ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

CARRERA INFORMÁTICA

TESIS PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN INFORMÁTICA

TEMA:

SISTEMA DE VIGILANCIA MEDIANTE CÁMARAS IP EN LAS OFICINAS DE LA CAPITANÍA DEL PUERTO DE LA CIUDAD DE MANTA

AUTORA:

GEMA VICTORIA ZAMBRANO ZAMBRANO

TUTOR:

ING. ÁNGEL ALBERTO VÉLEZ MERO

CALCETA, ABRIL 2014

DERECHOS DE AUTORÍA

Gema Victoria Zambrano Zambrano declaro bajo juramento que el trabajo aquí descrito es de mi autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Ley de Propiedad Intelectual y su reglamento.

…….

GEMA V. ZAMBRANO ZAMBRANO

CERTIFICACIÓN DEL TUTOR

Ángel Alberto Vélez Mero certifica haber tutelado la tesis **SISTEMA DE VIGILANCIA MEDIANTE CÁMARAS IP EN LAS OFICINAS DE LA CAPITANÍA DEL PUERTO DE LA CIUDAD DE MANTA**, que ha sido desarrollada por Gema Victoria Zambrano Zambrano, previa a la obtención del título de Ingeneria en Informática, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Féliz López.

……..

ING. ÁNGEL A.VÉLEZ MERO

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaran que han **APROBADO** la tesis **SISTEMA DE VIGILANCIA MEDIANTE CÁMARAS IP EN LAS OFICINAS DE LA CAPITANÍA DEL PUERTO DE LA CIUDAD DE MANTA**, que ha sido propuesta, desarrollada y sustentada por Gema Victoria Zambrano Zambrano, previa a la obtención del título de Ingeniería en Informática, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

……	**……**
Ing. Edys Solórzano Intriago	Ing. Orlando Ayala Pullas
MIEMBRO	**MIEMBRO**

……

Ing. Daniel A. Mera Martínez

PRESIDENTE

AGRADECIMIENTO

Expreso mis más sinceros agradecimientos a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López que me dio la oportunidad de una educación superior de calidad y en la cual he forjado mis conocimientos profesionales día a día; además de brindarme la oportunidad de ser parte de esta familia politécnica la cual me motiva a esforzarme día a día para ser una gran profesional.

A mí querido Dios, porque es quién me ha dado la oportunidad de vivir y ser feliz, y ha estado conmigo en la realización de este trabajo, además ha sido mi sustento, apoyo y fortaleza.

A mis padres, porque gracias a sus esfuerzos, me han dado la oportunidad de estudiar, de prepararme para el presente y el futuro de mi vida; y me han enseñado valiosos valores de fe, amor e integridad que los he puesto en práctica y que estarán siempre presentes en el camino de mi vida.

A los profesores por impartir e innovar sus conocimientos y así poner en práctica las enseñanzas aprendidas en clases y sobre todo por su apoyo en todas las circunstancias.

Y a todas las personas que de un modo u otre han apoyado en la realización de este trabajo, logrando contribuir con mucha paciencia y orientación para la conclusión de esta meta.

.....

Gema V. Zambrano Zambrano

DEDICATORIA

Todo el esfuerzo, dedicación y empeño que he puesto en este trabajo, se lo dedico a mi querido Dios, quién siempre ha estado a mi lado y me ha dado la sabiduría, conocimientos, las fuerzas y el apoyo necesario para terminar exitosamente este trabajo.

A mis adorables padres, por toda la entrega personal que siempre me han dado, porque han sido el ejemplo más grande de mi vida y su amor me ha llenado de mucha felicidad; ya que siempre han sido la luz que guían mis pasos para el camino del éxito y del bien.

A mis queridos Abuelos que desde el cielo guían mis pasos y que estuvieron en los momentos más felices de mi vida, el logro del presente trabajo es primordialmente para ellos.

A mis verdaderos amigos que aunque estén distantes, lejos ellos me han apoyado en cualquier circunstancia de mi vida y siempre han estado en los momentos más difíciles.

A mis profesores que me brindan sus conocimientos permitiéndome adquirir nuevas enseñanzas para ponerlas en práctica y continuar contribuyendo con el desarrollo de la sociedad.

La vida nos pone muchas pruebas pero estas no son un final, lo importante es seguir adelante con seguridad y no detenerse, y sobre todo vencer los obstáculos y confiar totalmente en Dios, quién es nuestra fortaleza.

.....

Gema V. Zambrano Zambrano

CONTENIDO GENERAL

CONTENIDO DE CUADROS Y FIGURAS

RESUMEN

El presente trabajo de tesis tuvo como objetivo Implementar un sistema de vigilancia basado en cámaras IP en la Capitanía del Puerto de la ciudad de Manta, el cual obtuvo una eficaz captura de imágenes y videos mediante un software de detección de rostro. Este sistema permite tener una base de datos de cada una de las personas que ingresan a la entidad, logrando monitorear todo lo que transcurre en las oficinas donde se encuentran ubicadas las cámaras de seguridad. Para la realización del software e implementación del sistema de vigilancia se llevó a cabo mediante la metodología de Ciclo de Vida en V y la ITIL, las cuales se desarrollaron mediante fases, así mismo como las medidas técnicas necesarias para éste alcance. Sin embargo para la recopilación de la información se trabajó en base al método científico inductivo-deductivo, que permitió generar las estipulaciones y llevar un análisis de la problemática planteada en base a los requerimientos de la institución, siendo necesario desarrollar un software de detección de rostro mediante códigos empleados en Java y framework como opencv y javacv, el cual fue diseñado para ser monitoreado por las cámaras de seguridad Trendnet TV-IP551W. El sistema es una aplicación útil y de fácil manipulación que permite acceder de forma remota a las imágenes guardadas así como a controlar e identificar las personas que ingresan y detectar si alguna de estas se encuentra realizando cualquier tipo de actividad que ponga en riesgo el funcionamiento adecuado de los procesos que se realicen dentro de sus oficinas.

PALABRAS CLAVES

Sistema de Vigilancia, Detección de Rostro, Monitoreo de Cámaras.

ABSTRACT

This thesis aimed to implement a surveillance system based on IP cameras at the Port Authority of Manta's city, which obtained effective capture images and videos using a face detection software. This system allows a database of each people who enter the institution, achieving monitor everything that takes place in the offices where the cameras are located above. To carry out the software and implementation of the monitoring system was conducted using the methodology of Life Cycle V and ITIL, which were developed through stages himself as the technical measures necessary for this scope. However for the collection of information is worked based on the inductive-deductive scientific method, which allowed the generation of the provisions and an analysis of the issues raised based on the requirements of the institution, being necessary to develop a software face detection codes used by Java and framework as opencv and javacv, which was designed to be monitored by security cameras Trendnet TV- IP551W. The system is a useful and easy to handle application that allows remote access to the stored images and to control and identify people entering and detect if any of these is performing any activity that threatens the proper functioning of the processes that take place within their offices.

KEY WORDS

Surveillance System, Face Detection, Monitoring Cameras.

CAPÍTULO I. ANTECEDENTES

1.1 PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

El avance de la tecnología ha permitido ser testigos de cómo el mundo cambia rápidamente, y el mercado tecnológico de seguridad es un sector que está en constante crecimiento además de que el mundo detrás de las cámaras de seguridad está en plena evolución. La tendencia de los sistemas de seguridad va hacia la miniaturización de las herramientas individuales, tales como cámaras, micrófonos y diversos dispositivos de uso personal; que buscan entregarles confianza y tranquilidad a los usuarios.

Cuando es necesario tener un control en el hogar e industria concerniente a la seguridad y a la administración de la misma, es imperativo el desarrollo de sistemas de vigilancia que contribuyan a tener una confianza en el cuidado de los bienes e individuos, además de la utilización de tecnología muy empleada y común para los usuarios, debido a que en más de una ocasión, los sistemas de supervisión se han convertido en los aliados perfectos de los cuerpos de seguridad, ya que las grabaciones han servido para evitar delitos, o como indicio para conseguir pruebas en el caso de que éstos se hayan producido.

La Capitanía del Puerto de Manta es una dependencia encargada de brindar servicios como matriculación marítima, búsqueda y rescate, servicio móvil, marítimo y auxilio marítimo, como toda institución que acoge a muchas personas a diario, se enfrenta al problema de mantener un control sobre las actividades que se realizan dentro de sus instalaciones sin tener los medios suficientes para poder efectuar un control eficaz dentro de sus oficinas.

Sin embargo cabe recalcar que la Capitanía posee equipos de elevado valor, tanto económico como operativo, este último debido a la información que se encuentra almacenada en ellos; ya que existe el acceso de personas desconocidas dentro de sus instalaciones, persistiendo el riesgo de que se presenten eventualidades no deseadas dentro de la institución.

Es por ello que se procuró establecer un método o una herramienta tecnológica que proporciona el control u observación en tiempo real de los movimientos que se realizan además de observar las personas que ingresan a las áreas de administración, jurídico, contabilidad, recaudación y atención al cliente mediante un software facial reconociendo de esta manera el tipo de persona que se acerca a realizar las diferentes operaciones; sabiendo que en cada una de las áreas se establece una atención de 100 personas al día y mientras que en el área de recaudación se atiende a 150 personas diarias.

Por la razón antes mencionada la autora del presente proyecto se plantea la siguiente interrogante:

¿De qué manera se puede controlar la vigilancia dentro de las oficinas de la Capitanía del Puerto de la ciudad de Manta?

1.2 JUSTIFICACIÓN

La Capitanía del Puerto de Manta es una entidad encargada de resguardar y preservar las costas de la provincia, así mismo de que los pescadores legalicen sus documentos y embarcaciones, siendo esto uno de los requerimientos primordiales para que los navegadores y pescadores realicen sus actividades dentro de las costas marítimas.

Sin embargo dentro de esta entidad se encuentran inconvenientes que alteran las normas, como lo es que surgían tramitadores que intervenían para agilizar los procedimientos de ciertos usuarios de una manera no correcta. Es por ello que la realización de este plan surgió con el fin de implementar un sistema de vigilancia mediante cámaras IP basado en un software de detección de rostros, lo cual dio a una mayor protección de los recursos disponibles en los departamentos y así mismo dar a conocer los acontecimientos y procesos que se efectúen en estos.

De acuerdo al reglamento para la elaboración de proyecto de tesis de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, en su artículo 1, que indica, “Todo tema de tesis de grado estará relacionado con las líneas de investigación de la carrera del postulante y enmarcado en las áreas y prioridades de investigación establecidas por la ESPAM MFL, en concordancia con el Plan Nacional de Desarrollo”, se llevó a cabo la elaboración del presente proyecto.

La vigilancia con cámaras permitió capturar y ver video a usuarios autorizados gestionar que las actividades se realizan con normalidad, además cuenta con un software facial que ayuda a detectar el rostro de las personas que se encuentran en el área de atención al cliente, beneficiando de esta manera a toda la entidad. Sin embargo la implementación de esta tecnología de supervisión ayudó a contribuir con el ambiente debido a que los dispositivos informáticos al emplearse no generan flatulencias tóxicas que destruyan la percepción del entorno.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Implementar sistema de vigilancia basado en cámaras IP en la Capitanía del Puerto de la ciudad de Manta, para mejorar la seguridad dentro de sus oficinas mediante un software facial que identifique a las personas que ingresan a esta entidad.

1.3.2. OBJETIVOS ESPECÍFICOS

- Analizar el seguimiento de las operaciones que se realizan dentro de la Capitanía del Puerto de Manta.

- Diseñar los puntos o estructuras estratégicas para la ubicación de las cámaras dentro de las áreas de la oficina y determinar los equipos necesarios para la instalación de las cámaras IP.

- Desarrollar el software facial que permita identificar la detección de rostro de las personas que ingresen en la entidad.

- Implementar el sistema de detección de rostro verificando su adecuado funcionamiento.

1.4 DEAS A DEFENDER

- La seguridad con cámaras IP mejoró la vigilancia dentro de las oficinas de la Capitanía a través de un software facial que les facilitó el reconocimiento de las personas que ingresen a esta y así llevar al tanto las actividades que realice el personal.

- El sistema de vigilancia permitió identificar a ciertas personas que ingresaban a la Capitanía con el fin de agilizar los trámites de ciertos usuarios y así mismo llevar una inspección de que los costos de cancelación de las diligencias que se realicen sean los correctos.

CAPÍTULO II. MARCO TEÓRICO

2.1. INTRODUCCIÓN SEGURIDAD INFORMÁTICA

En la actualidad la tecnología de la información es sin lugar a dudas, lo que más rápidamente ha evolucionado en el mundo, siendo base importante en las operaciones administrativas y financieras de las empresas de hoy, cambiando los hábitos de las personas, lanzándolas a realizar transacciones en Internet de todo tipo, en forma automática, sin intermediarios y en cualquier lugar. Todo este nuevo mundo digital necesita que existan mecanismos que controlen la legitimidad de la información y que aseguren que la misma no ha sido cambiada o alterada (Amaya, 2007).

Es por este motivo que la seguridad informática juega un rol muy importante dentro del mundo informático y es debido a esto que las empresas recientemente han comenzado a demandar especialistas con conocimientos del más alto nivel en el campo de la Seguridad Informática (MSIA, 2011).

Generalmente, la seguridad informática consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

La seguridad informática se resume, por lo general, en cinco objetivos principales:

- Integridad: garantizar que los datos sean los que se supone que son

- Confidencialidad: asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian

- Disponibilidad: garantizar el correcto funcionamiento de los sistemas de información

- Evitar el rechazo: garantizar de que no pueda negar una operación realizada.

- Autenticación: asegurar que sólo los individuos autorizados tengan acceso a los recursos (Kioskea, 2010).

2.1.1 SEGURIDAD INFORMÁTICA

Según Cantú, (2011) define a la seguridad informática como una punta principal al iniciar desde un simple proyecto computacional ya sea software o hardware, hasta la implementación de aplicaciones, redes, o cualquier cosa que pueda ser escalón para atentar contra la seguridad.

La información es una de las cuestiones principales que resguarda el tema de seguridad informática, asumiendo que toda información en cualquier cantidad se desee tener a la mano sin importar distancias, esto conlleva a la utilización de equipos de cómputo conectados a Internet, donde pueden ser comprometidos sin una previa revisión del mismo sistema o red (Trujillo, 2009).

Sin embargo para Voutssas, (2010) describe que para poder comprender el concepto integral de la seguridad informática, es indispensable entender los diversos conceptos básicos que la rigen, ya que de otra forma no es posible establecer una base de estudio.

• Recursos Informáticos: el equipo de cómputo y telecomunicaciones; los sistemas, programas y aplicaciones, así como los datos e información de una organización. También se les conoce como "activos informáticos"

• Amenaza: fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los recursos informáticos de la organización.

• Impacto: la medida del efecto nocivo de un evento.

• Vulnerabilidad: característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza.

• Riesgo: la probabilidad de que un evento nocivo ocurra combinado con su impacto en la organización.

• Principio básico de la seguridad informática: la seguridad informática no es un producto, es un proceso.

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Conviene aclarar que no siendo posible la certeza absoluta, el elemento de riesgo está siempre presente, independientemente de las medidas que se tomen. La seguridad absoluta no es posible entonces la seguridad informática es un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos, y que misma necesita de un alto nivel de organización por lo que se puede resumir: Sistema de seguridad = Tecnología + Organización (Ávila, *et al.* 2009).

Lo importante es proteger la información, si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque (hardware, software y datos), son los datos y la información los objetivos principales de protección de las técnicas de seguridad. La seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad y disponibilidad de la información (Morejón, *et al.* 2008).

Según la definición Mojsiejczuk, (2007) la seguridad es la cualidad de seguro, y seguro es algo libre y exento de todo peligro, daño o riesgo. Entonces se puede decir que la seguridad informática es un sistema informático exento de peligro.

Sin embargo se debe tener en cuenta que la seguridad no es un producto sino un proceso, por lo tanto se puede definir a la seguridad informática como: un conjunto de métodos y herramientas destinados a proteger la información y por

ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas (Velasco, 2008).

De acuerdo a las definiciones estipuladas anteriormente la autora concluye que la seguridad informática es el área en donde relaciona diversas técnicas o métodos para asegurar la integridad de la información de datos o bienes (Moreno, 2011).

2.1.2 FUNCIÓN DE SEGURIDAD INFORMÁTICA

La función de la seguridad informática permite llevar a toda institución normas de control y procedimientos que se le faciliten a estas que lleven a cabo un acuerdo sobre la mejor manera de organizar un área de seguridad informática en una empresa (ITI, 2009).

En las organizaciones se requiere gestionar la seguridad informática para asegurar un entorno informático institucional, mediante la administración del recurso humano y tecnológico, para ello es necesario emplear dispositivos reguladores de las funciones y actividades desarrolladas por el personal de la institución (Villegas, *et al*. 2011).

2.1.2.1 COMPONENTES PRINCIPALES DE UN ÁREA DE SEGURIDAD INFORMÁTICA

Según la definición de Tipantuña, (2010).Existen diversas funciones que debe desempeñar un área de seguridad informática y éstas se pueden agrupar de la siguiente manera:

a) Normatividad
b) Operaciones (O Producción)
c) Supervisión (O Soporte)
d) Desarrollo

Hay un par de áreas que no son tan comunes: normatividad y desarrollo. Al revisar las responsabilidades y funciones de cada área quedará más claro el por qué. Por lo pronto les comento que es menos probable encontrar estas 2

áreas en empresas medianas o pequeñas, mientras que en empresas grandes es más común que existan las 4 áreas junto con la figura del líder de área.
Líder de área: Esta figura, a la cual se le suele conocer como CISO (Chief Information Security Officer - Oficial de Seguridad informática). Entre sus responsabilidades se encuentran:

- Administración del presupuesto de seguridad informática
- Administración del personal
- Definición de la estrategia de seguridad informática (hacia dónde hay que ir y qué hay que hacer) y objetivos
- Administración de proyectos
- Detección de necesidades y vulnerabilidades de seguridad desde el punto de vista del negocio y su solución

El líder es quien define, de forma general, la forma de resolver y prevenir problemas de seguridad con el mejor costo beneficio para la empresa.

A. Normatividad -Es el área responsable de la documentación de políticas, procedimientos y estándares de seguridad así como del cumplimiento con estándares internacionales y regulaciones que apliquen a la organización. Dado que debe interactuar de forma directa con otras áreas de seguridad y garantizar cumplimiento, es conveniente que no quede al mismo nivel que el resto de las áreas pero todas reportan al CISO. Por esta razón se le suele ver como un área que asiste al CISO en las labores de cumplimiento.

B. Operaciones -Es el área a cargo de llevar a cabo las acciones congruentes con la estrategia definida por el CISO lograr los objetivos del área (en otras palabras, la "gente que está en la trinchera").

Entre sus responsabilidades se encuentran:

- Implementación, configuración y operación de los controles de seguridad informática (Firewalls, IPS/IDS, antimalware, etc.)

- Monitoreo de indicadores de controles de seguridad
- Primer nivel de respuesta ante incidentes (típicamente a través de acciones en los controles
- de seguridad que operan)
- Soporte a usuarios
- Alta, baja y modificación de accesos a sistemas y aplicaciones
- Gestión de parches de seguridad informática (pruebas e instalación)

C. Supervisión -Es el área responsable de verificar el correcto funcionamiento de las medidas de seguridad así como del cumplimiento de las normas y leyes correspondientes (en otras palabras, brazo derecho del área de normatividad).

Entre sus responsabilidades se encuentran:

- Evaluaciones de efectividad de controles
- Evaluaciones de cumplimiento con normas de seguridad
- Investigación de incidentes de seguridad y cómputo forense (2° nivel de respuesta ante incidentes)
- Atención de auditores y consultores de seguridad

D. Desarrollo -Es el área responsable del diseño, desarrollo y adecuación de controles de seguridad informática (típicamente controles de software).

Entre sus responsabilidades se encuentran:

- Diseño y programación de controles de seguridad (control de acceso, funciones criptográficas, filtros, bitácoras de seguridad de aplicativos, etc.)
- Preparación de librerías con funciones de seguridad para su uso por parte del área de Desarrollo de Sistemas,
- Soporte de seguridad para el área de Desarrollo de Sistemas
- Consultoría de desarrollos seguros (integración de seguridad en aplicaciones desarrolladas por Sistemas) (AEPD, s. f).

