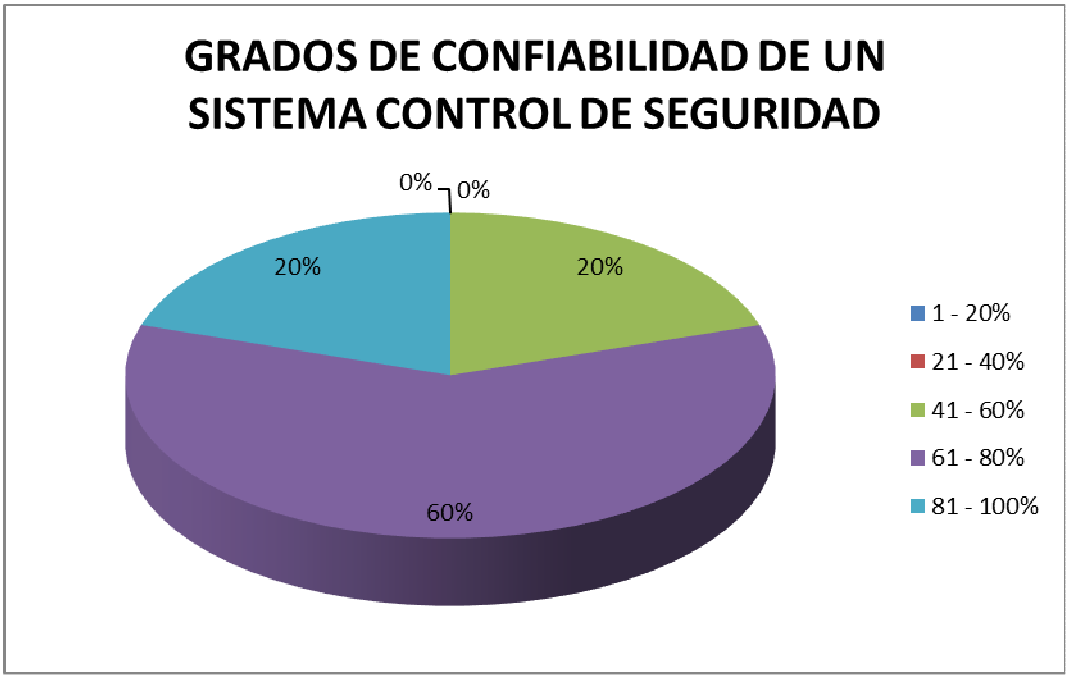


Elaborada por: Los autores

La pregunta 6 determina que, hay un alto grado de confiabilidad por parte de los encuestados hacia la existencia de un sistema control de seguridad implementado en el Área Administrativa.

6. **¿Cuál es su grado de confiabilidad ante un sistema de control de seguridad biométrico de reconocimiento facial?**

Gráfico 14: Encuesta - Pregunta 6

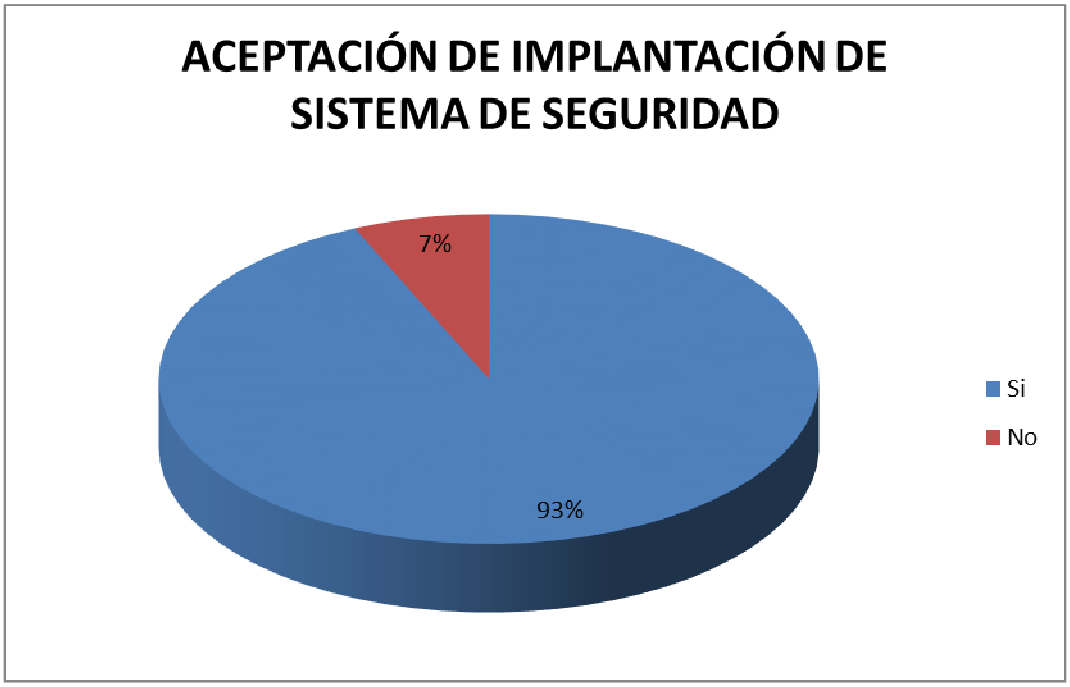


Elaborada por: Los autores

La pregunta 7 demuestra que, un 93% del personal que labora en el Área administrativa está de acuerdo en la implantación de un sistema de control por medio de un sistema de seguridad biométrico de reconocimiento facial mediante un dispositivo de cámara, el cual actuaria de sensor capturando imágenes de las personas asistentes al lugar.

7. **¿Estaría de acuerdo en ser vigilado por un dispositivo (cámara) a la entrada y salida del Área Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil?**

Gráfico 15: Encuesta - Pregunta 7

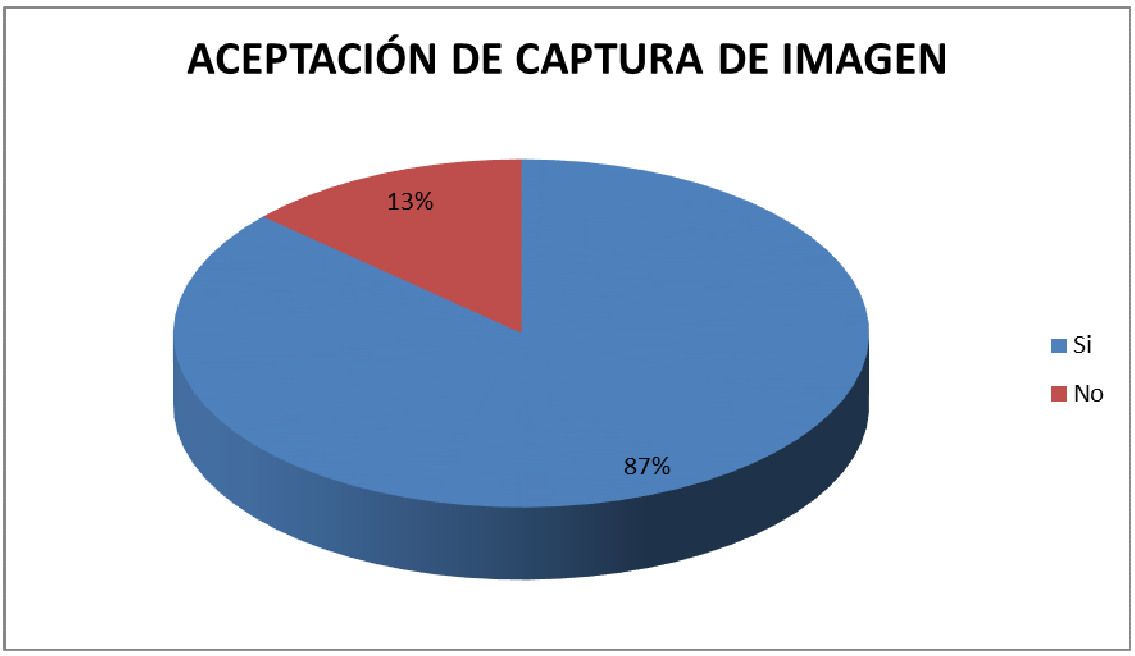


Elaborada por: Los autores

La pregunta 8 confirma, con un 87%, que el personal del Área Administrativa autoriza a la captura de la imagen de su rostro, para que mediante el sistema de control de seguridad biométrico de reconocimiento facial se ratifique que es personal del Área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil, incluyéndola así en la base de datos y brindar ágiles resultados en la comparación con rostros de personas ajenas a esta área.

8. **¿Estaría de acuerdo en que se capture su rostro por un dispositivo (cámara) para comprobar si usted es un rostro reconocido por el sistema de control de seguridad?**

Gráfico 16: Encuesta - Pregunta 8



Elaborada por: Los autores

En la encuesta se pudo comprobar que el personal que labora en el Área Administrativa se siente algo inseguro debido a los diferentes acontecimientos hasta hoy ocurridos, su grado de confiabilidad ante un sistema de control de seguridad es un punto favorable y aceptable para el proyecto, la mayoría está dispuesta a cooperar para así obtener un ambiente laboral seguro.

Entrevista

Directora de Carrera de Ingeniería en Sistemas Computacionales

En la entrevista realizada a la Directora de Carrera pudimos conocer que el actual sistema de seguridad que posee el Área Administrativa de la Facultad de Ingeniería es, un control de video-vigilancia compuesto por cámaras ubicadas cerca oficina de Decanato, de llegar a suceder algún acontecimiento de inseguridad, se desconoce cuál sería el proceso a seguir. También se identificó que el espacio más sensible y accesible del área es desde la puerta de ingreso hacia el pasillo principal; tiene conocimiento de un sistema de seguridad como el de control con huella digital; y está definitivamente convencida que un sistema de control de seguridad automatizado brindaría mayor seguridad si se ubicase en el lugar sensible del Área Administrativa.

Profesor Tiempo Completo

La profesora a tiempo completo comentó que, entre los sistemas de seguridad existentes en el Área Administrativa tiene conocimiento de la guardianía y el sistema de cámaras de video-vigilancia, confirma al igual que en la entrevista anterior del desconocimiento de un proceso a seguir en el caso de que ocurriese algún suceso de inseguridad, además conoce de otro sistema de seguridad como el de tarjetas magnéticas de apertura de puertas, confía que un sistema de control de seguridad automatizado daría mayor seguridad en el área para el personal laboral y cree que la mejor ubicación es el pasillo principal del Área Administrativa, el mismo que es accesible por personas ajenas al área.

Observación

La observación realizada a las implementaciones de prueba del dispositivo biométrico nos ayudó a optimizar la detección de rostros, con la menor cantidad de falsos positivos (detecciones sin caras), también nos permitió optimizar tiempo de detección, procesamiento y reconocimiento debido a la implementación de multi-hilos en la aplicación. En el Anexo 4 se explica cómo se efectuó el instrumento de la observación.

CAPíTULO IV: PROPUESTA

4.1 Viabilidad Técnica

Los recursos que se utilizarán para la creación de este proyecto serán detallados a continuación:

Recursos de Hardware:

- Raspberry Pi 2 B o modelo superior
- Cámara Raspberry Pi 5MP

Recursos de Software:

- Java
  - ZK Framework 2.0.1
  - Maven 1.5.1
  - OpenCV 3.0
  - HIbernate (ORM) 4.0
  - Máquina Virtual Java 1.8 o superior para Raspberry Pi
- Base de Datos MySql 5.1
- Servidor web (Tomcat)

Recursos Externos:

- Api Dropbox (almacenamiento en la nube)
- Api Kairos (algoritmo de reconocimiento de rostros)

4.1.1 Descripciones del Hardware

4.1.1.1 Raspberry Pi 2 B

Para este proyecto utilizamos esta placa reducida la cual ofrece características similares a las de un PC siendo un microprocesador. Permite instalar y ejecutar aplicaciones brindando agilidad en los procesos internos del aplicativo en base a su procesador de cuatro núcleos; se puede acceder a su interface de red para la conexión a internet mediante la cual se envían los datos al aplicativo, se puede interactuar directamente con su sistema operativo Raspbian, su tamaño beneficia a la portabilidad relacionado a la constante reubicación del dispositivo, su bajo consumo de energía de 2.5watts y bajo costo ayuda a que sea un dispositivo eficiente y rentable económicamente, sin dejar de lado que es un dispositivo que lleva bastante tiempo en el mercado lo que ayuda a que su comunidad esté bien asentada y provea información veraz del uso y sus aplicaciones.

4.1.1.2 Cámara Raspberry Pi

Según el estudio respecto a las cámaras especificadas anteriormente en el número 3.4 se escoge este dispositivo debido a sus características principales tales como: funcionalidad estable para con el aplicativo, captar imágenes de rostros aún con baja iluminación, la accesibilidad a la manipulación de sus componentes como la resolución de la imagen y calibración del lente de la cámara; aprovechando de mejor manera sus características para la detección de la imagen, este dispositivo permite utilizar su mayor resolución de (2592 x 1944 píxeles) lo cual beneficia al proyecto por la alta calidad de la imagen. Además de tener una mayor compatibilidad con el microprocesador es un *plus*, debido a que ambos pertenecen a la misma compañía.

4.1.2 Descripciones del Software

4.1.2.1 Lenguaje de Programación

Para el desarrollo de este proyecto se utiliza el lenguaje Java, es un lenguaje fuertemente tipado lo que determina su programación de alto nivel, con propósito general y orientado a objetos; incluye la recolección automática de memoria (garbage collector), necesita ser compilado una sola vez para ser ejecutado desde cualquier plataforma que posea Máquina Virtual de Java JVM.

Componentes utilizados para el desarrollo de la aplicación en JAVA:

- *ZK Framework*

  Es un *framework* de código abierto basado en AJAX, utilizado para la creación de las interfaces con las que el usuario interactúa en la aplicación; simplifica los métodos y llamadas al sistema en las aplicaciones web, debido al fácil desarrollo de lenguaje de programación en xml.

- *Maven*

  Es un componente de JAVA, utiliza una estructura xml la cual permite declarar las dependencias que usará el proyecto de forma ágil, dentro de su archivo pom.xml (Proyecto de Modelo de Objetos).

- *OpenCV*

  Es una librería de visión por computadora desarrollada en C++, se puede acceder a sus múltiples métodos especificados a continuación mediante sus interfaces creadas para varios lenguajes de programación entre ellos JAVA, es compatible con sistemas operativos como Linux, Windows y Mac. Módulos suministrados por OpenCV:

  - **Core**

    Contiene varios objetos que construyen la funcionalidad básica de OpenCV, entre los cuales utilizamos:

- mat.class.- convierte la imagen en un objeto Mat
- matofrect.class.- contenedor de la clase Rect, permite trabajar con rectángulos sobre la imagen.
- point.class.- permite escribir sobre la imagen detectada.

