UNIVERSIDAD AMERICANA DE ACAPULCO

"EXCELENCIA PARA EL DESARROLLO"

FACULTAD DE INGENIERÍA EN COMPUTACIÓN

INCORPORADA A LA UNIVERSIDAD NACIONAL
AUTONÓMA DE MÉXICO
CLAVE DE INCORPORACIÓN 8852-16

"SISTEMA DE MONITOREO EN TIEMPO REAL"

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

PRESENTA
GERARDO CABRERA HERNÁNDEZ
ANTONIO GONZÁLEZ RIVERA

DIRECTOR DE TESIS
M. EN C. JOSÉ MARIO MARTÍNEZ CASTRO

ACAPULCO, GRO., ABRIL DEL 2016.

AGRADECIMIENTOS

Gracias a la Universidad Americana de Acapulco por habernos preparado para el camino laboral al cual nos enfrentamos hoy en día.

A nuestra directora de tesis, que le dedico su apreciable tiempo a leer y comentar este trabajo desde su versión inicial hasta la presente.

A nuestra directora técnica por no dejar de insistir en que este trabajo no podía quedar sin terminar.

A los profesores que nos apoyaron compartiendo sus conocimientos y que han resuelto nuestras dudas a años de terminado el periodo universitario.

Gracias a la Ing. Eloisa por no quitar el dedo del renglón.

Gracias al Ing. José Mario por su tiempo y dedicación.

DEDICATORIA

GERARDO CABRERA HERNÁNDEZ.

Esta tesis está dedicada a mi madre Diana María por estar ahí en mis momentos de flaqueza y enfermedad para ayudarme a superarlos, a mi padre José Luis por estar siempre presionándome para exigirme ser mejor en todo lo que hago, a mis hermanos José Luis y Jorge Alberto por sus enseñanzas en esta vida, a Ana Karen por su compresión y paciencia, además de hacerme tolerable mi existencia y a mi hermana Diana Victoria por darme una inspiración para superarme y lograr nuevas metas…Víctor Daniel.

ANTONIO GONZÁLEZ RIVERA.

Este trabajo lo dedico a mi familia, quienes me han ayudado a ser quien soy, a mi Madre Doña Linda, que siempre tuvo una oración para mí, su amor incondicional, quien fue mi pilar y mis otra mamás Linda Rivera, que me tomo como su hijo aun no siéndolo, María Antonia y Naty, quienes de lejos me guiaron y apoyaron en todas mis locuras, a Miguel Rivera quien me exigió a desarrollarme con un diferente reto cada día, a mi querida esposa Saira que no sabría que hacer sin ella y sin olvidar al Sr. Guillermo Cisneros, cuando la electrónica era difícil, él con un simple gesto de bondad, me hizo encontrar la pasión para terminar mi carrera.

CONTENIDO

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Dado los altos índices de inseguridad en la ciudad y puerto de Acapulco[1], se dio a la tarea de desarrollar un sistema de monitoreo de alarmas a través de un botón de pánico, en tiempo real, primero en el Municipio de Acapulco, para después abarcar más Municipios e inclusive Estados.

Este sistema cuenta con elementos que hoy en día se consideran de uso cotidiano, lo cual reducirá el costo total en el momento de su implementación, tratando de no afectar la situación económica de las dependencias.

En el presente trabajo se irá profundizando en los conceptos básicos que componen el sistema de monitoreo, así como los pasos a seguir para poder realizar su implementación y funcionamiento, empezando por su uso y aprovechamiento en las escuelas públicas y privadas, para después sugerir y lograr su instalación en otros lugares de interés y concurrencia, alcanzado con esto el objetivo, que consiste en mejorar el tiempo de respuesta por parte de los diversos cuerpos de seguridad en caso de necesitarlos cuando se presente una situación de emergencia, con lo cual se pretende lograr un ambiente de seguridad que la población merece y necesita.

Por tal motivo, en el presente trabajo se propone una solución al problema usando como caso de estudio al puerto de Acapulco, Gro., el contenido del presente documento se compone de los siguientes capítulos:

[1] Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, 2012

En el Capítulo 1 hablaremos de la situación de inseguridad en el Municipio de Acapulco durante el 2012, motivo por el cual se ve la necesidad del desarrollo de un sistema de vigilancia eficiente.

En el Capítulo 2 mencionamos el caso específico de la seguridad en el sistema escolar público y privado de Acapulco, Gro., que durante el año 2012 fue catalogada como la 2da. ciudad con mayor índice delictivo a nivel mundial por el Consejo Ciudadano para la Seguridad Pública y Justicia Penal A.C.

En el Capítulo 3 se definen conceptos básicos relacionados con el proyecto, que van desde seguridad pública hasta conceptos usados en la Ingeniería de Software.

En el Capítulo 4 se explican las razones por las cuales fueron seleccionados los requerimientos mínimos del sistema, como el hardware y software.

En el Capítulo 5 se verán los resultados del sistema, así como las mejoras pendientes o posibles para este sistema.

En el Capítulo 6 se validará la hipótesis con base a los resultados.

Planteamiento del Problema

Desde hace tiempo el tema de la seguridad pública está en el centro del debate de nuestra comunidad. En el ámbito social, la seguridad y la justicia han pasado a ser objeto de análisis y crítica constantes, lo cual es lógico si se recuerda que la Seguridad Pública es una de las exigencias más sentidas de la ciudadanía y necesita ser atendida de manera eficiente y oportuna por el Gobierno [2].

La Seguridad Pública forma parte esencial del bienestar de una sociedad. Un Estado de Derecho genera las condiciones que permiten al individuo realizar sus actividades cotidianas con la confianza de que su vida, su patrimonio y otros bienes jurídicos tutelados están exentos de todo peligro, daño o riesgo. Ante la realidad de un Estado que no cumple con una de sus principales funciones, la de suministrar seguridad, los ciudadanos tendrán que centrar todos, o gran parte de sus esfuerzos, en la defensa de sus bienes y derechos.

A efecto de poder contar con una visión integral del problema que hoy en día constituye una de las exigencias más sentidas de la población y reclama una solución pronta y eficaz por parte del Estado, es necesario remontarnos a la génesis del mismo y en primera instancia determinar cuáles son las razones por las que el hombre se ha organizado en comunidad.

La respuesta a esta pregunta se encuentra en las agrupaciones más primitivas, donde se pone de manifiesto que una de las principales

[2] Diario Oficial de la Federación, 2009

razones que llevan al hombre a unirse con otros de su misma especie es una cuestión de seguridad.

Mediante un acuerdo social, busca la defensa de los bienes que considera fundamentales para su sobrevivencia y posteriormente, para su desarrollo como miembro de la comunidad.

En años recientes se ha sido testigo de cómo se han incrementado los índices delictivos en nuestro país, por consecuencia, la inseguridad en todos los niveles sociales están a la orden del día[3].

Los secuestros, extorsiones, robos, por solo mencionar algunos de los males que aquejan a la sociedad, han sobrepasado los sistemas digitales implementados en cuanto a seguridad se refiere, por ende, es necesario explorar otros tipos de opciones donde se puedan aprovechar los actuales desarrollos e inventos tecnológicos.

En el transcurso del año 2012, en el Puerto de Acapulco, Gro., la inseguridad en las escuelas públicas y privadas estaban en su punto más crítico, el crimen organizado se infiltraba en las instalaciones para secuestrar profesores e inclusive alumnos; el Sistema Municipal de Seguridad Pública estaba rebasado, se requería de una solución de carácter inmediato; por lo cual se instalaron sistemas de seguridad que funcionaban a base de un botón de pánico comunicado por medio de línea telefónica o radio frecuencia, el cual, al ser presionado, se daba aviso a las autoridades para llegar en el menor tiempo posible al lugar del siniestro y prestar sus servicios.

[3] Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, 2012

Lamentablemente, como era de esperarse, el sistema tenía fallas de comunicación entre los equipos, debido a la ingeniería usada para su aplicación.

Errores como que los aparatos no tenían el alcance correcto de señal a la que fueron colocados, ocasionando puntos ciegos donde la señal se perdía, personas no capacitadas para la instalación que no conectaban bien los equipos e incluso, había escuelas donde simplemente era un adorno más.

En las pocas instituciones educativas donde se logró instalar, se pudo investigar el funcionamiento, el cual era en su totalidad ineficiente, ya que al ser generada la alarma, no existía una forma computarizada de acceso a la información y se buscaba de forma manual en listas de hojas de cálculo, el código de alarma que se había generado, así como después el lugar de dónde provenía esta; dependiendo totalmente de la habilidad de búsqueda de la persona encargada del monitoreo.

Justificación

Como se menciona en párrafos anteriores, la inseguridad alcanzo niveles preocupantes. Es por eso que el Sistema de Monitoreo en Tiempo Real, disminuiría el tiempo en el que son presentadas las alertas a las corporaciones de seguridad, así como daría una visión en tiempo real de los sucesos que estén aconteciendo en el lugar que se presentó la alarma.

Con un manejo detallado de información del sistema se puede disminuir el tiempo de llegada de las corporaciones de seguridad, gracias a una delimitación exacta de la alerta, así como las posibles rutas a seguir y una o más formas de contacto con el responsable del sitio de donde se presentó la alerta.

Al ser una plataforma portable, el sistema puede ser accesado desde varias corporaciones de seguridad, brindando un mejor manejo de información a los cuerpos de seguridad.

Hipótesis

Se desarrollará un Sistema de Monitoreo en Tiempo Real, el cual reducirá los tiempos de respuesta de los cuerpos de Seguridad Pública a través de botones de pánico, cámaras de circuito cerrado y geolocalización, lo cual proveerá rutas para su llegada al sitio de la emergencia y referencias de ubicación de donde se produjo el siniestro, lo que facilitará su llegada.

Objetivo General

Desarrollar un Sistema de Monitoreo en Tiempo Real que disminuya el tiempo en que se presentan las alertas a los miembros de Seguridad Pública y que esto les permita reaccionar de manera pronta y expedita.

Objetivos Específicos

Se instalarán terminales en 669 escuelas públicas y 335 escuelas privadas[4], dotadas de un botón de pánico, ya sea alámbrico o inalámbrico y de cámaras de vigilancia. Este sistema cuenta con elementos que hoy en día se consideran de uso cotidiano, lo cual reducirá el costo total en el momento de su implementación.

Se desarrollará e implementará un software de monitoreo y almacenamiento de información que permita llevar un control real y estadístico sobre la Seguridad Publica en el Municipio de Acapulco, Guerrero.

Se realizará la instalación del equipo de cómputo con acceso al Sistema de Monitoreo en los centros de comando de las fuerzas de Seguridad Pública para responder a las alarmas y permitirles el acceso a las cámaras en tiempo real.

[4] Secretaría de Educación Guerrero, 2011

CAPÍTULO 1 – ESTADO DEL ARTE

A través del tiempo el hombre ha logrado ir desarrollando nuevas tecnologías para usarlas para su comodidad, facilitar las tareas, su convivencia, su transporte, sus comunicaciones[5].

Tales tecnologías, como se puede apreciar en la Figura 1.1, muestran cómo poder acortar distancias con los aviones, los automóviles; comunicarse constantemente con los teléfonos celulares, mejorar la calidad de los trabajos con las computadoras, almacenar información usando el internet. En estos tiempos las necesidades siguen siendo las mismas, pero preocupa en especial estos últimos años, la inseguridad, la cual ha ido en aumento constantemente. Gracias a la combinación de algunas de estas tecnologías mencionadas se tiene ahora la oportunidad de también cubrir la necesidad de sentirse seguros.

Figura 1.1 Tecnologías de la información aplicadas a la vida diaria.

[5] Programa de las Naciones Unidas para el Desarrollo, 2003

Figura 1.2 Aplicaciones para un sistema IP de vigilancia.

En la Figura 1.2 se observan las diversas aplicaciones de los Sistemas IP de Vigilancia.

Hoy día, la vigilancia IP puede utilizarse en infinidad de situaciones; desde aplicaciones sencillas residenciales, hasta sistemas profesionales de magnitud gubernamental o multinacional.

En la Figura 1.3, que se aprecia en la siguiente página, se muestra la imagen de un “Sistema de Monitoreo en Tiempo Real Centralizado”, administrado desde un Control Center, lo que permitirá un mejor manejo de la seguridad al estar todo el monitoreo unificado en un mismo sistema.

A continuación se expondrán algunas aplicaciones de productos de Vigilancia IP implementadas a la medida en diferentes mercados. Sin embargo, cabe mencionar, que son consideraciones personales, ya que

existen muchos otros ambientes donde la vigilancia IP puede ser aplicada, en este caso, solo mencionaremos algunas, como son:

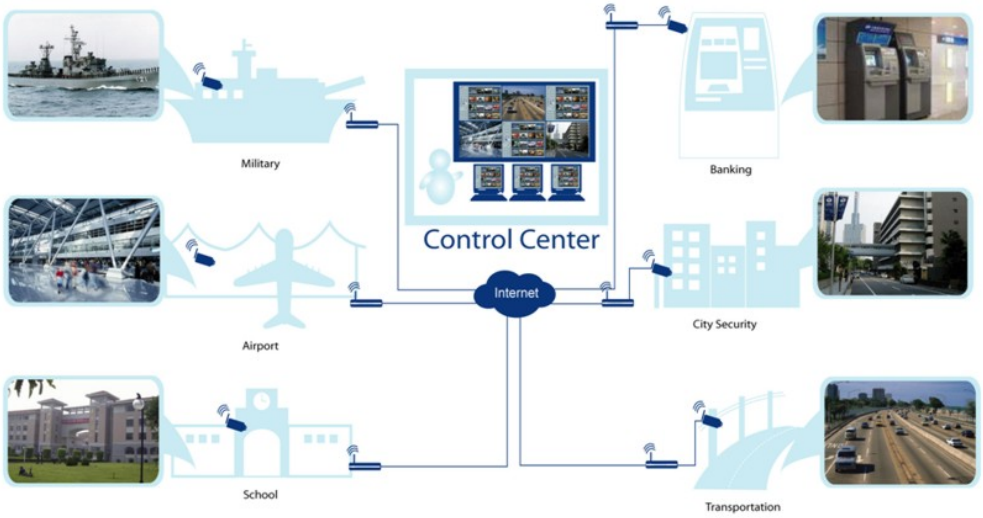


Figura 1.3 Sistema de Seguridad Pública Centralizado IP.

1.1 Educación

Se implementan sistemas tanto para la seguridad interna de los colegios, escuelas y universidades, como para dar valores agregados a los servicios que ofrecen estas instituciones. ¿A qué padre o madre no le gustaría ver “en vivo” que está haciendo su hijo en su escuela o colegio?

Ahora pueden conectarse vía Internet desde su casa o trabajo al sitio Web de la escuela/colegio, entrar a una cámara IP del aula de sus hijos y ver si está atento o distraído, o ver en la cámara del área de deportes

si está participando activamente en los ejercicios, entre otras actividades más.

Sin duda, de esta manera la familia puede tener una visión directa que le permita participar más activamente en la educación de sus hijos y a su vez, el colegio tiene la posibilidad de recibir un mayor y oportuno apoyo de los padres, como para corregir conjuntamente cualquier conducta inapropiada de los niños. O quizá solo por la satisfacción de ver a sus niños/niñas en momentos que de otra manera seria imposible.

1.2 Transporte

Cabe resaltar los sistemas de vigilancia de tráfico en ciudades, en trenes, estaciones de metro, etc. Los sistemas IP pueden ser incluso inalámbricos sin dejar de ser efectivos, así como pueden incorporar funciones de “inteligencia”, como reconocimiento de rostro, detección de objetos abandonados, lectura de matrícula de autos y otras más que son de alto valor en cualquier aplicación.

1.3 Banca

Se pueden implementar las aplicaciones tradicionales de seguridad en bancos principales, sucursales y oficinas ATM (Automated Teller Machine/Cajeros automáticos), pero además la potencia de la Vigilancia IP permite desarrollar Centrales de Monitoreo donde, por ejemplo, una institución bancaria puede monitorear todas sus sucursales.

Esta aplicación es muy importante, ya que no solo se puede ver el vídeo “en vivo” de cualquier cámara instalada en cualquier sucursal, sino que, se puede grabar este vídeo, buscar información grabada con anterioridad, hacer respaldos de información, etc. Así, ante un eventual robo, si los asaltantes deterioran el equipo en que grababa localmente se puede recurrir a información almacenada en la Estación General de Monitoreo o detectar el evento en vivo y disuadir verbalmente desde la estación remota a que los asaltantes prosigan, pues están siendo observados y grabados, mientras se envía personal de refuerzo a la sucursal afectada.

1.4 Gobierno

Para sistemas de vigilancia con monitoreo local y remoto en edificios gubernamentales que se caracterizan por ser amplios y con alto flujo de personas. También para Sistemas de Vigilancia Urbano en áreas turísticas, centros históricos de ciudades, patrullas, etc.

1.5 Comercios minoristas / Plazas y Centros Comerciales

Generalmente utilizan la vigilancia IP para sistemas de seguridad interno, con monitoreo local y remoto y se benefician de las funciones complementarias que son integrables a esta tecnología, como su

posibilidad de monitoreo centralizado de varias sucursales de un mismo negocio.

En las plazas comerciales se suelen colocar botones de pánico en los estacionamientos con los que los usuarios pueden solicitar ayuda; una cámara automáticamente los ubica para dejar constancia en video del hecho y reciben asistencia remota con audio bi-direccional de la estación de monitoreo mientras le llega la asistencia física.

1.6 Industrial

Un amplio uso específico en el control de los procesos de fabricación, los sistemas de logística, transporte, control de calidad, evitar robos internos y supervisar la integridad de los inventarios. Además, al igual que las plazas y los centros comerciales, se benefician de las funciones complementarias que son integrables a esta tecnología, como su posibilidad de monitoreo centralizado de varias sucursales, de un mismo negocio, pero en este caso, a nivel mundial.

1.7 Casinos / Entretenimiento

La alta calidad de las imágenes que acompaña la vigilancia IP, no solo de las vistas en tiempo real, sino también de las almacenadas en las grabaciones, unido a que se puede administrar y supervisar de manera muy eficiente una gran cantidad de cámaras simultáneamente.

Lo anterior permite dar respuestas inmediatas a situaciones conflictivas y/o mantener un record amplio y detallado por largos periodos de tiempo de las actividades en este tipo de centros, donde algunos segundos pueden ser la diferencia entre tener o no pérdidas cuantiosas.

Se considera necesario mencionar, que hasta la fecha, en que fue redactado el presente documento, el proyecto sigue en prototipo, es por eso que no podemos agregar referencias. Los anteriores aplicaciones son solo algunas de las posibilidades existentes, ya que hay muchas más donde se espera pueda ser aplicado el sistema cuando llegue a ser terminado en su totalidad, ya que hasta el momento, no hay otro sistema como el que se propone.