Básicamente se trata de un área de desarrollo enfocada a cuestiones de seguridad. La razón de requerir un área dedicada para esto es que la integración de controles efectivos en software es una tarea muy compleja; el perfil de un programador promedio no incluye experiencia ni conocimientos en seguridad (y particularmente en criptografía). Esta es la razón por la cual sólo las grandes empresas cuentan con un área de desarrollo de seguridad que está formada por especialistas en vez de programadores ordinarios (Salazar, 2009).

2.1.3 SISTEMAS DE VIGILANCIA

En los últimos años, la vigilancia controlada remotamente es una de las más solicitadas en el mundo de la seguridad, ya que es un recurso fácil, efectivo y directo de poder saber lo que está ocurriendo en nuestra casa o negocio. La video vigilancia o televigilancia se trata de poder tener acceso a las imágenes que envían las cámaras de un determinado espacio a través de nuestro propio ordenador o monitor de televisión (Gocella, 2009).

Según la definición de Cachiguango, (2010). En la actualidad, los niveles de inseguridad en nuestro país ha promovido a la creación de entornos con sistemas de captura de imágenes; convirtiéndose los sistemas de video vigilancia en un vital componente de Ia segundad, supervisión y control de acceso, reducción del riesgo de robo, daño a bienes o a personas e inclusive han llegado a convertirse para muchas empresas, en una buena alternativa de manejo y control de actividades de su personal, siendo cada vez más comunes en los edificios de oficinas, estructuras externas, escuelas, hoteles, hosterias, incluso en calles de una ciudad.

La vigilancia y Ia seguridad son temas que han adquirido mayor relevancia. Cada día más y más personas demandan de un completo sistema de vigilancia, que permita evitar los delitos o poder identificar a los autores de un robo.

2.1.3.1 VIDEO VIGILANCIA

La videovigilancia es un sistema que sirve para supervisar su casa o negocio a distancia sin necesidad de tener un ordenador instalado en el lugar vigilado, sólo con disponer de una conexión a Internet y una toma de corriente eléctrica. La Videovigilancia le permite conectarse a un dispositivo (servidor Web de vídeo) provisto de cámaras desde cualquier lugar para visualizar lugares diversos como empresas, comercios, hogares, etc. proporcionándole además acceso para gestionar el equipo y poder realizar cambios en su configuración, recuperar imágenes grabadas o en tiempo real (Gocella, 2009).

La implementación y el uso de la video-vigilancia (tecnología de Circuito Cerrado de Televisión - CCTV) en las sociedades alrededor del mundo, ha estimulado un gran debate en varios tópicos (Vivien, 2008).

2.2. CÁMARAS DE SEGURIDAD

Las cámaras de vigilancia o cámaras de seguridad son cámaras de video que se emplean para video-vigilancia, es decir, para llevar a cabo tareas de monitoreo y observación visual a distancia de personas, objetos o procesos con fines de control de seguridad. Las cámaras de vigilancia pueden ser analógicas, digitales, cámaras IP o mini-cámaras y se emplean en sistemas de CCTV (Circuito cerrado de televisión), video-vigilancia IP, espionaje mediante cámara oculta, reconocimiento aéreo o satélites espía (Berns. 2011).

Según Valeriano, (2011) las Cámaras son videocámaras especialmente diseñadas para enviar las señales (video, y en algunos casos audio) a través de Internet desde un explorador (por ejemplo el Internet Explorer) o a través de concentrador (un HUB o un SWITCH) en una Red Local (LAN).

En las cámaras se pueden integrarse aplicaciones como detección de presencia (incluso el envío de mail si detectan presencia), grabación de imágenes o secuencias en equipos informáticos (tanto en una red local o en una red externa (WAN), de manera que se pueda comprobar por qué ha

saltado la detección de presencia y se graben imágenes de lo sucedido (Fuente, *et al.* 2005).

De acuerdo a lo mencionado la autora define que las cámaras de seguridad como cámaras de video que se emplean para monitorear u observar los diferentes procedimientos de acuerdo en el lugar donde estén ubicadas (Herrera, 2005).

2.2.1 CÁMARAS IP

Las cámaras IP son dispositivos autónomos que cuentan con un servidor web de video incorporado, lo que les permite transmitir su imagen a través de redes IP como redes Lan, Wan e Internet. Las cámaras IP permiten al usuario tener la cámara en una localización y ver el vídeo en tiempo real desde otro lugar a través de Internet (Avila, *et al.*2009)

Las cámaras IP tienen incorporado un ordenador, pequeño y especializado en ejecutar aplicaciones de red. Por lo tanto, la cámara IP no necesita estar conectada a un PC para funcionar. Esta es una de sus diferencias con las denominadas cámaras web. (AI, 2005).

Según Richarte, (2012) estipula que las cámaras IP, también conocidas como cámaras de red o, simplemente, netcams, han pasado de ser un costoso dispositivo a convertirse en muy poco tiempo en un elemento imprescindible para la seguridad del hog además puede describirse como una cámara y un ordenador combinados para formar una única unidad. Los componentes principales que integran este tipo de cámaras de red incluyen un objetivo, un sensor de imagen y uno o más procesadores y memoria (Albusac, 2008).

Una cámara IP ó también conocida como cámara de red puede ser descrita como la combinación de una cámara y una computadora en una sola unidad, la cual captura y transmite imágenes en vivo a través de una red IP, habilitando a usuarios autorizados a ver, almacenar y administrar el video sobre una infraestructura de red estándar basada en el protocolo IP (Urrutia, 2011).

2.2.1.1 TIPOS DE CÁMARAS IP

Hay diferentes clases de cámaras de red, que pueden servir a las distintas necesidades de cada usuario, hogar, oficina o corporación.

- Cámaras Fijas.
- Cámaras Poe.
- Cámaras Hd.
- Cámaras Móviles.
- Cámaras Para Exterior (Izquierdo, *et al.* 2012).

2.2.1.2 VENTAJAS DE LAS CÁMARAS IP

- Las cámaras IP ofrecen mayor resolución que las cámaras de video tradicionales o webcams
- Las cámaras IP permiten ver en tiempo real qué está pasando en un lugar, aunque usted esté a miles de kilómetros de distancia.
- Las cámaras IP pueden ser vistas sólo por las personas autorizadas. También se puede ofrecer acceso libre y abierto si el vídeo en directo se desea incorporar al web site de una compañía para que todos los internautas tengan acceso.
- Algunas cámaras IP disponen de un filtro de infrarrojos automático, este filtro se coloca delante del ccd sólo cuando las condiciones de luz son adecuadas proporcionándonos de esta manera imágenes en color, cuando las condiciones de luz bajan este filtro se desplaza y la cámara emite la señal en blanco y negro produciendo más luminosidad y de esta manera podemos iluminar la escena con luz infrarroja y ver en total oscuridad.
- Algunas cámaras IP tienen sensor de movimiento
- Las cámaras IP gestionan la exposición (el nivel de luz de la imagen), el equilibrio de blancos (el ajuste de los niveles de color), la nitidez de la imagen y otros aspectos de la calidad de la imagen (AI, 2005).

2.2.2 TRANSMISIÓN SOBRE UNA RED IP EN TIEMPO REAL

La principal característica de una transmisión por red en tiempo real es la necesidad de velocidad, por encima de cualquier otro aspecto. Es vital que el flujo de datos pueda transmitirse al mismo tiempo que se genera, porque si se retrasa dejaría de considerarse "tiempo real" (Zambrano, 2009).

Esto conlleva que si un paquete se pierde es mejor descartarlo, porque si se vuelve a enviar se producen retrasos. Es mejor perder una cantidad mínima de paquetes, que produzcan algún error aceptable en destino, que no controlar las pérdidas e ir realizando esperas de paquetes reenviados. Si las pérdidas son muy severas, siempre se puede reducir la calidad de la señal, para bajar el ancho de banda y las pérdidas (Laurenciano, 2011).

El paralelismo más claro es compararlo con una llamada de teléfono. La red ha de permitir que la voz se transmita sin esperas, porque de lo contrario no sería posible la comunicación en tiempo real. Es mejor perder algún dato y que en algún momento se oiga algún ruido, que no provocar esperas incómodas como si fuese un walkie-talkie (Fernández, 2011).

2.3 RECONOCIMIENTO FACIAL

-Características del Autentificador: Responde a una característica de tipo morfológico variable con el tiempo. En particular, la estructura facial responde a dos tipos de cambios temporales: La variación no agresiva, característica del crecimiento y del envejecimiento del individuo (variación caracterizada por aparecer de forma relativamente lenta), y la variación agresiva, debida principalmente a factores como operaciones de cirugía estética, accidentes, etc, de acción prácticamente inmediata (Salas, 2011).

-Sistema de Reconocimiento: Los sistemas de reconocimiento facial están englobados dentro de las técnicas FRT (Face RecognitionThecniques). Estas técnicas de aproximación al reconocimiento facial, pueden clasificarse en dos categorías según el tipo de aproximación holística o analítica. La

aproximación holística (método de las eigen faces) considera les propiedades globales del patrón, mientras que la segunda considera un conjunto de características geométricas de la cara (Herrera, 2005). Existen dos divisiones de este segundo tipo de aproximación: la basada en los vectores característicos extraídos del perfil, y la basada en los vectores característicos extraídos a partir de una vista frontal de la cara (Espinoza, 2001).

El rostro humano es un objeto dinámico que tiene un alto grado de variabilidad en su apariencia lo cual hace que su detección sea un problema difícil de tratar en visión por computador (Arguello, 2011).

2.3.1 EXTRACCIÓN DE CARACTERÍSTICAS

Una de las partes más importantes en un sistema de reconocimiento lo constituye la extracción de características.

Estos sistemas podrían ser clasificados en tres categorías: Los que trabajan con imágenes fijas, señales de vídeo normalmente de baja resolución y los que trabajan con imágenes 3D de la cabeza. Es importante resaltar que es difícil comparar cada una de estas categorías, ya que las investigaciones de cada una de ellas se realizan sobre bases de datos totalmente diferentes (Arguello, 2011).

2.3.2CLASIFICACIÓN DE EXPRESIONES FACIALES

Como algoritmo de decisión multiclase se emplea un clasificador sencillo con el fin de dar mayor importancia a las características, en particular se usa un clasificador estadístico basado en el vecino más cercano (KNN), el cual visto de un modo práctico encuentra los k patrones del conjunto de entrenamiento más próximos al patrón observación con una métrica dada (para el caso de este estudio la distancia Euclidiana), anota las clases a las que pertenecen dichos patrones y decide por votación mayoritaria entre las clases de los k patrones (Alvarez; Guevara, 2009).

2.4 CICLOS DE VIDA DE DESARROLLO

Según la definición de INTECO, (2009). El ciclo de vida es el conjunto de fases por las que pasa el sistema que se está desarrollando desde que nace la idea inicial hasta que el software es retirado o remplazado (muere). También se denomina a veces paradigma. Entre las funciones que debe tener un ciclo de vida se pueden destacar:

- Determinar el orden de las fases del proceso de software
- Establecer los criterios de transición para pasar de una fase a la siguiente
- Definir las entradas y salidas de cada fase
- Describir los estados por los que pasa el producto
- Describir las actividades a realizar para transformar el producto
- Definir un esquema que sirve como base para planificar, organizar, coordinar, desarrollar.

Un ciclo de vida para un proyecto se compone de fases sucesivas compuestas por tareas que se pueden planificar. Según el modelo de ciclo de vida, la sucesión de fases puede ampliarse con bucles de realimentación, de manera que lo que conceptualmente se considera una misma fase se pueda ejecutar más de una vez a lo largo de un proyecto, recibiendo en cada pasada de ejecución aportaciones a los resultados intermedios que se van produciendo (realimentación).

Fases: una fase es un conjunto de actividades relacionadas con un objetivo en el desarrollo del proyecto. Se construye agrupando tareas (actividades elementales) que pueden compartir un tramo determinado del tiempo de vida de un proyecto. La agrupación temporal de tareas impone requisitos temporales correspondientes a la asignación de recursos (humanos, financieros o materiales).

Entregables: son los productos intermedios que generan las fases. Pueden ser materiales o inmateriales (documentos, software). Los entregables permiten

evaluar la marcha del proyecto mediante comprobaciones de su adecuación o no a los requisitos funcionales y de condiciones de realización previamente establecidos.

2.4.1 MODELO EN V

El modelo en v se desarrolló para terminar con algunos de los problemas que se vieron utilizando el enfoque de cascada tradicional. Los defectos estaban siendo encontrados demasiado tarde en el ciclo de vida, ya que las pruebas no se introducían hasta el final del proyecto. El modelo en v dice que las pruebas necesitan empezarse lo más pronto posible en el ciclo de vida. También muestra que las pruebas no son sólo una actividad basada en la ejecución. Estas actividades deberían ser llevadas a cabo en paralelo con las actividades de desarrollo, y los técnicos de pruebas necesitan trabajar con los desarrolladores y analistas de negocio de tal forma que puedan realizar estas actividades y tareas y producir una serie de entregables de pruebas. Los productos de trabajo generados por los desarrolladores y analistas de negocio durante el desarrollo son las bases de las pruebas en uno o más niveles. El modelo en v es un modelo que ilustra cómo las actividades de prueba (verificación y validación) se pueden integrar en cada fase del ciclo de vida. Dentro del modelo en v, las pruebas de validación tienen lugar especialmente durante las etapas tempranas, por ejemplo, revisando los requisitos de usuario y después por ejemplo, durante las pruebas de aceptación de usuario.

El modelo en v es un proceso que representa la secuencia de pasos en el desarrollo del ciclo de vida de un proyecto. Describe las actividades y resultados que han de ser producidos durante el desarrollo del producto. La parte izquierda de la v representa la descomposición de los requisitos y la creación de las especificaciones del sistema. El lado derecho de la v representa la integración de partes y su verificación. V significa “Validación y Verificación”.

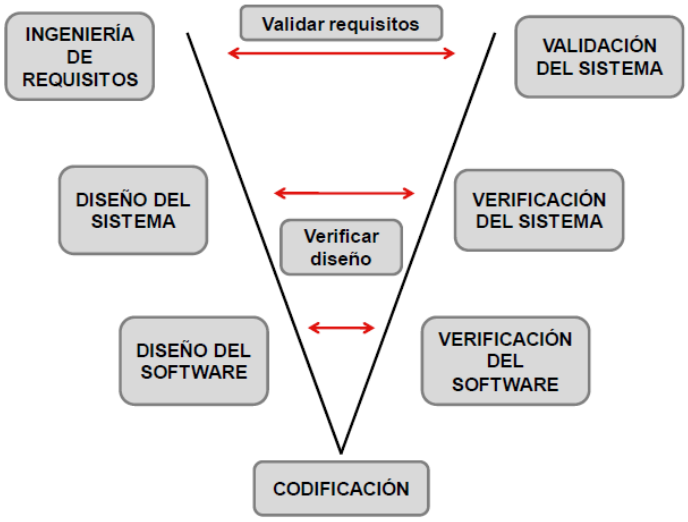


Figura.02.01 Modelo del Ciclo de Vida en V

Fuente: INTECO, 2009

Realmente las etapas individuales del proceso pueden ser casi las mismas que las del modelo en cascada. Sin embargo hay una gran diferencia. En vez de ir para abajo de una forma lineal las fases del proceso vuelven hacia arriba tras la fase de codificación, formando una v. La razón de esto es que para cada una de las fases de diseño se ha encontrado que hay un homólogo en las fases de pruebas que se correlacionan (INTECO, 2009).

2.4. 2 VENTAJAS

Las ventajas que se pueden destacar de este modelo son las siguientes:

- Es un modelo simple y fácil de utilizar.
- En cada una de las fases hay entregables específicos.
- Tiene una alta oportunidad de éxito sobre el modelo en cascada debido al desarrollo de planes de prueba en etapas tempranas del ciclo de vida.
- Es un modelo que suele funcionar bien para proyectos pequeños donde los requisitos son entendidos fácilmente (INTECO, 2009).

2.5 LIBRERÍA OPENCV

2.5.1 HISTORIA

El 13 de Junio del 2000, Intel® Corporation anunció que estaba trabajando con un grupo de reconocidos investigadores en visión por computador para realizar una nueva librería de estructuras/funciones en lenguaje C. Este anuncio tuvo lugar en la apertura del IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR). Había nacido The Open Computer Vision Library y lo hacía bajo licencia BSD (Software Libre).

La librería OpenCV es una API de aproximadamente 300 funciones escritas en lenguaje C que se caracterizan por lo siguiente:

- Su uso es libre tanto para su uso comercial como no comercial.
- No utilizar librerías numéricas externas, aunque puede hacer uso de alguna de ellas, si están disponibles en tiempo de ejecución.
- Es compatible con The Intel® Processing Library (IPL) y utiliza The Intel® Integrated Performance Primitives (IPP) para mejorar su rendimiento, si están disponibles en el sistema.
- Dispone de interfaces para algunos otros lenguajes y entornos: EiC - intérprete ANSI C escrito por Ed Breen. Hawk y CvEnv son entornos interactivos (escritos en MFC y TCL, respectivamente) que utilizan el intérprete EiC; Ch - intérprete ANSI C/C++ creado y soportado por la compañía SoftIntegration; Matlab® - gran entorno para el cálculo numérico y simbólico creado por Mathworks; y muchos más (Arévalo, et al. s.f).

2.5.2 DEFINICIÓN DEL OPENCV

Según Igual, (2008). Las siglas Opencv provienen de los términos anglosajones “Open Source Computer Vision Library”. Por lo tanto, Opencv es una librería de tratamiento de imágenes, destinadas principalmente a aplicaciones de visión por computador en tiempo real. Raul carlos medranda

OpenCV (Open Source Computer Vision Library) es una librería de código abierto escrita en C y C++ y es capaz de correr bajo Linux, Windows y Mac OSX. Fue desarrollada por Intel y ahora es mantenida por Willow Garage. Se enfoca principalmente en procesamiento de imágenes en tiempo real.

Una de las metas de OpenCV, es proveer una infraestructura de visión por computador fácil de usar, que ayude a las personas a construir aplicaciones de visión por computador sofisticadas de manera rápida. La librería contiene más de 500 funciones que abarcan muchas áreas en visión, incluyendo imágenes médicas, seguridad, calibración de cámaras y robótica (Tamallo, 2012).

Según OpenCv, (2013). OpenCV (Open Source Computer Vision Library) es una biblioteca de licencia BSD de código abierto que incluye varios cientos de algoritmos de visión por ordenador. El documento describe la llamada API de OpenCV 2.x, que es esencialmente una API C + +, como opuesta a la API 1.x OpenCV basado-C.

OpenCV tiene una estructura modular, lo que significa que el paquete incluye varios compartido o estáticas bibliotecas. Los siguientes módulos están disponibles:

- core - un módulo de compacto que define las estructuras de datos básicas, incluyendo la densa Mat matriz multi dimensional y funciones básicas utilizadas por todos los demás módulos.
- imgproc - un módulo de procesamiento de imagen que incluye lineal y filtrado de imágenes no lineal, las transformaciones de imágenes geométricas (cambiar el tamaño, afín y deformaciones perspectiva genérica reasignación basada en la tabla), conversión de espacio de color, histogramas, y así sucesivamente.
- Vídeo - un módulo de análisis de vídeo que incluye la estimación de movimiento, la sustracción del fondo, y el seguimiento de algoritmos de objetos.

- calib3d - algoritmos de la geometría de múltiples vistas de base, calibración única y equipo de música de cámara, objeto plantear la estimación, algoritmos de correspondencia estéreo, y los elementos de la reconstrucción 3D.
- features2d - detectores de características sobresalientes, descriptores y matchers descriptor.
- objdetect - Detección de objetos e instancias de las clases predefinidas (por ejemplo, caras, ojos, tazas, gente, coches, y así sucesivamente).
- highgui - una interfaz fácil de usar para la captura de vídeo, imagen y codecs de vídeo, así como las capacidades simples de interfaz de usuario.
- gpu - algoritmos acelerados por GPU de diferentes módulos OpenCV.
- Algunos otros módulos de ayuda, como Flann y Google envoltorios de exámenes, enlaces Python y otros.

2.5.3 ESTRUCTURA Y CARACTERÍSTICAS DE LA LIBRERÍA OPENC

La librería OpenCV está dirigida fundamentalmente a la visión por computador en tiempo real. Entre sus muchas áreas de aplicación destacarían: interacción hombre-máquina (HCI4); segmentación y reconocimiento de objetos; reconocimiento de gestos; seguimiento del movimiento; estructura del movimiento (SFM); y robots móviles (Arévalo, et al. s.f).