- **Imgproc**

  Permite el procesamiento de imágenes, recibiendo como parámetro el objeto Mat detectado.

- **Imgcodecs**

  Permite leer y escribir un objeto Mat de un archivo.

  Codifica la imagen a tipo jpg, png y bmp.

- **Videoio**

  Este módulo posee el objeto videocapture.class el cual permite abrir la cámara del dispositivo y por medio del objeto videoio.class se puede setear la resolución de la cámara.

- **Objdetect**

  Mediante la clase CascadaClassifier.class la cual contiene algoritmos entrenados generados en archivos .xml, para la detección de objetos.
  Este proyecto implementa el algoritmo de detección facial y de ojos, a continuación el detalle.

  Para la detección facial podemos usar los siguientes métodos de cascada Haar:

  - Frontalface_default.xml: La información del archivo se puede extraer de su propia cabecera. Utiliza el algoritmo Adaboost con imágenes de 24x24 y obteniendo 25 etapas en el detector.
  - Frontalface_alt2.xml: Utilizando el algoritmo Gentle Adaboost, que minimiza la función exponencial de pérdidas de Adaboost.

  Entre los dos métodos mencionados el último es el más eficiente, aunque sus imágenes de entrenamiento son de 20x20 píxeles y las etapas utilizadas son 20.

Para la detección de ojos existe un único método de cascada Haar

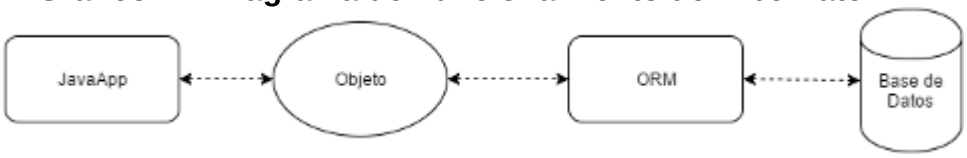
- haarcascade_eye.xml, detecta ojos de un rostro de un objeto Mat.

- *Hibernate (ORM) 4.0*

  Es una herramienta de mapeo objeto/relacional desarrollada para la plataforma JAVA. Hibernate utiliza un lenguaje de consulta potente (HQL) muy parecido a SQL. HQL es completamente orientado a objetos y comprende nociones como herencia, polimorfismo y asociación.

  Proporciona una capa más de seguridad hacia la base de datos.

Gráfico 17: Diagrama de Funcionamiento de Hibernate



Elaborado por: Los autores

- *Máquina Virtual Java*

  Es una herramienta proveniente de Oracle System Foundation. Permite interpretar las aplicaciones desarrolladas en JAVA, trabaja una capa más arriba del Hardware descifrando los bytecode. El proyecto utiliza la máquina virtual versión 1.8 ubicada entre las más actuales y es instalada en el microcontrolador.

4.1.2.2 Base de Datos MySql

Esta base de datos es de licenciamiento gratuito, su instalación es fácil y ligera sin dejar de ofrecernos todas sus características a pesar de su gratuidad.

Tabla 7: Comparación de Bases d Datos

Base de Datos	Ventajas	Desventajas
MySql	▪ Mayor velocidad. ▪ Uso de menos recursos de CPU y memoria.	▪ No soporta transacciones roll-backs. ▪ No considera claves referenciales.
PostgreSQL	▪ Licenciamiento BSD. ▪ Soporta transacciones referenciales. ▪ Por su arquitectura de diseño, soporta escalabilidad.	▪ Consumo mayor de recursos de CPU y memoria. ▪ Es más lenta que MySql al interactuar con las consultas.

Elaborada por: Los autores

Al hacer la comparación entre las dos bases de datos, escogemos a MySql por su velocidad y su menor uso de recursos, adicional su buena combinación con el servidor web Apache hace que esta nos brinde mayor estabilidad.

4.1.2.3 Servidor Web

Utilizamos como servidor web el Apache Tomcat, ya que es de código abierto y fue desarrollado por los miembros de Apache Software Foundation, es un contenedor de servlets basado en el lenguaje JAVA, el cual es complementario a las aplicaciones desarrolladas en JAVA a nuestro sistema.

4.1.3 Descripciones de Recursos Externos

4.1.3.1 API Dropbox

Para abaratar costos se ha decidido usar un servidor de almacenamiento de imágenes en la nube, a continuación detallamos las especificaciones de las comúnmente utilizadas

Tabla 8: Comparación de Recursos Externos

Herramienta de Almacenamiento	Ventajas	Desventajas
Dropbox	▪ Mayor velocidad de transferencia. ▪ Menor complejidad. ▪ Seguridad en los archivos. ▪ Trabaja con un sistema de archivo.	▪ Menor almacenamiento gratuito.
Google Drive	▪ Mayor almacenamiento gratuito. ▪ Mayor documentación.	▪ Menor velocidad de transferencia. ▪ Mayor complejidad. ▪ Trabaja con los ID de los archivos.

Elaborada por: Los autores

API Dropbox es el servidor de almacenamiento de imágenes en la nube que se ha seleccionado para este proyecto, debido a su facilidad de interacción, ser fiable y a su librería con amplios componentes que nos permite conectarnos a su servicio desde el aplicativo. El detalle de su costo:

Tabla 9: Especificaciones de API Dropbox

Características	Para personas	Para equipos	
Plan	Pro	Business	Enterprise
Valor Mensual	US$8,25	US$12,50 /usuario	Para conocer los precios, comunícate con Dropbox
Almacenamiento	1 TB	Todo el espacio que necesites	Todo el espacio que necesites

Fuente: Sitio Web Dropbox
Elaborada por: Los autores

4.1.3.2 API Kairos

Se utiliza Kairos como servicio de reconocimiento facial, el cual necesita previamente el enrolamiento mínimo de un rostro en una imagen formato jpg o png para ser inscritos en una galería, para cuando se requiere del reconocimiento se vuelve a enviar otra imagen la cual se verificará si coincide con las imágenes registradas en la galería. El detalle de su costo:

Tabla 10: Especificaciones Costo/Beneficio API Kairos

Características	**Detalle**			
Plan	Trial	Starter	Growth	Pro
Valor Mensual	US$ 0,00	US$149,00	US$449,00	US$1499,00
Llamadas API	5.000	10.000	100.000	500.000

Fuente: Sitio Web Kairos
Elaborado por: Los autores

4.2 Viabilidad Económica

A continuación se detallan el costo de las herramientas implementadas para el proyecto Control de Seguridad Biométrico de Reconocimiento Facial como Caso de Estudio Implementación en La Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil.

Tabla 11: Materiales proporcionados por la Facultad de Ingeniería

Detalle	**Precio**
Punto eléctrico para Raspberry Pi	$0,00
Punto de Red para Raspberry Pi	$0,00

Elaborado por: Los autores

Estos materiales e instalación fueron facilitados al Centro de Investigación y Desarrollado Tecnológico CIDT de la Facultad de Ingeniería.

Tabla 12: Materiales Usados para Ambiente de Desarrollo

Cantidad	Detalle	Valor Unitario	Valor Total
2	Microcontrolador Raspberry Pi 3 Modelo B	$35,99	$71,98
2	Cámara Raspberry Pi	$14.99	$29.98
1	Cámara USB	$20.00	$20.00
1	Cámara IP Domo Hikvision DS2CD2110I	$83.65	$83.65
1	Estante de madera	$30.00	$30.00
1	Cable HDMI a VGA	$20.00	$20.00
1	Servidor Core Dos Duo - Alojamiento de servicios del sistema	Gratis	Gratis
1	Servicio API Kairos - Reconocimiento Facial	Gratis	Gratis
1	Servicio Dropbox - Almacenamiento en la Nube	Gratis	Gratis
TOTAL			**$255.61**

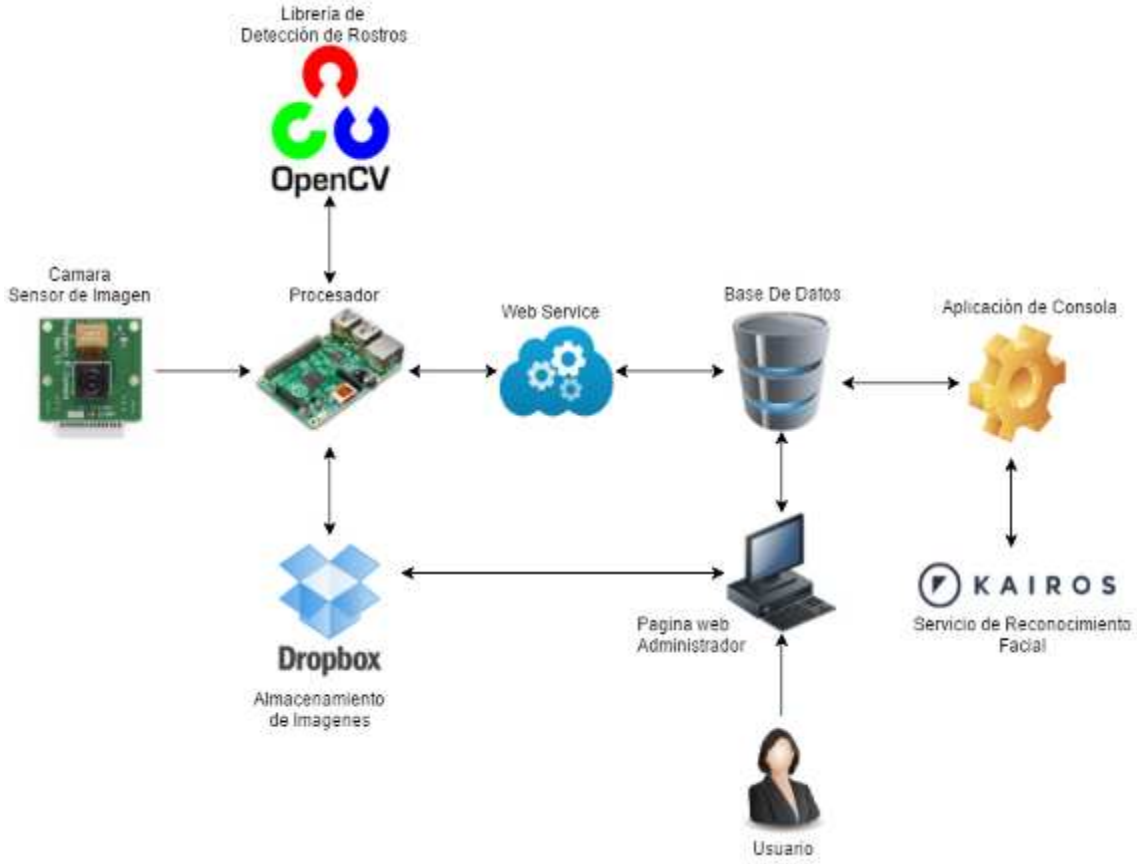
Elaborado por: Los autores

La información de la tabla 12 muestra el detalle de herramientas adquiridas para el desarrollo del proyecto con sus respectivos valores tanto por unidad y valor total, algunas herramientas fueron adquiridas en el extranjero y otras nacionalmente; el valor total demuestra que es un valor accesible para la Facultad de Ingeniería en cuanto se trata de mantener resguardada la seguridad de su personal administrativo.

CAPITULO V: DISEÑO PROPUESTA TECNOLÓGICA

5.1 Diseño de Arquitectura del Sistema

Gráfico 18: Arquitectura del Sistema Propuesto



Elaborado por: Los autores

Etapas de Funcionamiento

- Etapa de Captura

  La Cámara Raspberry Pi es el sensor de imágenes, la cual captura los frames y los almacena en la memoria ram del dispositivo Raspberry Pi.

- Etapa de Detección

  En el sistema se integra la librería OpenCV, la cual toma los *frame*s (cuadros de imagen) almacenados y aplica las características Haar filtrando las imágenes que contengan rostro(s).

- Etapa de Almacenamiento en la Nube

Las imágenes con rostro(s) serán enviadas a la API Dropbox para generar las URLs públicas para el sistema.

- Etapa de Procesamiento

  Las URLs devueltas al sistema por la API de Dropbox son enviadas por lotes al Web Service, el cual registrará las mismas en la base de datos convirtiéndolas en transacciones pendientes.

- Etapa de Consumo Servicio Kairos

  La aplicación de consola detectará las nuevas transacciones depositadas en la base de datos y serán enviadas al API Kairos, para su posterior enrolamiento o reconocimiento de un rostro.

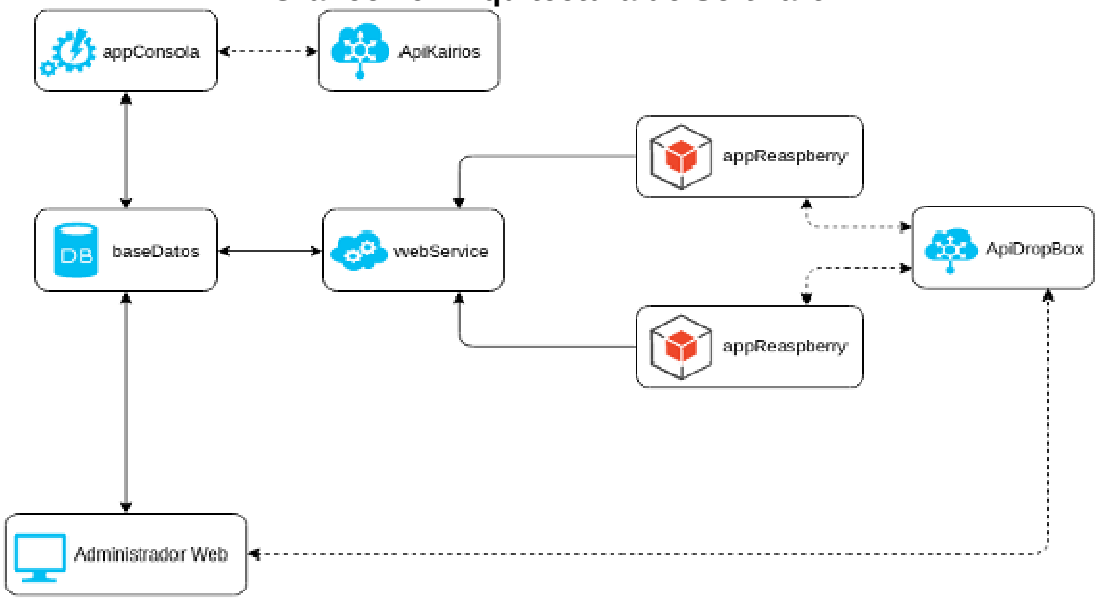
- Etapa de Administración

  El usuario podrá acceder al administrador web donde realizará consultas de los rostros reconocidos y no reconocidos; y además registrará a las personas pertenecientes al Área Administrativa de la facultad.

5.2 Diseño de Arquitectura de Software

El siguiente gráfico muestra la arquitectura de software del sistema propuesto.