CAPÍTULO 2 - CASO DE ESTUDIO

Acapulco de Juárez es una ciudad y puerto mexicano, ubicado en la costa sur del país, a 304 kilómetros de la Ciudad de México, en el Estado de Guerrero, siendo la mayor ciudad y única zona metropolitana del mismo, superando en gran medida a la Capital, que es Chilpancingo de los Bravo. Es cabecera del Municipio homónimo y uno de los principales destinos turísticos de México. Además de ser considerada la décima sexta metrópoli más grande del país y la vigésimo primera ciudad más poblada de México. Según el Conteo de Población y Vivienda del año 2010, Acapulco cuenta con 789,971 habitantes, distribuidos en las diversas localidades que integran el Municipio, como se muestra en la siguiente tabla[6], la cual llamaremos Figura 2.1:

Clave	Nombre	Población			Porcentaje Municipal
		2010	2005	Variación respecto a 2005	
120010001	✓ **Acapulco de Juárez**	673 479	616 394	▲ 9.2%	85.25%
120010110	Xaltianguis	6 965	6 579	▲ 5.8%	0.88%
120010110	Kilómetro 30	6 301	6 163	▲ 2.2%	0.79%
120010166	Tres Palos	5 001	4 306	▲ 16.1%	0.63%
120010158	San Pedro las Playas	4 292	3 488	▲ 23.0%	0.54%
120010081	Amatillo	3 298	3 025	▲ 9.0%	0.41%
120010167	Tuncingo	2 570	2 008	▲ 27.9%	0.32%
120010128	Los Órganos de Juan R. Escudero	2 532	2 141	▲ 18.2%	0.32%
120010155	Lomas de San Juan	2 377	2 083	▲ 14.1%	0.30%
120010102	Ejido Nuevo	2 372	1 948	▲ 21.7%	0.30%
120010153	San Isidro Gallinero	2 347	1 981	▲ 18.4%	0.29%
120010087	El Bejuco	2 271	1 873	▲ 21.2%	0.28%
120010121	Lomas de Chapultepec	2 173	2 051	▲ 5.9%	0.27%
120010164	Texca	2 107	1 848	▲ 14.0%	0.26%
Total Municipio		**789 971**	**717 766**	**▲ 10.0%**	**100%**

Figura 2.1 Demografía del Municipio de Acapulco de Juárez, INEGI 2010.

[6] INSTITUTO NACIONAL DE ESTADISTICA Y GEOGRAFIA, 2011

La tabla anterior, que hemos llamado Figura 2.1 muestra la concentración poblacional registrada en las diversas localidades del Municipio de Acapulco de Juárez[7], localizada principalmente en la propia cabecera municipal. Sin embargo, la cantidad de elementos encargados para la Seguridad Pública Municipal han sido insuficientes para auxiliar en muchos casos los incidentes más comunes como accidentes viales, asaltos, entre otros; por el tiempo que lleva desde el reporte a la aparición de la Seguridad Pública o Protección Civil.

Los siguientes datos de información y comparación están basados solo en el transcurso de los años 2011 – 2012, ya que fueron los años durante los que se realizó la investigación para poner en práctica el prototipo. No se tienen datos de los años posteriores, ya que el sistema hasta la fecha, como se mencionó, sigue en desarrollo.

La Figura 2.2 muestra un comparativo de los robos denunciados en las Agencias de Ministerio Público en los años 2011 y 2012[8], observando, que la diferencia no es significativa entre ambos periodos. A diferencia, el índice de secuestros si muestra un incremento significativo en este periodo.

[7] INEGI 2010
[8] Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, 2012

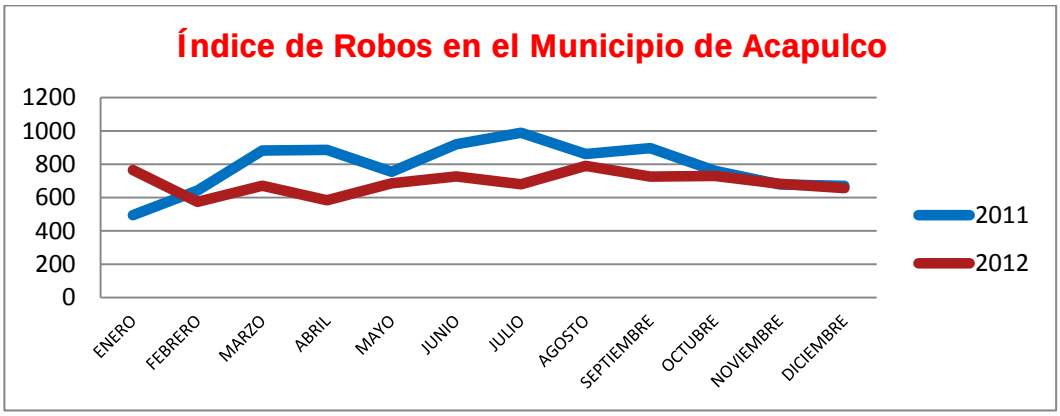


Figura 2.2 Robos 2011 y 2012.

En la Figura 2.3 se puede apreciar el cambio significativo en los secuestros a diferencia del año anterior y estos son solo los denunciados en Agencias de Ministerio Público y de los no denunciados, se especula que pueden ser más del doble[9].

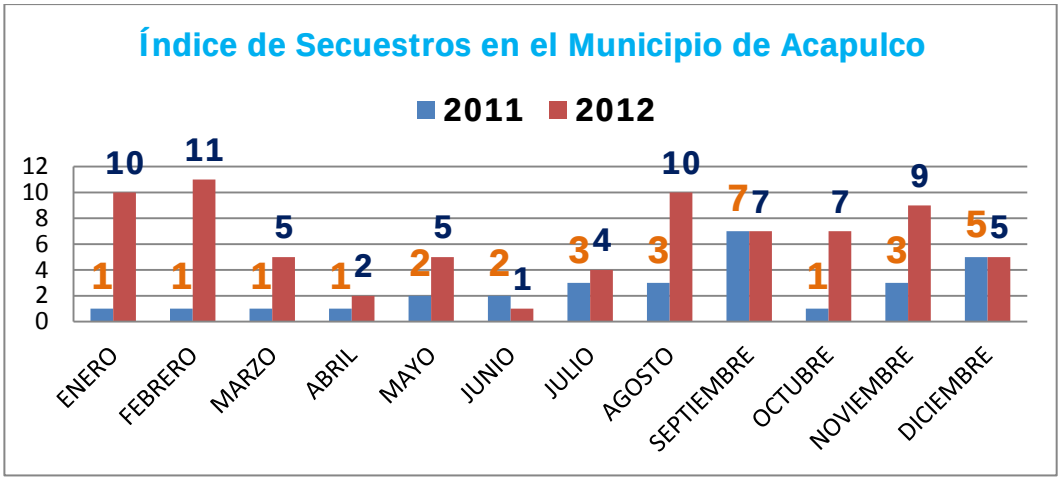


Figura 2.3 Secuestros 2011 y 2012.

[9] Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, 2012.

En la Figura 2.4 se muestra como el índice de homicidios en el puerto se mantuvo, pero al final despunto en el 2012[10]. De lo cual se puede ver el porqué del surgimiento de la necesidad de un mejor sistema de monitoreo.

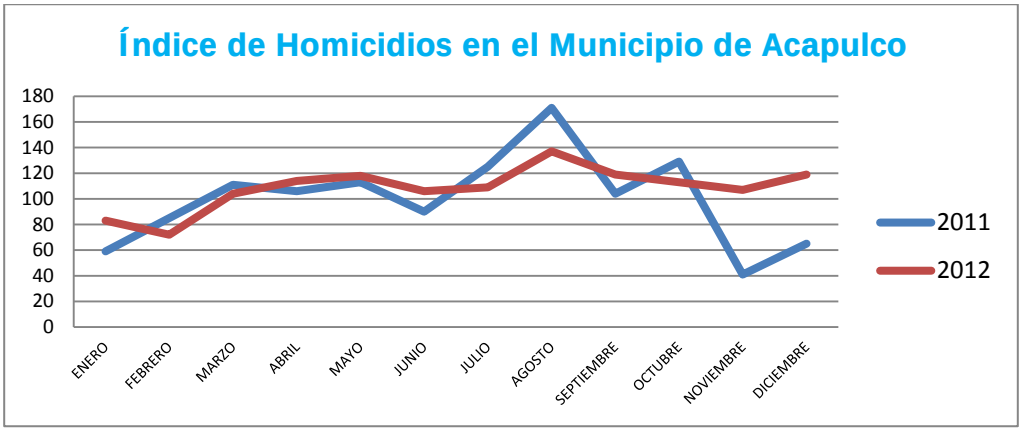


Figura 2.4 Homicidios 2011 y 2012.

En las Figuras 2.5 y 2.6 se muestra en el robo común con violencia (RCCV) en los dos años estudiados [11] un significativo y alarmante incremento en el número de casos y peor aún, solo son los reportados a los Ministerios Públicos y se estima que ni la mitad de los casos llegan a ser declarados. De las gráficas se puede observar como el robo de vehículos es el más recurrente y en especial, a vehículos particulares, con exceso de fuerza y en algunas ocasiones, terminando en un secuestro exprés.

[10] Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, 2012.
[11] Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, 2012.

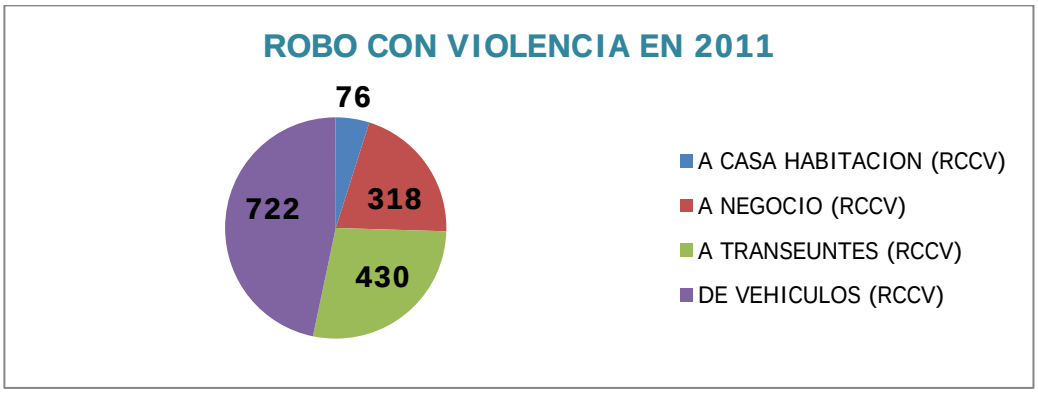


Figura 2.5 Robo con violencia 2011.

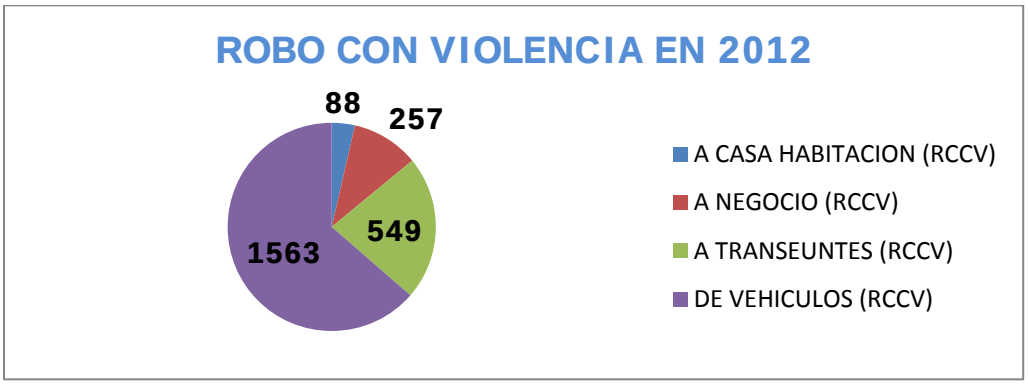


Figura 2.6 Robo con violencia 2012.

La seguridad escolar se ha convertido en un asunto de principal importancia para educadores, estudiantes y ciudadanos; la que se hace necesaria a partir de la alarmante serie de atentados con armas de fuego en los colegios, secuestros a estudiantes, profesores, así como al personal administrativo. En esta atmósfera emocionalmente cargada, los administradores de los colegios deben luchar para alcanzar sus verdaderas necesidades de seguridad escolar sin desperdiciar sus escasos recursos en medidas que tal vez no tengan ningún resultado positivo.

Durante los últimos años las escuelas públicas y privadas han tratado de implementar diversos programas con el fin de mantener la seguridad interna de las instituciones.

En un principio, al carecer de tecnologías informáticas de bajo costo y acceso, el sistema de control se basaba en tarjetas de papel o cartulina (credencial), donde se mecanografiaban los datos del estudiante junto con una fotografía, la cual servía como identificación para ingresar al plantel. Este sistema era inseguro en su totalidad, ya que las credenciales eran fácilmente falsificadas.

En la Figura 2.7 se muestra un ejemplo de identificación escolar usada en la década de los 90's, donde se puede apreciar la falta de elementos de seguridad.


SECRETARIA DE EDUCACION PUBLICA
DIRECCION GENERAL DE EDUCACION SECUNDARIA
Departamento de Escuelas Secundarias en el D. F.
ESCUELA SECUNDARIA DIURNA NUM. 15 "ALBERT EINSTEIN"
Calz. México - Tacuba 215 90-91 México 17, D. F.
Alumno
Año Grupo 35-V Núm. 4
México, D. F., a 3 Oct. de 19 90
El Director
ALBERT EINSTEIN"
PROFR. ANGEL MORENO AVILA

Figura 2.7 Ejemplo de Identificación Escolar.

Un control de acceso competente es la principal preocupación de la seguridad escolar. Desde la escuela primaria hasta el campus universitario más grande, prevención y disuasión son las claves para

proteger la seguridad de los estudiantes. El control de acceso fue una vez un asunto de grandes ciudades, pero hoy día muchas escuelas suburbanas y rurales están también interesadas en un intento por detener los índices de inseguridad en sus instalaciones.

A medida que han bajado los costos de los sistemas de seguridad, se han implementado medidas que solo eran usadas en instituciones bancarias, como las tarjetas con banda magnética, o los lectores biométricos.

Las tarjetas con banda magnética durante un periodo de tiempo fue una alternativa viable para la seguridad escolar, viéndose desechada al hacerse de venta pública los dispositivos y el material con que son elaboradas. En la Figura 2.8 se muestra como estaba dividida la banda magnética en la cual se podía almacenar los datos generales del estudiante.

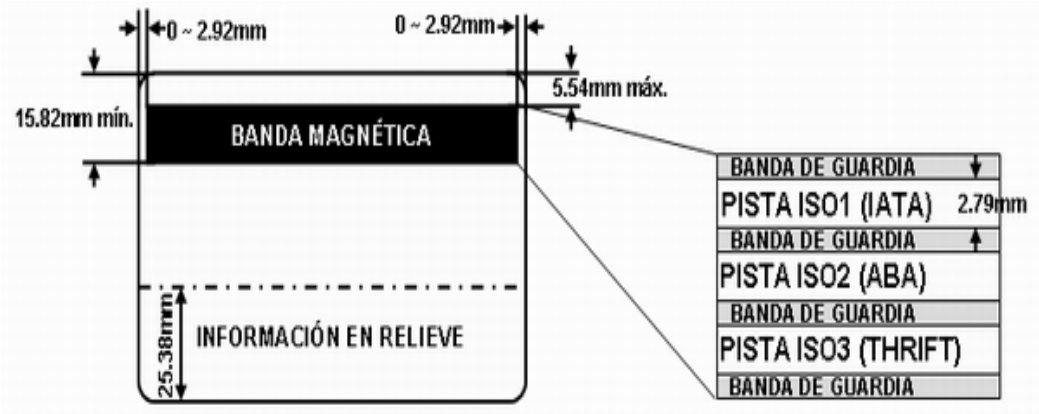


Figura 2.8 Reverso de Tarjeta con Banda Magnética.

El lector biométrico (huella digital) que se muestra en la Figura 2.9, fue el siguiente paso en un intento por mejorar la seguridad en algunos planteles educativos, implementándose además sistemas con scanners, para evitar que los alumnos ingresaran con armas que pusieran en peligro la seguridad interna de la institución educativa.

Figura 2.9 Lector Biométrico Digital.

De primera instancia, los sistemas de seguridad anteriormente descritos, no eran de uso general en todo el sistema educativo del municipio, ya que estos dependen de los presupuestos elaborados por la administración y en muchas ocasiones, por programas de seguridad implementados por el municipio; es necesario mencionar que estos programas tenían como prioridad la seguridad interna de los planteles, cuando el problema real provenía de las cercanías de las instituciones.

Acapulco, al no ser un municipio con antecedentes de inseguridad, no tenía manuales, ni guías elaboradas para poder enfrentar el problema, lo que llevo a implementar programas de seguridad improvisados, en muchos casos, sin supervisión técnica especializada en el área. Lo que

derivó en continuos fracasos, poniendo en peligro la seguridad del personal, así como del alumnado.

Uno de los programas que se implementaron en el año 2012 en el Municipio de Acapulco fue el de “Mochila Segura”, pero el problema no radicaba en lo que pudieran ingresar los alumnos a las instituciones.

Otro de los programas implementados era “Escuela Segura”, basada en el patrullaje por parte de los cuerpos de Seguridad Pública Municipal y Federal, que consistía en rondines periódicos cuya vulnerabilidad residía en el lapso del traslado entre instituciones, estos periodos eran aprovechados por la delincuencia organizada para llevar acabo extorsiones e inclusive, secuestros.

En septiembre del 2011 se empezaron a instalar los botones de pánico en las Escuelas Públicas del Municipio de Acapulco [12], el cual funcionaba de la siguiente manera:

1) La plataforma electrónica o gabinete donde estaba montado el botón de pánico estaba conectada a la línea telefónica, esta línea contaba con un dispositivo de comunicación muy básico, se le programaba para que una vez presionado el botón, marcará un número telefónico específico y mandará unos tonos.

2) La llamada era recibida por un modem conectado a una computadora en un Centro de Control de una empresa privada, la cual prestaba el servicio de enlace con la seguridad pública.

[12] Adriana Covarrubias, 2011

3) Esta computadora mantenía un programa en ejecución que monitoreaba las llamadas de emergencia; una vez recibida la llamada de emergencia, el sistema identificaba mediante los tonos un número de serie y lo mostraba en la pantalla, el operador de dicha computadora tenía que recurrir a una hoja de cálculo en Excel donde estaban almacenados los datos de todas las instituciones educativas integradas al programa del botón de emergencia e identificar manualmente el número de serie que acaba de recibir.

4) En ese momento el operador se comunicaba vía teléfono a la central de seguridad municipal para brindarle la ubicación donde se había efectuado el siniestro.

La Figura 2.10 muestra una alarma de la manera que en algún momento se pretendió que funcionara; pero debido a algunas falsas alarmas se requirió un nuevo paso en el sistema, que era la corroboración de que la alarma fuera real.

Figura 2.10 Sistema de Seguridad.

En dicho proceso se perdían hasta 5 minutos o más, el cual era suficiente para que la emergencia no se atendiera de manera oportuna, dando como resultado fatalidades en algunos casos.

La idea del proyecto nace de la necesidad de contar con un sistema que permita una respuesta inmediata a una emergencia en carácter de seguridad, sin pérdida de tiempo para poder brindar los servicios necesarios acordes a la situación presentada.

Se consiguió una cita con personal de Seguridad Federal para saber cuáles eran las características particulares con las que debía contar el sistema, las cuales no especificaban algún equipo en especial, dando luz verde para usar las herramientas con las que se contaban, de preferencia herramientas gratuitas y de uso libre.

2.1 Solución Propuesta

La solución es inédita, como propuesta nace de la necesidad de mejorar los tiempos de respuesta de los cuerpos de Seguridad Pública para lograr una atención al delito de una forma rápida y expedita, teniendo como base las tecnologías informáticas más avanzadas y de bajo costo.

Este sistema cuenta con elementos que hoy en día se consideran de uso cotidiano, lo cual reducirá el costo total en el momento de su implementación, tratando de no afectar la situación económica de las dependencias.

Dicho sistema está compuesto por 3 elementos básicos: El sistema de alerta y vigilancia, un centro de procesamiento y una área de monitoreo.

- El sistema de alerta y vigilancia está conformado por el botón de pánico, que es un interruptor que al ser presionado enviará un bit de datos al sistema de vigilancia IP; y el sistema de cámaras, que es el que se encargará de mostrar en tiempo real, mediante las cámaras de video, lo que está sucediendo en el lugar del siniestro, esto gracias al servidor de video al cual se puede accesar desde un explorador web.