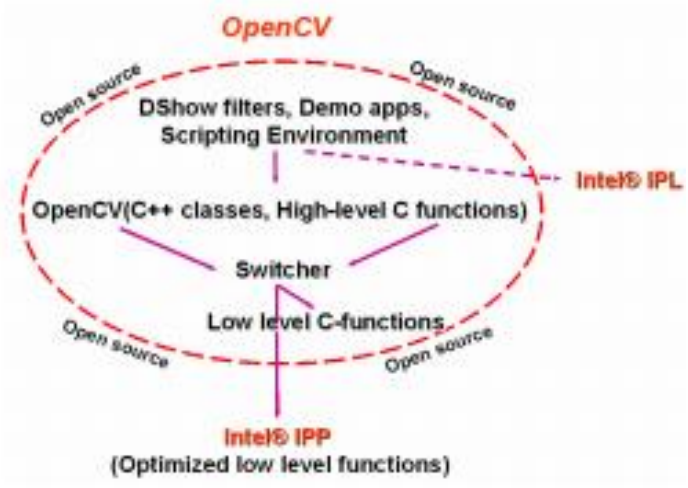


Figura.02.02 Estructura de la Librería OpenCV

Fuente: Arévalo, et al. s.f

2.6 INTRODUCCIÓN A LA METODOLOGÍA ITIL

Ante la creciente complejidad que significa para las empresas de hoy la administración de las tecnologías de información TI (Tecnología de la Información) y de sus sistemas de información SI (Sistema de Información), es pertinente el estudio de las mejores prácticas y de los estándares que se han estado posicionando y son utilizadas por las organizaciones de tecnologías de información, según lo expresa el índice de competencia del World Economic Forum, que compara 80 países entre el año 1998 y el 2003, y analiza las empresas que han tenido experiencias exitosas a través de las TI.

Teniendo en cuenta la necesidad de alinear el negocio con el uso de las TI, se requiere optimizar la tecnología en cualquiera de los niveles a fin de mantener procesos eficientes, y de esta manera, crecer a costos razonables y predecibles.

En la actualidad, para las organizaciones el concepto de calidad trasciende las características físicas y funcionales de los bienes y servicios. Esta idea está enmarcada en un ambiente competitivo, que requiere una cultura de gestión orientada hacia los procesos, personas y servicios mediante la mejora continua (Cárdenas, *et al.* 2009).

2.5.1 ITIL

ITIL (Information Technology Infrastructure Library) es el conjunto de buenas prácticas más aceptado y utilizado en el mundo, extraído de organismos del sector público y privado que están a la vanguardia tecnológica a nivel internacional. ITIL es aplicable a cualquier tipo de organización en todo el mundo debido a que los negocios han experimentado una creciente dependencia en los servicios informáticos de calidad.

La metodología ITIL está basada en la administración de servicios desde el punto de vista del negocio, y ha crecido en popularidad en la medida que los negocios dependen de la tecnología y buscan la mejor forma de aprovechar sus recursos humanos y tecnológicos.

2.6.1.1 ITIL EVOLUCIÓN

La metodología ITIL se remonta a finales de 1980, la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL) se ha convertido en el estándar mundial en la Gestión de Servicios Informáticos.

En un principio fue como una guía para el gobierno de UK, la estructura base ha demostrado ser útil para las organizaciones en todos los sectores a través de su adopción por innumerables compañías como base en consulta, educación y soporte de herramientas de software.

Hoy en día, ITIL es conocido y utilizado mundialmente; pertenece a la OGC, sin embargo las publicaciones son con “Derecho de Autor" (que por cierto, no las hace de dominio público). ITIL fue desarrollada al reconocer que las organizaciones dependen cada vez más de la Informática para alcanzar sus objetivos corporativos.

Actualmente la metodología ITIL cuenta ITIL V1, ITIL V2 e ITIL V3. La versión vigente de ITIL es la versión 3.

ITIL V1: fue producido originalmente a finales de 1980 y constaba de 10 libros centrales cubriendo las dos principales áreas de Soporte del Servicio y Prestación del Servicio. Estos libros centrales fueron más tarde soportados por 30 libros complementarios que cubrían una numerosa variedad de temas, desde el cableado hasta la gestión de la continuidad del negocio.

ITIL V2: las publicaciones propias son diferentes, se trataba de siete grupos distintos.

• Servicio de Apoyo
• La Prestación de Servicios
• La gestión de la infraestructura TIC
• Para llevar a cabo la planificación de la gestión de los servicios
• Aplicaciones de gestión
• La perspectiva empresarial
• Administración de la seguridad

Dentro de estos conjuntos son las descripciones y definiciones de las diversas disciplinas ITIL.

La ITIL V2 [3] fue sustituida oficialmente en 30 de Mayo de 2007, por ITIL v3, tras un largo período de rehabilitación denominado ITIL Refresh.

ITIL V3: comprende un conjunto de textos fundamentales con el apoyo de otros complementarios y materiales basados en Web.

Si bien ITIL V2, los volúmenes fueron sólo disponibles en Inglés, lo que limitó su uso en países que no hablaban Inglés, los títulos fundamentales en la versión 3 se están traduciendo a otros idiomas.

Entre el objetivo inicial están los idiomas portugués, español, japonés, hindú y árabe, mandarín y holandés. Esta iniciativa está dirigida por el ITSMF, con los recursos y el apoyo de OGC.

ITIL V3 utiliza la palabra "continua" en contraposición a ITIL V2 referencias a la "continua" mejora de los servicios (CSIP). Continua implica una actividad que se realice de forma gradual, periódicamente, como parte de un proceso.

Continua es más adecuada para la definición de las actividades destinadas a operar sin pausa, como el objetivo final de disponibilidad. Nace como un código de buenas prácticas dirigidas a alcanzar esas metas mediante:

• Un enfoque sistemático del servicio TI

• El establecimiento de estrategias para la gestión operativa de infraestructura TI (Ocampo, *et al*. 2009).

2.5.1.2 Áreas a las que se dirige ITIL

ITIL ofrece guías para la administración de los procesos de TI relacionados a:

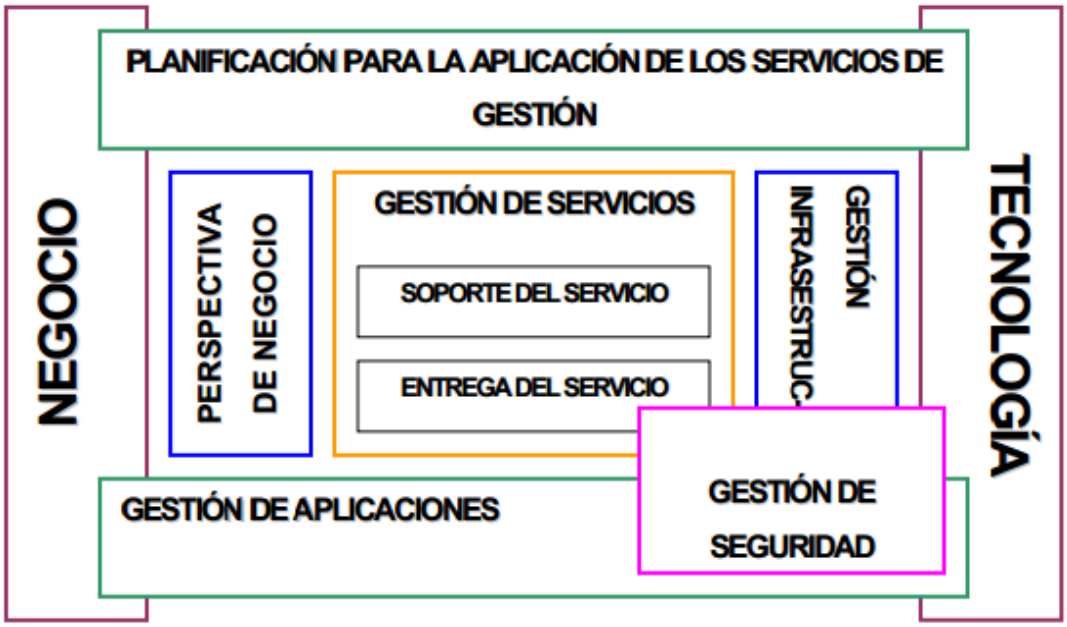


Figura 02.03 Planificación para la aplicación de los Servicios de Gestión

CAPÍTULO III. DESARROLLO METODOLÓGICO

La tesis de grado se desarrolló en la Capitanía del Puerto de la ciudad de Manta dentro de sus oficinas, tales como el área de administración, personal marítimo, departamento marítimo, sala de dirección y atención al cliente, la cual permitió tener una vigilancia del lugar durante las 24 horas del día tiempo real, y a su vez observar las actividades que se realizan para detectar, registrar y permitir responder a posibles violaciones en la seguridad o sustracción de bienes, para ello se llevó a cabo un software de detección de rosto que le ayudará a identificar a las personas que ingresen a la dependencia detectando en vivo las caras de los individuos y comparando por medio de una base de datos. Además el presente trabajo se realizó en 9 meses a partir de la adquisición de los equipos tecnológicos y la culminación del sistema de detección de rostro..

3.1 MÉTODOS

Los métodos que se aplicaron para la realización del sistema de seguridad son los siguientes:

3.1.1 MÉTODO CIENTÍFICO

Inductivo-Deductivo: Este método permitió observar los hechos tal y como se presentaron obteniendo estipulaciones de las actividades que se realizan dentro de las oficinas de la Capitanía del Puerto de Manta y de esta manera se pudo realizar la implementación del sistema de vigilancia mediante cámaras IP, por ende se empezó con una investigación de las dificultades que existían dentro de la Capitanía para poder cumplir con los objetivos establecidos empleando las herramientas necesarias, siendo necesario la aplicación de las técnicas de observación.

3.1.2 MÉTODO INFORMÁTICO

Para la ejecución del sistema de vigilancia se empleó la metodología del Ciclo de Vida o Modelo en V que puede ser establecida rápidamente en toda empresa, siendo un conjunto ordenado de buenas prácticas para realizar análisis, diseño, pruebas e implementación del sistema. Dentro de esta metodología se utilizaron las siguientes fases:

La Fase de Especificaciones, se analizó el seguimiento de las operaciones que se realizan dentro de la Capitanía del Puerto de Manta estableciendo de esta manera los requisitos del sistema de vigilancia, en la cual se obtuvo una entrevista informal con el Comandante José Vaca y se le planteó un método de vigilancia mediante cámaras IP con software de detección de rostro dentro de ciertas oficinas de la Capitanía (Anexo 1 y 2), proporcionando las herramientas y los equipos tecnológicos para llevar a cabo la implementación de dicho procedimiento.

Mediante la Fase de Diseño de Alto Nivel y de detalle se realizó el respectivo boceto de la ubicación de las cámaras dentro de cada una de las oficinas ya mencionadas y de esta manera se pudo monitorear bien las actividades que se realizan dentro de los departamentos de la Capitanía (Anexo 4), además del desarrollo del software facial, que permitió identificar las personas que ingresen a las diferentes áreas.

Dentro del diseño de la estructura de las cámaras se tomó en cuenta la estructura del edificio, en el cual dentro de cada piso cuenta con algunos departamentos, solo siendo necesarias la instalación de las cámaras en 8 oficinas tales como el Área de Financiero, Arpas y Rastrillo, Jurídico, los departamentos Marítimo e Auxilio Marítimo y el Pasillo de Dirección; obteniendo lo siguiente, en el primer piso 4 cámaras, en el segundo dos cámaras y finalmente en el tercer piso 2 cámaras teniendo un total de 8 cámaras IP dentro de todo el edificio (Anexo 4). Sin embargo fue necesario mantener un buen fluido eléctrico, para ello se necesitó el uso de un UPS que

mantenga los equipos de las cámaras encendidas hasta cinco horas sin fluido eléctrico evitando los cortos circuitos que se puedan generar y deteriorar el buen funcionamiento de los dispositivos.

Además dentro de las especificaciones del software se determinó los requerimientos necesarios para el desarrollo de este, siendo importante obtener los rostros de las personas que ingresan a cada una de las oficinas. La codificación se desarrolló en base a estudios e investigaciones que se llevaron a cabo dentro de la Capitanía, siendo necesario desarrollar la programación en lenguaje Java y Eclipse como entorno de desarrollo del sistema contando con las librerías de visión artificial como lo son opencv y javacv que son framework para aplicaciones en tiempo real, obteniendo estos conocimientos mediante auto capacitaciones sobre la detección de rostros en base a códigos de java.

Fase de Implementación se realizó una vez adquiridos los equipos y esquematizado el diseño de la ubicación de las cámaras, se empezó a extender el cableado estructurado en las áreas donde se colocaron los equipos (Anexo 4). Cada cámara está colocada técnicamente, para su conexión cable con categoría 5E, conectores RJ45 ponchando cada cable con el estándar 568B para cableado estructurado (blanco naranja, naranja, blanco verde, azul .blanco azul, verde blanco café, café) para los cuales fue necesario utilizar la ponchadora, el estilete, cortafrío, desarmador estrella, broca, taladro, escalera, martillo. Luego para colocar las cámaras primero se verificó el ángulo de observación y posteriormente se procedió a ajustar fuerte para evitar movimiento, en la colocación de las cámaras primeramente se marcó el punto donde se fijó cada una (Anexo 12).

Las cámaras fueron colocadas en un área estratégica para lograr capturar el mayor porcentaje del área de enfoque, el almacenamiento de datos se lo realizó en un servidor colocado en la oficina del Comandante de la Capitanía que posee una capacidad de almacenamiento de 1 Tb con 4 Gb de RAM con una velocidad de procesamiento de 2.7 GHz AMD EPROM y una tarjeta de Video. Luego se procedió a la instalación del software de las cámaras en la

PC, configurando los protocolos de internet de cada una, permitiendo de este modo visualizar video o capturar la imagen a través del servidor previo a la configuración apropiada del servidor.

La fases del Test Unitario, Integración y Operacional consistió en verificar que los componentes del software funcionaran correctamente (Anexo 3), es decir que el módulo de descomprensión de imágenes se acoplara correctamente con las imágenes que se encuentran almacenando dentro de la base de datos del sistema, realizando esto mediante un algoritmo de entrenamiento que es el que inicia el proceso para posteriormente acceder al algoritmo de reconocimiento y así mismo que los datos se calcularan con precisión en el tiempo requerido.

Una de las maneras de utilizar el reconocimiento facial es mediante la comparación de determinados rasgos en la imagen, es decir con ayuda de varios ángulos del rostro que posteriormente se almacenan en una base de datos. Con esto no solo se conoce en todo momento la cantidad de personas que se encuentran dentro la zona vigilada, sino que por medio de este componente se puede conocer su identidad; con la integración de este sistema se evitaría la intervención humana tanto en el sistema de seguridad como en la parte del usuario, solo se necesitará esta intervención en casos precisos como una alarma con el sistema o la introducción de datos en el sistema como también recopilación de videos.

Figura 03.01. Ejemplos de detección del rostro para dos sujetos.

De esta manera el sistema admitió ver si la ubicación de las cámaras y el software instalado en estas, están siendo bien empleado y si están en buen funcionamiento lo cual se pudo obtener una aceptación de parte del Comandante de la Capitanía sobre la herramienta tecnológica empleada, y así brindar un servicio confiable.

Sin embargo también se llevó a cabo la metodología ITIL la cual permitirá ver la seguridad o almacenamiento ya que esta se basa en el desarrollo de normas, métricas de evaluación y en la excelencia de la calidad de los servicios, desarrollando eficazmente los procesos que cubren las actividades más importantes de las organizaciones dentro de los SI (Sistema de Información), siendo necesario disponer de políticas de seguridad para llevar a cabo la ejecución de este obteniendo métricas e indicadores clave que permitieron evaluar los niveles de servicio dentro de la organización.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

Mediante la implementación de un sistema de vigilancia con un software de detección de Rostro instalado dentro de las oficinas de la Capitanía del Puerto de la Ciudad de Manta se consiguió capturar imágenes de tramitadores que frecuentaban los diferentes departamentos de la Capitanía, así mismo de tener un registro de las imágenes y videos de las actividades que se realizan a diario.

En la fase de Análisis de Requerimientos se realizó una entrevista con el Comandante José Vaca donde se planteó la propuesta del sistema de vigilancia (Anexo 1), en el cual él explicó que requeriría de un sistema de vigilancia que le permitiera tener en cuenta las actividades que se efectúan dentro de la entidad, así mismo de que si existía algún tipo de anomalía. De acuerdo a lo mencionado anteriormente se desarrolló una investigación dentro de la Capitanía para así poder llevar a cabo los requerimientos necesarios que nos permitieron desarrollar tanto el software de detección facial como el diseño de la ubicación de las cámaras (Anexo 2).

Determinando los requerimientos se procedió a realizar la fase de Diseño de Alto Nivel, especificando las ubicaciones de las cámaras, y analizando las posibles interferencias que podrían ocurrir en base a la mala ubicación de esta, es decir viendo las estructuras eléctricas dentro del Edifico, detallando de esta manera el buen diseño del lugar de las cámaras y así lograr un buen alcance para que el sistema facial (Anexo 4).

Una vez que se adquirieron e instalaron los equipos necesarios, en relación con el diseño ya establecido (Anexo 4), se procedió a la configuración de las direcciones o protocolos IP de cada una de las cámaras ya ubicadas y así definir la identificación de cada una de ellas mediante una dirección Física dentro del servidor. Para la correcta configuración de las cámaras con cada una de las IP se le realizó un ping para que verifique si existía conectividad o no con la cámara y el servidor.

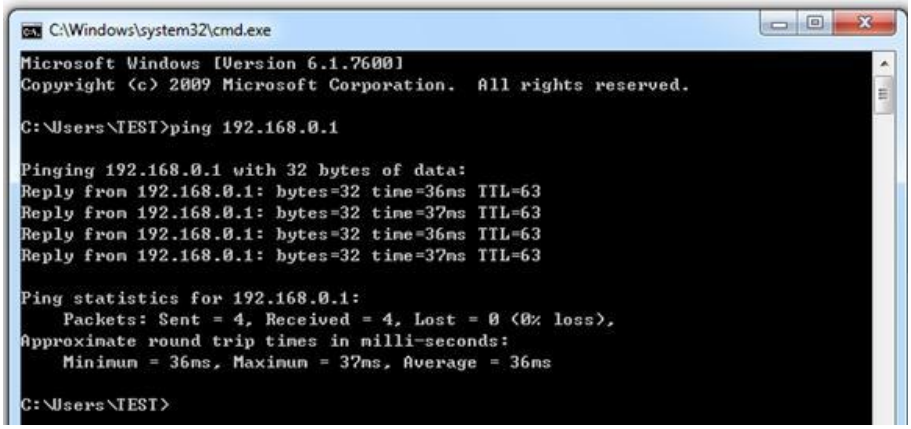


Figura. 04.01 Tiempo de respuesta y el tráfico de espera de la cámara IP

Fuente: Autora

Cuadro. 04.01 Direccionamiento IP y Puerto de Enlace

UBICACIÓN DE LA CÁMARAS	DISPOSITIVO	DIRECCIÓN IP	PUERTO DE ENLACE ASIGNADO
Dpto_Financiero1_Caja1	TV-IP551W	192.168.10.18	89
Dpto_Financiero1_Caja2	TV-IP551W	192.168.10.12	82
Dpto_Financiero2_Caja3	TV-IP551W	192.168.10.13	83
Dpto_Zarpe_Arribo	TV-IP551W	192.168.10.11	81
Dpto_Jurídico	TV-IP551W	192.168.10.17	88
Pasillo_Dirección	TV-IP551W	192.168.10.14	84
Dpto_Marítimo	TV-IP551W	192.168.10.16	86
Dpto_Personal_Marítimo	TV-IP551W	192.168.10.15	85

De acuerdo a las pruebas realizadas se observó si existía conexión del servidor con cada una de las cámaras haciendo esto mediante un ping a cada dirección IP ya asignada, logrando de esta manera una correcta configuración; así mismo se procedió a revisar la captura de video de las cámaras, logrando demostrar la eficacia en resolución de imagen y de tiempo de respuesta.