Gráfico 19: Arquitectura de Software



Elaborado por: Los autores

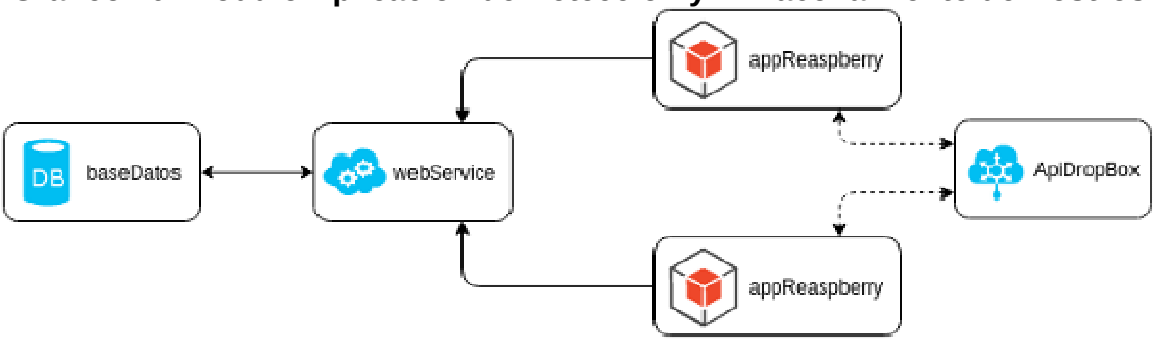
El proyecto se lo dividió en los siguientes módulos:

- Módulo 1 - Aplicación de Detección y Almacenamiento de Rostros
- Módulo 2 - Aplicación de Consola
- Módulo 3 - Administrador Web

5.2.1 Módulo 1 – Aplicación de Detección y Almacenamiento de Rostros

El módulo se encarga de la detección de caras capturadas por la cámara Raspberry Pi, mediante la aplicación instalada en los dispositivos Raspberry Pi 2 b, para luego ser enviadas al servidor de almacenamiento de imagen en la nube Dropbox. Este nos retorna la URL de la imagen almacenada; la cual es enviada al web service para su posterior almacenamiento en la base de datos del sistema.

Gráfico 20: Módulo Aplicación de Detección y Almacenamiento de Rostros



Elaborado por: Los autores

AppRaspberry(faceraspv0_1)

Detecta los rostros, almacena la imagen en el API Dropbox para luego enviar URL de las imágenes al web service para su posterior almacenamiento en la base de datos.

La aplicación está desarrollada con la siguiente estructura:

Paquetes:

- **faceraspv0_1.main**: contiene el Main.java de la aplicación.

- **faceraspv0_1.queue**: la aplicación maneja cuatro colas en RAM, cada cola maneja un cerrojo mutex (lock) con su respectiva variable de condición (condition) para proteger la cola y no ser consumida al mismo tiempo por varias instancias del sistema:

  ```
  private Lock lock = new ReentrantLock();
  private Condition noLlena = lock.newCondition();
  private Condition noVacia = lock.newCondition();
  ```

  Las colas utilizadas en el aplicativo manejan el tipo de despacho FIFO:

  - **FaceQueue.java**, esta cola de tipo Mat recibe las imágenes capturadas por la cámara.
  - **ImgAptasQueue.java**, la cola de tipo Mat contendrá las imágenes que evaluadas por los filtros detecten por lo menos un rostro y dos ojos.
  - **PathQueue.java**, encola las direcciones de las imágenes que se guardan temporalmente para ser enviadas a Dropbox.
  - **ApiQueue.java**, esta cola contendrá la URL que se genera después de haber subido la imagen a Dropbox.

- **faceraspv0_1.thread**: la aplicación es multihilos. Ejecuta cinco hilos simultáneamente para agilizar el procesamiento del sistema. Los hilos usados son:

  - **PrFaceThread.java**, hilo productor se encarga de leer las imágenes enviadas desde la cámara y colocarlas en la cola FaceQueue.java
  - **CoPrFiltroFaceThread.java**, hilo consumidor y productor, su función es consumir de la cola FaceQueue.java los objetos tipo Mat y evaluar si encuentra rostros y ojos para agregarla a la cola(productor) ImgAptasQueue.java, en caso de cumplir las condiciones.
  - **CoPrImgAptasThread.java**, hilo consumidor y productor encargado de remover de la cola(consumidor)

ImgAptasQueue.java las imágenes y guardar las en una ruta física del dispositivo, esta ruta será agregada a la cola(productor) PathQueue.java para su posterior despacho.

- **CoDropboxThread.java**, hilo consumidor y productor obtiene las rutas de las imágenes de la cola(consumidor) PathQueue.java para enviarlas a Dropbox, agregando a la cola(productor) ApiQueue.java la URL de la imagen que se subió y eliminando físicamente la imagen anteriormente almacenada.
- **CoApiThread.java**, hilo consumidor que se encarga de obtener las URL de la cola ApiQueue.java para enviarlas al web service del aplicativo en formato JSON.

- **faceraspv0_1.util**: almacenará clases útiles para el sistema tales como Util.java, que contiene métodos para validar si existe conexión a internet en el aplicativo.

WebService(webservicefacev0_1)

El sistema cuenta con un web service REST, para recibir las peticiones POST de los dispositivos que tengan instalados el aplicativo **faceraspv0_1**.

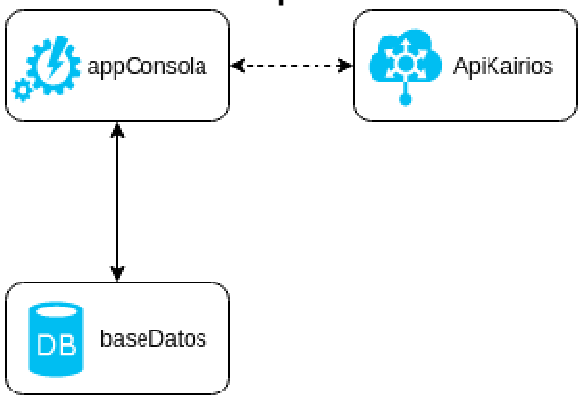
El servicio se encuentra estructurado de la siguiente forma, teniendo en cuenta las siguientes capas:

- Modelos, donde se encuentran las tablas de la base mapeadas.
- DAO(data Access object), las sentencias que hibernate interpretará para comunicarse con la base de datos.
- Service, la capa de servicio donde se encontraran referenciados los métodos de su respectivo DAO.
- Controller, el que realiza la respectiva conexión de las clases entre el modelo y el servicio.

5.2.2 Módulo 2 – Aplicación de Consola

En esta sección la aplicación por consola se encarga de los procesos internos del sistema, consultar todos aquellos registros en la base de datos, para armar las peticiones que se enviaran al servicio de reconocimiento de Kairos, almacenando la respuesta de estas peticiones.

Gráfico 21: Módulo - Aplicación de Consola



Elaborado por: Los autores

AppConsola(consolaface)

Esta aplicación usa hibernate para la conexión de la base de datos y maven para las dependencias del proyecto. Sigue el mismo estándar en los demás módulos, sus capas son:

- Dato de Acceso al Objeto DAO
- Servicios
- Modelos

Partimos de los objetos modelos para generar los DAO y los respectivos servicios.

La aplicación posee la siguiente estructura:

El paquete **consoleface.dao** contiene todas las clases DAO (Data Access Object) del sistema. Estas realizan todas las operaciones transaccionales con la base de datos de los objetos modelos antes mapeados (tablas), tales como: select, insert y update utilizando sentencias de hibernate.

- TransaccionDao.java
- TransaccionInputDao.java
- TransaccionOutputDao.java
- ReconocidoDao.java
- ApiKeyKairosDao.java

El paquete **consoleface.main**, se encuentra la clase main.java.

El paquete **consoleface.model** contiene los objetos modelos de la aplicación, las tablas mapeadas a la base de datos. Se tienen los siguientes objetos:

- ApiKeyKairos.java
- App.java
- PassApp.java
- Reconocido.java
- Transaccion.java
- TransaccionInput.java
- TransaccionOutput.java
- UserKairos.java

Cada uno de estos objetos representa una tabla en la base de datos.

Gráfico 22: Modelo Entidad-Relación del Sistema Control de Seguridad

Elaborado por: Los autores

El paquete **consoleface.service**, contiene las clases que acceden al DAO.

- TransaccionService.java
- TransaccionInputService.java
- TransaccionOutputService.java
- ReconocidoService.java
- ApiKeyKairosService.java

El paquete **consoleface.thread**, contiene las clases con el código que ejecutan los hilos, que realizarán operaciones simultáneas. Posee las siguientes clases:

- **TransaccionThread.java**, consulta las transacciones que llegan a la tabla para armar los JSON que insertará en el objeto TransaccionInput.java(tabla), actualiza el estado de la transacción.
- **KairosThread.java**, actualiza el estado de la transacción. Consulta las transacciones que enviará a KAIROS y registrará las respuestas en el objeto TransaccionOutput.java(tabla).

- **ReadResponseKairosThread.java**, lee las respuestas de Kairos desde el objeto TransaccionOutput.java, analizando el JSON y registrando su respuesta en el objeto Reconocido.java.

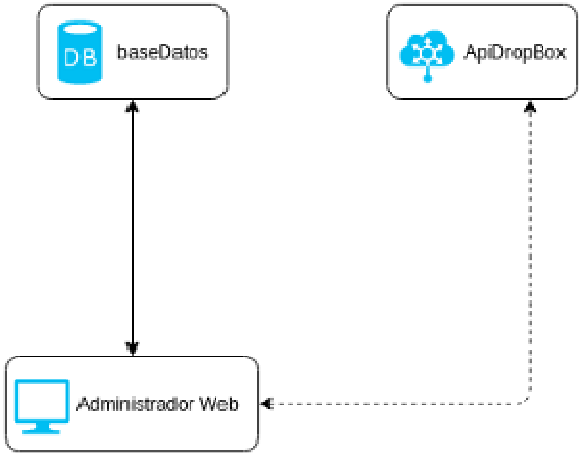
El paquete **consoleface.util** guarda las clases útiles para la aplicación tales como:

- HibernateUtil.java, instancia la sesión para activar un registro de log diario en caso existir errores se guardaran en un archivo .log.

5.2.3 Módulo 3 – Administrador Web

A través del administrador web el usuario podrá interactuar con el sistema, realizando consultas directas a la base de datos de los registros almacenados en base a las transacciones generadas previamente en los módulos anteriores. Además de generar reportes y enrolar usuarios en el API KAIROS.

Gráfico 23: Módulo - Administrador Web



Elaborado por: Los autores

CAPÍTULO VI: RESULTADOS DE PRUEBAS

6.1 Prueba de Reconocimiento Facial

Finalmente se realizó la prueba del circuito completo del proyecto, teniendo como base de registros de enrolados a 10 personas, a continuación se detalla los punto a considerar que se identificaron en el transcurso de la misma.

Para la prueba fueron tomadas 5 personas generando los siguientes resultados.

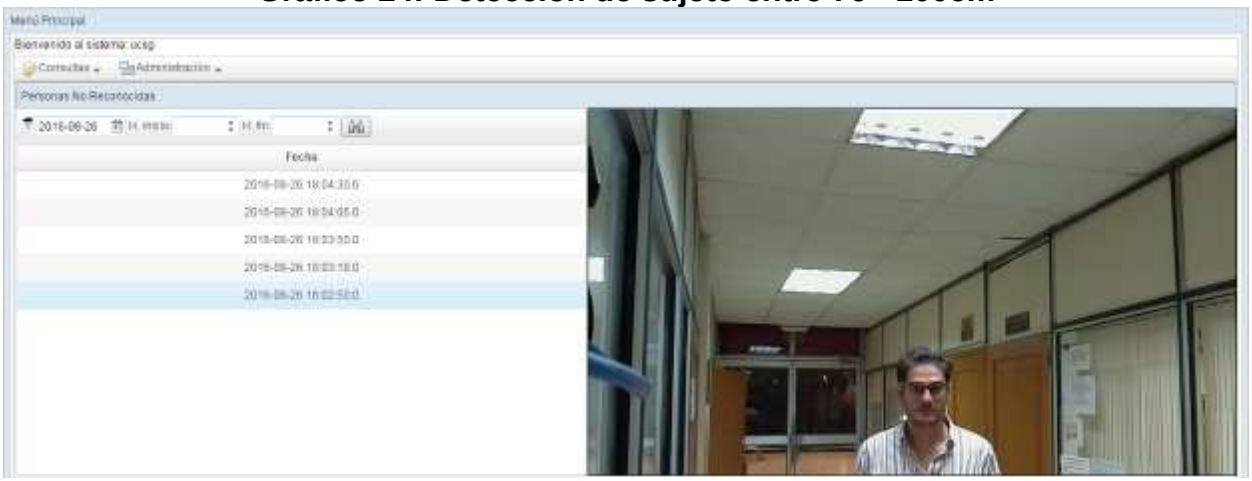
Tabla 13: Efectividad de Reconocimiento Facial en el Sistema según la Distancia

Distancia	Reconocimiento Exitoso	Reconocimiento Fallido
0 – 25cm	80%	20%
26 – 50cm	40%	60%
51 – 75cm	20%	80%
76 – 100cm	0%	100%

Elaborado por: Los autores

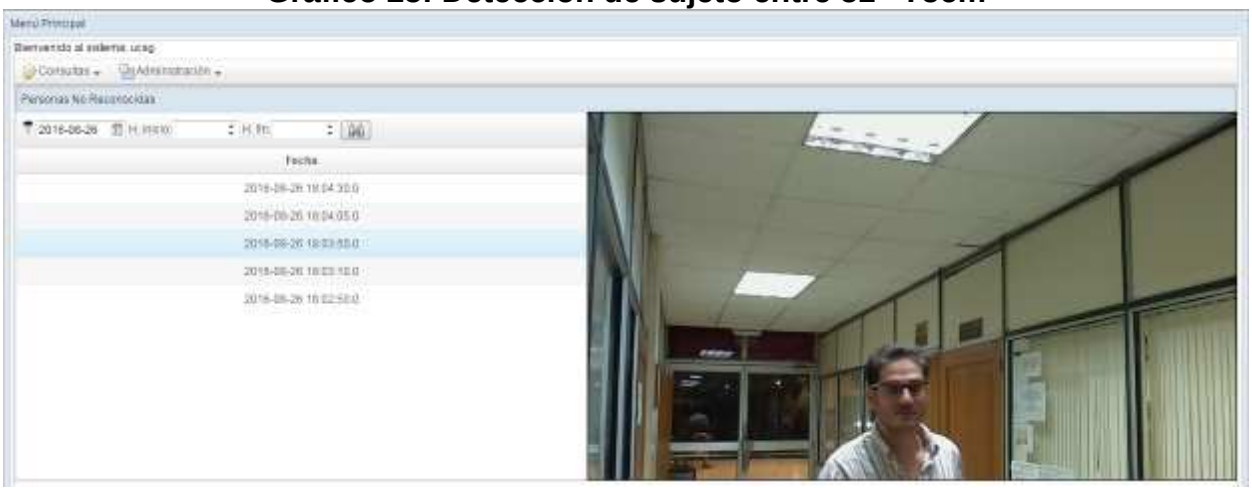
A continuación se selecciona las capturas de pantalla realizadas al sistema de uno de los asistentes enrolados, mostrando las detecciones tomadas desde diferentes distancias, coincidiendo para este caso las siguientes como reconocimiento fallido debido a la distancia de la posición del sujeto.