- El centro de procesamiento consta de 2 elementos: El servidor de cómputo para procesamiento, que es el equipo donde se encuentra instalado el programa que se encargara de recibir la alerta por parte del sistema de vigilancia IP; y el software que se encarga de la administración y despliegue de información, que está continuamente a la espera de alertas, está enlazado con una base de datos que cuenta con la información del lugar donde el sistema IP de vigilancia fue previamente instalado. En la base de datos del sistema se almacena el número de la alerta, la hora en que fue emitida, el teléfono del lugar del incidente, la dirección, el nombre del responsable del lugar, la dirección IP desde donde se puede accesar de manera remota al sistema de vigilancia IP, así como un sistema de geolocalización basado en el Google Maps.

- Área de Monitoreo: Consiste en el software para monitoreo, que es aplicación desarrollada en PHP, la cual es accesada desde un

explorador web, la aplicación muestra a la persona encargada del monitoreo en el momento en que fue emitida la alarma, toda información necesaria para atender el incidente, permitiendo reducir los tiempos de reacción a los cuerpos de Seguridad Pública; y la terminal de monitoreo, que es el equipo de cómputo en el cual se podrá accesar al software de monitoreo.

2.2 Funcionamiento

El momento en que se lleva a cabo la incidencia, el botón de pánico es presionado emitiendo la alerta, el sistema de vigilancia IP envía su ID al software para la administración de la información, el cual identifica y obtiene toda la información de la base de datos, la cual es desplegada de manera inmediata por el software de monitoreo a la personada encargada del área, permitiendo de manera inmediata contactar a los cuerpos de Seguridad Pública brindándoles información de la dirección del incidente, su localización usando referencias particulares de la zona, así como comunicarles en tiempo real lo que está pasando.

Cabe señalar, que la mejora más notoria es el acceso a la visión de lo que está aconteciendo en el lugar que se presentó la alerta, proporcionando información fundamental para poder atenderla, como qué tipo de cuerpo de seguridad es el más adecuado, así como si es necesario asistencias médicas.

CAPÍTULO 3 - CONCEPTOS Y DEFINICIONES BÁSICAS

Si bien es conocido que un grupo de piezas apiladas no es más que eso, se necesita una mente que las conozca para poder darles un propósito, hay que acomodarlas, estableciendo el funcionamiento que cada una de ellas puede y debe hacer. Dentro de este capítulo se definirán los conceptos y se describirán componentes que se usarán para llevar a cabo el proyecto, así como el hardware como software que se utilizará.

3.1 Hardware

El término hardware se refiere a todas las partes tangibles de un sistema informático; sus componentes son: Eléctricos, electrónicos, electromecánicos y mecánicos. Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.[13]

3.1.1 Computadora

Se puede definir como una máquina compuesta de elementos físicos (hardware), en su mayoría de origen eléctrico-electrónico, capaz de realizar una gran variedad de trabajos a gran velocidad y con gran precisión, está formada por un conjunto de componentes electrónicos que por sí mismos no son capaces de realizar demasiadas funciones.

[13] Diccionario de la lengua española, 2005

Estos componentes electrónicos necesitan de otros componentes no físicos que los pongan en funcionamiento; se está refiriendo a programas (software). Los programas servirán para tal fin: Procesar datos (información).

Para que los componentes electrónicos de un ordenador sean capaces de funcionar y realizar un proceso determinado, es necesario ejecutar un conjunto de órdenes o instrucciones. Estas instrucciones, ordenadas y agrupadas de forma adecuada, constituyen un programa. El conjunto de varios programas se denomina aplicación.

La Figura 3.1 muestra una computadora con sus componentes básicos, agregando un sistema de ventilación mejorado y una fuente de poder estable, se puede configurar un servidor de datos.

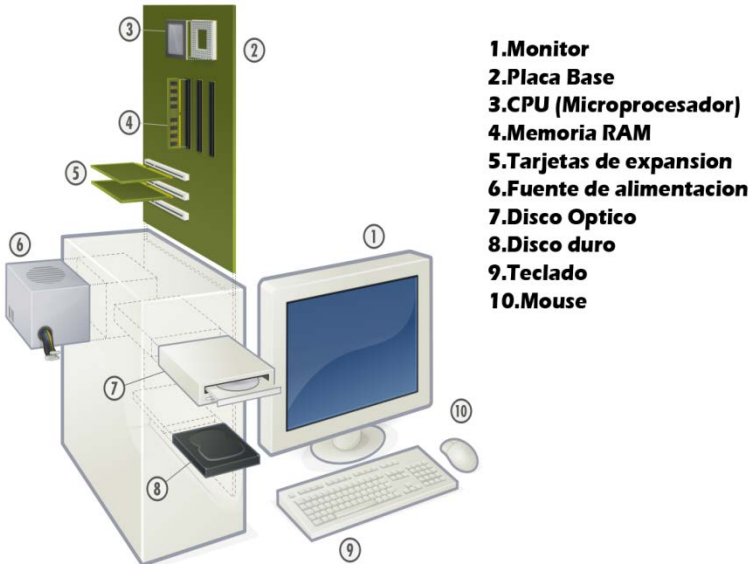


Figura 3.1 Partes que integran una computadora.

3.1.2 Sistemas de Video IP

El vídeo IP, también conocido como Video Over IP (del inglés), es uno de los grandes resultados que trajo la era digital con la globalización de la información y es el término que se ha utilizado para nombrar la tecnología que sorprendió al mundo al capturar, comprimir y convertir las secuencias de imágenes en movimiento (video) en un flujo de datos que puede ser trasmitido por redes de computadoras, también conocidas como Redes IP (LAN/WLAN/ WAN/Internet).

El transporte de vídeo por redes de datos ha sido posible hoy día, gracias a los avances en las técnicas de digitalización y compresión de imágenes, al crecimiento en las redes de datos (IP Networks) y el desarrollo y comercialización cada vez mayor de equipos de vídeo digitales que han sido de interés mundial (satélites, televisión digital por cables, DVD, etc). [14]

[14] MidiSec, 2010

En la Figura 3.2 que aparece a continuación, se muestran los diferentes tipos de cámaras que se usan hoy en día para los sistemas de Video IP.

Figura 3.2 Cámaras para sistema de Video IP.

3.1.3 Vigilancia IP

Una de las grandes aplicaciones que ha encontrado el video IP, es sin duda en el campo de los sistemas electrónicos de seguridad y vigilancia, ya que la industria ha desarrollado hardware y software suficientemente potentes y eficientes como para realizar todas las funciones de los sistemas analógicos tradicionales y superarlos

ampliamente con la incorporación de funciones “inteligentes” que eran solo fantasía hasta hace pocos años. [15]

Los sistemas de vigilancia IP, son aquellos en que las imágenes y audio son capturados por las cámaras y micrófonos, se comprimen y transmiten por una red de datos local o Internet (LAN / WAN) y pueden ser accesados desde uno o varios puntos en cualquier lugar del mundo mediante computadoras convencionales (o hardware especialmente diseñado) para descomprimir los datos, visualizarlos, analizarlos, grabarlos y hasta generar acciones de manera automática en respuesta a diferentes eventos pre-definidos o a voluntad de un operador.

En la Figura 3.3 se muestra un sistema de vigilancia IP, el cual puede ser accesado a través de Internet, previamente configurado con una dirección IP o un dominio.

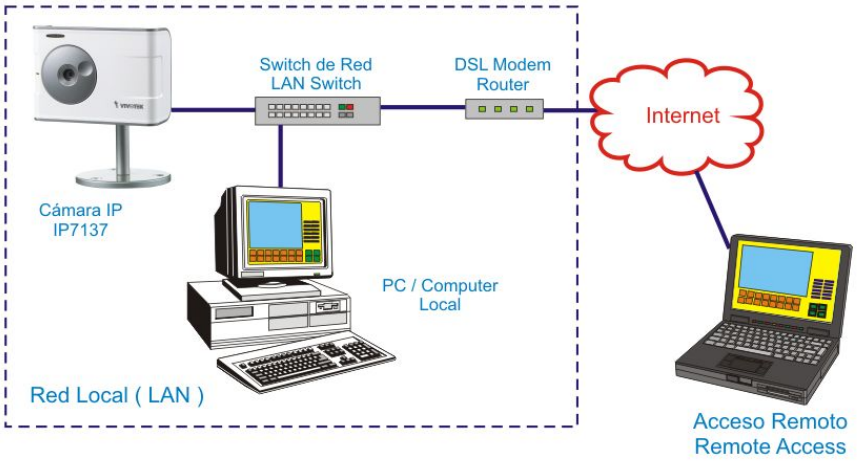


Figura 3.3 Sistema de Vigilancia IP vía Internet.

[15] MidiSec, 2010

Un detalle importante dentro de los sistemas de vigilancia IP es que no solo involucran video, sino también audio y éste puede ser bi-direccional, es decir, en una estación de monitoreo se puede escuchar las conversaciones y sonidos generados en los locales donde están las cámaras y micrófonos, así como (si se desea), el operador puede hablar a individuos que están en los mismos locales donde se colocaron las cámaras.

El audio bi-direccional puede ser muy útil para disuadir a sospechosos antes que comentan el delito o para coordinar el trabajo de los agentes de seguridad en diferentes posiciones de un objetivo protegido.

Entre los elementos que componen un sistema de vigilancia IP merita resaltar[16]:

- Las cámaras IP
- Servidores de video
- Decodificadores de video IP
- Grabadoras digitales de red
- Software inteligente para centrales de monitoreo

Un sistema IP es completamente digital, o sea, “datos” y se requiere de computadoras o algún hardware especialmente preparado para “decodificar” ese flujo de información y volverlo a convertir en video.

[16] dointech, 2010

En la Figura 3.4 que aparece enseguida, se muestra un sistema de vigilancia IP, que puede ser accesado a través de una red LAN, el cual previamente debió haber sido configurado con una dirección IP para ingresar desde el ordenador designado para el control y vigilancia.

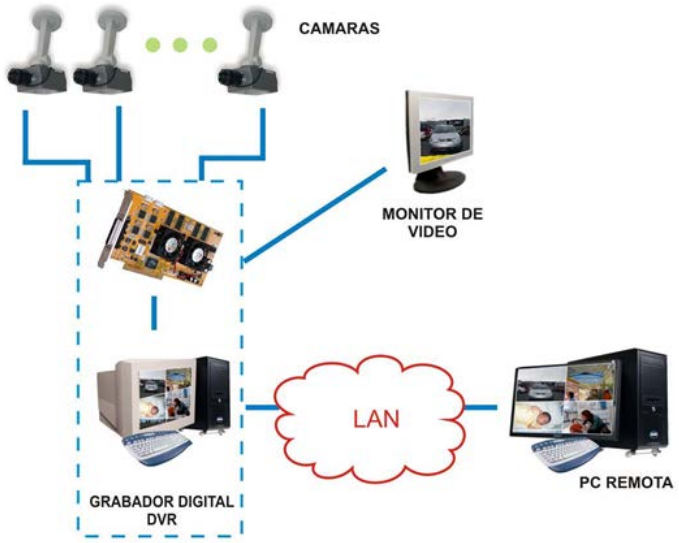


Figura 3.4 Sistema de Vigilancia IP vía LAN

A diferencia de los sistemas de vídeo analógicos convencionales, la vigilancia IP no requiere de un cableado punto a punto por cada cámara, pues las redes de datos que son su medio de transporte, llevan el video, el audio y las señales de control a través de una estructura nódulo-modular, no solo distinta, sino también más eficiente, conveniente y versátil para las instalaciones y futuras expansiones.

En la Figura 3.5 se muestra un sistema de vigilancia IP el cual puede ser accesado a través del Internet, la ventaja de las tecnologías actuales es que permiten el acceso al sistema desde una tableta, incluso desde un teléfono celular con acceso a internet.

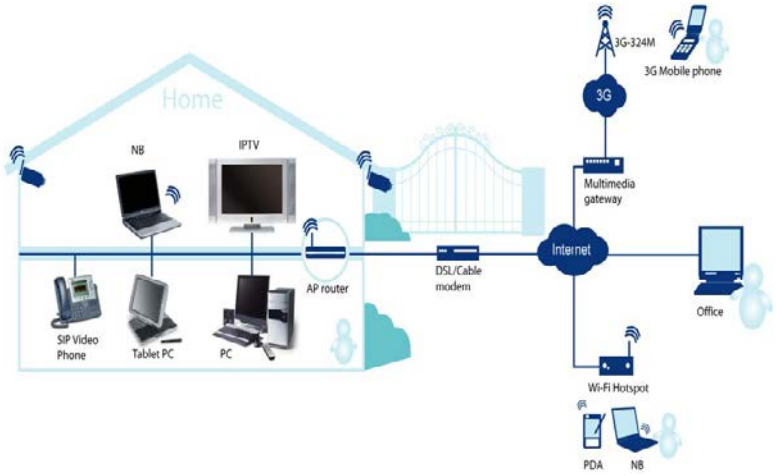


Figura 3.5 Sistema IP mediante tecnologías de uso diario.

3.1.4. Servidor de Cómputo

Para el prototipo se usó un equipo genérico integrado por un procesador Intel x86 Pentium IV a 3.2 GHz, con 1gb en RAM, disco duro 3.5” con una capacidad de 160Gb, todo esto montado en una tarjeta madre genérica, siendo sustituido por un equipo Dell Dimension C521 integrado por un procesador AMD Athlon 64 3800+, con 1gb en RAM, disco duro 2.5” con una capacidad de 80Gb.

Esencialmente, cualquier equipo de cómputo basado en la arquitectura de procesador x86 o x64 con una velocidad mínima de 1GHz, 1gb en RAM y por lo menos un disco duro de 20Gb de capacidad de almacenamiento es capaz de solventar las necesidades básicas para la implementación del software, sin embargo, dependiendo de la demanda de servicios basados en el acceso vía Internet y/o el proceso de solicitudes de atención del software, este pudiera ser sustituido por equipos más potentes, siempre y cuando estos sean basados en la misma arquitectura[17].

3.1.5 Grabador de Video Digital (DVR)

El DVR Hikvision (Figura 3.6) fue escogido de las múltiples gamas del mercado, porque es el que cuenta con el mejor balance entre calidad y costo, ya que a pesar de ser económico, presenta casi todas las ventajas que podría prestar un DVR de mayor precio. Con un servicio DNS dinámico exclusivo para esta marca incorporado en el equipo.

En la actualidad, en Acapulco, los equipos de monitoreo de cámaras existentes, la mayoría son análogos, grabando y monitoreando los eventos en el sitio donde fueron estas instaladas. Los requerimientos de la población estaban rebasando los equipos de circuito cerrado y para poder satisfacer las necesidades de monitoreo remoto surgieron los DVR's (Digital Video Recorder).

[17] APR, 2013

El DVR es la nueva tendencia en la tecnología de seguridad, ya que complementa las instalaciones análogas de cámaras, con un sistema digital que abre nuevas posibilidades de uso del equipo de CCTV (Circuito Cerrado de Televisión), permitiendo al usuario de estos monitorear sus cámaras desde varios puntos remotos, así como el acceso a las grabaciones y alertas generadas por los equipos, como por ejemplo, detección de movimiento o falla de voltaje de alimentación.

De las tecnologías de grabación de circuito cerrado la que destaca en fidelidad y viabilidad es la Norma H.264, por ello, se decidió usarla para la ejecución técnica del proyecto. Utilizando esta norma de compresión de datos se puede almacenar de manera más factible y prolongar el periodo de tiempo de grabación, así como disminuir la taza de transferencia de datos vía WEB, manteniendo la seguridad en todo momento gracias el protocolo de encriptación de esta tecnología.

Figura 3.6 DVR Hikvision.

De igual manera, se utilizó un equipo Hikvision de la serie DS7204, que se caracteriza por tener cuatro entradas análogas de video y dos de

alarmas de tipo N/O (Normally Open) y N/C (Normally Closed), configurables para el envió de alertas vía web a nuestro servidor[18].

Este equipo Hikvision se configura para recibir cámaras montadas en el sitio a monitorear, que van a estar grabando por un periodo de tiempo no menor a 2 semanas de manera cíclica para el respaldo de eventos ocurridos, así como cualquiera de los dos tipos de botones de pánico, alámbricos o inalámbricos.

El alámbrico, es un interruptor genérico de dos polos un tiro, que opera de manera silenciosa y cuenta con restablecimiento fácil, el cual puede ser instalado en cascada para poder poner varios botones en diferentes puntos clave del sitio a monitorear y cuando se presione cualquiera de ellos generar la alarma.

El dispositivo inalámbrico de la marca AccessPro, es un receptor que cuenta con 1 relevador que es activado por medio de radio frecuencia por el transmisor Prot400 (Figura 3.7), aceptando hasta 20 transmisores; dependiendo del sitio, quedarían asignados a personas para su uso y cuidado, que de igual manera que el alámbrico, funciona en cascada para la generación de la alarma.

[18] Hikvision, 2012

El transmisor Prot400 utiliza una frecuencia de transmisión 433.92 MHz que permite la transmisión de datos de manera codificada, a diferencia de las otras radiofrecuencias, además de permitir un radio de operación de hasta 300 metros, encadenando los equipos al transmisor para evitar interferencia entre equipos similares por medio de un código de reconocimiento único entre el transmisor y el receptor.

Figura 3.7 Transmisor Prot400.

De manera conjunta al equipo instalado en el sitio, se tiene una caja negra de componentes que al ser presionado un botón de pánico va a enviar una alerta al servidor de monitoreo.

3.2 Software

Es el equipamiento lógico de un sistema informático, que comprende el conjunto de los componentes lógicos o

aplicaciones necesarias que hacen posible la realización de tareas específicas; son un conjunto de instrucciones que deben tomar los componentes físicos para realizar su función. [19]

3.2.1 Sistema Operativo (Linux)

El sistema operativo que fue seleccionado para el desarrollo del proyecto fue Linux, esta selección se basó en la disponibilidad del código fuente de la mayoría de las aplicaciones, lo cual permite, con los conocimientos de programación adecuados, agregar nuevas funciones, modificar las actuales o eliminarlas por cuestiones de seguridad. [20]

Otra de las razones, es que hay una gran cantidad de distribuciones y sub distribuciones, las cuales tienen fines diversos acordes a las necesidades del administrador del sistema y/o del programador y el factor determinante, es que muchas de las distribuciones Linux requieren un mínimo de requerimientos en el sistema para ejecutar la mayoría de las aplicaciones y no es obligatoria una interfaz gráfica para que se ejecuten los servicios requeridos por el sistema.

También no se debe de omitir el hecho que la mayoría de las licencias de las múltiples distribuciones de Linux son gratuitas y que cuentan con un soporte por parte de la comunidad que las usa, razón sobrada para no considerarlo como la primera opción en la selección del Sistema Operativo.

[19] Diccionario de la lengua española, 2005
[20] Brittani Sponaugle, 2013

La distribución que se eligió fue Ubuntu 12.04 LTS (Figura 3.8) para servidores en su versión para la arquitectura x86, ya que este está orientado al usuario promedio, además cuenta con el soporte técnico ofrecido a manera de pago por parte de Canonical Ltd. Está basado en Debian, los requerimientos mínimos son: Procesador x86 a 1 GHz, Memoria RAM de 1 GB, Disco Duro de 15 GB (swap incluida), tarjeta gráfica y monitor capaz de soportar una resolución de 800x600, lector de CD-ROM, puerto USB o tarjeta de red.

Ubuntu da soporte para actualizaciones de aplicaciones y parches de seguridad a sus versiones estándar por 2 años, a las versiones LTS (Long Time Service) da un soporte para actualizaciones y parches de seguridad por 5 años, razón por la cual se decidió usar una versión LTS[21].

Figura 3.8 Logo Ubuntu.