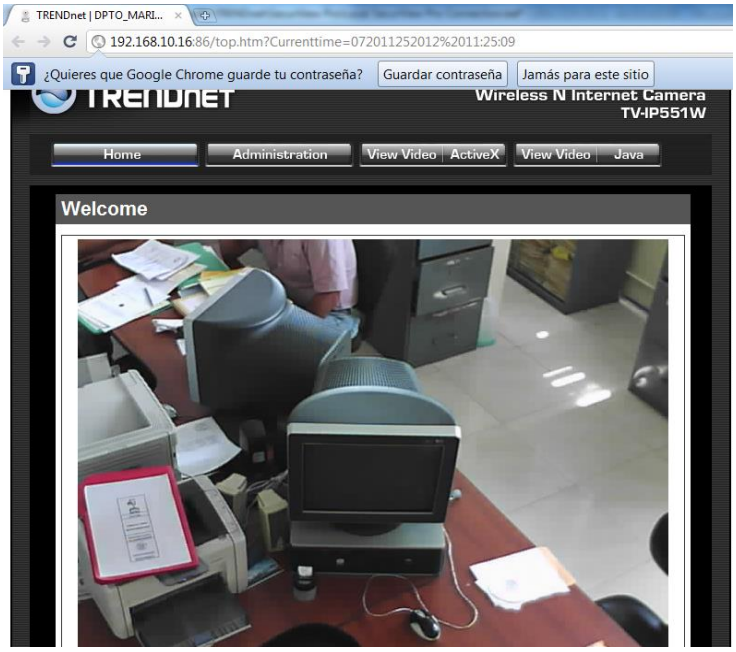


Figura 04.02 Captura de imagen por medio del navegador

Fuente: Autora

Con el desarrollo del sistema de detección se logró comparar imágenes de varios rostros y que el sistema detectara cuantos semblantes había en esa fotografía, tomando en cuenta el aspecto de cada uno, es decir los diferentes ángulos. A su vez permite la identificación de la persona que se encuentre registrada dentro de la base de datos.

Figura 04.03 Comparación de varios semblantes

Fuente: Autora

Dentro de la ejecución del sistema se realizaron varias pruebas, en donde se tomaron fotografías de diferentes personas en tres ángulos, frente, derecho e izquierdo del rostro para que así los algoritmos empiecen a efectuar su reconocimiento, con esto se pretendió automatizar el registro de seguridad en el acceso a la institución de una forma rápida y confiable mediante el almacenamiento de imágenes capturadas en el servidor central; cabe recalcar que se realizó la aplicación tanto a modo escritorio como web.

PRUEBA 1

PRUEBA 2


Figura 04.04 Ficha técnica de Prueba de Algoritmo de Entrenamiento

Fuente: Autora

Sin embargo el tiempo que tarde el algoritmo en realizar el entrenamiento es de 1 segundo y medio al igual que el reconocimiento; y la detección tiene un alcance a 1 metro y medio de distancia dependiendo de las características de la cámara.

```
//Entrenamiento
        /*
         IplImage[] trainImages = new IplImage[10];
         for(int i=1; i<=10; i++){
            //trainImages[i-
1]=cvLoadImage("C:/facerecognizer/data/images/training/terry"+i+".jpg");
           trainImages[i-
1]=cvLoadImage("C:/facerecognizer/data/images/training/cr7"+i+".jpg");
            CvSeq faces = reconocer.detectFace(trainImages[i-1]);
            CvRect r = new CvRect(cvGetSeqElem(faces,0));
            trainImages[i-1]=reconocer.preprocessImage(trainImages[i-1], r);
         }
         reconocer.learnNewFace("cr", trainImages);
        */

//Reconocimiento

        IplImage target = new IplImage();
         //target =
cvLoadImage("C:/facerecognizer/data/images/training/terry_target.jpg");
        target =
cvLoadImage("C:/facerecognizer/data/images/training/cr7_target.jpg");
         CvSeq faces2 = reconocer.detectFace(target);
         CvRect r2 = new CvRect(cvGetSeqElem(faces2,0));
         target=reconocer.preprocessImage(target, r2);
         System.out.println("PERSONA IDENTICADA:
"+reconocer.identifyFace(target));
```

Figura 04.05 Algoritmo de entrenamiento y reconocimiento facial

Fuente: Autora

Con ayuda de la metodología ITIL se procedió a realizar las buenas prácticas siguiendo la normativa ITIL, y así lograr la correcta ubicación de las cámaras para tener una mayor seguridad de los datos e información en base a las normas y las métricas de evaluación permitiendo evaluar los niveles de seguridad.

El sistema de vigilancia realizado dentro de las oficinas de la Capitanía del Puerto de la ciudad de Manta, es una herramienta tecnológica que permitió resolver los problemas de inseguridad que existían dentro de sus departamentos y logrando de esta manera que las actividades que se realizan a los usuarios sean correctas.

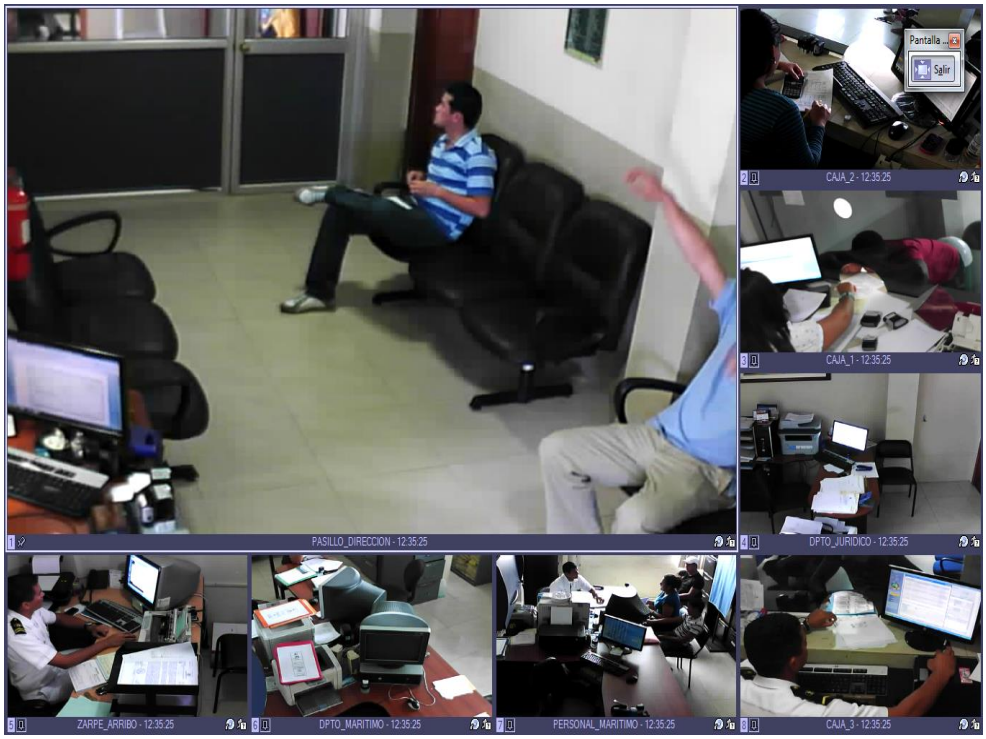


Figura 04.06 Captura de imagen de todas las cámaras por medio del sistema de la cámara.

Fuente: Autora

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Analizando las operaciones que se realizaban dentro de la Capitanía permitió conocer las necesidades y detallar el problema para plantear la propuesta de la herramienta tecnológica.

- El Diseño de los puntos y la ubicación de las cámaras en ciertos departamentos de la entidad, fueron las más optimas y precisas para detección facial.

- El Desarrollo del Software se lo realizo con las librerías de visión artificial opencv y javacv lo que permitió identificar a las personas que ingresaban a la Capitanía.

- La implementación del sistema, y el funcionamiento de las cámaras dieron las pautas para brindar un registro de video y almacenamiento de los datos necesarios para la detección de rostro de cada una de las personas que ingresaban a la Capitanía.

- La implementación de un sistema de vigilancia dentro de las oficinas de la capitanía del Puerto de la ciudad de Manta constituyó una necesidad primordial para el control de internos y el monitoreo de zonas de acceso frecuentes en donde se manipula dinero o se realiza tramites de todo índole.

5.2 RECOMENDACIONES

- Analizar bien el área en donde se presenta el problema y estipular bien la recolección de la información para obtener datos reales que permitan y así lograr un diseño eficaz y correcto.

- El diseño de las áreas en donde se van a ubicar las cámaras deben estar estipuladas en concordancia con las necesidades que se planteen dentro la Entidad, así mismo se deberá determinar el recorrido necesario de éstas sin que puedan interferir con otros tecnológicos o que puedan ser afectados por el ambiente.

- Para la implementación de las cámaras de vigilancia se debe hacer uso de programas que sean seguros para la manipulación de ellas, para lo cual se requiere que los dispositivos a emplear sean de excelente calidad y que mantengan relación con la eficacia del programa garantizando fidelidad, calidad de las imágenes captadas.

- Para el monitoreo del sistema de vigilancia se debe llevar a cabo unos días de prueba o de validación para verificar su adecuado funcionamiento y así atestiguar que las imágenes y videos almacenados en el servidor sean de excelente calidad, además de que el software que éstas se encuentran manipulando esté realizando su función específica.

- Para incrementar la seguridad es conveniente que el acceso al sistema de vigilancia solo tenga disponibilidad para el personal autorizado, es decir delimitar el acceso a la información del servidor y las imágenes captadas por las cámaras. Cualquier modificación en las configuraciones de protección planteadas en el software pueden ocasionar fallas graves de seguridad.

BIBLIOGRAFÍA

AEPD (Agencia Española Protectora de Datos), s.f. Guía de video vigilancia. Nilo. Madrid, España. p 24.

AI (Asesoría Informática). 2005. Cámaras IP. (En línea). Consultado, 1 de Jun. 2012. Disponible en http://www.aseinformatica.com/camarasip.php.

Albusac, J. 2008. Vigilancia Inteligente: Modelo de entornos reales e interpretación de conductas de seguridad. Tesis. Máster Tecnologías Informáticas. Universidad Castilla La Mancha. Madrid, España. p 36.

Alvarez, D & Guevara, M. 2009. Reconocimiento de Expresiones faciales prototipo usando ICA. Rereira, Co. Scientia Et Techica. Universidad Tecnológica de Pereira. 15:41.

Amaya, C. 2007. Diseño De La Red Inalámbrica Y Sistema De Seguridad Mediante Cámaras Inalámbricas Con Monitoreo Remoto Para El Edificio De La Empresa Metropolitana De Obras Públicas De Quito (Emop-Q). Tesis. Ing. Electrónica y Telecomunicaciones. Sangolquí. Ec. p 22.

Arévalo, M; González, J; Ambrosio, G, s.f. La Librería de Visión Artificial OpenCV Aplicación a la Docencia e Investigación. Dpto. De Ingeniería de Sistemas y Automática, Universidad de Málaga. España. p 2,3,5.

Arguello, H. 2011. Sistema de reconocimientos basados en la imagen facial. Colombia. Revista avances en Sistemas e Informática. Universidad Nacional de Colombia. 8:3

Ávila, N; González, D; Nacipucha, L. 2009. Implementación De Un Sistema De Seguridad Para La Empresa Devies Corp En La Ciudad De Milagro Para Prevenir. Tesis. Ingeniera Comercial y Empresarial Especialización Finanzas y Economista con Mención en Gestión Empresarial

Especialización Finanzas. Escuela Superior Politecnica Del Litoral Facultad De Economía Y Negocios. Guayaquil, Ec. p 44-47.

Berns, F. 2011. Cámaras de Vigilancia. (En línea). Consultado, 1 de Jun. 2012. Disponible en http://www.articulo.org/articulo/41871/que_son_las_camaras_de_vigilancia.html.

Borghello, C. 2011. Sistema de Seguridad Informática sus Implicancias e implementación. Tesis. Lic. Sistemas. Universidad Tecnológica Nacional. p 33.

Cachiguango, Y. 2010. Diseño de una red de video vigilancia local y remota sobre IP en tiempo real para una hostería aplicando el concepto de Green It. Tesis de Ingeniero Electrónica y Telecomunicaciones. Escuela Superior Politécnica Nacional. Quito, Ec. P 13

Cantú, A. 2011. Seguridad Informático e Sistema para Comunicación de Redes LAN, Inalámbrica y Bluetooth. (En línea). Consultado, 28 de Jun. 2012. Disponible en http://www.pc-teros.es/tutoriales/tesis-seguridad-informatica-diabliyo-t985.html

Cárdenas, M; Constanza, Y; Bautista, R; Willmer, D. 2009. Modelo de gestión basado en el ciclo de vida del servicio de la Biblioteca de Infraestructura de Tecnologías de Información (ITIL). Medellín, Co. Revista Virtual Universidad Católica del Norte. 27: 6.

Espinoza, V. 2001. Evaluación de Sistemas de Reconocimiento Biométrico. Tesis. Ing. Electrónica y Automática. Escuela Universitaria Politécnica de Mataró. Adscrita a la UPC. Mataró, Barcelona. p 59.

Fernández, O. 2011. Adquisición y transmisión de video 3D sin comprimir sobre redes IP. Tesis. Ing. Técnica de Telecomunicaciones. Universidad Politécnica de Cataluña. España, Barcelona. p 17.

Fuente, A; Villacorta, J; Puente, L; Mateos, L. 2005. Un Sistema Avanzado De Vigilancia Basado En Información Multisensorial. Revista Facultad de Ingenieros. Universidad Tarapacá.13: 22.

Herrera, F. Viviendas Domóticas. 2005. Revista Ingeniería e investigación. 25: 26.

Igual, R & Medrano, C. 2008. Tutorial de OpenCV (En Línea). Consultado, 20 de Dic. 2013. Disponible en: http---docencia-eupt.unizar.es-ctmedra-tutorial_opencv.pdf

INTECO (Instituto Nacional de Tecnologías de Comunicación). 2009. Ingeniería Del Software: Metodologías Y Ciclos De Vida. p 24-29.

ITI (Instituto Tecnológico Informático). 2009. La Vigilancia Tecnológica aplicada al Sector TIC. Ven. Revista del Instituto Tecnológico Informática. 15: 13-15.

Izquierdo, A; Villacorta, Juan; Val, L; Raboso, M. 2010. Un Sistema Avanzado De Vigilancia Basado En Información Multisensorial. Chi. Revista Facultad de Ingeniería. 13: 77,78.

Gocella, R. 2009. Sistema de Cámara de Vigilancia, Metodología de la Investigación. Tesis de Técnico Superior en Programación. Universidad Tecnológica Nacional. Mar del Plata, Arg. p 15-18.

Kioskea. 2010. Introducción a la Seguridad Informática. (En línea). Consultado, 1 de Jun. 2012. Disponible en: http://es.kioskea.net/contents/secu/secuintro.php3

Laurenciano, J. 2011. Desarrollo y evolución de un sistema automático para la transmisión de imágenes y datos desde equipos remotos (fijos o móviles) para aplicaciones audiovisuales y multimedia. Tesis. Ing. Técnica de Comunicación. Universidad Politécnica de Cataluña. España, Barcelona. p 37.

Mojsiejczuk, G. 2007. Seguridad en los Sistemas. Tesis. Lic. Sistemas de Información. Universidad Nacional del Nordeste Facultad de Ciencias Exactas, Naturales y Agrimensura. Corrientes – Argentina. p 3.

Morejón, G; Hernández, B; Rodríguez, I; Moreno, T; Seife, E. 2008. Problemas éticos y de seguridad asociados al uso de las tecnologías de la información y el conocimiento en Salud. Cu. Revista MediSur. 6: 88.

Moreno, T. 2011. Diseño y construcción de un prototipo de monitoreo y seguridad basado en cámaras ip. Tesis. Ing. Informática. Escuela Politécnica Nacional. Ec. p 36.

Ocampo, C; Moreno, R; Milena, S. 2009. Implementación De Modelo De Procesos De Gestión De Servicios Con ITIL (Information Technology Infrastructure Library). Pereira, Co. Scientia Et Technica, 15: 215, 216.

OpenCV. 2013. The OpenCV Reference Manual, Release 2.4.8.0. (En Linea). Consultado, 20 de Ene. 2014. Disponible en: http://docs.opencv.org/opencv2refman.pdf

Richarte, J. 2012. Vigilancia y Seguridad de Cámaras IP. (En línea). Consultado, 28 de Jun. 2012. Disponible en http://img.redusers.com/imagenes/pwr/pwr089/notagratis.pdf.

Salazar, L. 2009. Seguridad Informática Un Enfoque Práctico. Tesis. Ing. Sistemas. Universidad Señor de SIPAN. Chiclayo. Perú. p 6-8.

Salas, J. 2011. Detección De Movimiento En Cámaras Fijas Sujetas A Vibración. Es. Revista DYNA. 78: 15.

Tamayo, J. 2012. Reconocimiento de figuras geométricas a través de una Webcam con OpenCV. Tesis de Ingeniería en Sistemas. Universidad de San Buenaventura. Medellín, Colombia. p 9.

Tipantuña, J. 2010. Diseño e implementación de un sistema de seguridad en tiempo real monitoreado por internet. Tesis. Ing. Electrónica y Computación. ESPOCH. Riobamba. Ec. p 34.

Trujillo, F. 2009. Diseño De Un Sistema De Vigilancia No Convencional Basado En Redes Zigbee (802.15.4) Para Realizar Un Control Sobre Equipos De Video E Integración A Sistemas de Supervisión de Mayor Jerarquía. Tesis. Ing. Eléctrico y Comunicaciones. Sangolquí. Ec. p 24.

Urrutia, W. 2011. Sistema de video vigilancia mediante cámaras IP para mejorar la seguridad ciudadana en zona central del cantón Baños de Agua Santa. Tesis de Ingeniería en Electrónica y Comunicaciones. Universidad Técnica de Ambato. Ambato, Ec. P 28-32.

Valeriano, J. 2011. Funcionamiento de las cámaras. (En línea). Consultado, 1 de Jun. 2012. Disponible en http://valetron.eresmas.net/CamarasIP.htm.

Velasco, A. 2008. El derecho informático y la gestión de la seguridad de la información. Revista de Derecho. Co. p 330.

Villegas, M; Meza, M y León, P. 2011. Las métricas, elemento fundamental en la construcción de modelos de madurez de la seguridad informática. Venezuela. Revista Electrónica de Estudios Telemáticos Universidad Rafael Belloso Chacín. 10:1.

Vivien, C. 2008. Valoración del CCTV como una Herramienta efectiva de manejo y seguridad para la resolución, prevención y reducción de crímenes. Centro Nacional para la prevención de la Criminalidad. Montreal. p 10

Voutssas, J. 2010. Preservación documental digital y seguridad informática. Centro Universitario de Investigaciones Bibliotecológicas de la UNA. México. P 132.

Zambrano, O; Toala, A. 2009. Implementación de un Sistema De Vigilancia Utilizando UnaWeb Cam, Asterisk Y Teléfonos Grandstream. Tesis. Ing. En Computación. Ciencias Multimedia. ESPOL. Guayaquil. Ec. p 22.