Gráfico 24: Detección de sujeto entre 76 - 100cm



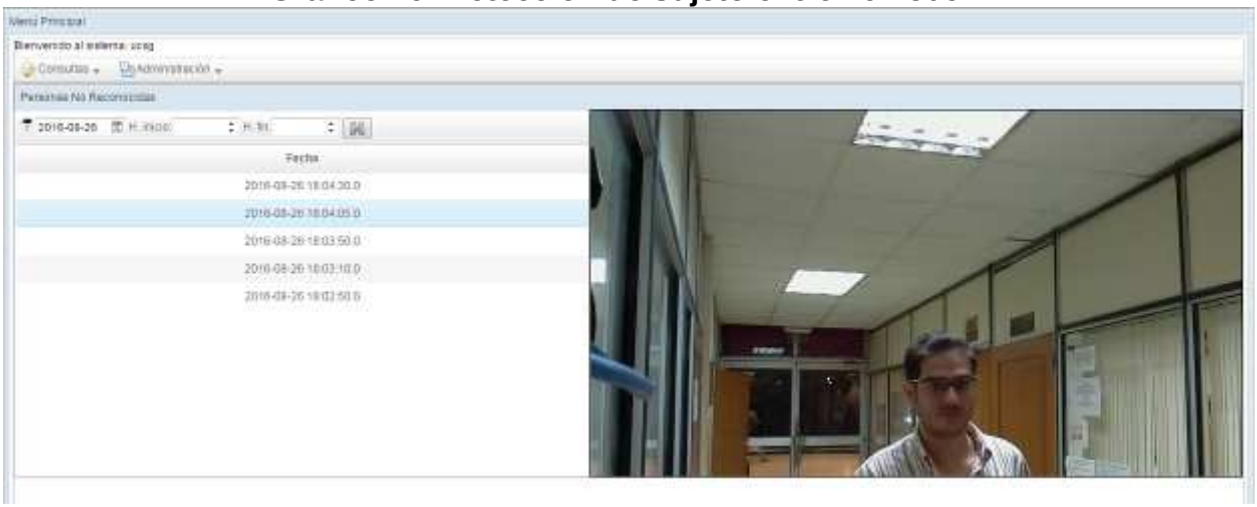
Elaborado por: Los autores

Gráfico 25: Detección de sujeto entre 51 - 75cm



Elaborado por: Los autores

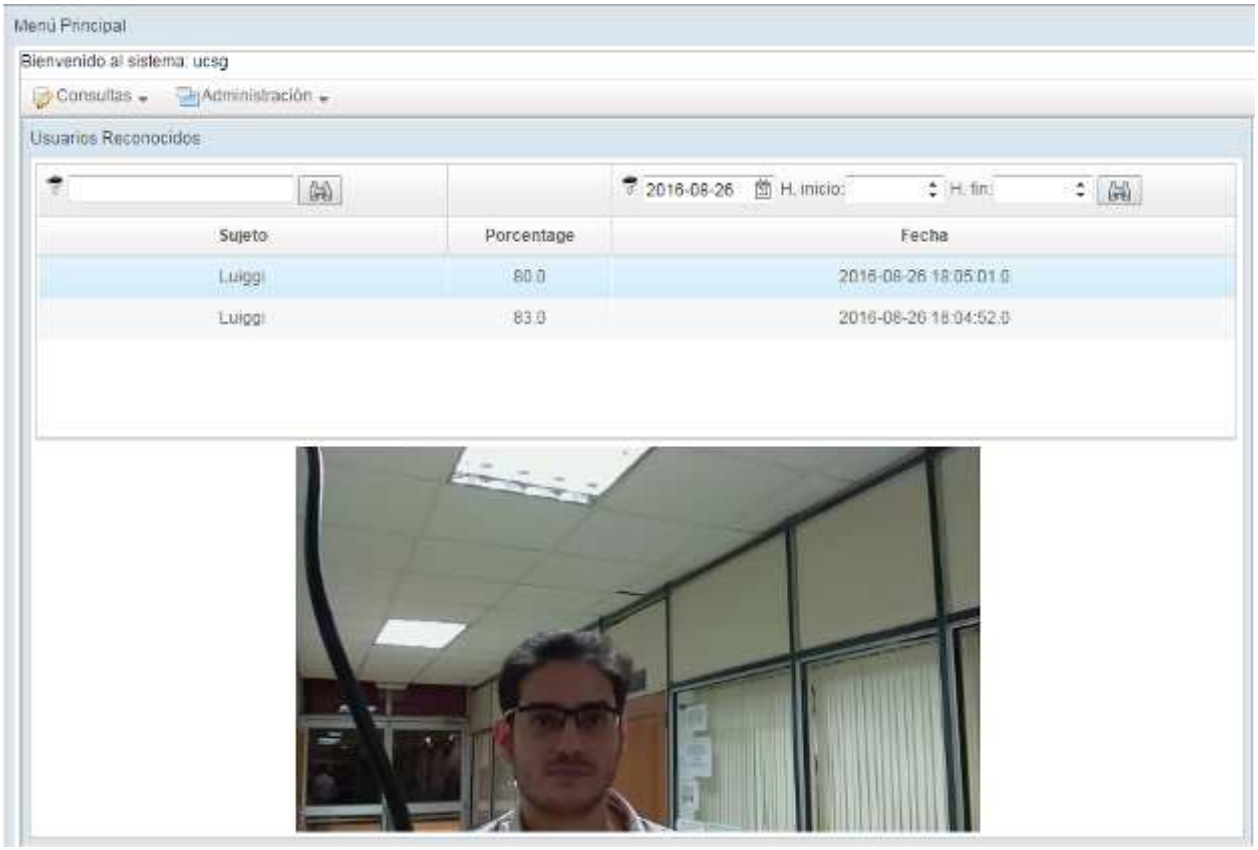
Gráfico 26: Detección de sujeto entre 26 - 50cm



Elaborado por: Los autores

En esta imagen se puede observar que el sujeto enrolado fue identificado, debido a su acercamiento entre 0 a 25cm. Siendo este un reconocimiento exitoso.

Gráfico 27: Detección de sujeto entre 0 - 25cm



Elaborado por: Los autores

Concluyendo que según las pruebas realizadas que es necesario estar frente al dispositivo a una distancia de 0 – 25cm para la efectividad del sistema de reconocimiento facial.

CONCLUSIONES

Efectuada la implementación del Control de Seguridad Biométrico de Reconocimiento Facial se ha llegado a la conclusión de que; un sistema de detección de rostros es ventajoso debido a la veracidad de una bitácora de registro siendo esta digital, gráfica y detallada, además de registrar imágenes las guarda en tiempo real, brindando un servicio que acelera búsquedas con fáciles detalles como la fecha y hora de lo ocurrido. Además de su bajo costo, es un sistema totalmente autónomo que no depende de la vigilancia adicional de una persona; concluyendo que es factible en base a las pruebas realizadas tanto de detección de rostros como de reconocimiento facial según las diferentes pruebas realizadas mediante la técnica de observación directa.

Se creó con la finalidad de evitar situaciones que puedan ser agravantes hacia el personal del área donde se lo implementó tales como: robos, hurtos, infiltraciones, etc.; llevando un control de registros de personas que frecuentan el lugar. Entre las desventajas están que una persona no enrolada no podrá ser identificada, pero la imagen de su rostro detectada quedará registrada, la cual puede ser accedida en cualquier momento; también que el sistema no puede ser cien por ciento fiable basándose en que, podría incluir dentro de los registros de notificaciones de no reconocidos a personas enroladas debido a la captura de su rostro con una distancia no adecuada según las pruebas realizadas.

El planteamiento de la aplicación ha permitido que se pueda realizar de mejor forma el diseño de un web service y aplicación de consola logrando los registros de las peticiones y procesándolos con los servicios de reconocimientos. Se ha logrado el correcto diseño del administrador web que ayudara a un buen monitoreo de la aplicación sirviendo directamente a la Facultad de Ingeniería con la posibilidad que en algún momento pueda ser parte a nivel universitario.

RECOMENDACIONES

A partir de la conclusión sería factible que como recomendación se tomen los siguientes puntos:

- Adicionar al sistema módulos estadísticos, para precisar por tiempos el registro máximo de personas.

- Manejo remoto de cámara desde el administrador web.

- Actualización remota del dispositivo.

- Entrenar nuevas características Haar para detectar otros objetos o posiciones de caras.

- Generar un banco de personas no deseadas.

- Se recomienda solicitar al Centro de Computo de la Universidad Católica de Santiago de Guayaquil el servicio de alojamiento interno en sus servidores.

- Si se desea, mejorar los servicios de almacenamiento en la nube Dropbox o de Reconocimiento Facial API Kairos para obtener mayor beneficio de sus componentes verificar valores en las tablas 9 y 10 respectivamente.

- Usar cámaras tipo domo con zoom óptico, para evitar la manipulación de la cámara pero manteniendo la resolución completa para la detección.

BIBLIOGRAFIA

Arias, F. G. (2012). *El Proyecto de Investigación: Introducción a la Metodología Cieníifica* (6ta ed.). Episteme.

Bradski, G. (2000). The OpenCV library. *Dr. Dobb's Journal, 25*(11), 120-125.

Burge, M., Klare, B., Klontz, J., & Klum, S. (2013). *Open Source Biometric Recognition, Biometrics: Theory, Applications and Systems.*

Consejo Nacional de Ciencia y Tecnología. (2006, agosto). *Biometría: Reconocimiento Facial*. Retrieved from http://www.biometria.gov.ar/metodos-biometricos/facial.aspx

Dankhe. (1986). *Diferentes Diseños. Tipos de Investigación.* (McGraw-Hill, Editor) Retrieved 1996, from http://www.revistaespacios.com/volumen17

Dengpan, M. (2010). Fundamentals and Advances in Biometrics and Face Recognition. In D. Mou, *Machine-based Intelligent Face Recognition* (pp. 13-70).

Grimson, V., & Mundy, J. (1994, Marzo). Computer vision applications. *Comunications of the ACM*, p. 44.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS. (2012). *Dictamen 02/2012 sobre reconocimiento facial en los servicios en línea y móviles.* Bruselas.

Guerrero, D. (2012, marzo 25). *Blog Diego Guerrero*. Retrieved from http://www.diegoguerrero.info/tag/reconocimiento-facial/

Hernández, E., Cabrera, A. J., Sánchez, S., & Cabrera, A. (2012). Impacto de la memoria cache en la aceleración de la ejecución de algoritmo de detección de rostros en sistemas empotrados. *Ingeniería Electrónica, Automática y Comunicaciones*.

Levin, & Rubin. (1996). Estadística para Administradores. México: Prentice Hall.

Llorca, A. (2015, octubre 15). *GENBETA*. Retrieved junio 20, 2016, from http://www.genbeta.com/actualidad/openface-un-nuevo-software-de-reconocimiento-facial-de-codigo-abierto

Marcel, S., & Rodríguez, Y. (2016). *IDIAP RESEARCH INSTITUTE*. Retrieved junio 01, 2016, from https://www.idiap.ch/scientific-research/resources/torch3vision

Misfud, E. (2012, abril 27). *Obervatorio Tecnológico*. Retrieved junio 23, 2016, from http://recursostic.educacion.es/observatorio/web/eu/cajon-de-sastre/38-cajon-de-sastre/1045-sistemas-fisicos-y-biometricos-de-seguridad

Ottado, G. (2010). *Reconocimiento de caras: Eigenfaces y Fisherfaces.*

Planells Lerma, J. (23 de marzo de 2009). *Academia.* Obtenido de http://www.academia.edu/9503665/Implementacion_del_algoritmo_de_deteccion_facial_de_Viola-Jones_Autor_Joaqu_%C4%B1n_Planells_Lerma_Director

Rodríguez, S. (2010, Diciembre). *Análisis del preprocesado de imágenes en el reconocimiento de caras en PCA.* Retrieved from http://lcsi.umh.es/docs/pfc_sergio/Memoria_Sergio_Rodriguez.pdf

Sabina, C. (1986). *El Proceso de Investigaci.* Humanitas.

Tashakkori, A., & Teddlie, C. (2003). *Handbook of Mixed Methods in Social & Behavioral Research.* Thousand Oaks: SAGE.

Valdés, F. (2015). *Reconocimiento de Huellas Dactilares Usando la Cámara de un Dispositivo Móvil (tesis de pregrado).* Santiago de Chile: Universidad de Chile.

Valveny, E. (2016). Detector Basado en Haar/Adaboost. *Detector de Objetos*. Barcelona. Retrieved from https://www.coursera.org/learn/deteccion-objetos/lecture/eczp1/l5-1-detector-de-caras-basado-en-filtros-de-haar-adaboost

Viola, P., & Jones, M. (2001). *Rapid Object Detection using a Boosted Cascade of Simple.* Retrieved from https://www.cs.cmu.edu/~efros/courses/LBMV07/Papers/viola-cvpr-01.pdf

VXL. (2016). *The VXL Homepage*. Retrieved junio 01, 2016, from http://vxl.sourceforge.net/

ANEXOS

Anexo 1: Encuesta al Personal Laboral del Área Administrativa

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

ENCUESTA

1. Persona encuestada
   - O Personal Administrativo
   - O Autoridad
   - O Profesor tiempo completo
2. ¿Qué tan seguro cree usted que es el Área de Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil?
   - O Muy Seguro
   - O Seguro
   - O Medio Seguro
   - O Inseguro
   - O Muy Inseguro
3. ¿Ha sucedido algún suceso de inseguridad en el área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil?
   - O Si
   - O No
4. Si su respuesta anterior fue si, ¿Cuál fue el suceso que ocurrió?