[21] Ubuntu server, 2012

Una gran ventaja, es que esta distribución cuenta con una gran variedad de distribuciones hermanas oficiales, como Kubuntu o Xubuntu (Figura 3.9), entre otras, lo cual permite compartir aplicaciones únicamente instalando las librerías necesarias[22].

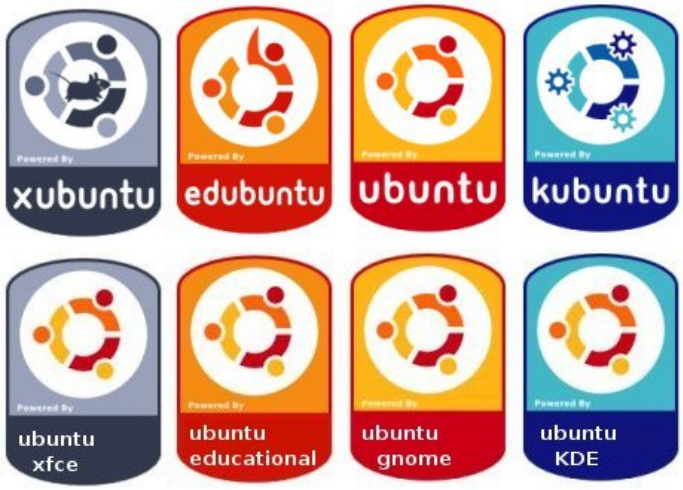


Figura 3.9 Distribuciones hermanas oficiales de Ubuntu.

En la Figura 3.10 y 3.11 se muestra de manera gráfica las capacidades de los diferentes tipos de Sistemas Operativos Linux, el cual, fue elegido por tener la mayor base de datos en software desarrollado y compatible, así como su soporte para hardware; de estos fue seleccionado Ubuntu como el sistema operativo para el proyecto, ya que como se aprecia, es el más balanceado de las distribuciones disponibles.

[22] Ubuntu flavours, 2012

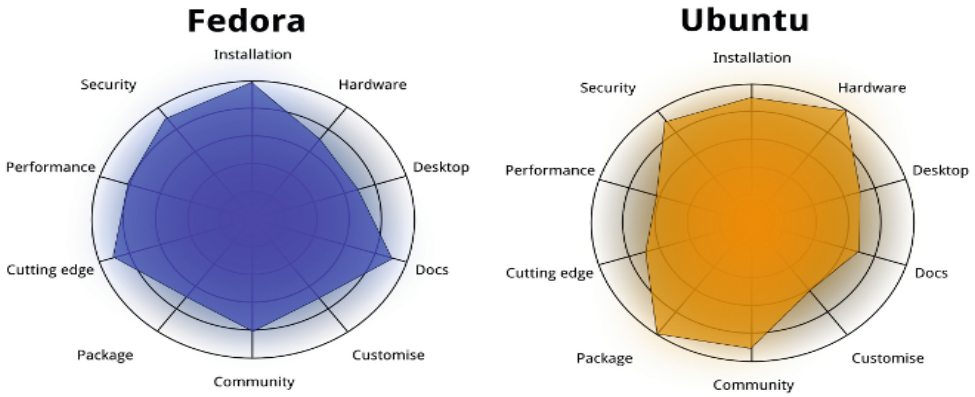


Figura 3.10 Comparativa de las principales Distribuciones Linux para Servidores (Tuxradar, 2011).

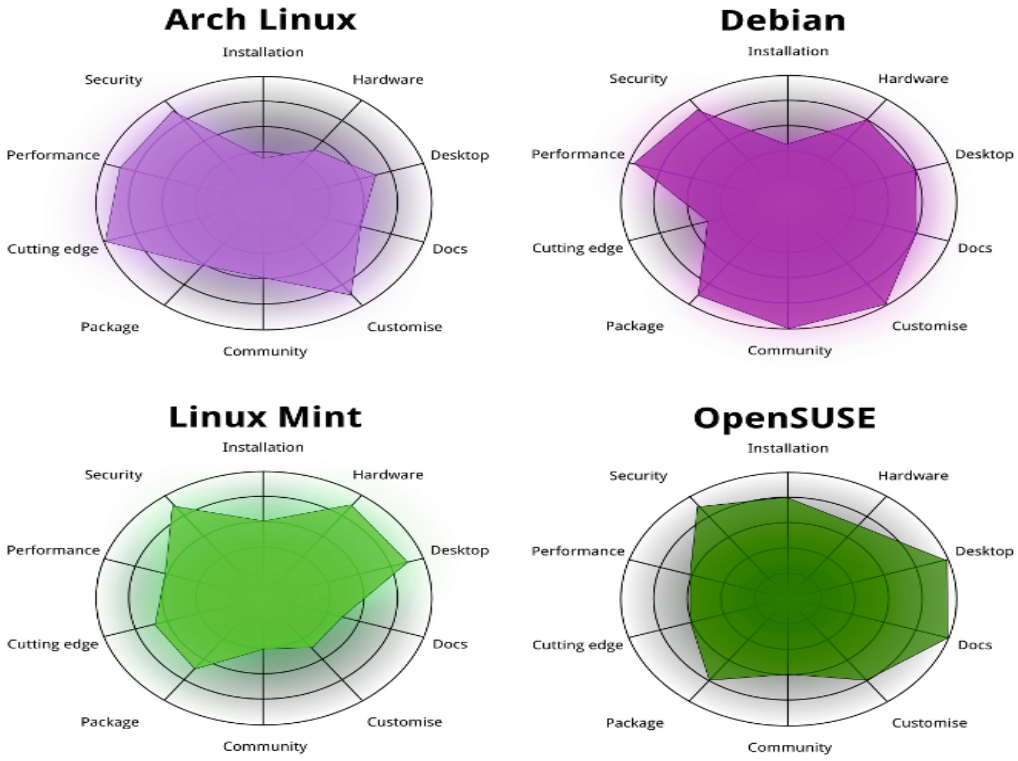


Figura 3.11 Comparativa de las principales Distribuciones Linux para Servidores (Tuxradar, 2011).

3.2.2 Servidor de Correo (Postfix)

Una de las características necesarias para que el sistema de monitoreo en tiempo real funcionará, era que el sistema de cámaras o DVR, tuviera un medio de comunicación para poder establecer contacto con el servidor que ejecutaría las diversas acciones para llevar a cabo el monitoreo y después de una breve investigación, resulto que la mayoría de los DVR, cuentan con la opción de enviar un correo electrónico en caso de que un suceso en particular se presente, este fue el medio de comunicación que fue elegido para captar la emergencia.

Para esto se necesitaba un medio de transporte que además funcionará como servidor de correo electrónico, que pudiera recibir el correo y además, pudiera ejecutar comandos a nivel de usuario, por tal motivo se seleccionó Postfix.

Postfix permite enviar el correo y su contenido al Shell de Linux, para después poder manipular dicha información, ya sea para guardarla en una base de datos o en su defecto, verificar si el origen del correo pertenece a una lista de confianza, lo cual serviría como un sistema de seguridad si la dirección del servidor de correo se viera comprometida[23].

En la Figura 3.12 se muestra el funcionamiento básico de Postfix como servidor de correo electrónico, el cual consiste en un programa que se encuentra a la espera de recibir correos entrantes y salientes, así como de administrar el manejo del correo.

[23] CS Notes, 2013

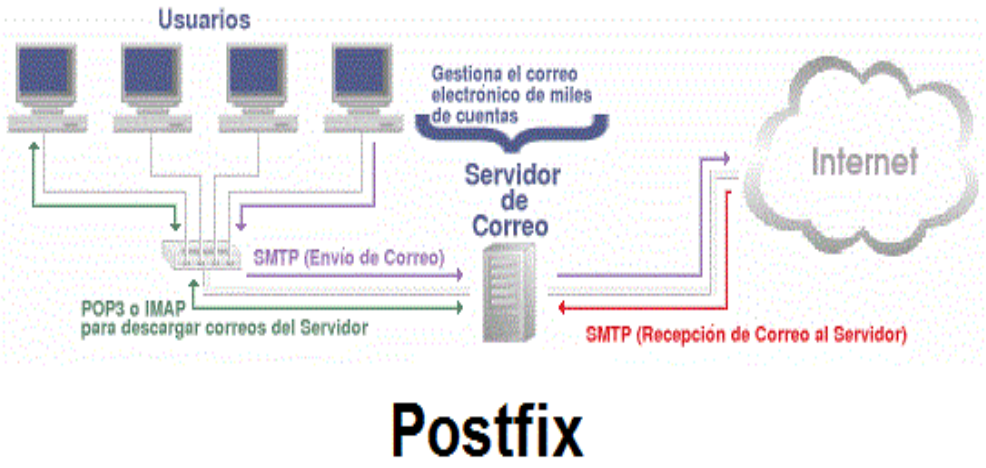


Figura 3.12 Postfix como servidor de Correo.

3.2.3 Base de Datos (MariaDB)

El sistema requería de un sistema de gestión de base de datos donde se pudiera almacenar información, identificar el origen de la emergencia, los datos de ubicación, coordenadas, teléfono de contacto, así como la dirección URL del DVR para poder accesar a las cámaras y ver lo que está pasando. El sistema de gestión de base de datos que se selecciono fue MariaDB por ser de acceso libre, sin costo y al ser derivada de Mysql cuenta con los mismos comandos[24].

[24] Maria DB, 2010

En la Figura 3.13 se muestra una comparativa entre MariaDB y Mysql, donde se muestra el desempeño superior de MariaDB, razón por la que fue seleccionado como el motor de base de datos.

Figura 3.13 Comparativa MariaDB vs Mysql.

3.2.4 Lenguajes de Programación (Batch Y PHP)

Una vez seleccionado el servidor de correo y el motor de la base de datos, se necesitaba un lenguaje de programación que pudiera manipular la dirección del correo así como su contenido, el cual había sido previamente recibido por Postfix y enviado al Shell de Linux. El lenguaje por default que permite recibir dicha información del Shell del Linux es Batch, que no es otra cosa que la ejecución de líneas de comandos simples del Shell de Linux, pero estas al estar contenidas en

un solo archivo permiten la posibilidad de manipular variables así como el manejo de niveles de error.

PHP es otro lenguaje de programación requerido, ya que el Shell de Linux no tiene forma alguna de comunicación con MariaDB, es necesario pasar la información enviada por Postfix al Shell de Linux y por medio de un Batch enviar mediante el uso de variables el contenido del correo a PHP y ya con este guardar o leer información de la base de datos. [25] [26] [27]

[25] PHP: Hypertext Preprocessor, 2001
[26] GNU Operating System, 2007
[27] Gerardo Cabrera Hernández, 2011

CAPÍTULO 4 - DESARROLLO E IMPLEMENTACIÓN

4.1 Metodología de Prototipo

Para el desarrollo del sistema se usó el modelo de proyecto a base de prototipos, ya que las necesidades prontas para una solución al problema de seguridad que vivía en su momento la Ciudad de Acapulco, Gro., así lo requerían, como fue mencionado tanto en el planteamiento del problema como en el capítulo 2, apartado 2.1., solución propuesta, del presente escrito.

El modelo de prototipos permite que todo el sistema, o algunos de sus partes, se construyan rápidamente para comprender con facilidad y aclarar ciertos aspectos en los que se aseguren que el desarrollador, el usuario y el cliente estén de acuerdo en lo que se necesita, así como también la solución que se propone para dicha necesidad y de esta forma minimizar el riesgo y la incertidumbre en el desarrollo, este modelo se encarga del desarrollo de diseños para que estos sean analizados y prescindir de ellos a medida que se adhieran nuevas especificaciones, es ideal para medir el alcance del producto, pero no se asegura su uso real.

Este modelo principalmente se lo aplica cuando un cliente define un conjunto de objetivos generales para el software a desarrollarse sin delimitar detalladamente los requisitos de entrada, procesamiento y salida, es decir, cuando el responsable no está seguro de la eficacia de un algoritmo, de la adaptabilidad del sistema o de la forma en que interactúa el hombre y la máquina. Este modelo se encarga principalmente de ayudar al ingeniero de sistemas y al cliente a

entender de mejor manera cuál será el resultado de la construcción cuando los requisitos estén satisfechos.

Definición: “Es un modelo del comportamiento del sistema que puede ser usado para entenderlo completamente o ciertos aspectos de él y así clarificar los requerimientos… Un prototipo es una representación de un sistema, aunque no es un sistema completo, posee las características del sistema final o parte de ellas”. [28]

Características de los prototipos: [29]

- Funcionalidad limitada.
- Poca fiabilidad.
- Características de funcionalidad pobres.
- Alto grado de participación del usuario el cual evalúa los prototipos, propone mejoras y detalla requisitos.
- Alto grado de participación del analista de sistemas, ya que en muchos casos los usuarios no pueden indicar los requisitos sin tener experiencia con el sistema.
- El prototipo da mayor conocimiento al usuario y analistas ayudando a que el usuario aprenda a utilizar el sistema.

[28] Leidy Reyes R., María del Carmen Ruiz, Mónica Vivanco E., 2009
[29] Idem

En la Figura 4.1 se muestran las fases para el desarrollo de un prototipo donde se llevan a cabo continuas revisiones hasta llegar al sistema final para las pruebas que llevaran al producto final.

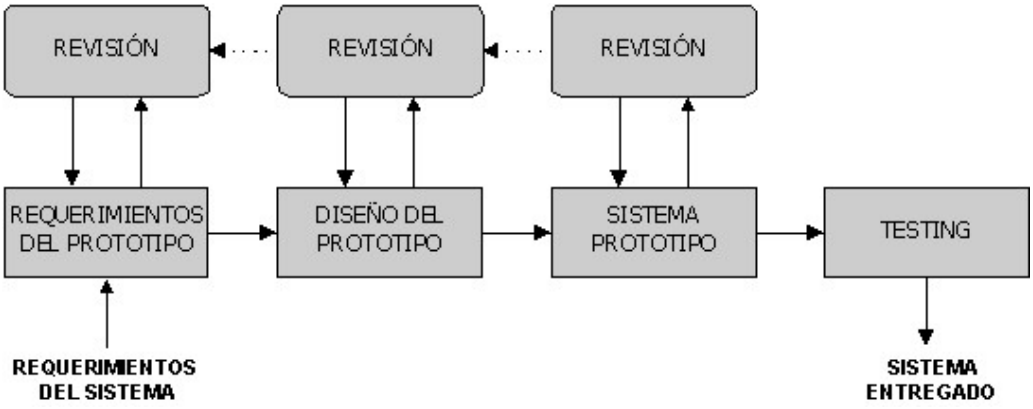


Figura 4.1 Fases para el desarrollo por prototipo.

4.2 Requerimientos del Prototipo

A continuación se listan los pasos necesarios para cubrir los requerimientos del prototipo.

4.2.1 Necesidades

De acuerdo a las necesidades del proyecto, se requería que el DVR además de tener la función innata de monitoreo y grabación de las cámaras en tiempo real, también pudiera tener acceso a internet para tener la capacidad de enviar un correo electrónico a nuestro servidor y

los puertos de entrada necesarios para poderle agregar un dispositivo que serviría como disparador (botón de pánico) el cual sería aprovechado para lanzar la emergencia.

Ya elegido el DVR Hikvision DS7204, con las características necesarias, se procedió a la conexión de las cámaras de circuito cerrado análogas, por medio de cable coaxial a los conectores traseros del DVR, así como con un cable dúplex también se conectó el botón de pánico a las entradas de alarma del DVR. Como se muestra en el esquema de la Figura 4.2.

Figura 4.2 Esquema del DVR.

Una vez solucionado la parte del hardware, se requería del software, que en base al correo electrónico enviado, fuera capaz de recibirlo y procesarlo, generando la emergencia para después poder ser atendida en el Call Center que tuviera a su cargo dicho monitoreo.

4.2.2 Diagrama de Caso de Uso del modo Monitor.

En la Figura 4.3 se muestra el Diagrama de Caso de Uso del modo monitor donde intervienen los 2 actores principales, en este caso, el operador del sistema de monitoreo y el usuario que genera la emergencia.

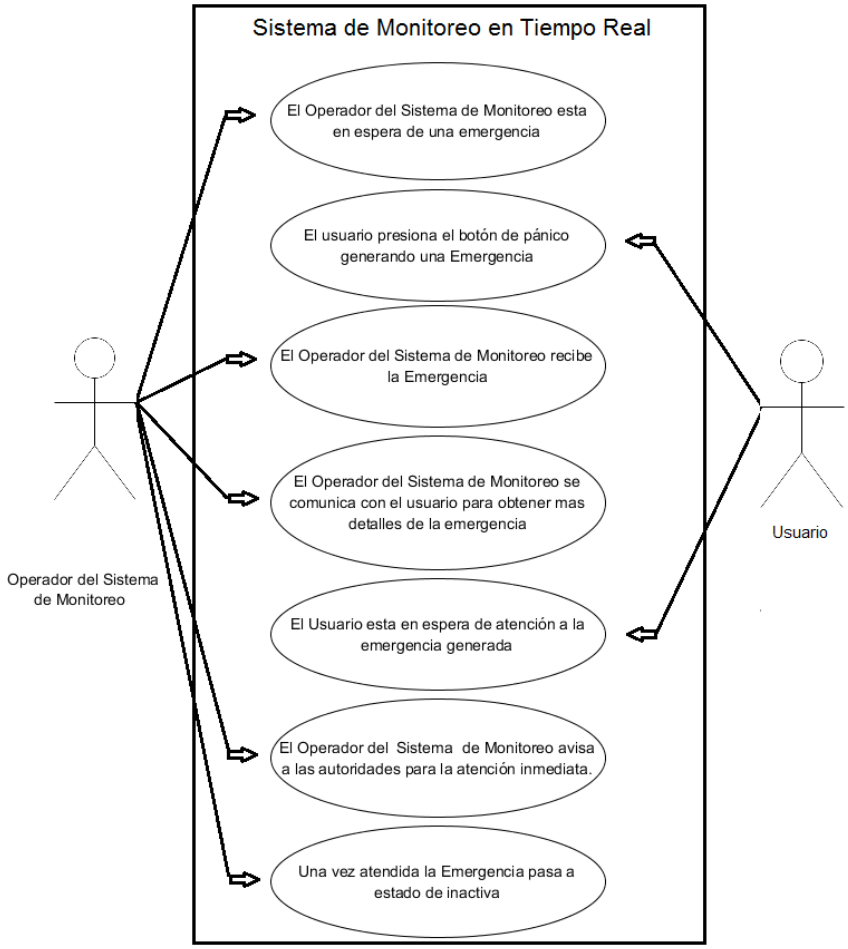


Figura 4.3 Diagrama de Caso de Uso modo Monitor.

4.2.3 Diagrama de Caso de Uso del modo Archivo.

En la Figura 4.4 se muestra el Diagrama de Caso de Uso del modo Archivo donde interviene solo 1 actor principal, en este caso, el operador del sistema de monitoreo.