ANEXOS

ANEXO 1

¿Cuál es el motivo principal por lo que desea implementar un sistema de seguridad dentro de su institución? La inseguridad que abarca en estos días, y estamos expuestos a la delincuencia.
¿Cómo se llevaba a cabo el control de vigilancia dentro de sus oficinas? Ante alguna posible entrada de delincuentes se tenía alarmas de intrusión que solo suena una alarma pero en la actualidad se ha descompuesto
¿Cree usted que es necesario instalar un Sistema de Vigilancia para ayudar a reducir los niveles delictivos dentro de la Capitanía del Puerto de Manta? Si creo factible que se instale este tipo de sistema debido a que con frecuencia hay ingreso de personas de diferentes lugares para realizar las diferentes operaciones que se realizan y estamos expuestos a cualquier peligro.
¿Le gustaría instalar cámaras IP de vigilancia en todas las oficinas de su institución? No, solo me gustaría en donde existes más movimientos de actividades, especialmente en los lugares donde se registra el ingreso de dinero
¿Cuántas cámaras de vigilancia le gustarían instalar? En realidad solo me gustaría instalar 8 cámaras.
¿Cuáles son las oficinas que le gustaría vigilar? Bueno sería una cámara en cada uno de los departamentos de Financiero que son 3 en total, una en el departamento de arribo, el departamento jurídico, departamento marítimo, personal marítimo, y finalmente una en el pasillo de dirección.
¿Quiénes tendrían acceso del sistema de vigilancia? Solo mi persona tendría acceso a él ya que el servidor debe estar instalado en mi oficina, puesto que a ella nadie tiene acceso solo la persona que yo autorice
¿Le gustaría además de las cámaras IP tener un software que le permita ver qué tipo de personas ingresa a la capitanía? Las constantes actividades que realizo me implican estar fuera de la oficina y me gustaría estar en contacto con todo lo que se realiza dentro de la capitanía, y por supuesto que me gustaría así sabría qué tipo de persona esta o ha ingresado a mi institución

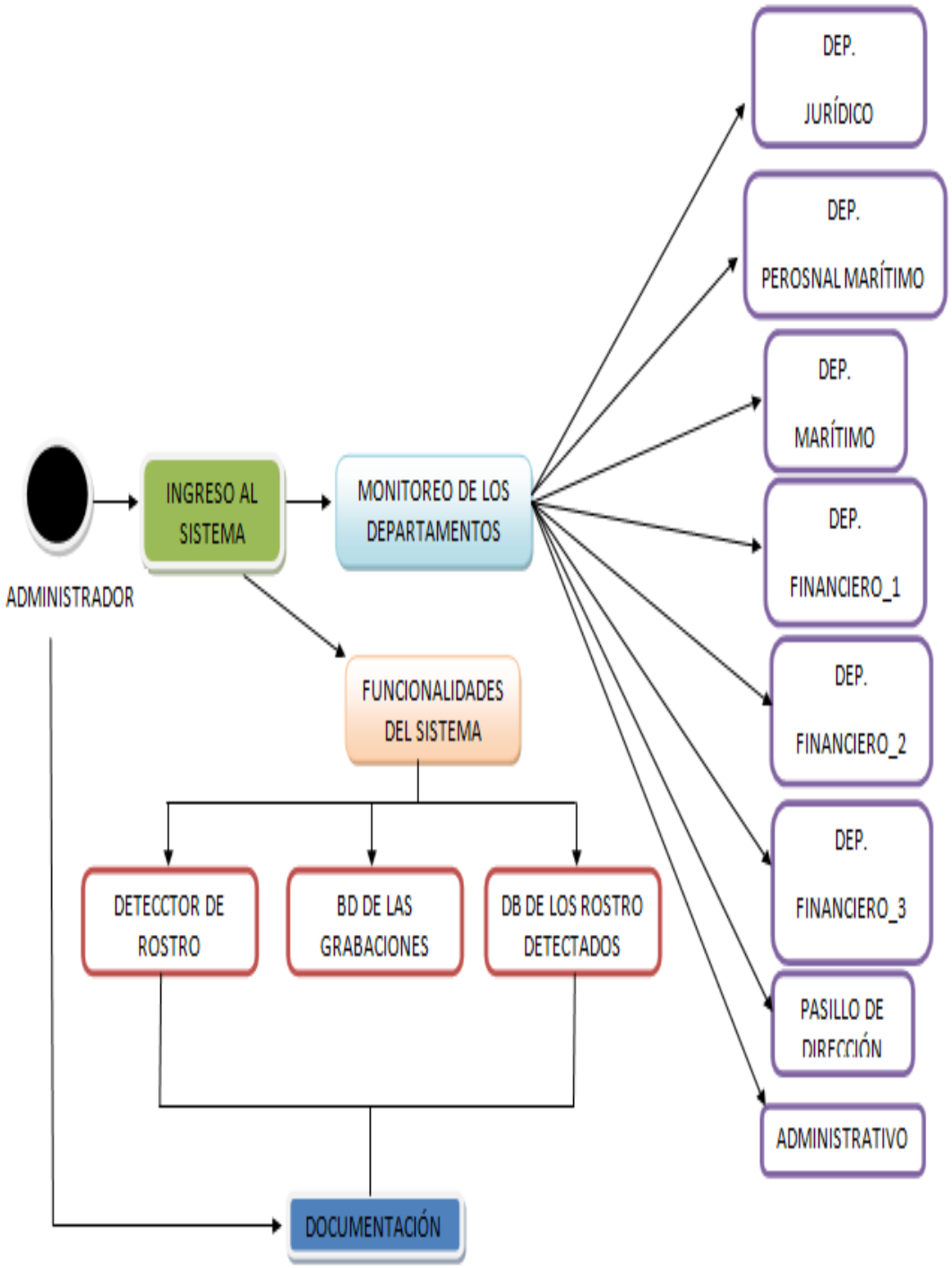
Entrevista realizada al Señor Comandante José Vaca Vera Comandante de la Capitanía del Puerto de Manta

ANEXO 2

REQUISITOS FUNCIONALES
• Implementar un Sistema de Vigilancia mediante cámaras de seguridad. • Monitoreo de las cámaras en los departamentos de Financiero, Departamento de Arribo, Departamento Jurídico, Departamento Marítimo, Personal Marítimo y en el Pasillo de Dirección. • El Servidor debe ser ubicado en la Oficina de Dirección de la Capitanía. • Restringir acceso, solo una persona autorizada. • Identificar a las personas que ingresan a la Capitanía. • Generar reportes de las personas ingresadas. • Ingreso, almacenamiento de registros según lo amerite el caso. • Acceder al sistema por medio de Login.
REQUISITOS NO FUNCIONALES
• Confiabilidad: La información manejada a través del software será precisa y confiable. • Amigable: La aplicación tiene un diseño simple de fácil de manejo, con opciones claras de visualización. • Seguridad: El acceso y monitorización del sistema solo tendrá acceso el administrador y es el único que puede manipular la información del sistema, representando así la seguridad de los datos ya que esto es lo más primordial. • Efectividad: La aplicación debe monitorizar las zonas en donde se encuentran ubicada las cámaras con rapidez y en tiempo real. • El desarrollo del sistema se realizará en el lenguaje de programación de java y eclipse como entorno de desarrollo ayudado con las librerías de detección facial como lo son opencv y javacv.
REQUISITOS DE IMPLEMENTACIÓN
La aplicación deberá funcionar sobre cualquier sistema operativo (Windows, Linux, Mac OS) siempre y cuanto tenga suficiente espacio en disco y memoria.

Ficha Técnica de los Requerimientos del Sistema de Vigilancia y Software Facial

ANEXO 3

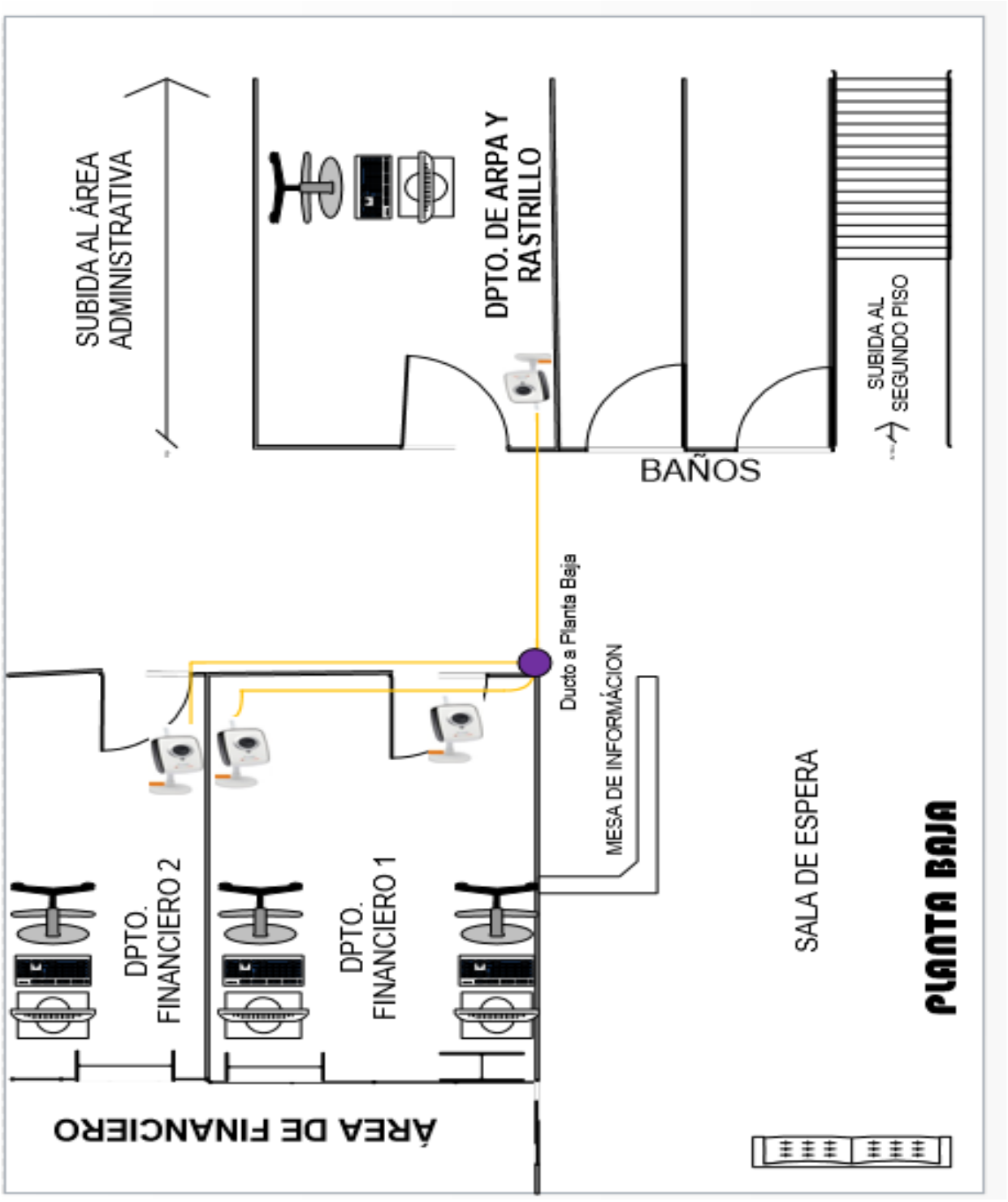


Caso de uso de la manipulación de las aplicaciones y disponibilidades del software de las cámaras

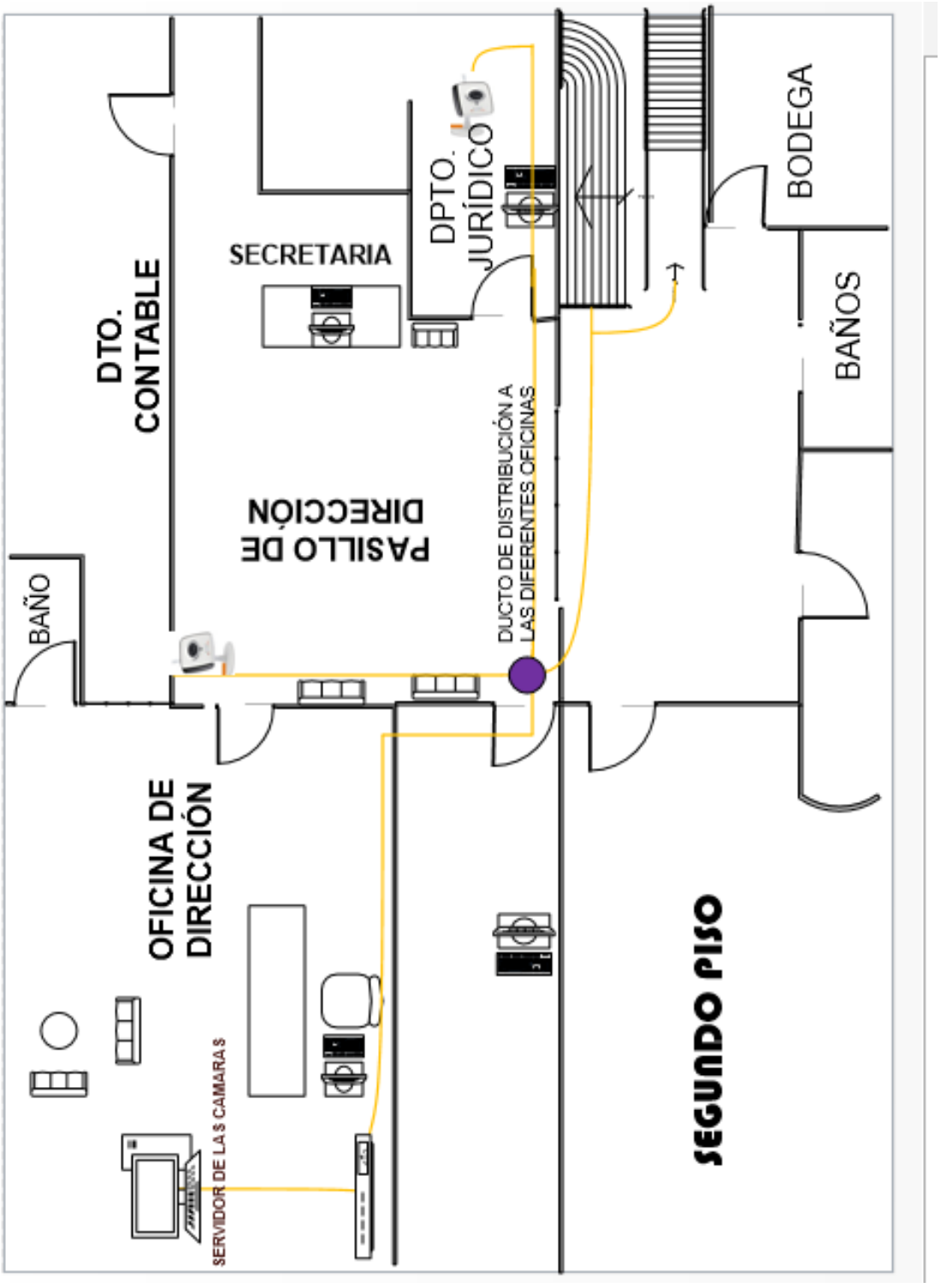
ANEXO 4

PLANO DEL EDIFICIO DE LA CAPITANÍA DEL PUERTO DE LA CIUDAD DE MANTA CON UBICACIÓN DE LAS CÁMARAS

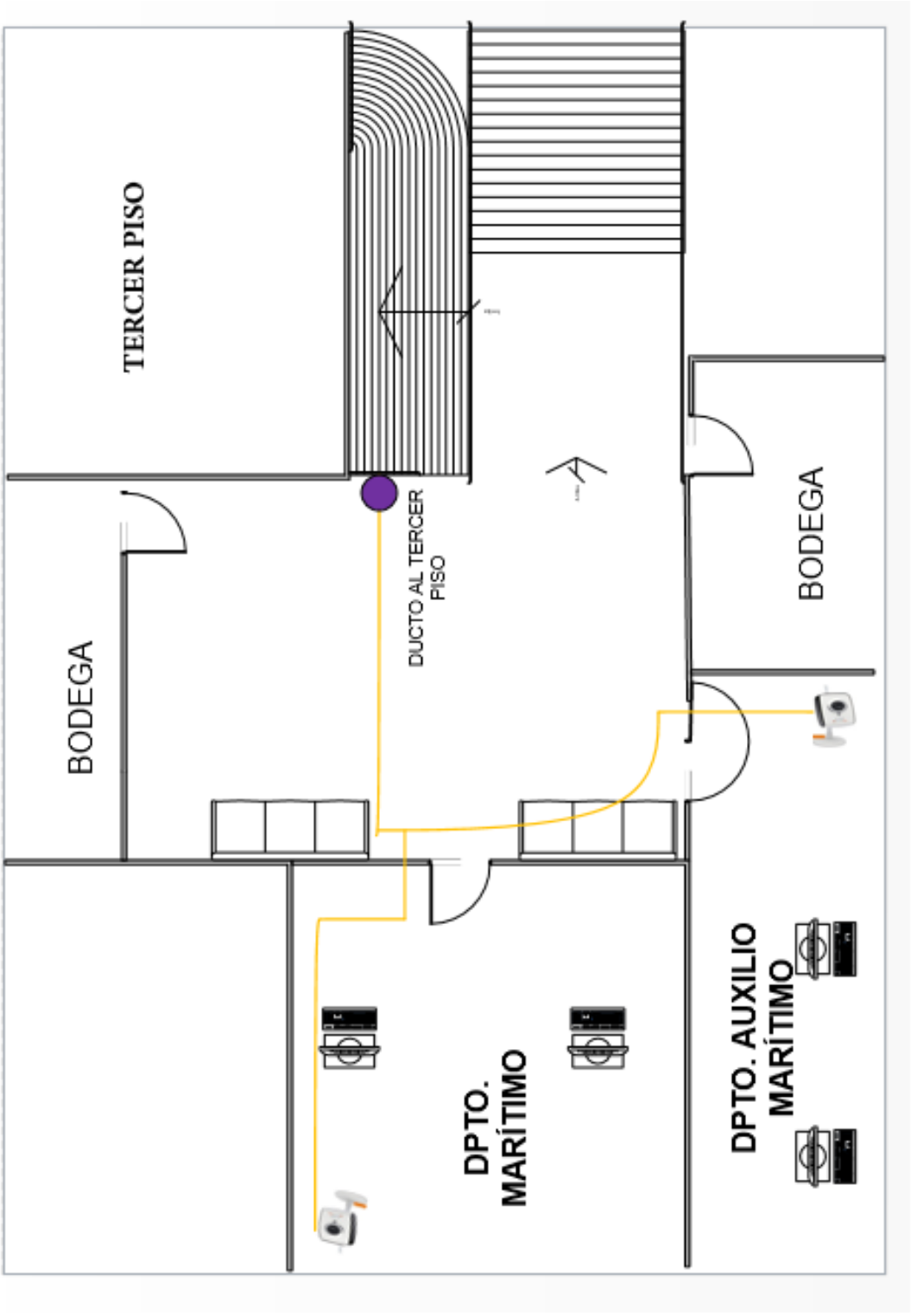
UBICACIÓN DE LAS CÁMARAS EN LA PLANTA BAJA DEL EDIFICIO DE LA CAPITANÍA DEL PUERTO



UBICACIÓN DE LAS CÁMARAS EN EL SEGUNDO PISO DEL EDIFICIO DE LA CAPITANÍA DEL PUERTO



UBICACIÓN DE LAS CÁMARAS EN EL TERCER PISO DEL EDIFICIO DE LA CAPITANÍA DEL PUERTO



ANEXO 5

CAPITANÍA DELPUERTO DE LA CIUDAD DE MANTA, LUGAR DONDE SE IMPLEMENTO EL SISTEMA DE VIGILANCIA

ANEXO 6

MATERIALES Y HERRAMIENTAS NECESARIAS PARA LA INSTALACIÓN DE LAS CÁMARAS DE SEGURIDAD

ANEXO 7

DISPOSITVOS TECNOLÓGICOS, CÁMARA Y SWITCH MODELO TRENDNET

ANEXO 8

CABLE UTP CAT 5E PARA LA COMUNICACIÓN DE LAS CÁMARAS IP

ANEXO 9

UBICACIÓN DE CANALETAS DE ACUERDO AL DISEÑO ESTIPULADO EN EL ANEXO 3

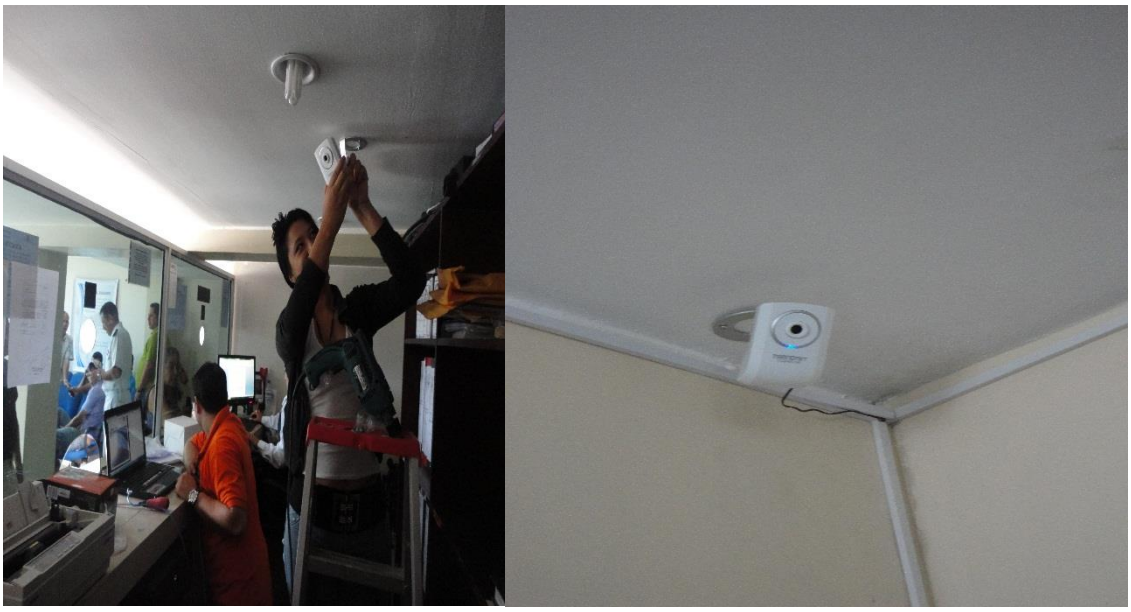
ANEXO 10

UBICACIÓN DEL CABLE CAT. 5E DENTRO DE LAS CANALETAS

ANEXO 11

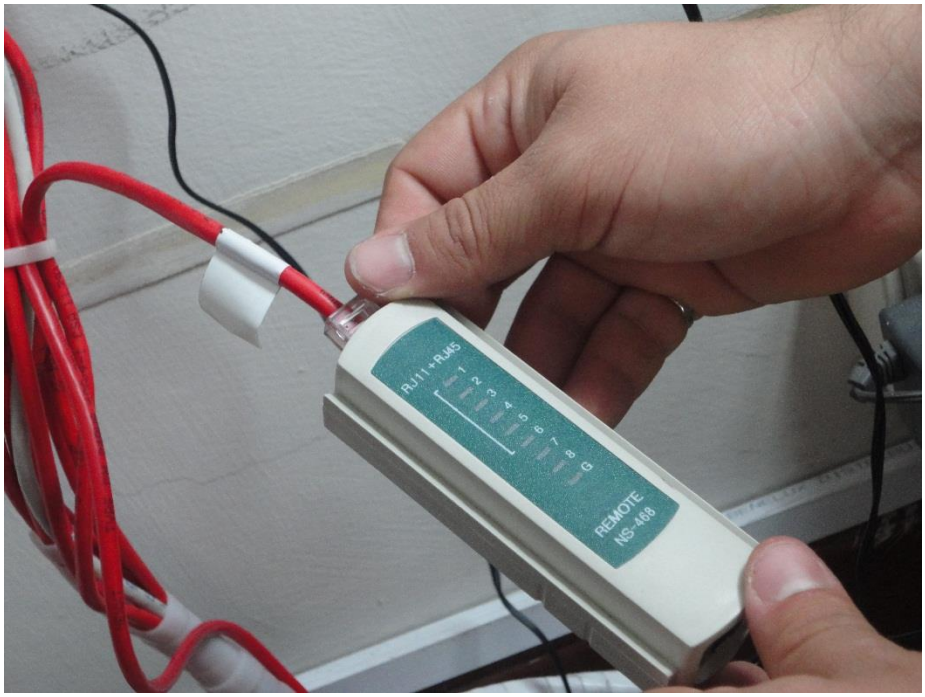
ESTRUCURACIÓN DEL PONCHADO DEL CABLE DE ACUERDO AL ESTÁNDAR DE LA IEEE, TIPO CLASE B