   _____

   _____
5. ¿Conoce usted de algún sistema de control de seguridad existente en el Área Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil?
   - O Si
   - O No

6. ¿Cuál es su grado de confiabilidad ante un sistema de control de seguridad biométrico de reconocimiento facial?
   - O 1-20%
   - O 21-40%
   - O 41-60%
   - O 61-80%
   - O 81-100%

7. ¿Estaría de acuerdo en ser vigilado por un dispositivo (cámara) a la entrada y salida del Área Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil?
   - O Si
   - O No

8. ¿Estaría de acuerdo en que se capture su rostro por un dispositivo (cámara) para comprobar si usted es un rostro reconocido por el sistema de control de seguridad?
   - O Si
   - O No

Anexo 2: Entrevista a Directora de Carrera Ingeniería en Sistemas Computacionales

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

ENTREVISTA

1. **¿Actualmente, tiene conocimiento acerca de algún control de seguridad que manipule la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil?**
   Están funcionando las cámaras que tenemos dentro de la facultad en el área administrativa, hay dos cámaras pero no es seguro totalmente.

2. **En caso de que se dé un suceso respecto a la seguridad del personal que labora en el área administrativa. ¿Cuál es el proceso a seguir?**
   No sabría qué contestarle, desconozco totalmente esa parte.

3. **¿Qué espacios del Área Administrativa le parecen sensibles o muy accesibles por personas ajenas a dicho lugar?**
   La parte de la puerta de la entrada, porque abren, dejan abierto y no se quienes entran; por ejemplo yo me encuentro acá en mi oficina y como se quién entra y sale y en ocasiones se va el señor de control de catedra.

4. **¿Entre los controles de seguridad, ha escuchado o participado de alguno?**
   Sí, el de huella digital.

5. **¿Cree usted que un sistema de control de seguridad más automatizado ayudaría a brindar mayor seguridad en el ambiente laboral para el personal que trabaja en la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil?**
   Definitivamente que sí.

6. **¿Cuál cree usted que sería una ubicación estratégica para sacarle mayor provecho a un sistema de control de seguridad?**
   Entrada de la puerta principal, los que nos encontramos acá adentro no se sabe quiénes son los que ingresan.

Anexo 3: Entrevista a Profesora Tiempo Completo

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

ENTREVISTA

1. **¿Actualmente, tiene conocimiento acerca de algún control de seguridad que manipule la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil?**
   Si hay conocimiento, el sistema de seguridad por guardianía y el sistema de cámaras.

2. **En caso de que se dé un suceso respecto a la seguridad del personal que labora en el área administrativa. ¿Cuál es el proceso a seguir?**
   Lo desconozco, no sé qué procedimiento el otro día ingresaron personas y fui a buscar a alguien y no encontré a nadie.

3. **¿Qué espacios del Área Administrativa le parecen sensibles o muy accesibles por personas ajenas a dicho lugar?**
   Justo el ingreso corredor y las oficinas de profesores a tiempo completo son vulnerables.

4. **¿Entre los controles de seguridad, ha escuchado o participado de alguno?**
   Los mencionado en la primera pregunta, y si he tenido controles de accesos con tarjeta magnética y me abre las puertas, apertura y cerrada de puertas.

5. **¿Cree usted que un sistema de control de seguridad más automatizado ayudaría a brindar mayor seguridad en el ambiente laboral para el personal que trabaja en la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil?**
   Por supuesto, porque necesitamos contar con más seguridad especialmente porque aquí hay mucha gente, no solamente es un área que se garantiza que hay estudiantes y docentes, o sea cualquier persona llega además con esto de que hay compañías la gente de afuera ingresan y no tenemos ninguna seguridad para el personal en especial en las tardes que no hay tantas autoridades.

6. **¿Cuál cree usted que sería una ubicación estratégica para sacarle mayor provecho a un sistema de control de seguridad?**
   El acceso justamente, las puertas principales de acceso.

Anexo 4: Observación - Implementación de Prueba de Dispositivo Biométrico de Reconocimiento Facial

<table>
<tr><td rowspan="4">UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL</td><td>Prueba:</td><td>1</td></tr>
<tr><td>Fecha:</td><td>9/06/2016</td></tr>
<tr><td>Observadores:</td><td>Liliana Solis
Luiggi Puga</td></tr>
<tr><td>Evento:</td><td>Efectividad de Detecciones de Rostros</td></tr>
<tr><td>Observación</td><td colspan="2">En este primer ensayo se puso a prueba la efectividad de la detección de rostro, se identificó que la aplicación estaba detectando mayormente gran cantidad de falsos positivos y pocas detecciones correctas, habiendo implementado en el desarrollo de la aplicación únicamente la característica de detección frontal de cara de la librería OpenCV.

Se detectaron 543 imágenes de las cuales:
▪ Detecciones correctas (ok) fueron 126, dando un 23.20%.
 
▪ Y, resultaron 417 falsos positivos, equivaliendo a un 76.80% consiguiendo que no sea efectiva la aplicación.

  </td></tr>
</table>

Elaborado por: Los autores

<table>
<tr><td rowspan="4">UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL</td><td>Prueba:</td><td>2</td></tr>
<tr><td>Fecha:</td><td>6/07/2016</td></tr>
<tr><td>Observadores:</td><td>Liliana Solis
Luiggi Puga</td></tr>
<tr><td>Evento:</td><td>Efectividad de Detecciones de Rostros</td></tr>
<tr><td>Observación</td><td colspan="2">En la segunda prueba realizada se tuvo mayor efectividad, debido a la integración de una nueva característica, la detección de ojos, reduciendo en gran cantidad los falsos positivos, optimizando las detecciones correctas de rostro.

Se detectaron 98 imágenes de las cuales:
▪ Detecciones correctas (ok) fueron 96, dando un 97.96% grado de efectividad al algoritmo de detección de rostros.

▪ Y, resultaron 2 falsos positivos, equivaliendo a un 2.04% consiguiendo mitigar casi en su totalidad los valores resultantes de la prueba anterior.

  </td></tr>
</table>

Elaborado por: Los autores

Anexo 5: Documento de Especificaciones Técnicas del Sistema

Objetivo

Diseñar y desarrollar:

- Aplicación de detección de rostros (instalada en las
- Web service para el consumo de los aplicativos.
- Aplicación de consola .jar para procesar todas las peticiones registradas por el web service.
- Raspberry).
- Página web que permita el monitoreo de los sistemas

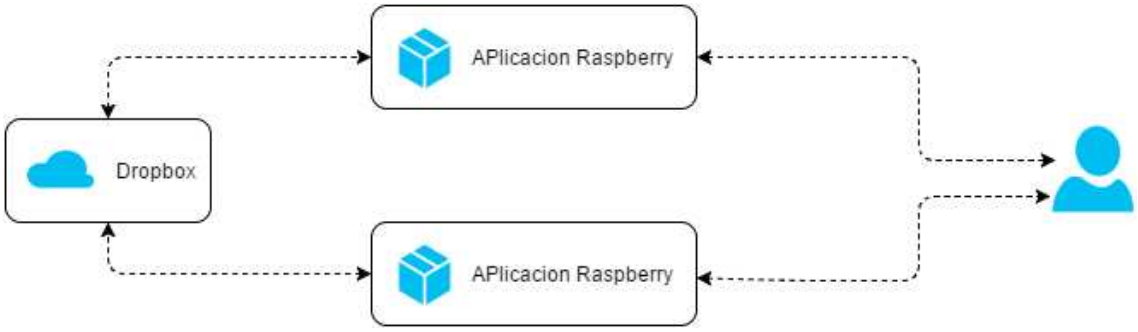
Consideraciones Generales

- Arquitectura
- Aplicaciòn de detección de rostros(raspface.jar)
- Web service (webserviceface.war):
    - JSON reconocimiento.
    - JSON enrolar
- Aplicación de consola(consolaface.jar)
- Administrador web(adminwebface.war)
- Base de datos

Procesos del Sistema

Arquitectura

Aplicación, deteccion de rostros:

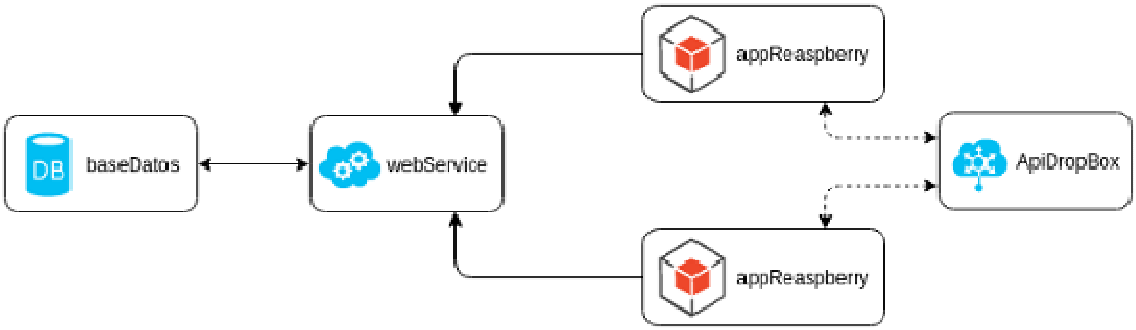


El aplicativo se encargara de detectar rostros y enviarlos a los diferentes servicios que se maneje en el istema, este a su ves manejara colas en la RAM he hilos para agilizar los procesos.

Para el reconocimiento y enrolamiento:

- Tomar n fotos.
- Enviarlas Dropbox.
- Servicio de reconocimiento/enrolamiento Kairos
- Armar el JSON para enviar al webservice.

WebService.



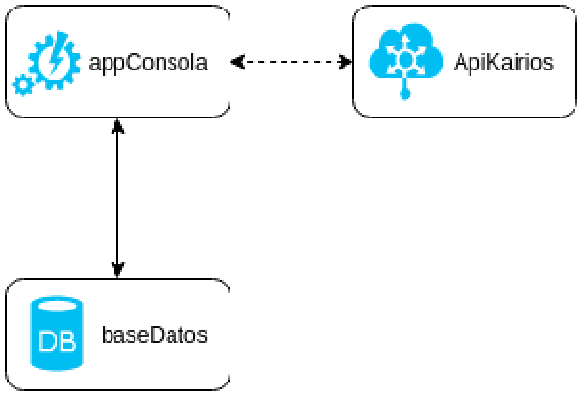
Para recibir las peticiones de los aplicativos se expondra los siguientes servicios (webservice) con lo siguiente:

- **Webservice de reconocimiento**: Recibira todas la peticiones de los aplicativos en formato JSON, estos seran validados y posteriormente almacenados en la tabla *tTransaccionesRec* estas transacciones naceran con status 0.

0	Transaccion no procesada
1	Transaccion procesada

- **Webservice de enrolamiento**: Recibira las peticiones de enrolamiento de los distintos palicativos, realiara lo siguiente:
    - Validar el usuario y el app.
    - Registrar la transaccion en la tabla *tTransaccionesEnroll*

Aplicación de consola:



Se creara un job (tarea) que lea de la tabla tTransacionesRec todas aquellas transaciones, que hayan sido depositadas por el webservice y que no hayan sido procesadas (status 0), armando los nuevos JSON que seran enviados a KAIROS que a su ves seran registrados en la tabla *tTRansaccionesDetalleREc* con su posterior rspuesta del servicio.

Esta respuesta se leera para identificar si identifico a la persona asi como su porcentaje de acierto, estos datos seran registrados en la tabla *tSujetosReconocidos*.

- Armar los nuevos JSON que se enviaran a Kairos
- Registrar en la tabla tTransaccionesDetalleEnroll los JSON input y output de kairos asi como su status de enrolamiento.

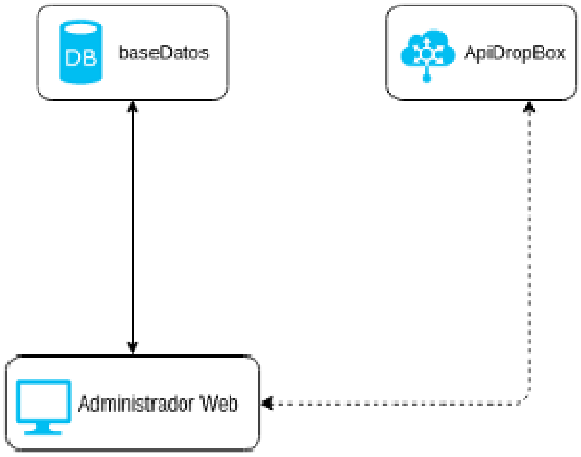
Formato del JSON reconocimiento:

{"app_rasp":"rasp001","key":"12345ASD","imagenes":[{"imagen":"www.asdf.com"},{"imagen":"www.asdf.com"},{"imagen":"www.asdf.com"},{"imagen":"www.asdf.com"}]}

Formato del JSON enrolar:

{"app_rasp":"rasp001","key":"12345ASD","user":"luiggi","pass":"123456789","nombre":"juan","apellido":"puga","imagenes":[{"imagen":"www.asdf.com"},{"imagen":"www.asdf.com"},{"imagen":"www.asdf.com"},{"imagen":"www.asdf.com"},{"imagen":"www.asdf.com"},{"imagen":"www.asdf.com"},{"imagen":"www.asdf.com"},{"imagen":"www.asdf.com"}]}

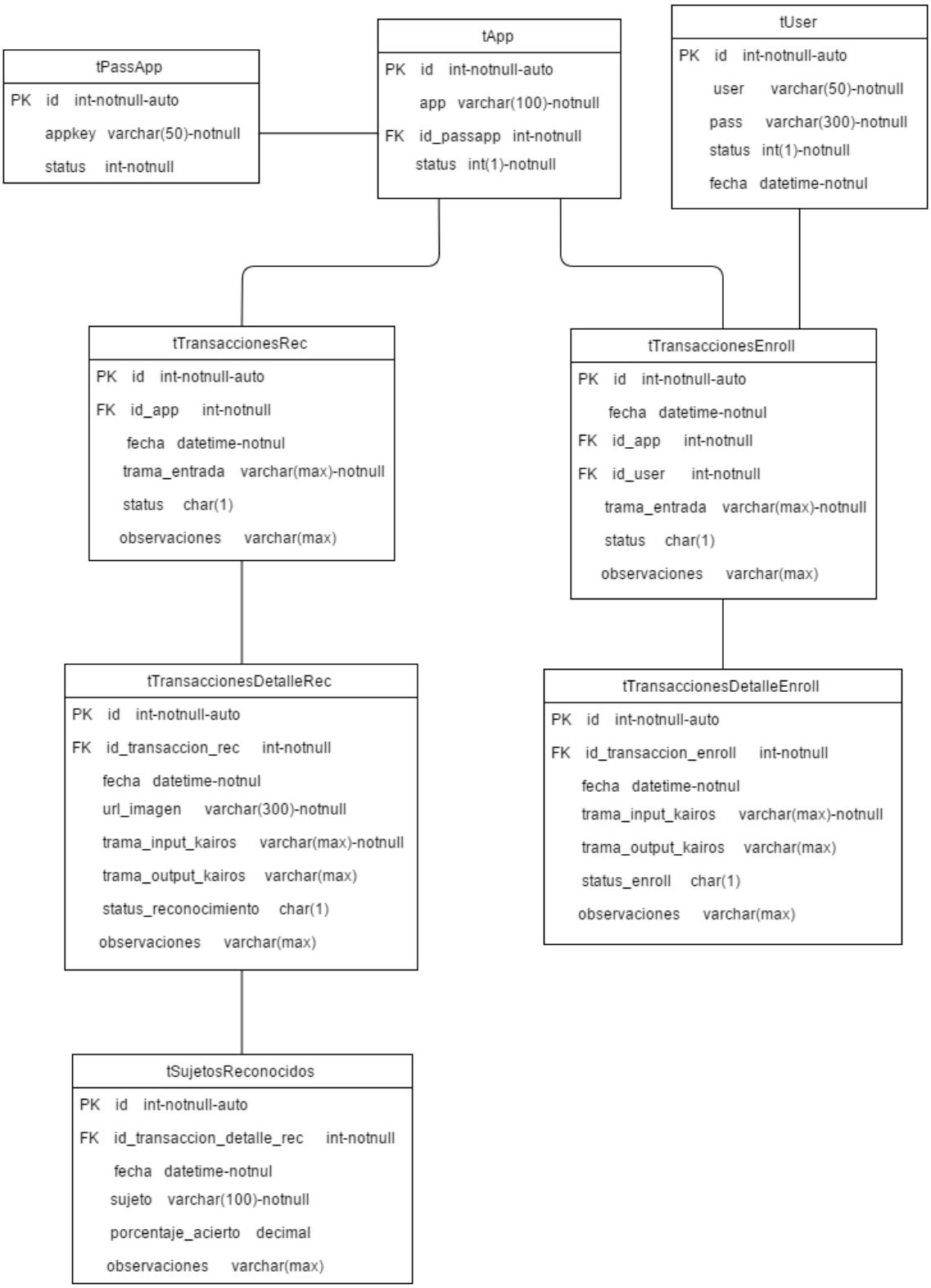
Administrador web:



Consultara las respuestas que fueron depositadas por la aplicación de consola, permitiendo visualizar las personas reconocidas y las no reconocidas, conectados al servidor de imágenes Dropbox, a través de la url que se obtuvo al inicio del sistema al subir la imagen (aplicación de detección)

Estructura de bases de datos

Se creara una nueva base de datos llamada **bFACE** y contendrá La siguientes tablas:



Especificaciones de las tablas:

Tabla: tPassApp.- Almacenara los keys disponibles y su status que podrá variar entre 1 y 0

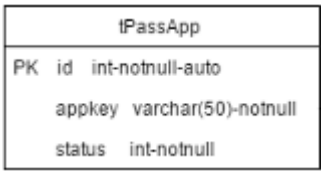


Tabla: tApp.- Guardar el nombre de los dispositivos físicos admitidos para el sistema.

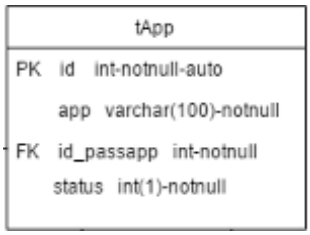


Tabla: tUser.- Guardar el nombre de los ususarios del sistema.

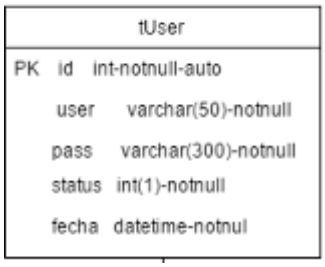


Tabla: tTransaccionesRec.- Almacenara todas las transacciones de reconocimiento de los diferentes aplicativos.

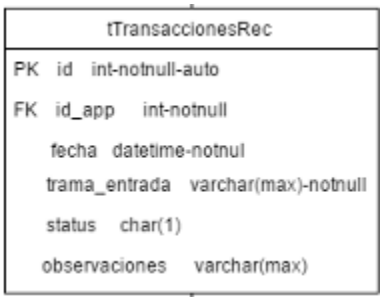


Tabla: tTransaccioneDetalleRec.- Almacenara el detalle de las transacciones que se enviaran a kairos.

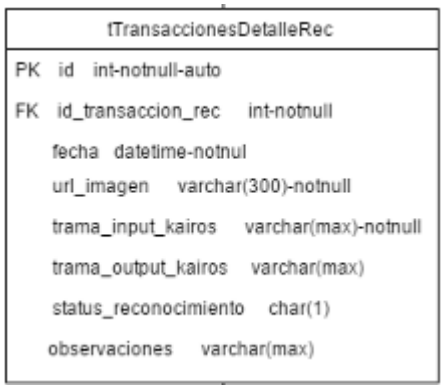


Tabla: tSujetosReconocidos.-Almacena datos de la persona que reconoció.

Tabla: tTransaccionesEnroll.- Almacenara todas las transacciones de enrolamiento de los diferentes aplicativos.

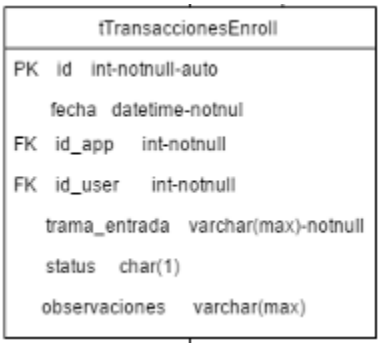
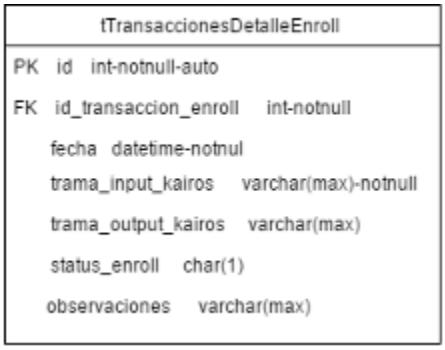


Tabla: tTransaccioneDetalleEnroll.- Almacenara el detalle de las transacciones input y output que se envían a kairos.



Anexo 6: Manual de Usuario – Control de Seguridad Biométrico de Reconocimiento Facial

El administrador debe acceder al sistema mediante una ventana de autentificación, ingresando las credenciales que se le proporciona:

Usuario y clave, luego dar *click* en el botón: *Login*

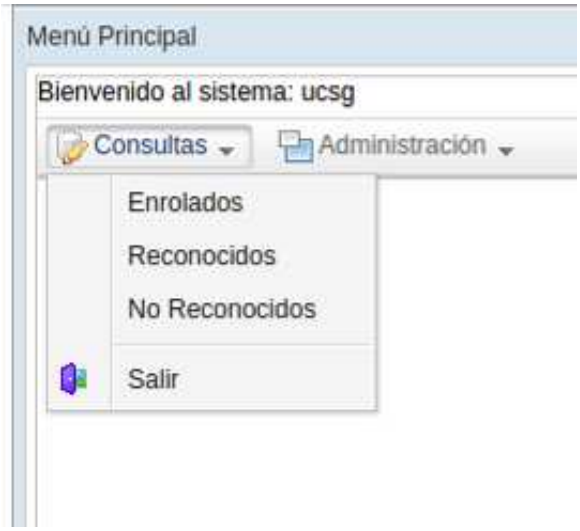
Se muestra en pantalla la siguiente notificación, en caso de que las credenciales sean incorrectas, de clic en ok y vuelva a ingresar las credenciales correctas.

Autentificadas las credenciales, ingresa a pantalla principal la cual posse una barra con el menú principal con dos opciones:

- Consultas, → realiza consultas al sistema.
- Administración, → registra a usuarios.

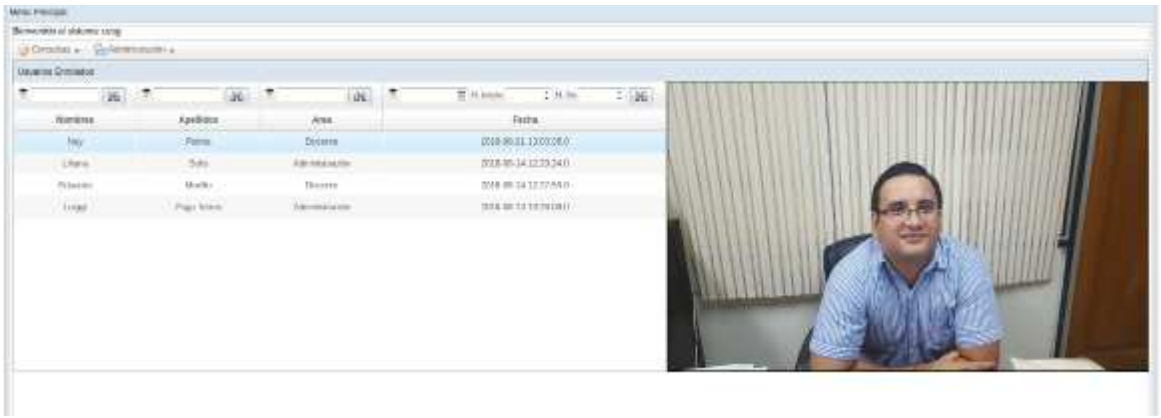
En el menú de **CONSULTAS** se encuentra un submenu con las siguientes opciones:

- Enrolados
- Reconocidos
- No Reconocidos
- Salir

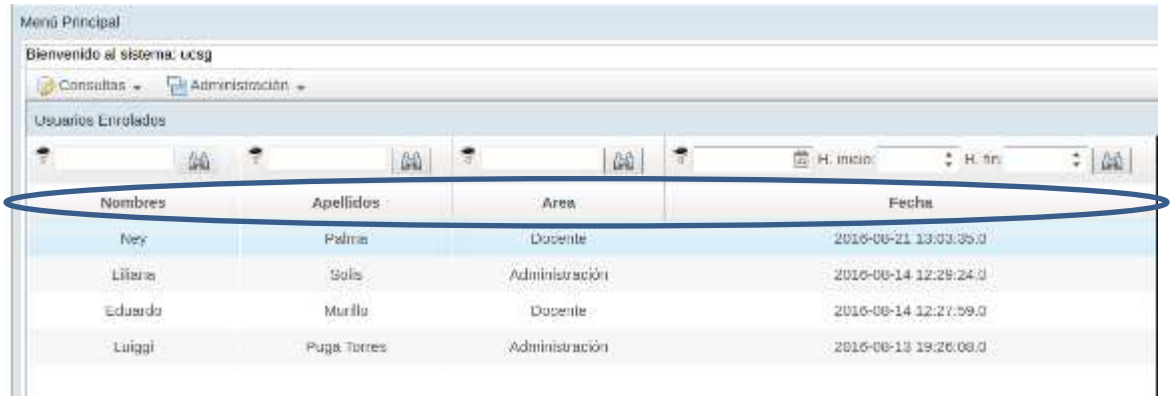


Enrolados

Permite visualizar la lista de las personas que han sido enroladas (registradas) en el banco de datos e imágenes.



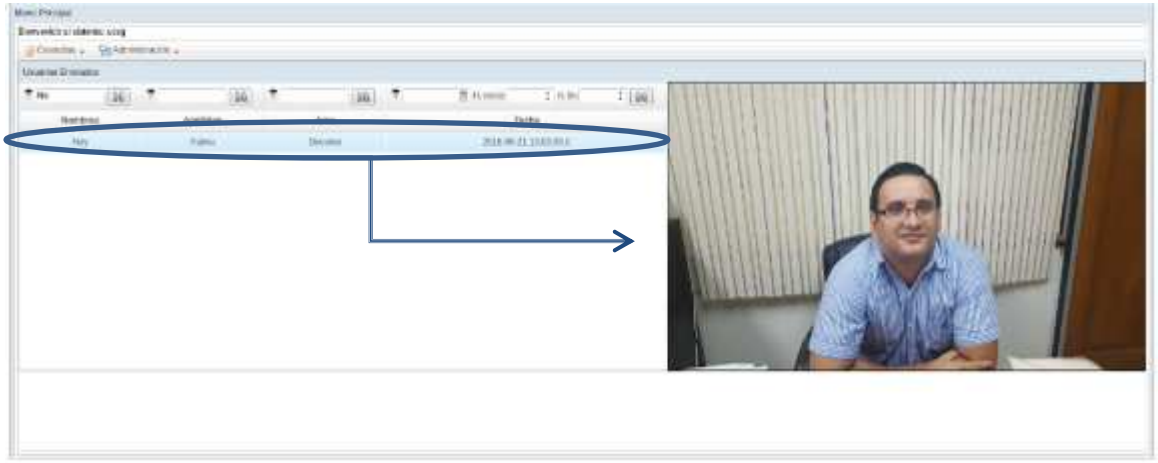
Para acelerar la busqueda de algún registro específico, contiene filtros como: Nombre, Apellido, Área o Fecha de Registro.
Los filtros están ubicados en la parte superior de cada columna.



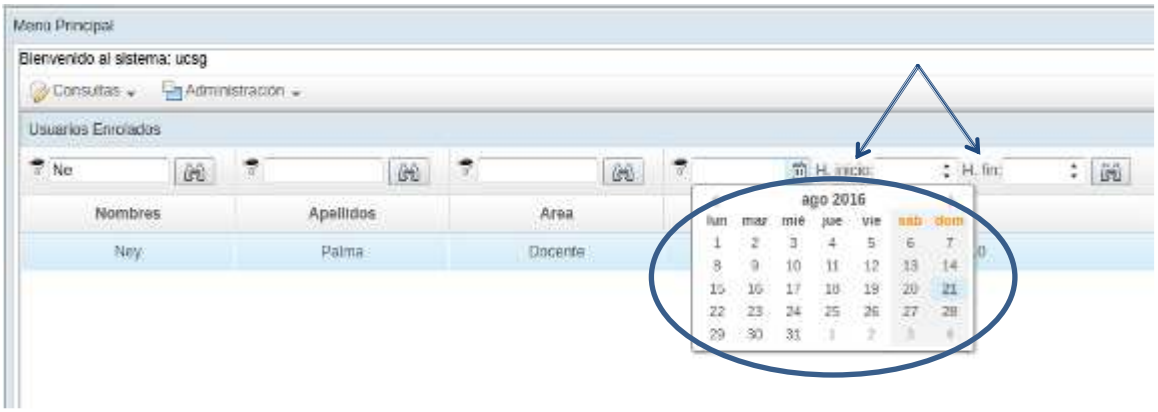
.

Para aplicar el filtro Nombre, puede ingresar desde las iniciales del nombre de la persona enrolada que desea buscar.

Da como resultado los datos de la persona buscada con su respectiva imagen.