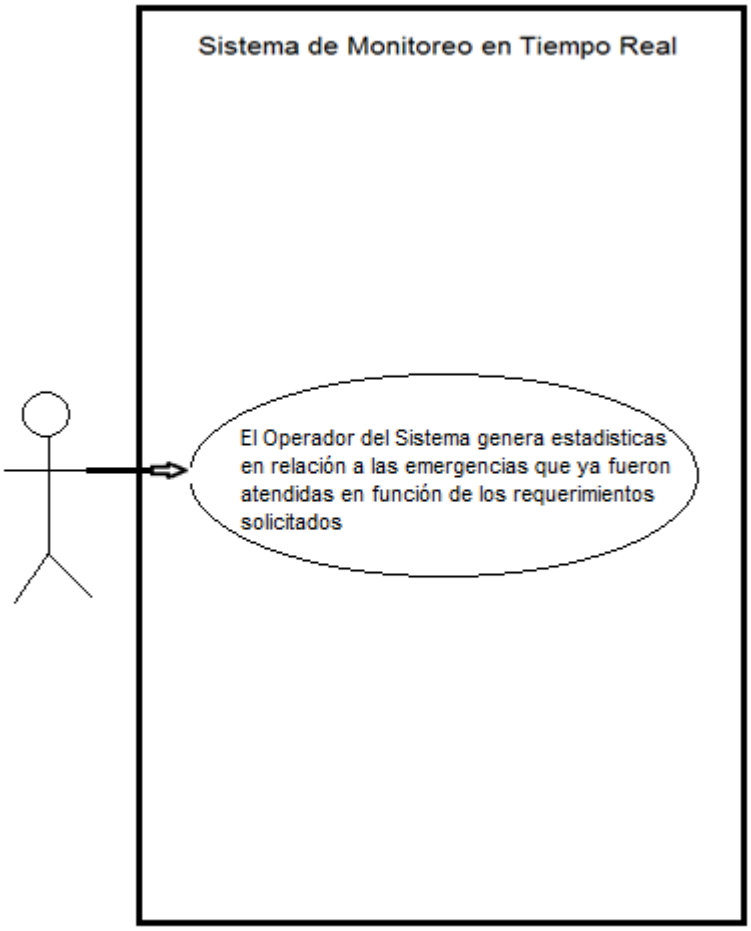


Figura 4.4 Diagrama de Caso de Uso del modo Archivo.

4.2.4 Especificaciones de Caso de Uso del modo Monitor.

En la Figura 4.5 se muestra las especificaciones del Caso de Uso en modo Monitor.

No. Caso de Uso 1	Nombre Caso de Uso Monitoreo	
Actores	Operador	
Objetivo	Monitorear el Sistema en espera de una Emergencia para darle seguimiento en caso de que esta se presente.	
Pre condiciones	1.-Haber iniciado sesión en el Sistema de Monitoreo en Tiempo Real.	
Pos condiciones	1.-El registro de la Emergencia quedará almacenado en el Sistema (BD) para su posterior consulta. 2.-La emergencia será atendida por las autoridades correspondientes.	
Flujo de Eventos	Paso	Acción
	1	El Sistema solicita Usuario y Contraseña.
	2	El Operador ingresa usuario y contraseña.
	3	El Sistema autentica.
	4	El Operador accesa al área de monitoreo.
	5	El Sistema monitorea la base de datos en busca de una emergencia.
	6	El Sistema despliega la Emergencia.
	7	El Operador verifica los datos mostrados por el Sistema.
	8	El Operador manda la ayuda necesaria y le da seguimiento a su atención.
	9	El Operador desactiva la emergencia.
Manejo de Situaciones Excepcionales	Paso	Acción
	1	El Sistema una vez que ha registrado una Emergencia, descartará las siguientes hasta que sea atendida la que se registró inicialmente.
Comentarios	En caso de que el Sistema no encuentre una emergencia activa estará en espera de que esta se presente y la desplegara automáticamente.	

Figura 4.5 Especificación de Caso de Uso modo Monitor.

4.2.5 Especificaciones de Caso de Uso del modo Archivo.

En la Figura 4.6 se muestra las especificaciones del Caso de Uso en modo Archivo.

No. Caso de Uso 2	Nombre Caso de Uso Archivo	
Actores	Operador	
Objetivo	Obtención de datos para la elaboración de informes y estadísticas.	
Pre condiciones	1.-Haber iniciado sesión en el Sistema de Monitoreo en Tiempo Real.	
Pos condiciones	Ninguna	
Flujo de Eventos	Paso	Acción
	1	El Sistema solicita Usuario y Contraseña.
	2	El Operador ingresa usuario y contraseña.
	3	El Sistema autentica.
	4	El Operador accesa al área de archivo.
	5	El operador genera estadísticas en relación a las emergencias que ya fueron atendidas en función de los requerimientos solicitados.
Manejo de Situaciones Excepcionales	Paso	Acción
	1	Ninguno
Comentarios	Ninguno	

Figura 4.6 Especificación de Caso de Uso modo Archivo.

4.3 Diseño del Prototipo

A continuación se listan los pasos necesarios para cubrir el diseño del prototipo.

4.3.1 Diagramas de Uso

La Figura 4.7 muestra el proceso de acceso al sistema desde la Interfaz Web.

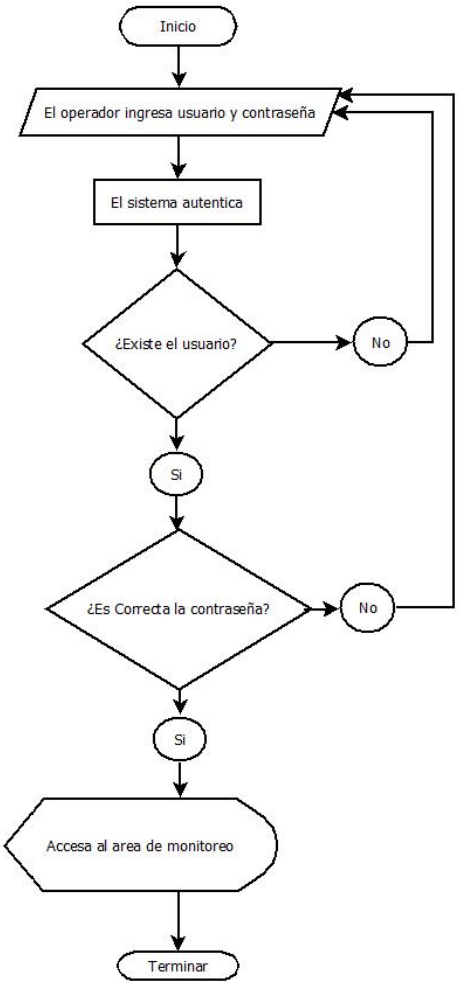


Figura 4.7 Diagrama del proceso de acceso a plataforma en modo monitor.

La Figura 4.8 muestra el proceso cíclico en el que se encuentra el servidor en espera de un alerta.

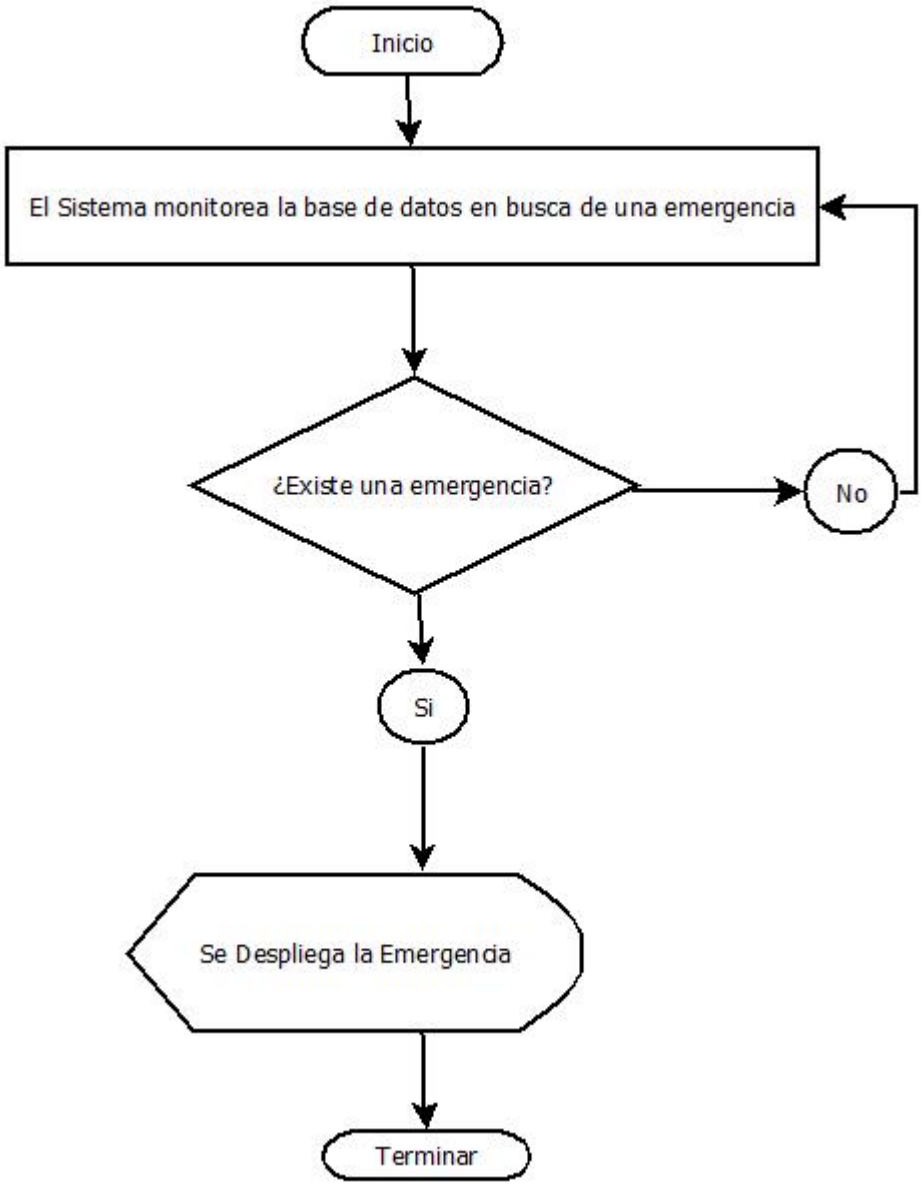


Figura 4.8 Diagrama de monitoreo de la emergencia.

La Figura 4.9 muestra el proceso de la activación de la alarma, desde el presionado del botón de pánico.

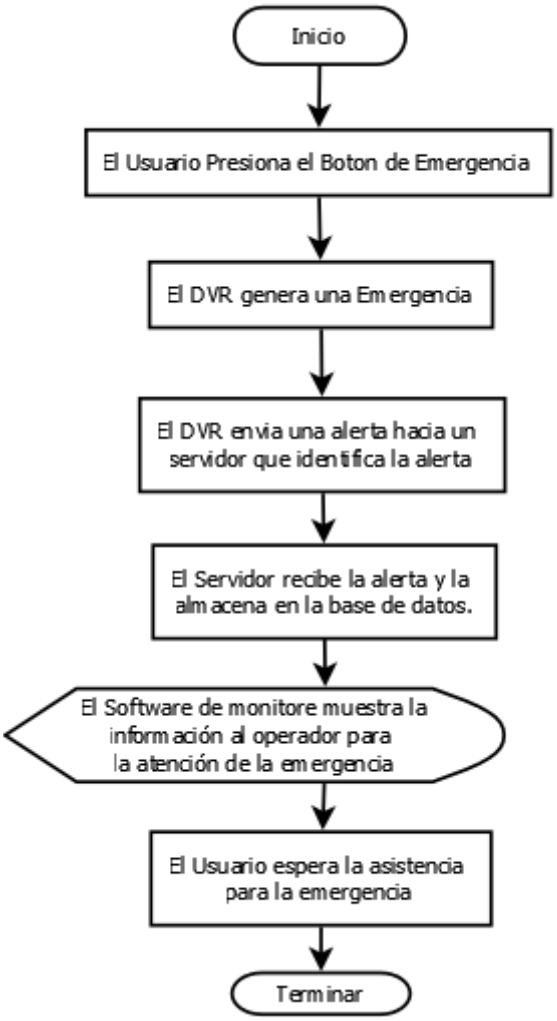


Figura 4.9 Activación de emergencia.

La Figura 4.10 muestra el proceso después de que el monitor presenta una alarma y como esta se inactiva.

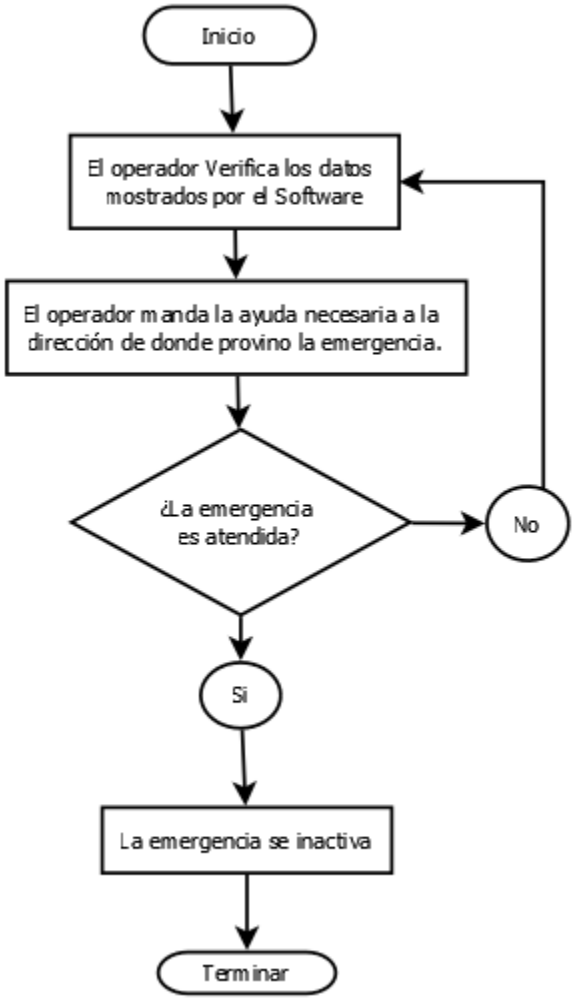


Figura 4.10 Diagrama de seguimiento de la emergencia.

La Figura 4.11 muestra el proceso de acceso a la plataforma de modo archivo, un área aun no desarrollada en su totalidad, pero que en su estado actual permite la visualización de un historial de las alarmas que se han recibido en el sistema.

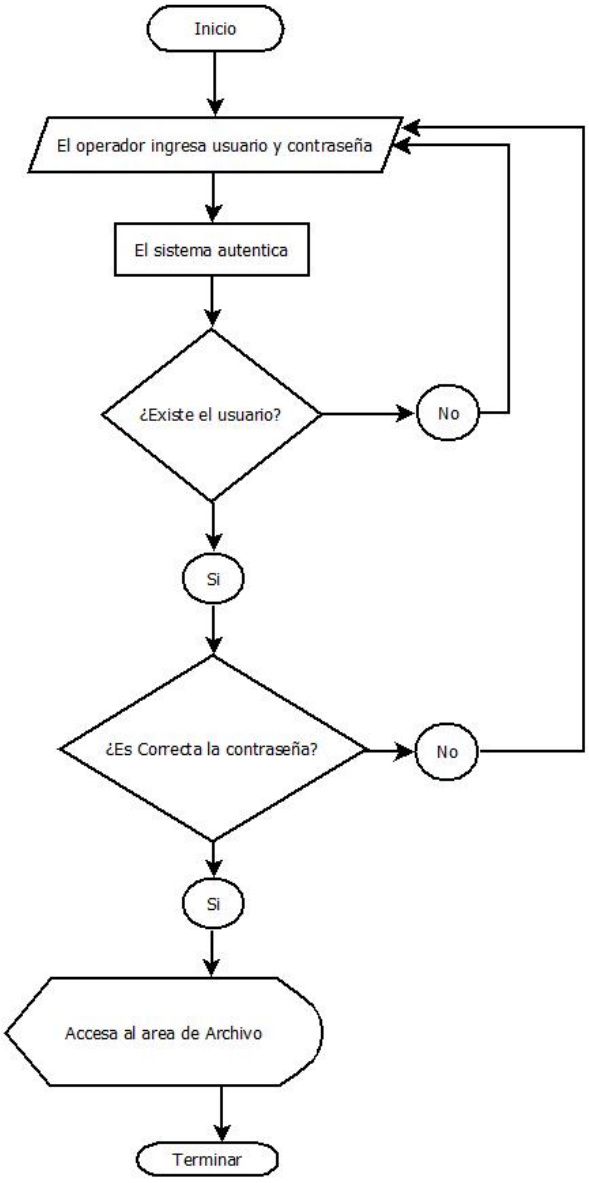


Figura 4.11 Diagrama de acceso a plataforma en modo archivo.

4.3.2 Diagramas de Entidad Relación

En la Figura 4.12 se muestra la relación entre el operador del sistema de monitoreo – emergencia, donde uno o varios usuarios en el Call Center pueden atender una y sola una emergencia hasta que esta se haya dado por terminada.

Figura 4.12 Diagrama entidad/relación operador del sistema – emergencia.

En la Figura 4.13 se muestra la relación entre el Usuario (Generador de Emergencia) – Emergencia, donde solo un usuario de donde proviene la emergencia pueden generar una y solo una emergencia hasta que esta se haya dado por terminada.

Figura 4.13 Diagrama entidad relación Usuario (Generador de Emergencia) – Emergencia.

En la Figura 4.14 se muestra la relación Emergencia – Catálogo precargado de Información, donde solo una emergencia activa puede tomar una y sola una vez la información necesaria del catálogo para mostrar los datos completos de la emergencia.

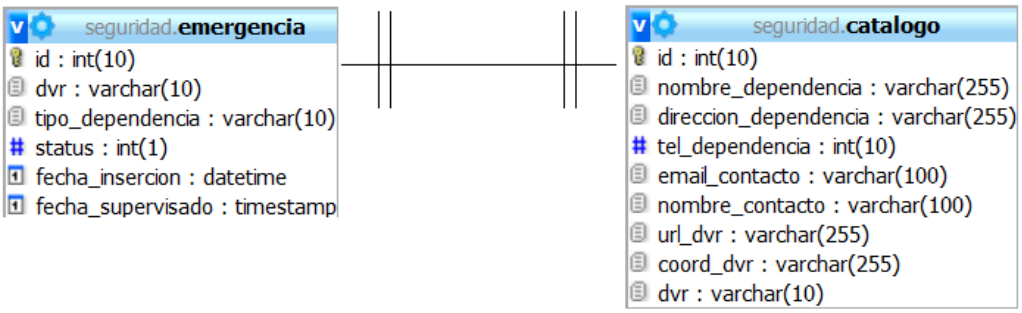


Figura 4.14 Diagrama entidad relación Emergencia – Catálogo precargado de Información.

4.4 Desarrollo del Sistema Prototipo

A continuación se listan los pasos necesarios para el desarrollo del sistema prototipo.

4.4.1 Implementación del Software

Una vez montado el servidor Ubuntu, fue necesaria la instalación de Postfix la cual fue de la siguiente manera:

Nota: Todo el proceso que a continuación se describe es autoría propia, algunas imágenes fueron extraídas de www.nosolounix.com [30],[31].

[30] www.nosolounix.com, 2012

Paso 1 – Instalar Servidor WEB en Ubuntu (Apache2).

Instalar Apache2

Apache2 es un potente servidor HTTP de código abierto. Con él se puede montar un servidor web de una forma sencilla y segura[32]. Para poder instalar un servidor de correo en Ubuntu que sea accesible vía web es indispensable instalar Apache. Para instalar Apache2 se escribe en una terminal lo siguiente:

sudo apt-get install apache2

Se debe accesar a http://localhost en nuestro navegador (Firefox por ejemplo) y como se muestra en la Figura 4.15 se puede apreciar que al escribir localhost, el servidor apache responde la petición mostrando que está funcionando correctamente.

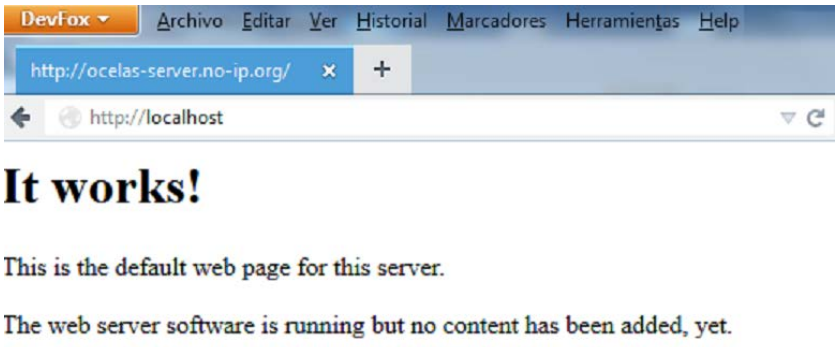


Figura 4.15 Apache instalado correctamente.