ANEXO 12



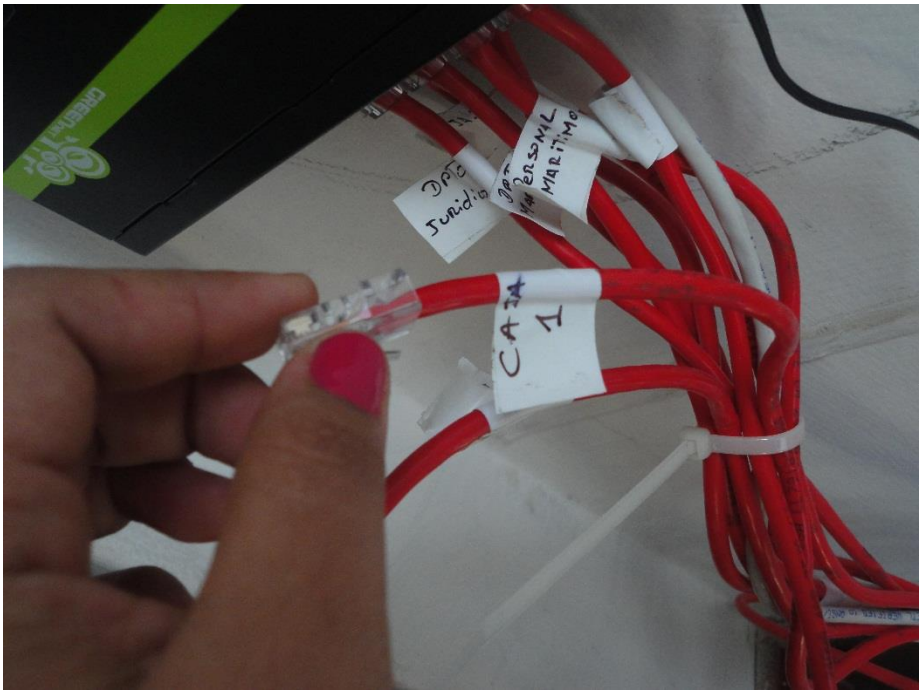
UBICACÍON DE LAS CÁMARAS IP DE ACUERDO AL DISEÑO DEL ANEXO 3

ANEXO 13



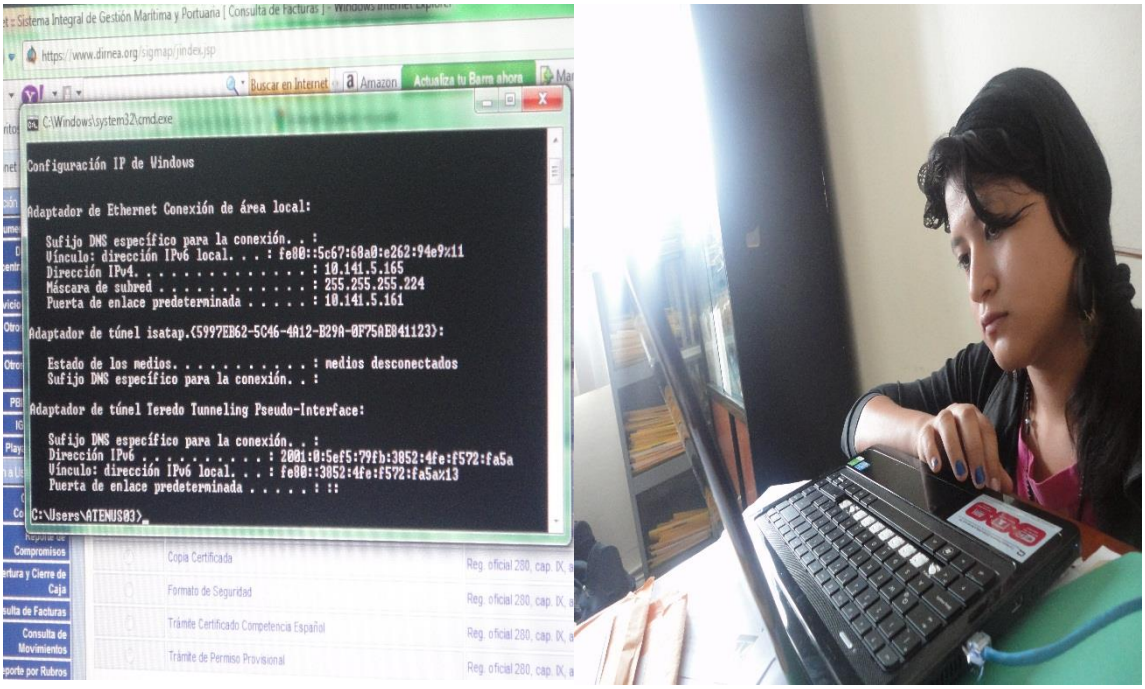
APLICACIÓN DEL TESTEADOR DE CLAVES PARA LA VERIFICACION DEL CABLE DE RED

ANEXO 14



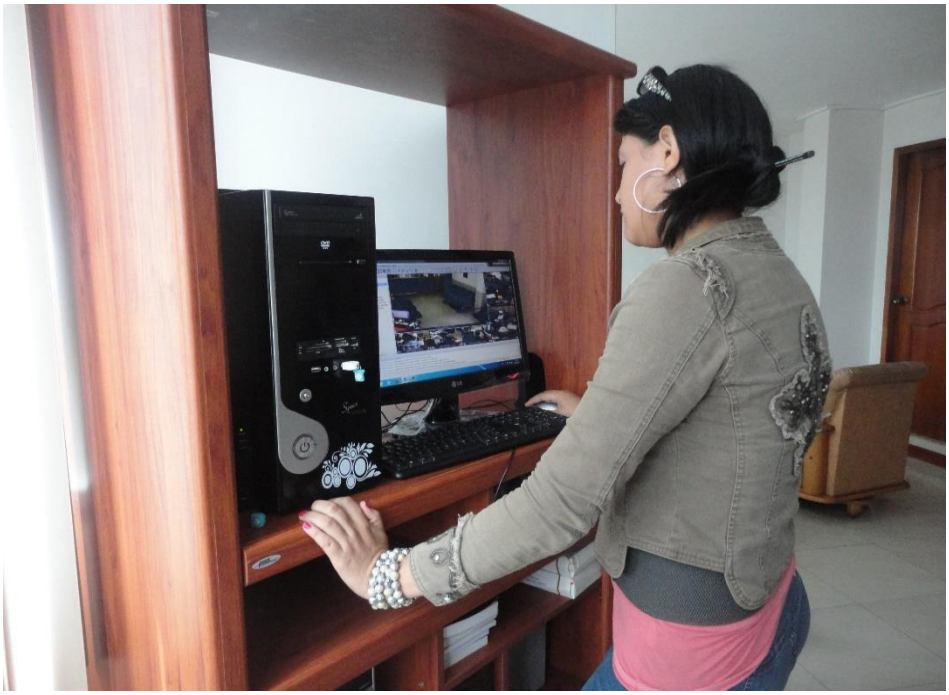
IDENTIFICACIÓN DE CADA CABLE DE RED EN EL SWITCH

ANEXO 15



CONFIGURACIÓN Y VALIDACIÓN DE RESPUESTA DE LA CÁMARA IP CON EL SERVIDOR

ANEXO 16



INSTALACIÓN Y CONFIGURACIÓN DEL SOFTWARE DE DETECCIÓN DE ROSTRO EN EL EQUIPO ASIGNADO COMO SERVIDOR

ANEXO 17

LOCALIZACIÓN DEL SERVIDOR QUE MANIPULA EL SOFTWARE DE DETECCIÓN DE ROSTRO PARA LAS CÁMARAS DE VIGILANCIA

ANEXO 18

El objetivo de esta encuesta o investigación de mercado es para determinar la acogida del Sistema de vigilancia que fue implementado dentro de las oficinas de la Capitanía del Puerto de Manta
.

Marque con un X las opciones que usted considere acertadas

1. ¿Está conforme con la seguridad que brinda el sistema de vigilancia instalado en su institución?

SI ☐
NO ☐
TALVEZ ☐

2. ¿Se ha detectado algún error o fallas con el sistema de vigilancia?

SI ☐
NO ☐
TALVEZ ☐

3. ¿Debería emplear más cámaras de vigilancia dentro de la Capitanía?

SI ☐
NO ☐
TALVEZ ☐

4. ¿Está de acuerdo en que toda institución debería emplear un sistema de vigilancia?

SI ☐
NO ☐

5. ¿Mejoro la seguridad dentro de la Capitanía con ayuda del sistema de vigilancia con cámaras IP?

SI ☐
NO ☐

6. ¿Está usted de acuerdo con los lugares en donde fueran ubicadas las cámaras de seguridad?

SI ☐
NO ☐

7. ¿Con que frecuencia se mantienen encendida las cámaras de vigilancia?

48 Horas ☐
24 Horas ☐
12 Horas ☐

8. ¿Cree usted que si fue conveniente la implementación de las cámaras?

SI ☐
NO ☐

ANEXO 19

TABULACIÓN DE LOS DATOS DE LA ENCUESTA

1. **¿Está conforme con la seguridad que brinda el sistema de vigilancia instalado en su institución?**

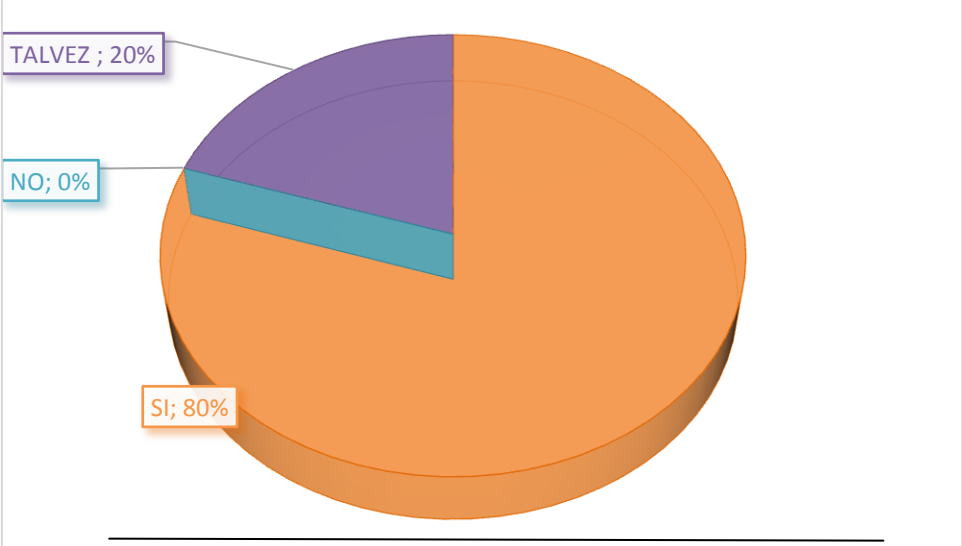


Gráfico 4-A. Confirmación de los trabajadores sobre el sistema de vigilancia

Tabla 4-A Resultados la confirmación de los trabajadores sobre el sistema de Vigilancia

OPCIONES	TOTAL
SI	40
NO	0
TALVEZ	10

Análisis e interpretación:

En la primera pregunta se obtuvo un resultado de 80% de los trabajadores que estuvieron conforme con el sistema mientras tanto también hubo un 20% que dijo q talvez no estaban conforme con el sistema.

2. ¿Se ha detectado algún error o fallas con el sistema de vigilancia?

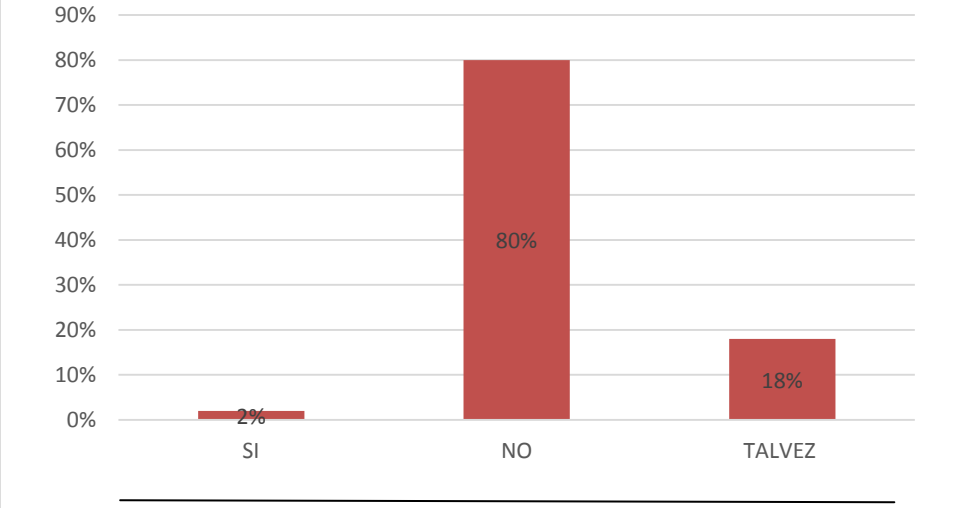


Gráfico 4-B. Resultados sobre detección de errores o fallos del sistema

Tabla 4-B Resultados sobre detección de errores o fallos del sistema de vigilancia

OPCIONES	TOTAL
SI	1
NO	40
TALVEZ	9

Análisis e interpretación:

En esta pregunta se obtuvo un resultado de 2% de los trabajadores dijeron que si hubo fallos en el sistema mientras tanto también hubo un 80% que dijo que no que no había pasado nada y un 18% que talvez no se había detectado fallos o errores con el sistema.

3. **¿Debería emplear más cámaras de vigilancia dentro de la Capitanía?**

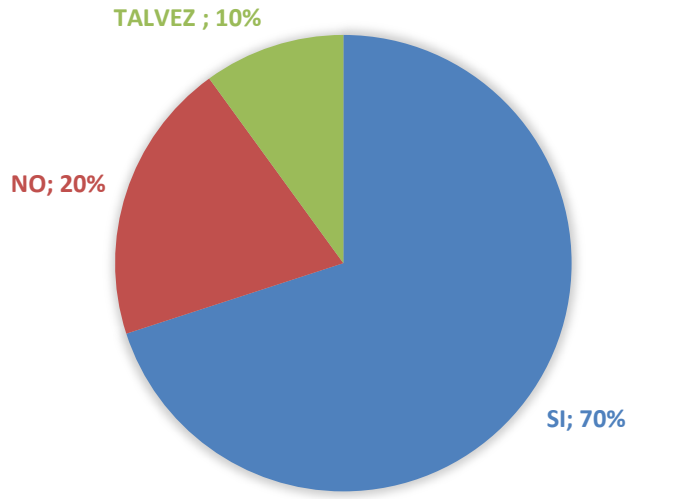


Gráfico 4-C. Resultados de si desean emplear más cámaras IP

Tabla 4-C Resultados di desean emplear más cámara

OPCIONES	TOTAL
SI	35
NO	10
TALVEZ	5

Análisis e interpretación:

En esta pregunta se obtuvo un resultado de 70% de los trabajadores dijeron que si se debe emplear más cámaras mientras tanto también hubo un 20% que dijo que no y un 10% que talvez se debe emplear más cámaras IP.

4. **¿Está de acuerdo en que toda institución debería emplear un sistema de vigilancia?**

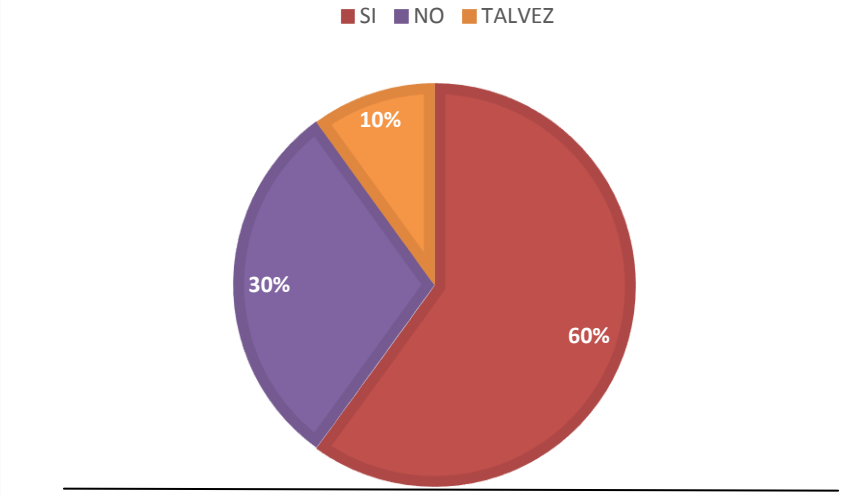


Gráfico 4-D. Resultados de que si todas las instituciones deben emplear un sistema de vigilancia

Tabla 4-C Resultados di desean emplear más cámara

OPCIONES	TOTAL
SI	35
NO	10
TALVEZ	5

Análisis e interpretación:

En esta pregunta se obtuvo un resultado de 60% de los trabajadores dijeron que si se debe emplear un sistema de vigilancia en toda institución, mientras tanto también hubo un 30% que dijo que no y un 10% que talvez.