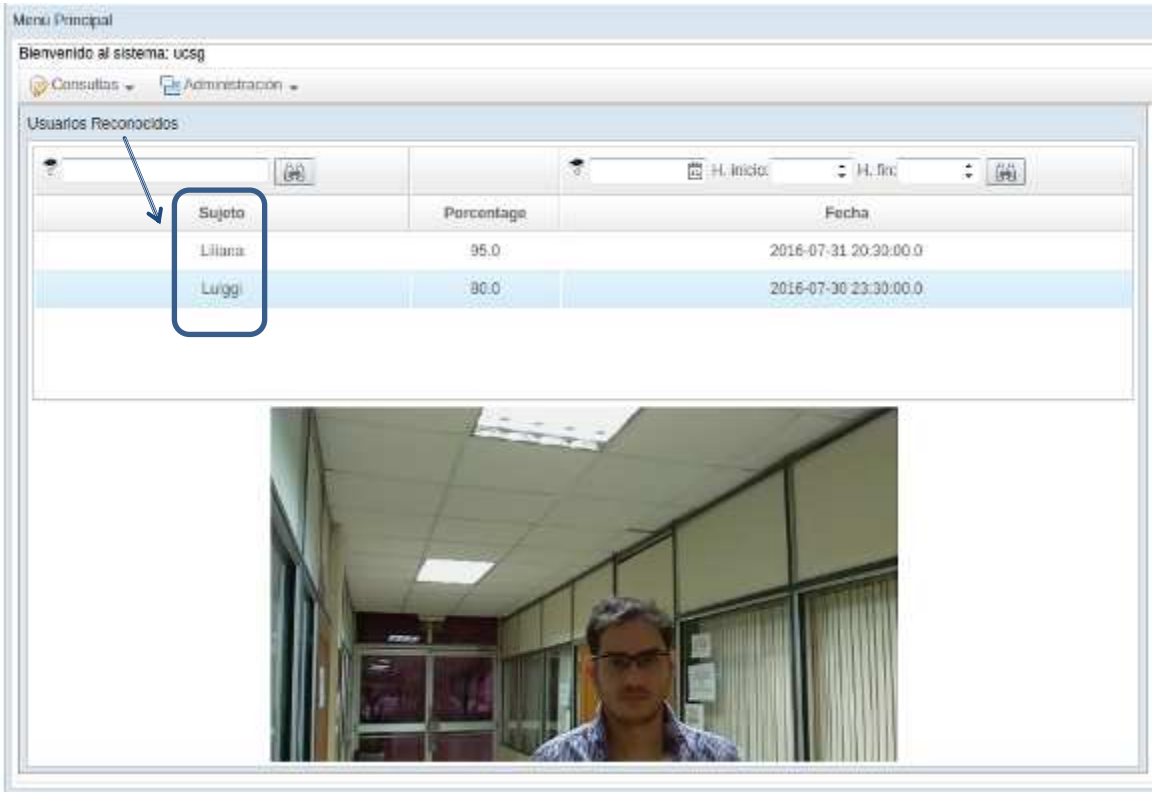


Para aplicar el filtro de fecha de registro, el administrador debe seleccionar el día de la semana y; si desea ser mas específico y lo recuerda puede ingresar la hora.

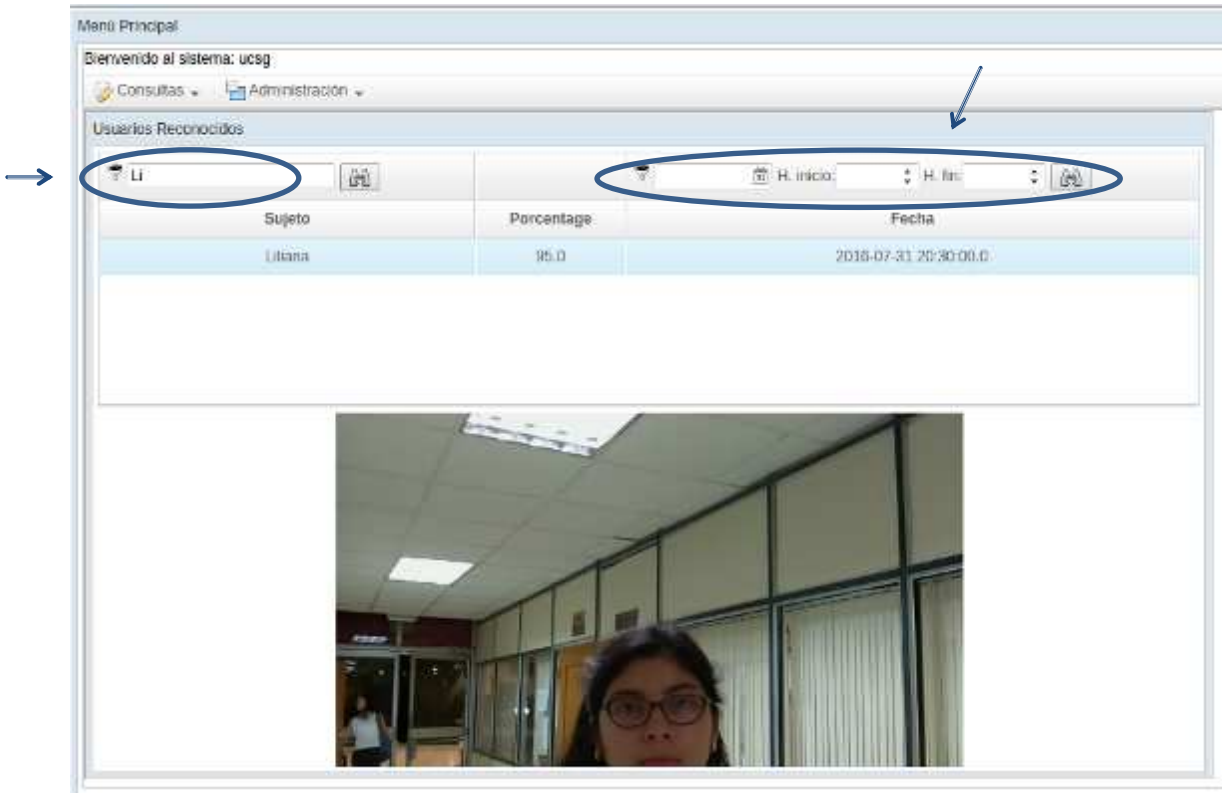


Reconocidos

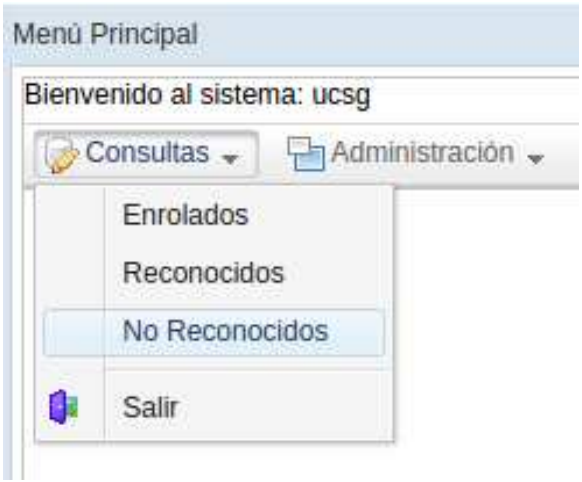
Esta opción muestra la lista de personas detectadas que han sido reconocidas en el sistema, de acuerdo a las personas enroladas. Muestra el Nombre, Porcentage de Acierto respecto a las imágenes enroladas y Fecha de reconocimiento.



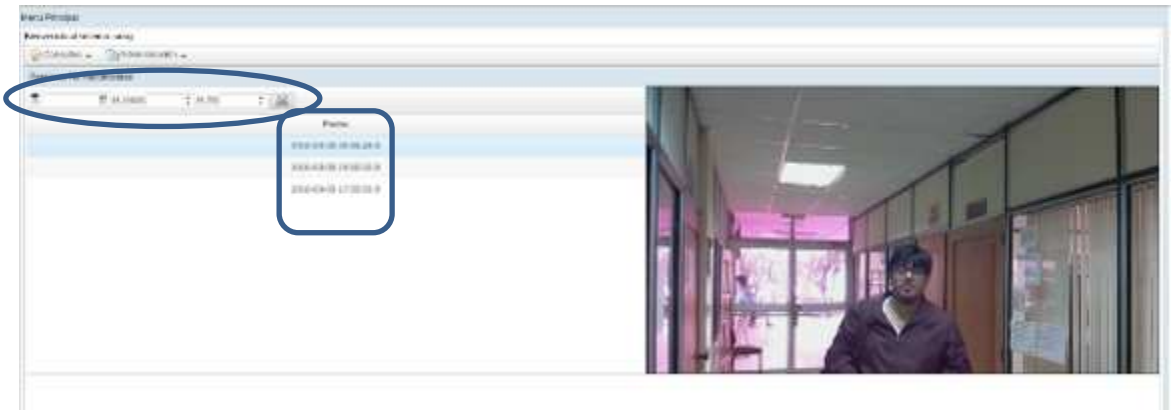
En esta opción tambien se puede aplicar filtros de busqueda por Nombre o Fecha de Reconocimiento.

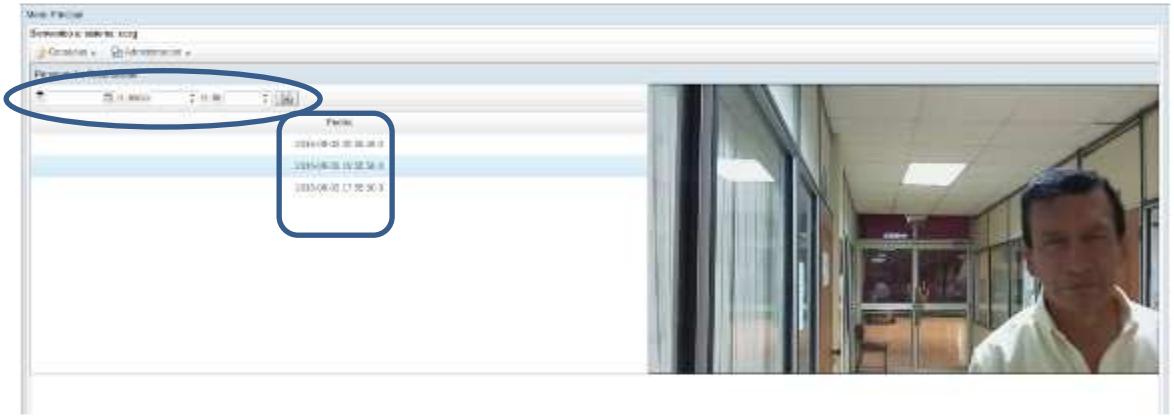


No Reconocidos

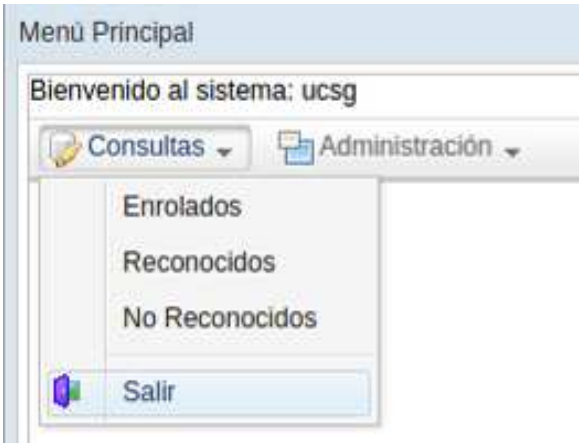


Esta opción muestra la lista de fechas de detecciones de personas con su respectiva imagen, en las que el sistema no encontró ninguna semejanza con las imágenes de personas enroladas.
El único filtro de búsqueda que posee es por fecha.





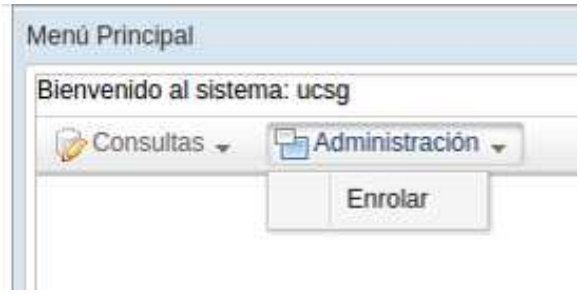
Salir



Como última opción del menú de Consiltas se encuentra Salir, permite cerrar la sesión del administrador en el sistema.

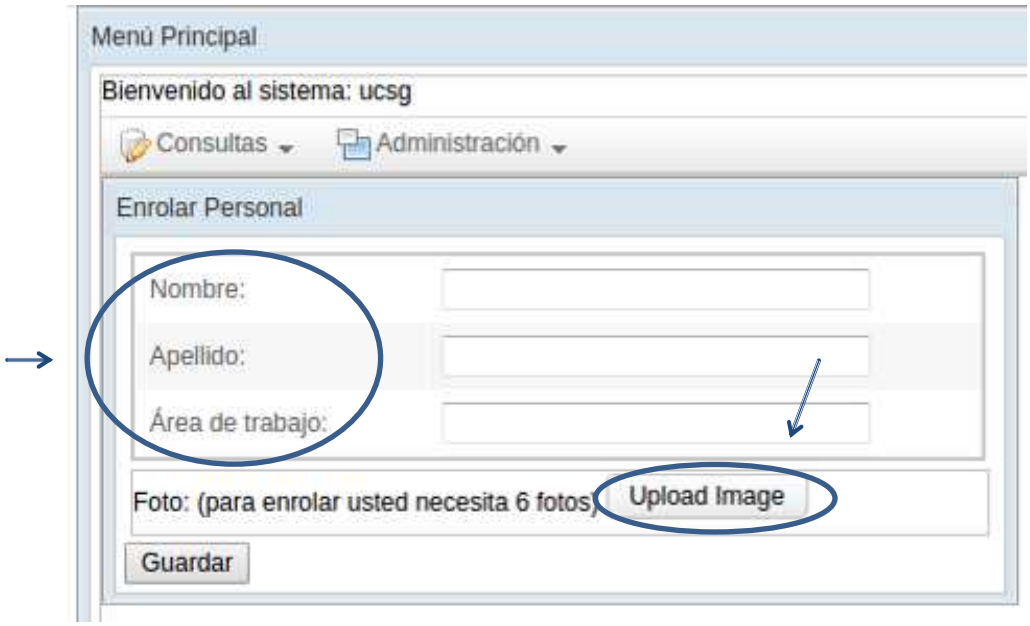
En menú **ADMINISTRACIÓN** se encuentra una única opción:

↳ Enrolar.