[31] Elías Hidalgo, 2012
[32] The Apache Software Foundation, 1998

Paso 2 – Instalar y configurar Servidor DNS en Ubuntu (bind9).

Instalar servidor DNS

DNS o Domain Name System, es un sistema cuyo principal cometido es asignar y resolver nombres a direcciones IP, de manera que cada vez que se necesite acceder a un sitio web no sea necesario recordar la dirección IP de la web, sino un nombre más fácil de recordar para las personas[33].

Por ejemplo: Es más fácil recordar www.google.com que 209.85.135.106.

Dicho esto, se puede ver claramente que un servidor DNS ayuda mucho en la labor de crear un servidor de correo en Ubuntu. Para instalar el servidor DNS se utiliza la aplicación bind9[34]. Para instalarlo, se escribe en una terminal lo siguiente:

sudo apt-get install bind9

A continuación, se configura bind9. Se localiza y edita el archivo /etc/bind/named.conf.local para indicarle como se llama la "zona" y así poder configurarla. Aquí se establece cual va a ser el dominio a ser usado. En este caso se eligió el dominio “misitio.com”.

En la Figura 4.16 se muestra un ejemplo de las líneas de configuración agregadas para el correcto funcionamiento de la “zona”.

[33] HOSPEDAJE-WEB, 2010
[34] debian.org, 2001

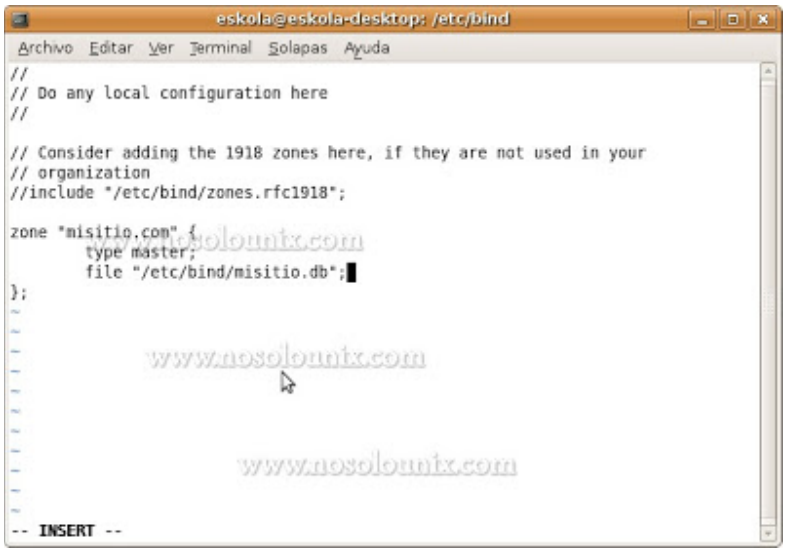


Figura 4.16 Establecer Dominio.

Se crea el archivo "db" que se ha indicado en el archivo anterior al indicarle la zona. Para ello, se puede copiar el archivo db.local y renombrarlo al que se decidió usar (para simplemente editar la información con los datos necesarios y no tener que escribir todo el archivo desde cero). En este caso el archivo se llama "misitio.db". Este archivo se ubica en la carpeta /etc/bind/, de manera que el archivo estaría en la siguiente ubicación:

/etc/bind/misitio.db

Se puede ver un ejemplo de cómo se ha editado el archivo en la siguiente imagen. En este archivo se configura el NameService (NS), el mail (que se explicará más adelante) y el servidor web (www). Recordar que en vez de la IP "192.168.126.34" se tiene que meter la IP de nuestra máquina.

En la Figura 4.17 se muestra el contenido y las configuraciones necesarias para el correcto funcionamiento del que, en este ejemplo, será nuestro dominio en función.

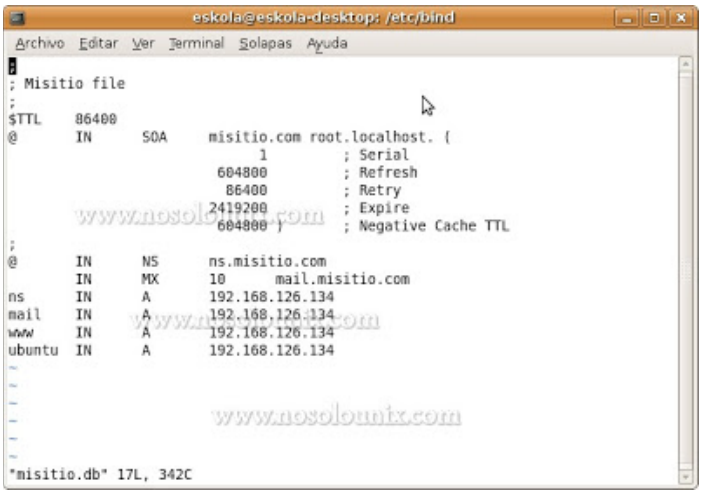


Figura 4.17 Configuración de NameService.

Se debe reiniciar bind9 para que los cambios se guarden mediante el siguiente comando:

sudo /etc/init.d/bind9 restart

Acto seguido, para poder trabajar con el servidor de correo en Ubuntu de forma local, se cambian las DNS de nuestra máquina y se le introduce como DNS la IP de la propia máquina. Para cambiarlo (teniendo el entorno grafico habilitado), habrá que dirigirse a Sistema > Administración > Red > Pestaña DNS y se eliminan las DNS que se tiene para trabajar el local y ahí se introducirá nuestra IP (la IP de la máquina servidor). En este caso se ha introducido la IP 192.168.126.134, pero se deberá introducir la IP local del servidor Ubuntu.

En la Figura 4.18 se muestra la ventana de configuración de red donde se añade el servidor DNS, el cual previamente ya ha sido configurado.

Figura 4.18 Configuración de la red.

Lo siguiente será abrir el navegador web y dirigirse a la siguiente dirección: http://www.misitio.com (ahí se debe introducir el dominio que se haya introducido en los pasos anteriores, en nuestro caso es misitio.com) y se puede observar una pantalla similar a la Figura 4.19, pero ya con una dirección.

En la Figura 4.19 se puede apreciar que una vez configurado el servidor DNS al momento de poner en la barra de dirección del navegador la dirección www.misitio.com, el navegador muestra el contenido del servidor de manera correcta.

Ya se ha instalado y configurado el servidor DNS para poder tener un servidor de correo en Ubuntu.

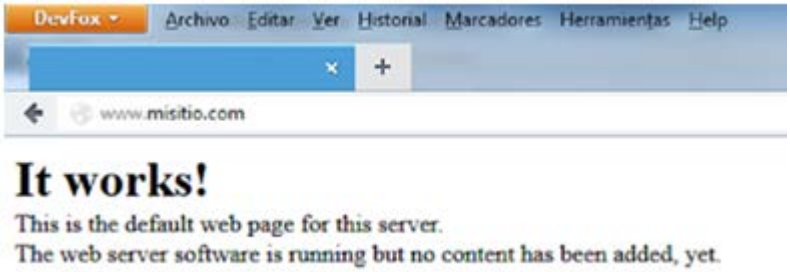


Figura 4.19 Dominio funcionando.

Paso 3 – Instalar Servidor de correo en Ubuntu (Postfix).

Instalar y configurar servidor de correo.

POSTFIX: Es un agente de transporte de correo de manera que permite enrutar y transferir correo electrónico. Por ello, si se necesita tener un servidor de correo en Ubuntu, se debe instalar Postfix[35].

Para instalar Postfix, solo se tiene que escribir lo siguiente en una terminal:

sudo apt-get install Postfix

Durante la instalación aparecen diferentes ventanas.

La Figura 4.20 muestra el despliegue de la información de las múltiples opciones a elegir dentro de la configuración inicial de POSTFIX.

[35] postfix.org, 1998

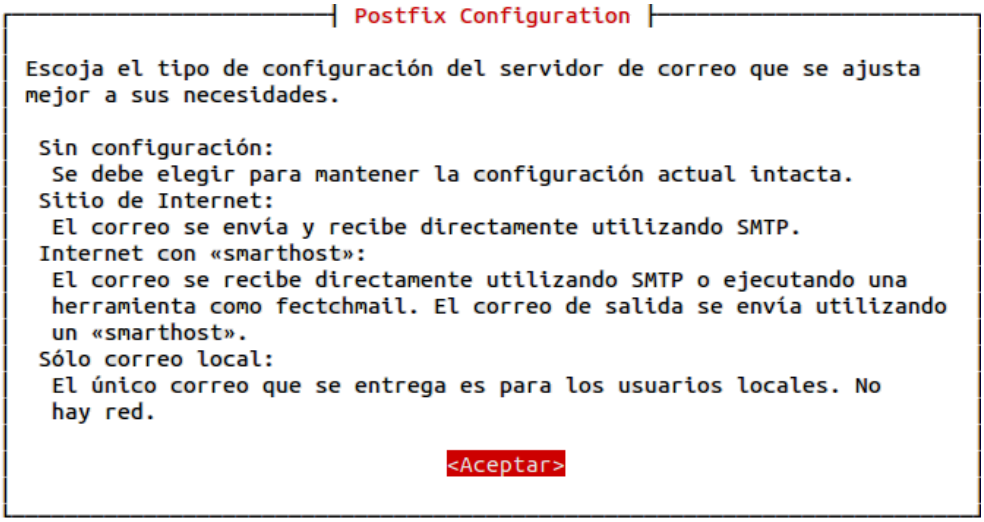


Figura 4.20 Postfix instalación 1.

Se selecciona “Sitio de Internet”, como se muestra en la Figura 4.21, que para nuestra plataforma es la correcta.

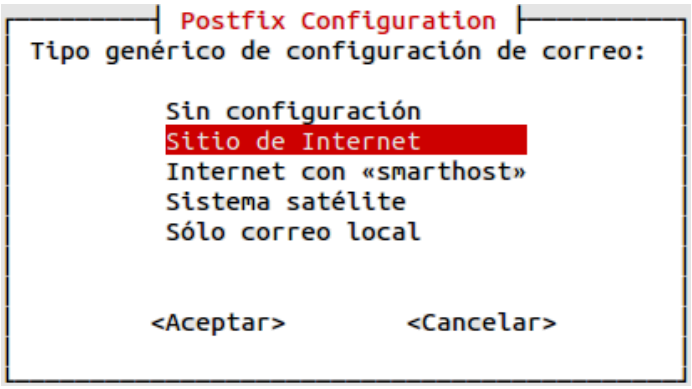


Figura 4.21 Postfix instalación 2.

En la siguiente se escribe el dominio que se haya escogido. Para poder tener un servidor de correo en Ubuntu.

En la Figura 4.22 se muestra la ventana donde se ingresa el que será el dominio al cual se enviaran los correos.

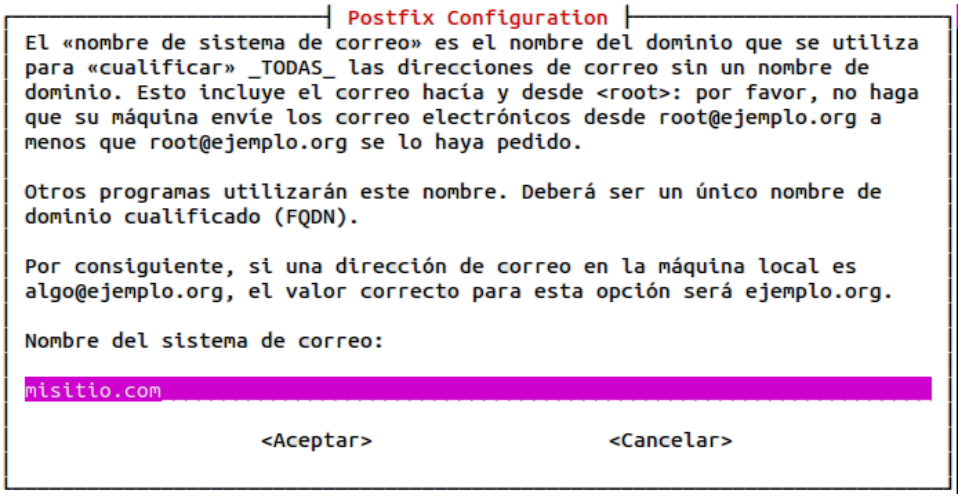


Figura 4.22 Postfix instalación 3.

A continuación se edita el siguiente archivo: /etc/postfix/main.cf Al final del archivo se le añaden las siguientes líneas de código.

inet_protocols = ipv4

home_mailbox = Maildir/

Mediante estas líneas se indica que protocolo se va a usar y donde se guardarán los e-mails. Asimismo, revisa que en la directiva mydestination de este mismo fichero se pueda ver:

mydestination = misitio.com

Para que los cambios surtan efecto, escribir en terminal lo siguiente:

sudo /etc/init.d/postfix restart

COURIER: Es un agente de transporte de correos (MTA), el cual proveerá de diferentes servicios para la funcionalidad del correo entrante (POP3, IMAP, WEBMAIL)[36]. Para conseguir el servidor de correo en Ubuntu, se instala courier-pop y courier-imap mediante los siguientes comandos en terminal:

sudo apt-get install courier-pop

En la Figura 4.23 se muestra una ventana donde pregunta si se desea que para la configuración de Courier se manejen varios directorios y varios archivos para su misma configuración, esto para la administración de ese servicio mediante un servicio Web como Squierrelmail o Roundcube, se seleccionará no, con el fin de que sea un único archivo plano y no exista ese permiso de administrador para la plataforma de correos, únicamente el acceso a los correos.

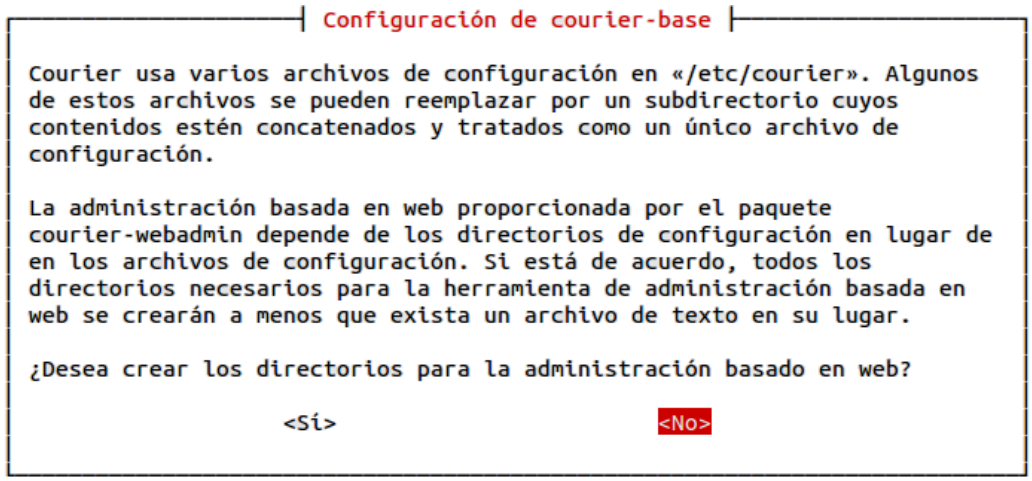


Figura 4.23 Postfix instalación 4.

[36] courier-mta.org, 1998

Instalar courier-imap:

sudo apt-get install courier-imap

MAILX: Es un cliente de correo para unix en modo consola, que permite redactar correos desde la línea de comandos.

Se debe instalar mailx, ya que más adelante se utilizará en uno de los pasos para tener el servidor de correo en Ubuntu.

sudo apt-get install mailx

SQUIRRELMAIL: Es una aplicación webmail en PHP[37]. El objetivo es que gracias al servidor Web que se ha instalado (Apache2), se podrán ver los e-mails que nos envíen.

Para instalar Squirrelmail, en una terminal se introduce lo siguiente:

sudo apt-get install squirrelmail

Una vez instalado, escribir en la terminal lo siguiente para configurarlo:

squirrelmail-configure

Se podrá observar un menú, como se puede ver en la Figura 4.24. Se muestra una lista de configuración preestablecidas para Squierrelmail, que van desde organización hasta el uso de base de datos para el almacenamiento de correo. Se elige la opción D (Configurar opciones predefinidas para servers imap específicos) que son opción por default.

[37] squirrelmail.org, 1999

Acto seguido, se selecciona el tipo de correo: Courier.

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Main Menu --
1.  Organization Preferences
2.  Server Settings
3.  Folder Defaults
4.  General Options
5.  Themes
6.  Address Books
7.  Message of the Day (MOTD)
8.  Plugins
9.  Database
10. Languages

D.  Set pre-defined settings for specific IMAP servers

C   Turn color on
S   Save data
Q   Quit

Command >> D
```

Figura 4.24 Squirrelmail instalación 1.

En la Figura 4.25 se muestra una ventana donde se pregunta el manejador de correo entrante, en este caso Courier.

```
---------------------------------------------------------
While we have been building SquirrelMail, we have discovered some
preferences that work better with some servers that don't work so
well with others.  If you select your IMAP server, this option will
set some pre-defined settings for that server.

Please note that you will still need to go through and make sure
everything is correct.  This does not change everything.  There are
only a few settings that this will change.

Please select your IMAP server:
    bincimap    = Binc IMAP server
    courier     = Courier IMAP server
    cyrus       = Cyrus IMAP server
    dovecot     = Dovecot Secure IMAP server
    exchange    = Microsoft Exchange IMAP server
    hmailserver = hMailServer
    macosx      = Mac OS X Mailserver
    mercury32   = Mercury/32
    uw          = University of Washington's IMAP server
    gmail       = IMAP access to Google mail (Gmail) accounts

    quit        = Do not change anything
Command >> courier
```

Figura 4.25 Squirrelmail instalación 2.

Se obtiene el resultado como el que se parecía en la Figura 4.26, donde se despliega la información que por default se ha configurado para Courier.

```
                imap_server_type = courier
            default_folder_prefix = INBOX.
                     trash_folder = Trash
                      sent_folder = Sent
                     draft_folder = Drafts
                show_prefix_option = false
             default_sub_of_inbox = true
show_contain_subfolders_option = false
                optional_delimiter = .
                     delete_folder = true

Press enter to continue...
```

Figura 4.26 Squirrelmail instalación 3.

Después se pulsa cualquier tecla para proceder con el resto de la configuración. Aparece una lista de las opciones de cómo se necesitará que funcione Squirrelmail. Lo siguiente será escribir 1 y pulsar ENTER de nuevo.

En la Figura 4.27 se solicita que se escoja el tipo de configuración, que va desde uso de dominio, o poder actualizar opciones de configuración previamente establecidas.

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Server Settings

General
-------
1.  Domain                : trim(implode('', file('/etc/'.(file_exists('/etc/mai
lname')?'mail':'host').'name')))
2.  Invert Time           : false
3.  Sendmail or SMTP      : SMTP

A.  Update IMAP Settings  : localhost:143 (courier)
B.  Update SMTP Settings  : localhost:25

R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit

Command >> 1

The domain name is the suffix at the end of all email addresses.  If
for example, your email address is jdoe@example.com, then your domain
would be example.com.

[trim(implode('', file('/etc/'.(file_exists('/etc/mailname')?'mail':'host').'name
')))]:
```

Figura 4.27 Squirrelmail instalación 4.