5. **¿Mejoro la seguridad dentro de la Capitanía con ayuda del sistema de vigilancia con cámaras IP?**

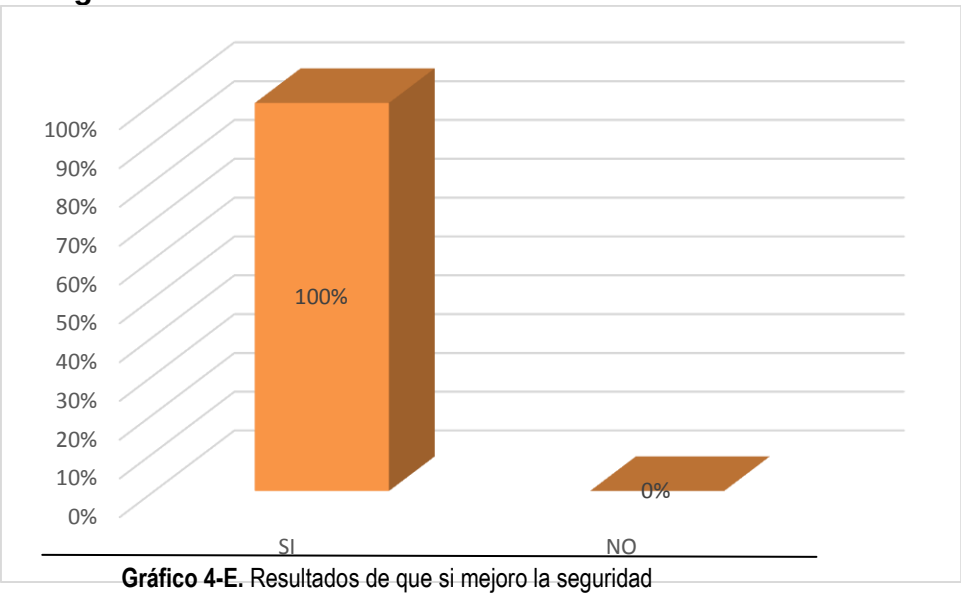


Gráfico 4-E. Resultados de que si mejoro la seguridad

Tabla 4-E Resultados de que si mejoro la seguridad

OPCIONES	TOTAL
SI	50
NO	0

Análisis e interpretación:

En esta pregunta se obtuvo un resultado de 100% de los trabajadores dijeron que si se mejoró la seguridad con ayuda del sistema.

6. ¿Está usted de acuerdo con los lugares en donde fueran ubicadas las cámaras de seguridad?

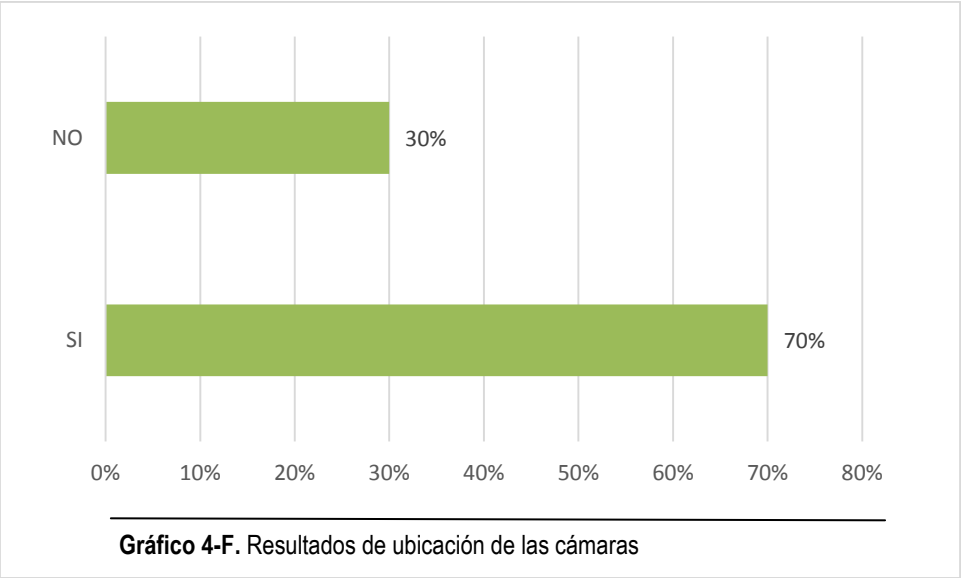


Gráfico 4-F. Resultados de ubicación de las cámaras

Tabla 4-F Resultados de ubicación de las cámaras

OPCIONES	TOTAL
SI	35
NO	15

Análisis e interpretación:

En esta pregunta se obtuvo un resultado de 70% de los trabajadores dijeron que si estaban en correcta ubicación y 30% no estaba conforme

7. ¿Con que frecuencia se mantienen encendida las cámaras de vigilancia?

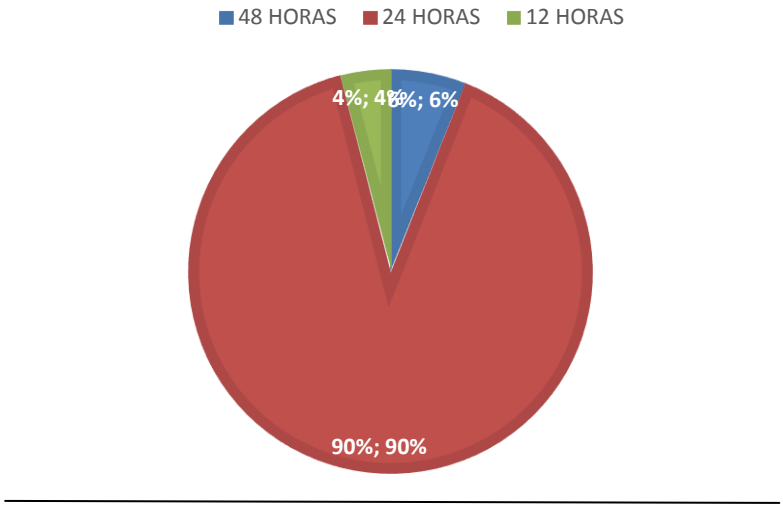


Gráfico 4-G. Resultados de Estado de encendido de las cámaras

Tabla 4-G Resultados de estado de encendido de las cámaras

OPCIONES	TOTAL
48 Horas	3
24 Horas	45
12 Horas	2

Análisis e interpretación:

En esta pregunta se obtuvo un resultado de 6% de los trabajadores dijeron que las cámaras estaban encendidas solo 48 horas, 90% dijo q las 24 horas y un 4% dijo que solo estaban encendidas 12 horas.

8. ¿Cree usted que si fue conveniente la implementación de las cámaras?

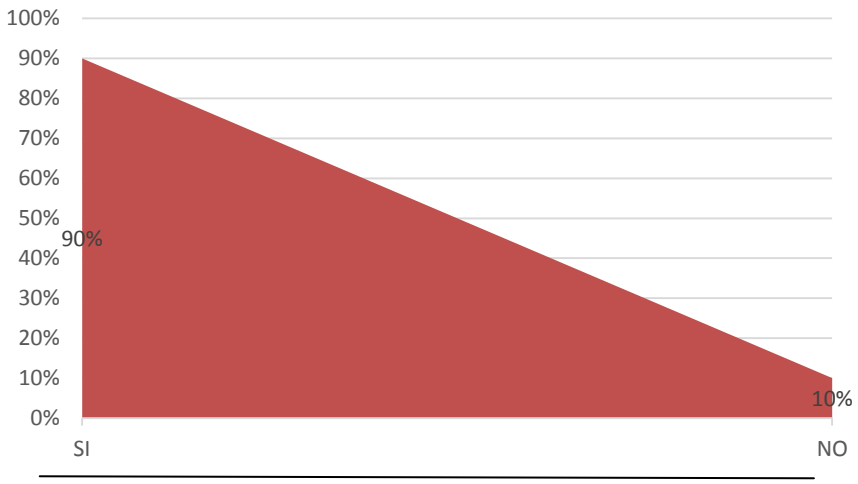


Gráfico 4-H. Resultados de satisfacción de la implementación del sistema

Tabla 4-H Resultados de satisfacción de la implementación del sistema

OPCIONES	TOTAL
SI	45
NO	5

Análisis e interpretación:

En esta última pregunta se obtuvo un resultado de 90% de los trabajadores creen que fue satisfactorio la implementación del sistema y un 10% dijo q no.

Análisis Final:

Por medio de la presente técnica de investigación se logró encuestar a 50 personas dentro de la Capitanía del Puerto de la ciudad de Manta, dando como resultado una satisfacción por la implementación del sistema de vigilancia, tomando en cuenta que la entidad se encuentra con un control eficaz y preciso en áreas donde se ubicaron las cámaras, así mismo se logró la acogida por parte del Comandante quien ahora posee eficientemente el acceso al registro y almacenamiento del sistema de vigilancia.

ANEXO 20

MANUAL DE USUARIO DEL SISTEMA DE VIGILANCIA CON CÁMARAS IP

MANUAL DE USUARIO

ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ

MANUEL FÉLIZ LÓPEZ

ABRIL DE 2014

GEMA VICTORIA ZAMBRANO ZAMBRANO

INTRODUCCIÓN

El sistema de vigilancia mediante cámaras ip como objetivo principal controlar e identificar el ingreso de las personas que ingresan a la Capitanía del Puerto de la ciudad de Manta, generando automáticamente reportes de la cantidad de personas que ingresan a la institución. Este sistema se caracteriza porque es accesible, dinámico, interactivo y sencillo de utilizar, ya que sus interfaces son dinámicas y la aplicación se encuentra desarrollada para ser ejecutada modo web y escritorio.

La autora se ha basado en la revisión de la evidencia científica actualizada, seleccionando los programas de Java y Eclipse para su desarrollo y codificación mediante librerías de OpenCV y JavaCv.

El propósito de este Manual es facilitar al usuario la operación de las diferentes opciones del sistema y configuración de la Cámara de seguridad.

REQUERIMIENTOS Y CARACTERISTICAS

Características Generales Sistema

- Interfaz Gráfica y amigable
- Personalización de menús
- Actualización de datos en tiempo real
- Generador de informes que permiten al usuario conocer la cantidad de personas que han sido detectadas.
- Entrada de datos y capturas de imágenes.
- Asistencia en la Implementación y capacitación para puesta en marcha del sistema
- No requiere Software adicional para manejo de base de datos.
- Corre sobre diversas plataformas de sistema operativo: (Windows®,
- UNIX®, Linux®).

Requerimientos Técnicos

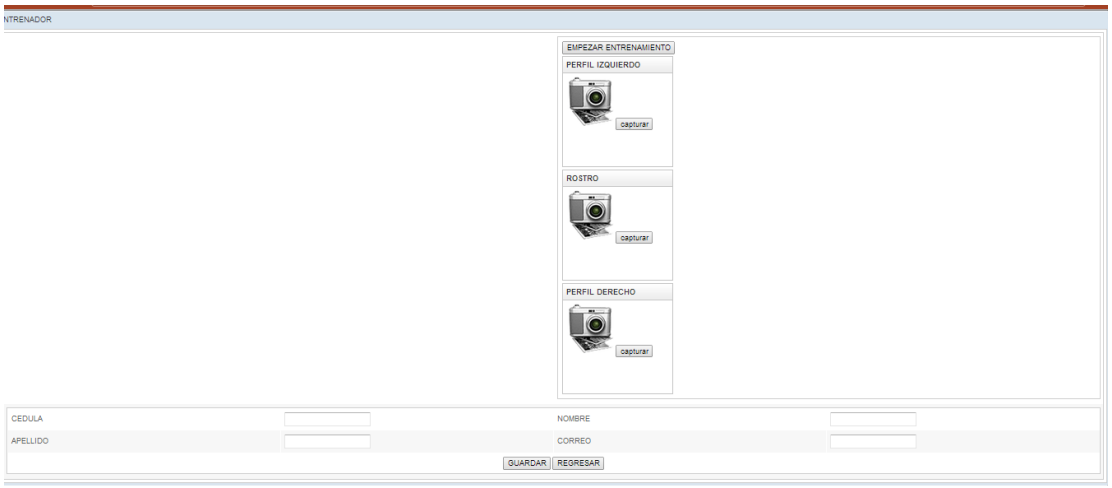
- Las características técnicas recomendados son los siguientes:
- Servidor de las aplicaciones
- Procesador 2.7 GHz AMD EPROM o superior
- 4 GB en memoria RAM.
- 500 Gigas disponibles en disco duro o superior.
- Monitor VGA a color.
- Unidad de DVD-ROM.
- Tarjeta de Video
- Cámara de Vigilancia IP

DESCRIPCIÓN DEL FUNCIONAMIENTO

El software cuenta con una interfaz amigable de fácil dominio para el usuario permiten acceder a ver la Cámara y a realizar la fase de entrenamiento.

Cabe recalcar que la aplicación está realizada a modo escritorio y modo web para su mayor satisfacción

La aplicación cuenta con la opción de entrenamiento que es la que permite al administrador realizar la captura de las imágenes en tres ángulos del rostro, frente, derecho e izquierdo.



Así mismo al realizar la captura de deben guardar los datos de la persona, tomando en cuenta que va generando la cantidad de personas que van siendo identificadas por el sistema.

El reconocimiento y contador de las personas que ingresan a la capitanía se lo realiza mediante dos algoritmos los cuales son el Algoritmo de Entrenamiento y Reconocimiento.

CÓDIGOS DEL SISTEMA

A continuación se detalla el código principal de los algoritmos de Entrenamiento y Reconocimiento

```
public class Main {


    public static void main(String args[]){
        try {

            ReconocimientoCaras reconocer =
ReconocimientoCaras.getInstance();



            //Entrenamiento
            /*
            IplImage[] trainImages = new IplImage[10];
            for(int i=1; i<=10; i++){
                //trainImages[i-
1]=cvLoadImage("C:/facerecognizer/data/images/training/terry"+i+".jpg"
);
               trainImages[i-
1]=cvLoadImage("C:/facerecognizer/data/images/training/cr7"+i+".jpg");
                CvSeq faces = reconocer.detectFace(trainImages[i-1]);
                CvRect r = new CvRect(cvGetSeqElem(faces,0));
                trainImages[i-
1]=reconocer.preprocessImage(trainImages[i-1], r);
            }
            reconocer.learnNewFace("cr", trainImages);
          */

            //Reconocimiento

            IplImage target = new IplImage();
            //target =
cvLoadImage("C:/facerecognizer/data/images/training/terry_target.jpg")
;
           target =
cvLoadImage("C:/facerecognizer/data/images/training/cr7_target.jpg");
            CvSeq faces2 = reconocer.detectFace(target);
            CvRect r2 = new CvRect(cvGetSeqElem(faces2,0));
            target=reconocer.preprocessImage(target, r2);
            System.out.println("PERSONA IDENTICADA:
"+reconocer.identifyFace(target));


        } catch (Exception ex) {
            Logger.getLogger(Main.class.getName()).log(Level.SEVERE,
null, ex);
        }

    }
}
```

Código para el Reconocimiento de Caras

```
public class ReconocimientoCaras {
```

```
    private static String faceDataFolder =
"C:\\Users\\vicky_000\\Documents\\facerecognizer\\data\\";
    public static String imageDataFolder = faceDataFolder +
"images\\";
    private static final String CASCADE_FILE =
"C:\\Users\\vicky_000\\Documents\\facerecognizer\\data\\haarcascades\\
haarcascade_frontalface_alt.xml";
    private static final String BinaryFile = faceDataFolder +
"frBinary.dat";
    public static final String personNameMappingFileName =
faceDataFolder + "personNumberMap.properties";

    final CvHaarClassifierCascade cascade = new
CvHaarClassifierCascade(cvLoad(CASCADE_FILE));
    private Properties dataMap = new Properties();
    private static ReconocimientoCaras instance = new
ReconocimientoCaras();

    public static final int NUM_IMAGES_PER_PERSON =10;
    double binaryTreshold = 100;
    int highConfidenceLevel = 70;

    FaceRecognizer ptr_binary = null;
    private FaceRecognizer fr_binary = null;



    private ReconocimientoCaras() {
            createModels();
            loadTrainingData();
    }

    public static ReconocimientoCaras getInstance() {

      return instance;
    }

    private void createModels() {
            ptr_binary = createLBPHFaceRecognizer(1, 8, 8, 8,
binaryTreshold);
            fr_binary = ptr_binary;
    }

    protected CvSeq detectFace(IplImage originalImage) {
            CvSeq faces = null;
            Loader.load(opencv_objdetect.class);
            try {
                    IplImage grayImage =
IplImage.create(originalImage.width(), originalImage.height(),
IPL_DEPTH_8U, 1);
                    cvCvtColor(originalImage, grayImage, CV_BGR2GRAY);
                    CvMemStorage storage = CvMemStorage.create();
                    faces = cvHaarDetectObjects(grayImage, cascade,
storage, 1.1, 1, 0);

            } catch (Exception e) {
                    e.printStackTrace();
            }
            return faces;
```

```
    }

    public String identifyFace(IplImage image) {
            String personName = "";
            Set keys = dataMap.keySet();

            if (keys.size() > 0) {
                    int[] ids = new int[1];
                    double[] distance = new double[1];
                    int result = -1;

                            fr_binary.predict(image, ids, distance);
                            result = ids[0];

                            if (result > -1 &&
distance[0]<highConfidenceLevel) {
                                    personName = (String)
dataMap.get("" + result);
                            }
            }

            return personName;
    }

    public boolean learnNewFace(String personName, IplImage[] images)
throws Exception {
            int memberCounter = dataMap.size();
            if(dataMap.containsValue(personName)){
                    Set keys = dataMap.keySet();
                    Iterator ite = keys.iterator();
                    while (ite.hasNext()) {
                            String personKeyForTraining = (String)
ite.next();
                            String personNameForTraining = (String)
dataMap.getProperty(personKeyForTraining);

if(personNameForTraining.equals(personName)){
                                    memberCounter =
Integer.parseInt(personKeyForTraining);
                            }
                    }
            }
            dataMap.put("" + memberCounter, personName);
            storeTrainingImages(personName, images);
            retrainAll();

            return true;
    }


    public IplImage preprocessImage(IplImage image, CvRect r){
            IplImage gray = cvCreateImage(cvGetSize(image),
IPL_DEPTH_8U, 1);
            IplImage roi = cvCreateImage(cvGetSize(image),
IPL_DEPTH_8U, 1);
            CvRect r1 = new CvRect(r.x()-10, r.y()-10, r.width()+10,
r.height()+10);
            cvCvtColor(image, gray, CV_BGR2GRAY);
            cvSetImageROI(gray, r1);
            cvResize(gray, roi, CV_INTER_LINEAR);
```

```
            cvEqualizeHist(roi, roi);
            return roi;
    }

    private void retrainAll() throws Exception {
            Set keys = dataMap.keySet();
            if (keys.size() > 0) {
                    MatVector trainImages = new MatVector(keys.size()
* NUM_IMAGES_PER_PERSON);
                    CvMat trainLabels = CvMat.create(keys.size() *
NUM_IMAGES_PER_PERSON, 1, CV_32SC1);
                    Iterator ite = keys.iterator();
                    int count = 0;

                    System.err.print("Cargando imagenes para
entrenamiento ...");
                    while (ite.hasNext()) {
                            String personKeyForTraining = (String)
ite.next();
                            String personNameForTraining = (String)
dataMap.getProperty(personKeyForTraining);
                            IplImage[] imagesForTraining =
readImages(personNameForTraining);

                            for (int i = 0; i <
imagesForTraining.length; i++) {
                                    trainLabels.put(count, 0,
Integer.parseInt(personKeyForTraining));
                                    IplImage grayImage =
IplImage.create(imagesForTraining[i].width(),
imagesForTraining[i].height(), IPL_DEPTH_8U, 1);
                                    cvCvtColor(imagesForTraining[i],
grayImage, CV_BGR2GRAY);
                                    trainImages.put(count,grayImage);
                                    count++;
                            }
                    }

                    System.err.println("hecho.");

                    System.err.print("Realizando entrenamiento ...");
                    fr_binary.train(trainImages, trainLabels);
                    System.err.println("hecho.");
                    storeTrainingData();
            }

    }

    private void loadTrainingData() {
            try {
                    File personNameMapFile = new
File(personNameMappingFileName);
                    if (personNameMapFile.exists()) {
                            FileInputStream fis = new
FileInputStream(personNameMappingFileName);
                            dataMap.load(fis);
                            fis.close();
                    }

                    File binaryDataFile = new File(BinaryFile);
```

```
                    binaryDataFile.createNewFile();
                    fr_binary.load(BinaryFile);
                    System.err.println("hecho");


            } catch (Exception e) {
                    e.printStackTrace();
            }
    }

    private void storeTrainingData() throws Exception {
            System.err.print("Almacenando modelos ...");

            File binaryDataFile = new File(BinaryFile);
            if (binaryDataFile.exists()) {
                    binaryDataFile.delete();
            }
            fr_binary.save(BinaryFile);

            File personNameMapFile = new
File(personNameMappingFileName);
            if (personNameMapFile.exists()) {
                    personNameMapFile.delete();
            }
            FileOutputStream fos = new
FileOutputStream(personNameMapFile, false);
            dataMap.store(fos, "");
            fos.close();

            System.err.println("hecho.");
    }


    public void storeTrainingImages(String personName, IplImage[]
images) {
            for (int i = 0; i < images.length; i++) {
                    String imageFileName = imageDataFolder +
"training\\" + personName + "_" + i + ".bmp";
                    File imgFile = new File(imageFileName);
                    if (imgFile.exists()) {
                            imgFile.delete();
                    }
                    cvSaveImage(imageFileName, images[i]);
            }
    }

    private IplImage[] readImages(String personName) {
            File imgFolder = new File(imageDataFolder);
            IplImage[] images = null;
            if (imgFolder.isDirectory() && imgFolder.exists()) {
                    images = new IplImage[NUM_IMAGES_PER_PERSON];
                    for (int i = 0; i < NUM_IMAGES_PER_PERSON; i++) {
                            String imageFileName = imageDataFolder +
"training\\" + personName + "_" + i + ".bmp";
                            IplImage img = cvLoadImage(imageFileName);
                            images[i] = img;
                    }

            }
            return images;
```

```
    }
}
```