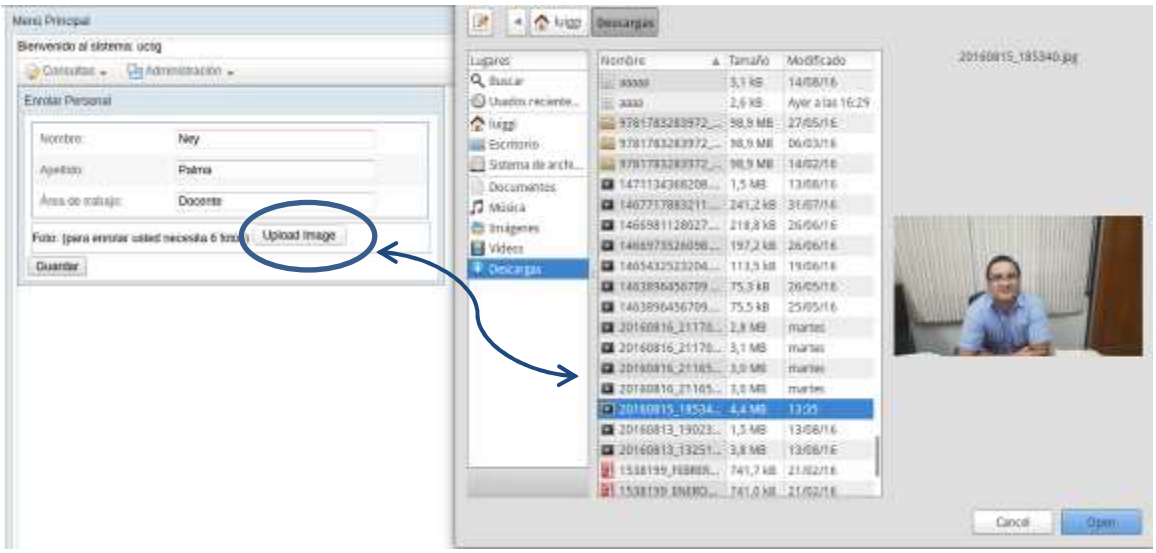
La opción enrolar permite registrar a los personas con sus respectivas imágenes, que posteriormente serán usadas para compararlas con las imágenes detectadas por el sistema.

Se ingresa Nombre, Apellido, Area de Trabajo y el botón Upload Image permite subir fotos del rostro de la persona a enrolar

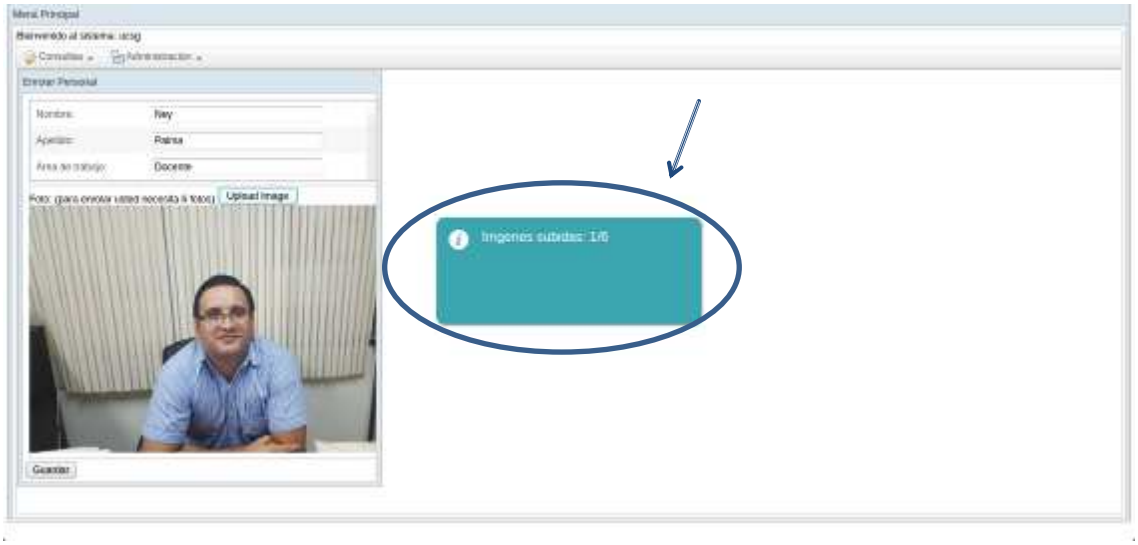


.

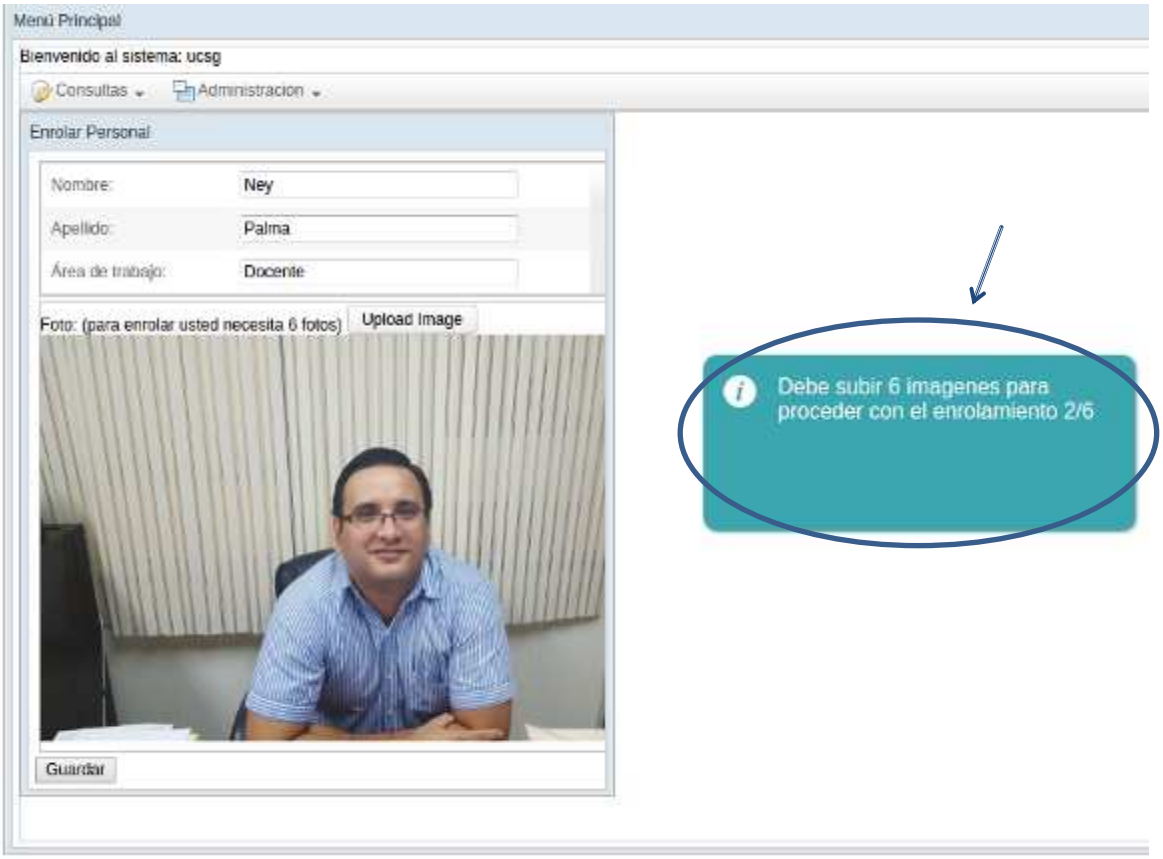
Para subir una foto se da *click* en el botón *Upload Image*, se busca en la dirección correspondiente y se selecciona la foto; este paso debe repetirse 6 veces ya que se requien 6 fotos para poder enrolar a una persona.



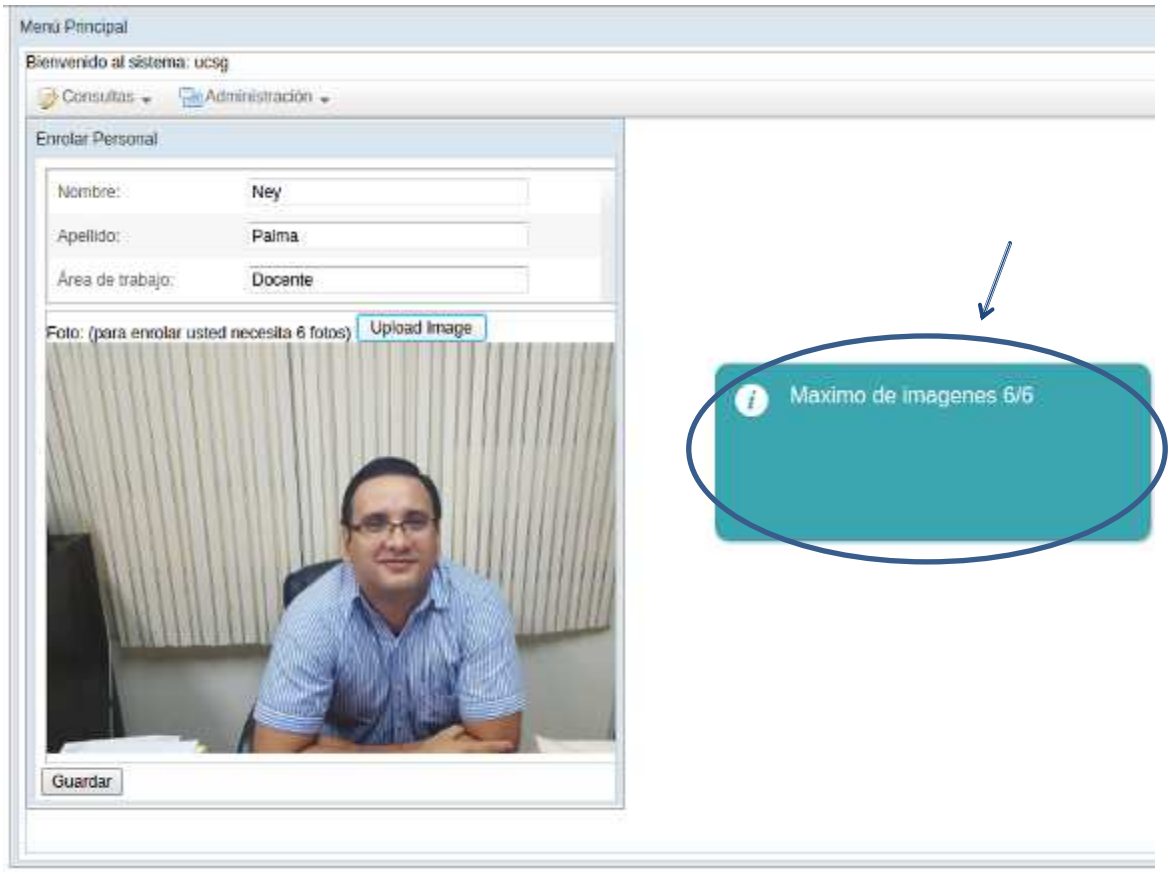
El sistema iniciará un contador el cual se muestra en pantalla, indicando la cantidad de fotos subidas.



En caso de no completar el ingreso de las 6 imágenes requeridas por el sistema y da *click* en el botón Guardar, el sistema informará al usuario con la siguiente notificación



El sistema tampoco permitirá subir mas imágenes de las requeridas.



Finalmente ingresados los datos solicitados en el formulario y las 6 imagenes, proceda a dar *click* en el botón Guardar para enrolar a la persona.

Notificación
El sistema cuenta con un envió automático diario de reportes vía correo electrónico, de las personas no reconocidas, a continuación se muestra el formato de la notificación:


Inbox

Sistema de Reconocimiento Facial de la UCSG

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

Personas No Reconocidas

Transacciones: [

Hora :2016-08-03 20:55:49.0 Imagen: link,

Hora :2016-08-03 19:55:50.0 Imagen: link,

Hora :2016-08-03 17:55:50.0 Imagen: link]

En este correo se especifica: la hora de transacción y el link que vincula la imagen de la persona detectada para ser visualizada.

DECLARACIÓN Y AUTORIZACIÓN

Nosotros, **Solis Calvopiña, Liliana Nathaly,** C.C: # **0926477472 y Puga Torres, Luiggi Ramiro**, con C.C: # **0924036965,** autores del trabajo de titulación: **Control de Seguridad Biométrico de Reconocimiento Facial como Caso de Estudio Implementación en el Área Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil** previo a la obtención del título de **INGENIERO EN SISTEMAS COMPUTACIONALES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaramos tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizamos a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, **22** de **Septiembre** del **2016**

f. _____
Nombre: **Solis Calvopiña, Liliana Nathaly**
C.C: **0926477472**

f. _____
Nombre: **Puga Torres, Luiggi Ramiro**
C.C: **0924036965**

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Control de Seguridad Biométrico de Reconocimiento Facial como Caso de Estudio Implementación en el Área Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil		
AUTOR(ES)	Solis Calvopiña, Liliana Nathaly ; Puga Torres, Luiggi Ramiro		
REVISOR(ES)/TUTOR(ES)	Murillo Bajaña, Eduardo Wenceslao		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Ingeniería		
CARRERA:	Carrera de Ingeniería en Sistemas Computacionales		
TITULO OBTENIDO:	Ingeniero en Sistemas Computacionales		
FECHA DE PUBLICACIÓN:		**No. DE PÁGINAS:**	107
ÁREAS TEMÁTICAS:	Sistema Control de Seguridad, Desarrollo de Sistemas		
PALABRAS CLAVES/ KEYWORDS:	DETECCIÓN DE CARAS; RECONOCIMIENTO FACIAL; SEGURIDAD DEL PERSONAL LABORAL; LIBRERÍA OPENCV; CARACTERÍSTICAS HAAR; BIOMÉTRICO, API KAIROS.		

RESUMEN/ABSTRACT (150-250 palabras):

La aplicación de este proyecto está orientada a salvaguardar la seguridad del personal laboral, basado en la detección y reconocimiento facial automático de las personas que ingresan y egresan al Área Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil.

Su diseño se basa en un sistema control de seguridad biométrico de reconocimiento facial. Este cuenta con dos herramientas principales; la librería OpenCV que permite la detección de caras bajo la aplicación de Característicos Haar, y el uso del API Kairos, el cual brinda el servicio de reconocimiento facial a través de la recepción de peticiones con el rostro detectado para identificar si coincide o no con uno de los rostros previamente enrolados.

El administrador podrá enrolar las imágenes de los rostros de las personas autorizadas con sus datos; consultar los registros de detecciones de personas reconocidas y no reconocidas, así como visualizar la lista de las personas enroladas; por último, recibirá diariamente por correo electrónico un informe de las personas no reconocidas.

Para la elaboración de este proyecto se usó el tipo de investigación descriptiva, y para la recolección de datos se aplicaron instrumentos como: encuestas, entrevistas y observaciones. Las encuestas y entrevistas permitieron corroborar la necesidad de la implementación de un sistema control de seguridad y las observaciones directas de las pruebas de funcionamiento del equipo para comprobar la efectividad del proyecto.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-997440036 +593-996504339	E-mail: lilinathy_4@hotmail.com pugaluiggi@gmail.com
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre:** Valencia Macías, Lorgia del Pilar	
	Teléfono: +593-4-2206950 ext. 1020	
	E-mail: lorgia.valencia@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	