A continuación se escribe el dominio del sitio web (en este caso misitio.com) que más adelante se utilizará para acceder al servidor de correo en Ubuntu. Se debe dejar como se ve en la Figura 4.28, donde se muestra como después de seleccionar la opción de dominio se escribe el dominio que previamente se ha configurado, en este caso misitio.com

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Server Settings

General
-------
1.  Domain                : trim(implode('', file('/etc/'.(file_exists('/etc/mai
lname')?'mail':'host').'name')))
2.  Invert Time           : false
3.  Sendmail or SMTP      : SMTP

A.  Update IMAP Settings  : localhost:143 (courier)
B.  Update SMTP Settings  : localhost:25

R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit

Command >> 1

The domain name is the suffix at the end of all email addresses.  If
for example, your email address is jdoe@example.com, then your domain
would be example.com.

[trim(implode('', file('/etc/'.(file_exists('/etc/mailname')?'mail':'host').'name
')))]: misitio.com
```

Figura 4.28 Squirrelmail instalación 5.

Al pulsar la tecla ENTER el resultado final será como se puede ver en la Figura 4.29, que muestra nuevamente el menú inicial de configuración.

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Server Settings

General
-------
1.  Domain                : misitio.com
2.  Invert Time           : false
3.  Sendmail or SMTP      : SMTP

A.  Update IMAP Settings  : localhost:143 (courier)
B.  Update SMTP Settings  : localhost:25

R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit

Command >>
```

Figura 4.29 Squirrelmail instalación 6.

Por último, escribir Q (Quit) para salir y se guardarán los datos.

En la Figura 4.30 se muestra que después de seleccionar la opción de salir (Quit), preguntará si deberá guardar los cambios, a lo que se contestará que si (Yes).

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Server Settings

General
-------
1.  Domain                 : misitio.com
2.  Invert Time            : false
3.  Sendmail or SMTP       : SMTP

A.  Update IMAP Settings   : localhost:143 (courier)
B.  Update SMTP Settings   : localhost:25

R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit

Command >> Q

You have not saved your data.
Save?  [Y/n]: Y
```

Figura 4.30 Squirrelmail instalación 7.

Lo siguiente que se hace es configurar el webmail de Squirrelmail para que se pueda acceder a él vía web mediante Apache. Para ello, se escribe lo siguiente en un terminal:

cd /var/www

sudo ln -s /usr/share/squirrelmail webmail

Una vez escrito, se comprueba que todo se ha realizado correctamente. Para ello, es necesario abrir en Firefox y dirigirse a la siguiente

dirección: http://www.misitio.com/webmail (en vez de misitio.com se introducirá el dominio que se haya configurado en pasos anteriores), donde se podrá ver nuestro servidor de correo en Ubuntu vía web.

En la Figura 4.31 se muestra una ventana donde al no haberse reiniciado Apache, las configuraciones de Squierremail no han entrado en función, por lo tanto intenta descargar el archivo index.php.

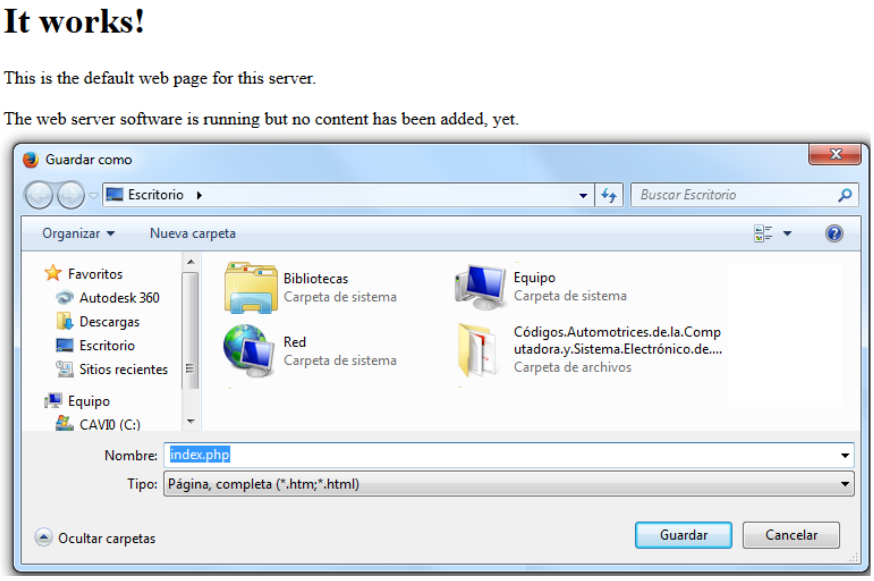


Figura 4.31 Squirrelmail instalación 8.

En caso de ver esto, es necesario borrar las cookies y toda la información privada de nuestro navegador. Después, habrá que reiniciar Apache mediante el siguiente comando en la terminal:

sudo /etc/init.d/apache2 restart

Se debe esperar a que Apache2 reinicie y se necesitará entrar a http://www.misitio.com/webmail y se podrá observar la pagina de inicio de Squirrelmail funcionando correctamente, como se ve en la Figura 4.32.

Figura 4.32 Squirrelmail instalación 9.

Paso 4 – Acondicionamiento de la configuración de Postfix y pruebas.

Crear usuarios y probar que el servidor funciona

El siguiente paso para poder probar el servidor de correo en Ubuntu es crear 2 usuarios. Para ello, se escribe en la terminal lo siguiente:

sudo adduser user1

Se contestan las diferentes preguntas que pide (lo más importante es el password, recordarlo, ya que se necesitará más adelante) y se hace lo mismo con otro usuario:

sudo adduser user2

En este punto, ya se está muy cerca de tener en funcionamiento el servidor de correo en Ubuntu. Lo siguiente que se hace es enviar un e-mail entre los usuarios creados a través de la terminal (para eso fue instalado mailx unos pasos atrás). Se debe iniciar sesión como user1 mediante el siguiente comando en terminal:

su user1

Se pide la contraseña de user1 (se introduce la contraseña correspondiente al crear los usuarios). Lo siguiente es enviar un e-mail al user2. Se escribe lo siguiente en la terminal:

mail user2

En Subject se escribe el asunto. Se pulsa ENTER y ahí se escribe el texto del mensaje. Cuando se haya acabado de escribir el mensaje, es necesario introducir un salto de línea (pulsando la tecla ENTER), se escribe un punto (es decir ".") y se vuelve a pulsar ENTER. Acto seguido, indicar si se quiere enviar el mensaje a más destinatarios (Cc). Como no es necesario enviar el mensaje a nadie más, se vuelve a pulsar ENTER.

Lo siguiente es comprobar que ese e-mail ha llegado correctamente. Para comprobarlo, es necesario abrir el navegador web, dirigirse a http://www.misitio.com/webmail e iniciar sesión con los datos del user2.

En la Figura 4.33 se muestra cómo se ingresan los datos tanto del usuario como su respectiva contraseña.

Figura 4.33 Acceso al servidor.

Se debe ver como en la siguiente Figura 4.34, la bandeja de entrada, donde se muestra el acceso exitoso al servicio de correo, mostrando además el correo previamente enviado con mail.

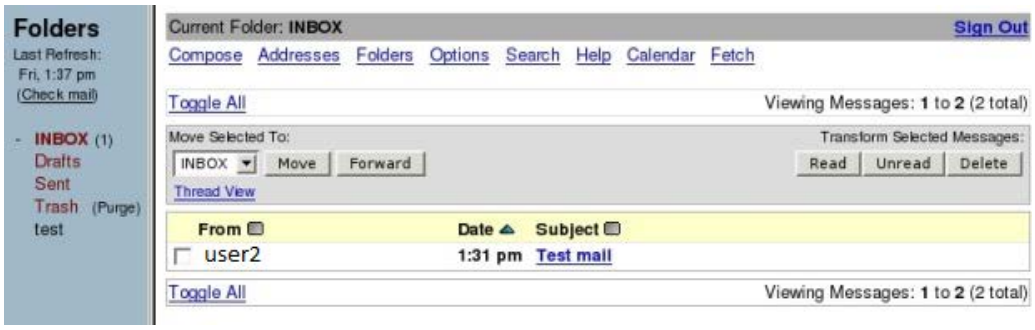


Figura 4.34 Bandeja Entrada.

En la Figura 4.35 se puede apreciar el contenido del correo, así como el usuario origen, en este caso user2 y el usuario destino user1.

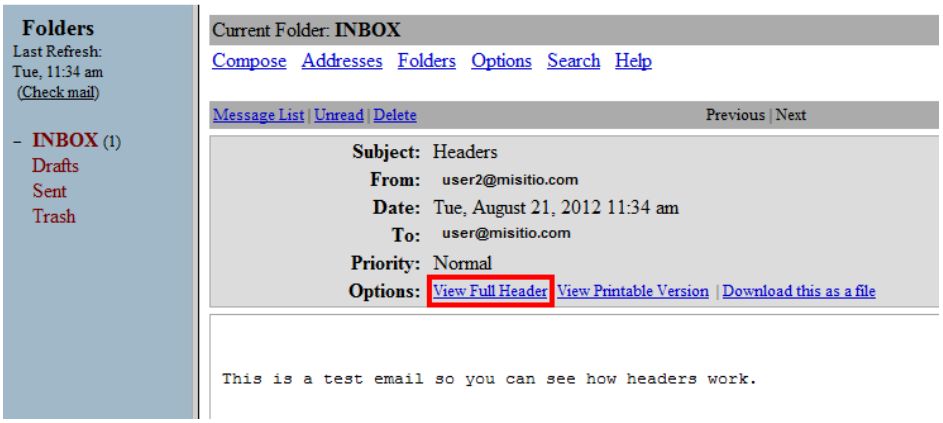


Figura 4.35 E-mail en Squirrelmail.

Una vez verificado que el correo funciona, se tiene que indicar a Postfix que no se va a almacenar el contenido del correo, puesto que,

esencialmente la información que se requiere vendrá de la propia dirección del correo electrónico.[38]

Para lograr dicho objetivo se tiene que editar el archivo master.cf ubicado en /etc/postfix/.

En la primera línea donde se establecen las condiciones de operación del servidor de correo entrante se hacen modificaciones quedando de la siguiente manera:

smtp inet n - - - - smtpd -o

Pero como se mencionó anteriormente, se necesitará como dato de relevancia la dirección de correo electrónico, para la cual es necesario modificar nuevamente la línea donde se establecen las condiciones de operación del correo entrante, dicha línea debe quedar de la siguiente manera:

smtp inet n - - - - smtpd –o content_filter=seguridad:dummy

Donde “seguridad” será un apartado de configuración en el mismo archivo master.cf, donde se le indicará a Postfix que la dirección de correo electrónico será enviado como una variable a un archivo ejecutable bash, la línea de configuración se muestra a continuación:

seguridad unix - n n - - pipe flags= user=ocelas:ocelas
argv=/home/ocelas/proyecto/php.sh ${original_recipient}

[38] Wed, 2012

Para dar de alta los correos electrónicos de los diferentes DVR´s que se estarán monitoreando, sin necesidad de crear las cuentas, se agrega una línea de configuración al archivo main.cf, ubicado en /etc/postfix:

virtual_alias_maps = hash:/etc/postfix/virtual

En el archivo virtual se podrán agregar “n” cantidad de direcciones de correos electrónicos, todos ellos teniendo el mismo dominio, usando únicamente una cuenta de correo inicial.

Cabe mencionar, que los alias se aprovechan para identificar el ID del DVR, así como al tipo de dependencia al cual pertenecen, misma que se estará monitoreando.

Ejemplo de virtual_alias_maps

dvr0001-escuelas ocelas@ocelas-server.no-ip.org

dvr0002-hospitales ocelas@ocelas-server.no-ip.org

Una vez recibido el correo electrónico por Postfix, se enviará la dirección a una variable, misma que se procesará por un archivo ejecutable programado en bash, en este caso /home/ocelas/proyecto/php.sh, que se encargará de separar el alias en 2 variables más divididas por un “-“, quedando de la siguiente manera:

dvr0001-escuelas@ocelas-server.no-ip.org en

dvr0001=dvr

escuelas=tipo_dependencia

Ya teniendo esta información, se pueden enviar los datos de dichas variables a un programa hecho en PHP, que se ejecuta en línea de comandos, para su posterior procesamiento e ingreso como emergencia en la base de datos, en este caso el archivo a ejecutar dicha función se llamara test.php.

A continuación se muestra el código en bash que realiza dicha operación: [39]

php.sh

```
#!/bin/bash
while read linea
    do
        cabecera=`echo $linea | cut -d':' -f1`
          if [ "$cabecera" = Subject ]
        then
        tipo_dependencia=`echo $1 | cut -d'@' -f1`
        dvr=`echo $direccion | cut -d'-' -f1`
        dependencia=`echo $tipo_dependencia | cut -d'-' -f2`
        /home/ocelas/proyecto/./test.sh "$dvr" "$dependencia"
```

Ya enviadas las variables “$DVR” y “$dependencia” a test.sh, este se encarga de almacenar la emergencia con toda la información pertinente en base al contenido de dichas variables conforme a un catálogo que previamente ha sigo cargado en la base de datos.

[39] Gerardo Cabrera Hernández, 2011

El código de dicho programa en PHP llamado test.sh se muestra a continuación:

test.sh

```
#!/usr/bin/php

<?

$dvr=$argv[3] ;  //recibe el dvr de la emergencia

$dependencia=$argv[4] ; //recibe la tabla donde buscara los datos generales de la dependencia

include( "/home/ocelas/proyecto/include/inter_dbc_innodb.php" );

$dbc=connect_db("seguridad");

//guarda en $status la fila donde hay una emergencia activa con los datos del dvr recibido si es que existe

$status="SELECT * FROM emergencia WHERE dvr='$dvr' and status='1'";

$result=mysql_query($status);  //??

// Mysql_num_row verificara si se recibieron resultados del status de la consulta anterior y guardara en la variable $count el valor de 1 si hay una emergencia activa con los datos esta se descarta, esto para no acumular la misma emergencia, esto dado por que el usuario que está generando la emergencia siga presionando el botón más de 1 vez.

$count=mysql_num_rows($result);