Código para el Panel de Video de la cámara

```
public class PanelVideo extends javax.swing.JPanel {

    private boolean hayConexion = false;
    private String direccionIP = "";
    public BufferedImage frame = null;

    /** Creates new form PanelVideo */
    public PanelVideo() {
        initComponents();
    }

    public boolean isHayConexion() {
        return hayConexion;
    }

    public void setHayConexion(boolean hayConexion) {
        this.hayConexion = hayConexion;
    }

    public String getDireccionIP() {
        return direccionIP;
    }

    public void setDireccionIP(String direccionIP) {
        this.direccionIP = direccionIP;
    }

    @Override
    public void paintComponent(Graphics g) {

      Graphics2D g2 = (Graphics2D) g;
        g2.setColor(Color.white);
        g2.fillRect(0, 0, getWidth(), getHeight());

        if (hayConexion) {



            URL nurl = null;
            try {
            nurl = new URL("http://192.168.0.100/IMAGE.JPG");
            URLConnection connection = nurl.openConnection();
            connection.setRequestProperty("admin", "admin");
            frame = ImageIO.read(nurl);
            if (frame != null) {

                g2.drawImage(frame, 0, 0, this);
                repaint();
            }
            } catch (MalformedURLException e) {
            e.printStackTrace();
            } catch (IOException e) {
                        // TODO Auto-generated catch block
                        e.printStackTrace();
```

```
                }
            Authenticator au = new Authenticator() {
            @Override
            protected PasswordAuthentication
getPasswordAuthentication() {
            return new PasswordAuthentication ("admin",
"admin".toCharArray());
            }
            };
            Authenticator.setDefault(au);
        } else {
            g2.setColor(Color.black);
            g2.drawString("No se ha establecido conexiÃ³n con el
dispositivo.", 5, 15);
        }
    }

    /** This method is called from within the constructor to
     * initialize the form.
     * WARNING: Do NOT modify this code. The content of this method is
     * always regenerated by the Form Editor.
     */
    @SuppressWarnings("unchecked")
    // <editor-fold defaultstate="collapsed" desc="Generated
Code">//GEN-BEGIN:initComponents
    private void initComponents() {

        setBorder(javax.swing.BorderFactory.createLineBorder(new
java.awt.Color(153, 153, 153), 2));
        setMaximumSize(new java.awt.Dimension(640, 480));
        setMinimumSize(new java.awt.Dimension(640, 480));
        setPreferredSize(new java.awt.Dimension(640, 480));

        javax.swing.GroupLayout layout = new
javax.swing.GroupLayout(this);
        this.setLayout(layout);
        layout.setHorizontalGroup(

layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
            .addGap(0, 636, Short.MAX_VALUE)
        );
        layout.setVerticalGroup(

layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
            .addGap(0, 476, Short.MAX_VALUE)
        );
    }// </editor-fold>//GEN-END:initComponents
    // Variables declaration - do not modify//GEN-BEGIN:variables
    // End of variables declaration//GEN-END:variables
}
```

Código para la interfaz del usuario

```
<zk>
    <window title="CAMARA" border="normal" position="center"
apply="practicas.menu" >

      <div align="center">
                  <hbox>
                  <groupbox  closable="false" >
                              <caption label="VER CAMARA" ></caption>
```

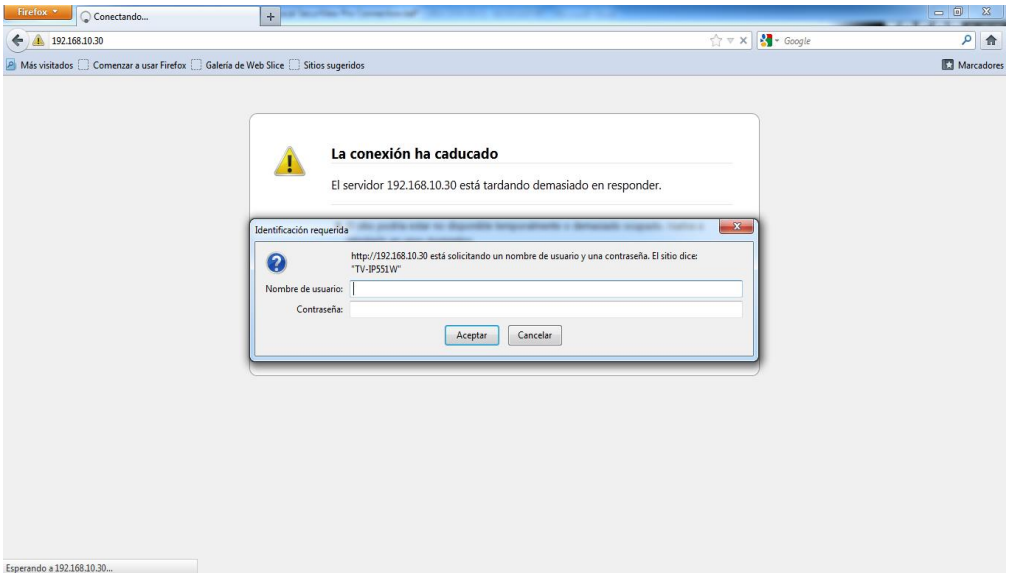
```
                                <image id="imgCapturar"
src="/imagen/capturar.png" />
                    </groupbox>

                    <groupbox  closable="false" >
                                <caption label="ENTRENAR" ></caption>
                                <image id="imgEntrenar"
src="/imagen/entrenar.png"/>
                    </groupbox>
                    </hbox>
            </div>

    </window>
</zk>
```

CONFIGURACIÓN DE LAS CÁMARAS IP MARCA TREDNET MODELO 551W

Para la configuración de este tipo de cámara, primeramente se debe realizar la respectiva configuración de la ip en el navegador que desee, colocando la dirección ip que viene por defecto en las cámaras las cuál es 192.168.10.30



Aquí se procede a introducir el nombre del usuario que por defecto es admin y el password que también es admin y aceptar.

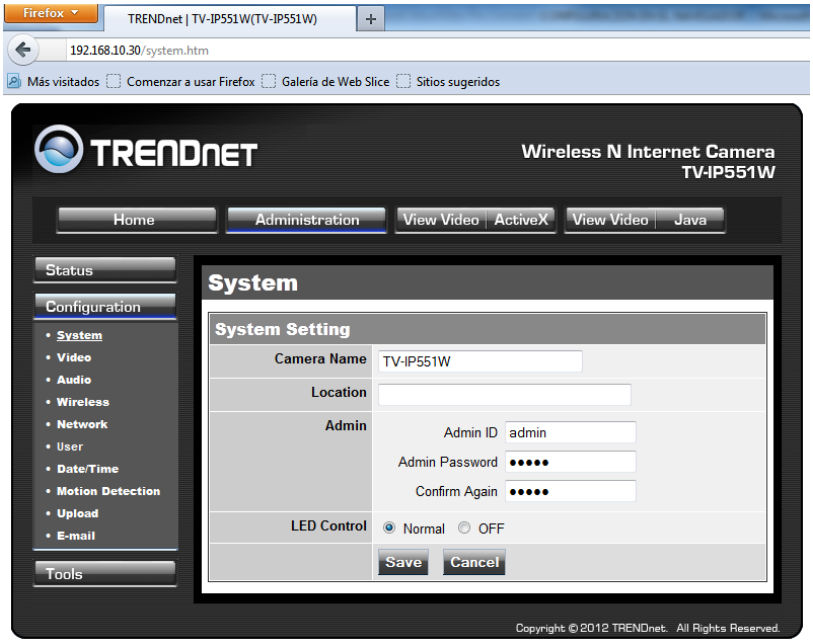
Luego ingresamos a la configuración de la cámara dentro del navegador.

Una vez ahí procedemos a dar clic en Administration en la opción Configuration.

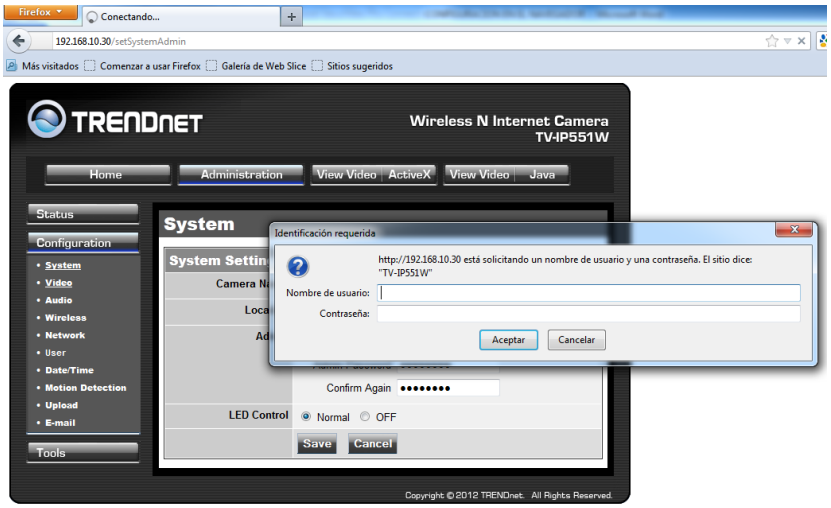
Aquí se le puede asignar las siguientes opciones Camera Name (nombre de la cámara), la Location (localización), En la sección de Admin tenemos otras opciones:

1. Admin Id: El nombre del usuario para acceder a cualquier configuración sobre esa cámara.
2. Admin Password: La clave o contraseña
3. Confirm Again: Para confirmar la contraseña asignada
4. Led Control: Si se desea tener las luces de la cámara encendida o no, para lo cual escogeremos Normal

5. Save: Para guardar los respectivas cambios o configuraciones.



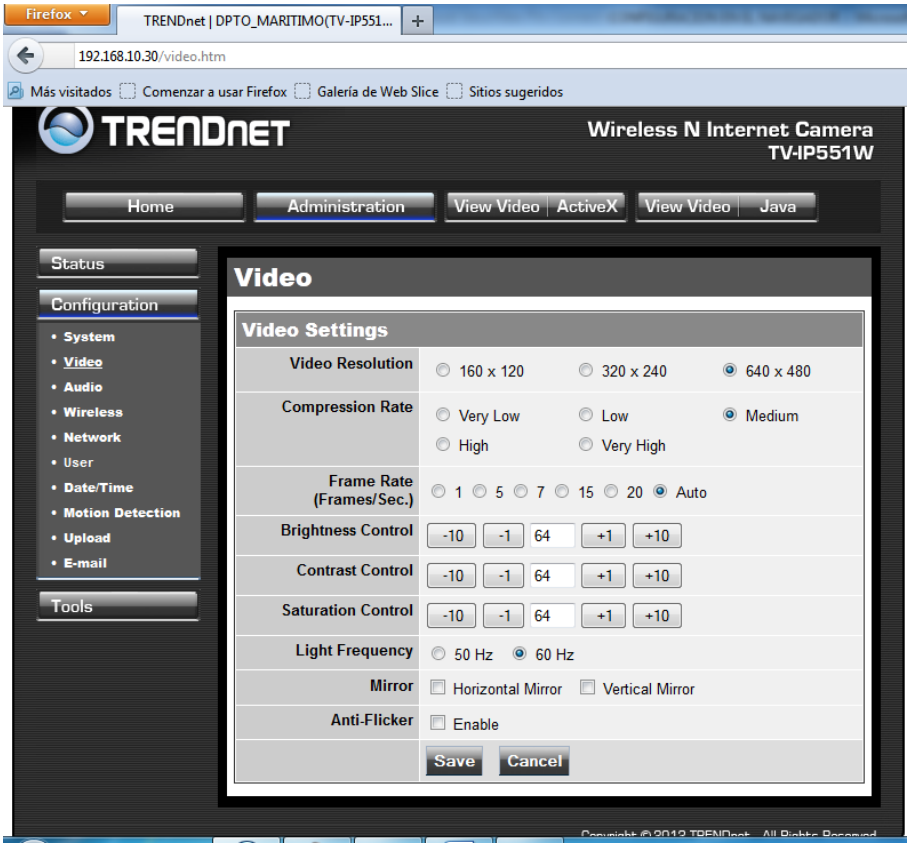
Ahora procedemos a comprobar los cambios realizados e ingresamos el usuario y password asignado en el paso anterior.



Ahora se procede a continuar con las siguientes opciones entre las cuales realizaremos lo siguiente:

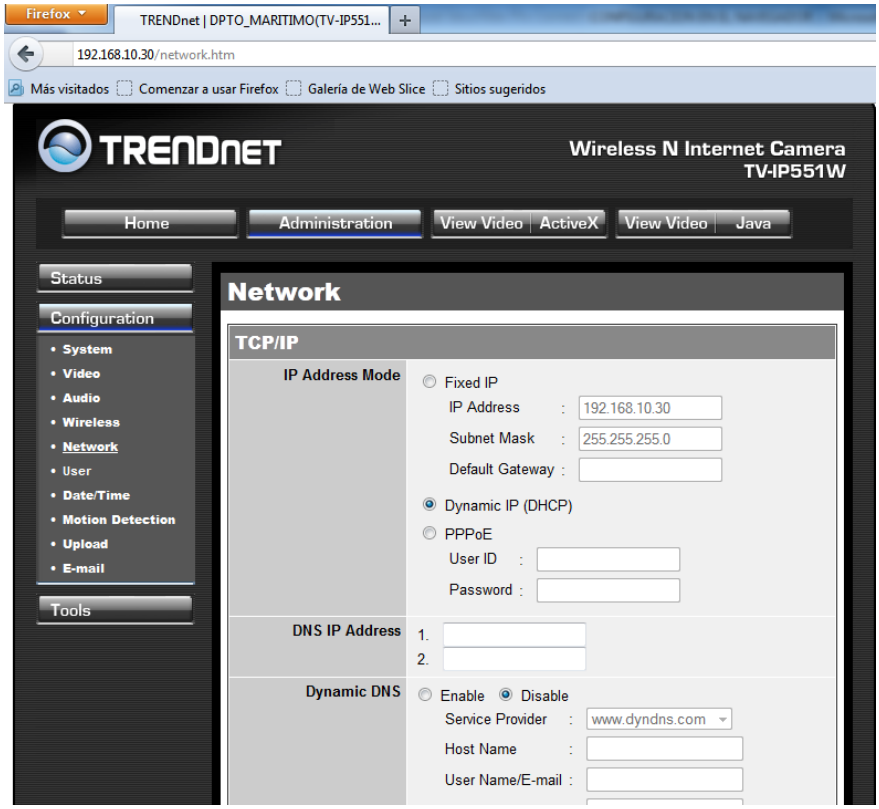
1. Administration
2. Configuration: en la opción Video
3. Video Resolution: Se procede a escoger la resolución que más le convenga al usuario, para este caso se escogió la resolución de 640X480

4. Configuration Rate: Se ha escogido la opción High.
5. Save: para guardar los cambios efectuados.



Después se prosigue con lo siguiente:

1. Administration: se escoge la Opción Configuration.
2. Configuration: Procedemos a escoger Network.
3. Ip Address Mode: En esta opción se puede realizar todas las configuraciones sobre la red o dirección ip que va a tener o asignar la cámara.
4. Fixed Ip: Aquí se le puede asignar la nueva dirección ip a la cámara ya dejara de tener la 192.168.10.30 que viene por defecto a la nueva que le asigne el usuario. En este caso se ha escogido la siguiente Ip: 192.168.10.16.
5. Subnet Mask: En esta opción se le asigna la máscara de subred, que por defecto es 255.255.255.0
6. Save: guardamos los cambios efectuados.

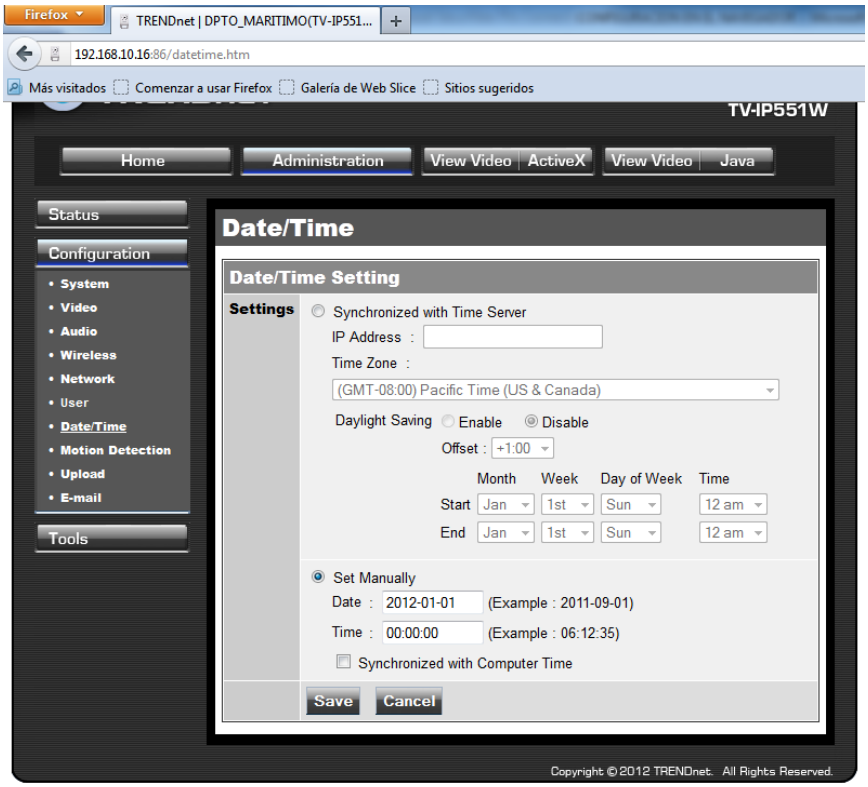


Hemos asignado una nueva dirección ip a nuestra cámara, para lo cual debemos introducir esa dirección en la barra de direcciones del navegador, o de lo contrario no se tendrá accedo a las demás configuraciones.

Una vez ingresado con la nueva dirección ip de la cámara se prosigue con lo siguiente:

1. Administration: se escoge la Opción Configuration.
2. Configuration: Procedemos a escoger Data Time.
3. Setting: Esta opción nos permite tener una sincronización del tiempo de la cámara junto con la pc.
4. Escogemos la opción Sychronized with Time Server.
5. Ip Address: Aquí introduciremos la dirección ip de la cámara la cual añadimos no hace poco, y para nuestro caso es **192.168.10.16**
6. Time Zone: Se le asigna la zona horaria en donde se encuentra, para este caso hemos escogido **(GMT-05 00) Bogotá, Lima, Quito, Rio Branco**

7. Además encontramos otras opciones como Daylight Setting la cual nos permite obtener el tiempo de grabación desde el día y la hora que deseemos hasta el fin de esa grabación.
8. Save: guardamos los cambios efectuados.



ANEXO 21

FUERZAS ARMADAS DEL ECUADOR

Manta, 5 de Marzo del 2014

CERTIFICACIÓN

Por medio de la presente, certifico que la Señorita **Gema Victoria Zambrano Zambrano**, realizo la **INSTALACIÓN DE CÁMARAS IP EN LA CAPITANÍA DEL PUERTO DE LA CIUDAD DE MANTA**, quedando instaladas 8 cámaras ip en las oficinas de nuestra institución, así mismo damos a conocer que los equipos se encuentran funcionando con normalidad.

La interesada pude hacer uso del presente documento en cuanto ella lo amerite.

Atentamente,

José Marcos Vaca
CAPITÁN DE NAVÍO-EM

CERTIFICADO DE CULMINACIÓN DE LA INSTACIÓN DE CÁMARAS