//$count==1 terminara el proceso se inserción y descartara la emergencia

if ($count==1){goto end;} //$count==0 insertara la emergencia en la tabla

else{
```

$qryRfc="SELECT tipo_dependencia FROM dependencia WHERE tipo_dependencia='$dependencia'"; //guarda en la variable $qryRfc el tipo de la dependencia (escuelas, hospitales, etc.) a $

$resRfc=$dbc->query($qryRfc); //??

while($row=$resRfc->fetch_array()){ // ??

$tipo_dependencia=$row['tipo_dependencia']; // ??

$qryIEm="INSERT INTO emergencia VALUES ('','$dvr','$tipo_dependencia','1',CURRENT_TIMESTAMP,")";

$dbc->query($qryIEm); //??

}}

end: //fin de proceso se insercion de emergencia

?>

Paso 5 – Instalar Base de datos MariaDB en Ubuntu.

Instalar MariaDB

MariaDB 5.1 es una liberación binaria en reemplazo de MySQL 5.1, pero con un rendimiento similar a MySQL 5.5 (gracias al motor XtraDB), alguno que otro bug, y más características[40]. Para instalar MariaDB se escribe en una terminal lo siguiente[41]:

sudo apt-get -y install mariadb-server mariadb-client

Paso 6 – Instalar PHP con soporte para Apache2 y MariaDB en Ubuntu.

Instalar PHP

[40] Maria DB, 2010
[41] RAHUL, 2012

PHP (acrónimo recursivo de *PHP: Hypertext Preprocessor*) es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML.

Lo que distingue a PHP de algo del lado del cliente es que el código es ejecutado en el servidor, generando HTML y enviándolo al cliente. El cliente recibirá el resultado de ejecutar el script, aunque no se sabrá el código subyacente que era[42]. Para instalar PHP con soporte para Apache2 y MariaDB se escribe en una terminal lo siguiente[43]:

sudo install php5 libapache2-mod-php5 php5-mysqlnd

4.4.2 Implementación del DVR

Para la implementación del DVR, es necesario que previamente el lugar tenga un equipo de video vigilancia instalado, ya que solo es necesario trasladar las conexiones de las cámaras al DVR Hikvision, el cual necesita una conexión a internet cableada, lo cual se hace conectando un cable de red del Router que se va a usar al DVR y la apertura de los puertos correspondientes para el monitoreo remoto.

En la Figura 4.36 se puede apreciar como en el apartado de redireccionamiento de puertos (port forward) de los routers, se muestran los puertos que se van accesar desde afuera de la red, el protocolo a usar (TCP/UDP) y la dirección IP y el puerto hacia dónde va dirigida la conexión.

[42] PHP: Hypertext Preprocessor, 2001
[43] howtoforge.com, 2012

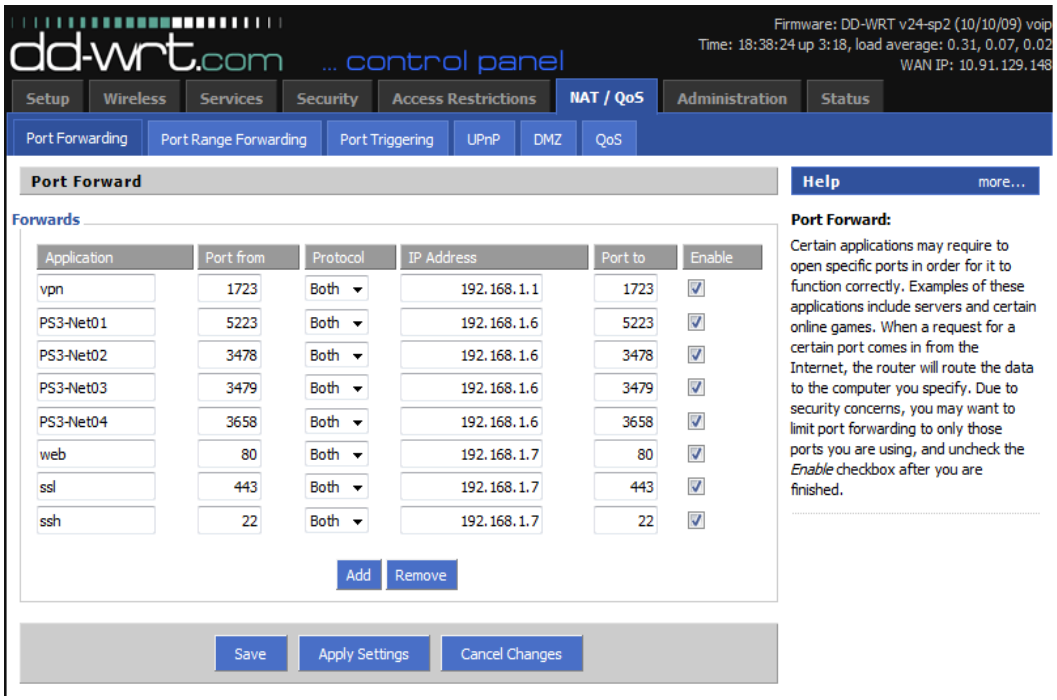


Figura 4.36 Apertura de Puertos en Router.

En la Figura 4.37 se muestran las conexiones que debe llevar el sistema de monitoreo en sitio, comprendido por el DVR, el botón de pánico que se pulsa para lanzar la alarma, las cámaras que hubiera ya en sitio y la conexión a internet para enviar la alarma al servidor. Cabe señalar que el botón de pánico también puede ser inalámbrico como el de la Figura 3.7 mostrado en el capítulo 3.

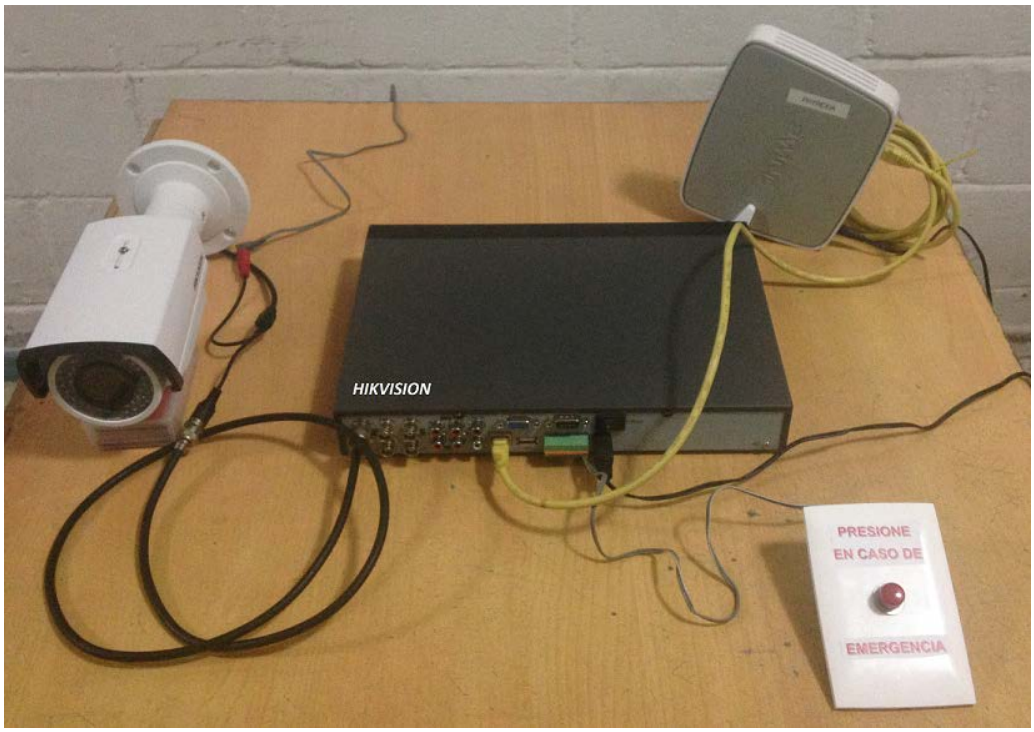


Figura 4.37 Conexiones del DVR.

Una vez realizadas las conexiones físicas, se procede configurar en el DVR, la dirección de dominio donde se va enviar la alerta al ser presionado el botón. En este proceso se requiere conocimiento previo de configuración de DVR's.

En la Figura 4.38 se muestra el menú de configuración del DVR, donde se debe especificar la cuenta de correo de donde se va a enviar la alerta y el correo destino para recibirla. Como se aprecia en la Figura en mención, es necesario completar los campos requeridos, pero este menú es solo una muestra y puede variar dependiendo el modelo del DVR, o su marca, pero esencialmente, no varían mucho.

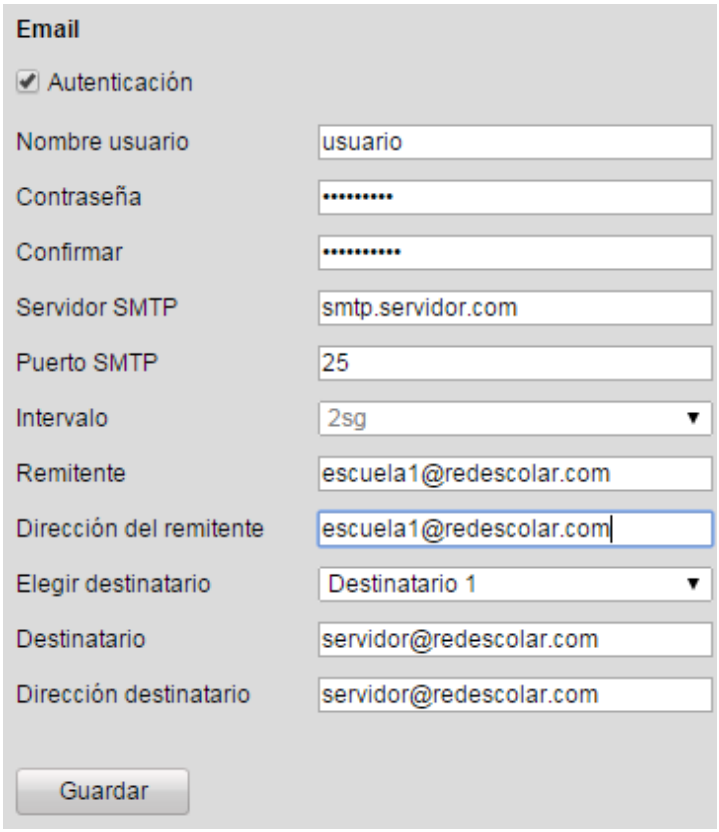


Figura 4.38 Menús de configuración Hikvision.

4.5 Pruebas de Funcionamiento

Una vez montado el DVR, el personal del Call Center entrará a la página principal del software desarrollado para el manejo de emergencia y digitará su usuario y contraseña, datos que previamente se almacenaron en la base de datos, en la tabla de usuarios. Para ello,

los requerimientos mínimos de la máquina para monitorear son una PC o Laptop, con bocinas, Internet Explorer 11 o Chrome o Safari.

La Figura 4.39 presenta la pantalla de inicio de sesión para entrar al sistema de monitoreo.

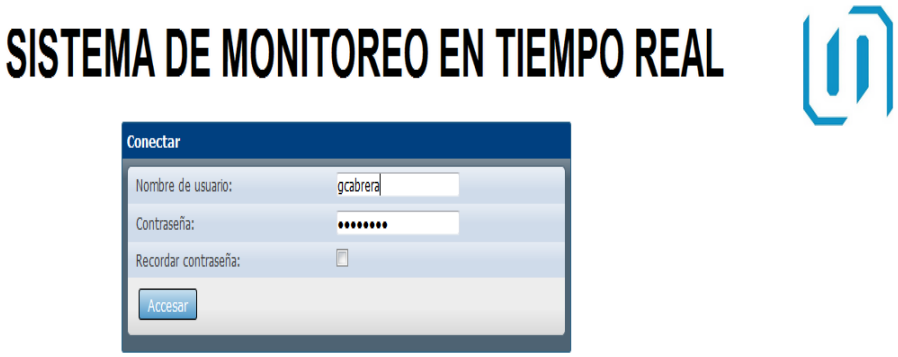


Figura 4.39 Entrando al sistema.

De no existir el usuario, únicamente se limpiarán los campos de Nombre de usuario y contraseña en espera de un usuario valido.

De existir el usuario, se pasará a la pantalla principal, donde se mostrarán, de existir, emergencias activas.

En la Figura 4.40 se ve la pantalla del sistema de monitoreo sin ninguna alerta activa, ni alertas previas.

Figura 4.40 Pantalla principal sin alertas.

En caso de presionarse el botón de emergencia del DVR, por el mecanismo anteriormente descrito, en la pestaña Monitor, el software automáticamente refrescará la pantalla mostrando la emergencia, así como la información necesaria para atenderla [44], la ubicación geográfica y las imágenes que estén grabando las cámaras; una vez atendida la emergencia, a un costado de la información del ID DVR, existe un botón que al presionarlo cambiará la emergencia como inactiva [45], quedando la plataforma lista para atender la siguiente emergencia.

La plataforma cuenta con la opción de mostrar las alertas que previamente han sido atendidas, la información a mostrar es exactamente la misma que en la pestaña Monitor, esta información se puede accesar desde la pestaña Archivo, esto en caso de que se requiera la información para darle un uso alternativo (estadísticas, control, etc.).

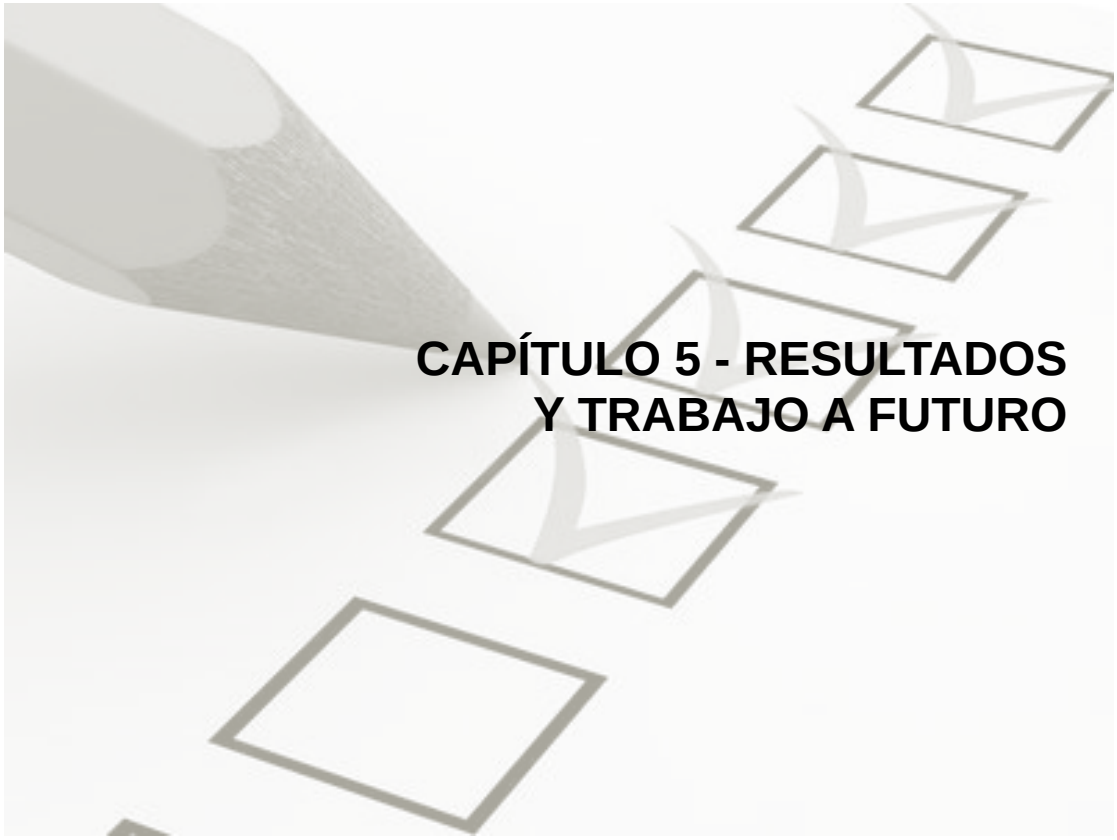
[44] Eliza Witkowska, 2011
[45] Brian21, 2007

En la Figura 4.41 se muestra la pantalla de una emergencia activa, con los respectivos datos para atenderla.

Figura 4.41 Pantalla principal del software con una alerta.

En la Figura 4.42 se muestra la pantalla de alerta desplegada, así como su ubicación geográfica y las imágenes que están grabando las cámaras.

Figura 4.42 Alerta desplegada, con mapa e imágenes.



CAPÍTULO 5 - RESULTADOS Y TRABAJO A FUTURO

5.1 Resultados

El sistema como tal se operó brevemente para varias demostraciones a funcionarios de dependencias gubernamentales. De estas ocasiones, se pudieron obtener varios resultados positivos y demostrar la eficacia del nuevo sistema.

A continuación, se relata a detalle las tres pruebas realizadas para demostrar la eficacia del sistema; las pruebas se llevaron a cabo en las oficinas de la Policía Federal, en Costera 125 y en conjunto con personal del Centro de Control, Comando, Comunicaciones y Computo (C4) y personal de una empresa de seguridad privada.

las pruebas, se realizó el montaje de los sistemas del Botón de Pánico Actual, el DVR y cámaras para el sistema de monitoreo local, personal de la policía local y de seguridad privada, en una oficina de la policía local, donde personal de la Policía Federal fingió un incidente en las afueras del edificio y cada sistema debía reportar las alarmas.

Resultado prueba A: Sistema de Monitoreo en Tiempo Real comparado con Sistema de Botón de Pánico actual.

Prueba A	Botón de Pánico	Monitor en Tiempo Real
Tiempo de espera tras generar la alerta.	20 seg.	3 seg.
Tiempo para identificación y envió de unidades tras recibir alerta.	315 seg.	30 seg.
Tiempo total entre generar la alerta y envió de unidades	335 seg.	33 seg.
Ganador		

En la prueba tipo A, el sistema se comparó funcionando con el sistema de Botón de Pánico actual; tras pulsar al mismo tiempo ambos botones de pánico, el Monitor en Tiempo Real generó la alerta en 3 segundos, desplegando un mapa con la ubicación de donde esta se generó, datos de contacto y una pantalla con visión de las cámaras instaladas para el monitoreo en tiempo real del lugar e identificando el caso de auxilio en 30 segundos; su competidor, el Sistema de Botón de Pánico género la alerta en 20 segundos, mostrando en pantalla un código hexadecimal, para cotejarlo manualmente con una base de datos donde se encuentra la información del lugar de donde se generó la alarma e identificando el tipo de incidente en más de 5 minutos, ya que es necesario hablar al lugar de donde se generó la alerta para preguntar qué tipo de auxilio requiere.

Resultado prueba B: Sistema de Monitoreo en Tiempo Real comparado con Llamada Telefónica al 066.

Prueba B

	Llamada a 066	Monitor en Tiempo Real
Tiempo de espera tras generar la alerta.	45 seg.	3 seg.
Tiempo para identificación y envió de unidades tras recibir alerta.	170 seg.	30 seg.
Tiempo total entre generar la alerta y envió de unidades	215 seg.	33 seg.
Ganador		

En la prueba tipo B, su competidor fue el sistema actual de llamada telefónica al 066, para solicitar auxilio; una persona ajena a la policía y la seguridad privada llama al número de emergencias local y al mismo tiempo se presiona el botón de pánico del Sistema de Monitoreo en Tiempo Real; se demoró la operadora en contestar la llamada 45 segundos, tomando 2 minutos y 50 segundos en recopilar la información de donde se requiere la asistencia de las autoridades; a diferencia del Monitor en Tiempo Real, que le llevo solo 30 segundos, como en la prueba tipo A.

Resultado prueba C: Sistema de Monitoreo en Tiempo Real comparado con Agencia de Seguridad Privada.

	Prueba C	
	Seguridad Privada	**Monitor en Tiempo Real**
Tiempo de espera tras generar la alerta.	10 seg.	3 seg.
Tiempo para identificación y envió de unidades tras recibir alerta.	40 seg.	30 seg.
Tiempo total entre generar la alerta y envió de unidades	50 seg.	33 seg.
Ganador		

En la prueba tipo C, su contrincante fue la eficacia humana, a cargo de una agencia de seguridad privada; se simuló nuevamente un incidente en la parte exterior del edificio, con un proceso de verificación de alarma por parte del personal de seguridad privada y después llamar al personal de su empresa localizada en la oficina ubicada en Costera 125 para que despliegue un equipo de auxilio, en este caso la verificación demoró unos 10 segundos y la llamada vía radio a sus oficinas demoró unos 40 segundos, tras estos, el personal de la empresa ya tenía los datos de incidente y el lugar del mismo, en comparación, el personal a cargo del Sistema de Monitoreo en Tiempo Real solo presionó el Botón de Pánico, no tuvo que salir del edificio; se constató que el manejo de

códigos y claves por parte del personal de la seguridad privada para reportar el incidente agiliza la captura de información y el entendimiento entre el despachador y el personal que reporta la alerta. Pero, pese a la diferencia de tiempo entre la prueba tipo B y la C, el Monitor en Tiempo Real, sigue teniendo un mejor tiempo de respuesta de 33 segundos.

De estas pruebas se pudo constatar la amplia ventaja en respuesta que tiene nuestro sistema sobre sus competidores, está claro que los sistemas en los que se depende de un operador para la captura y obtención de datos existe una amplio margen de retraso, el cual disminuye al hacerlo automatizado, se elimina el error humano y se agiliza el tiempo de respuesta.

Otra de las ventajas que tiene el sistema, es que es prácticamente compatible con cualquier tipo de cámara análoga existente en el mercado y con casi todos los sistemas DVR actuales.

5.2 Trabajo a Futuro

Dentro de las aplicaciones futuras y módulos que se le pueden adjuntar al sistema, cabe señalar que es indispensable generar leyes severas que castiguen el uso indebido de estas terminales y los equipos de alarma, ya que de no aplicarse, la cantidad de falsas alarmas generadas degradarían la confiabilidad y el uso del sistema. Ya que al encontrarse al acceso público se puede propiciar que alguien quiera causar alborotos o bromas a los cuerpos de seguridad.

Dicho lo anterior, se podrá desglosar algunas de las aplicaciones a futuro en las siguientes:

5.2.1 Mapeo de vialidades

El mapeo de las vialidades, consiste en un mapa que recopile y muestre información del estado de las vialidades, si se encuentran obstruidas por alguna obra o incidente, para poder así trazar rutas óptimas para mejorar el tiempo de llegada de los cuerpos de seguridad; utilizando información que sería recopilada de las patrullas de seguridad pública que se encuentren circulando en la ciudad y constante comunicación con el Ayuntamiento sobre las obras de mantenimiento o reparaciones que se estén llevando a cabo en las calles. Esta información se vaciaría por medio de un personal de captura que marcaría en el plano base las vialidades obstruidas.

En la Figura 5.1 se muestra una línea vertical color rojo que simboliza que esta calle se encuentra obstruida por obras y también muestra el trazado en color azul de la ruta más óptima para llegar al incidente.

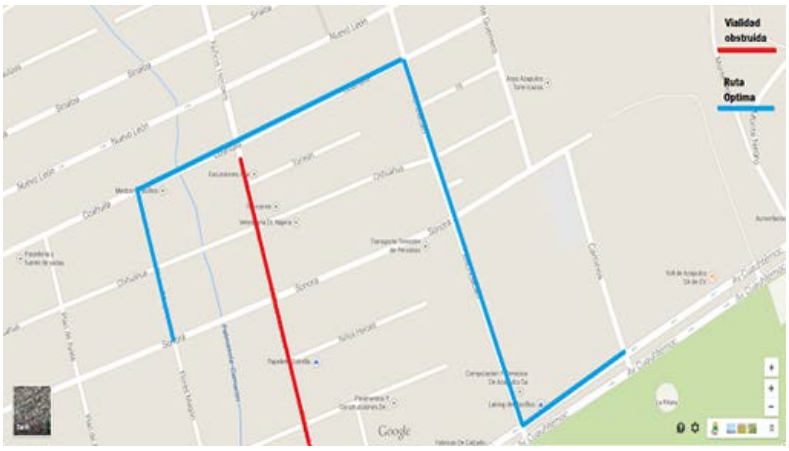


Figura 5.1 Mapa de rutas óptimas.

Todo esto con el fin de poder delimitar que vías se pueden tomar y cuál es la ruta óptima para llegar a un incidente y no llegar a un punto cerrado por la realización de alguna obra.

5.2.2 Botón de pánico en sitios de interés

El botón de pánico en sitios de interés va a ser útil para aumentar la confianza de ciertas zonas en la ciudad, tales como plazas, estacionamientos públicos, o bien, en áreas peatonales concurridas, siempre y cuando se encuentre a la vista y bien señalado, acompañado de una cámara apuntando a la persona que oprima el botón y otra robótica para monitorear su entorno.

De esta manera, al momento de ser activado el botón se tendría una imagen de la persona en cuestión que disparó la alarma, así como una cámara robótica que se podría controlar desde la central de monitoreo

para observar los alrededores y ubicar el incidente. La cámara robótica contaría con movimiento de 360 grados y varias opciones de zoom para poder ver a distancia.

En la Figura 5.2 se muestra un ejemplo de una terminal de botón de pánico para áreas concurridas y sitios de interés, con las cámaras propuestas para monitoreo de entorno y del usuario.

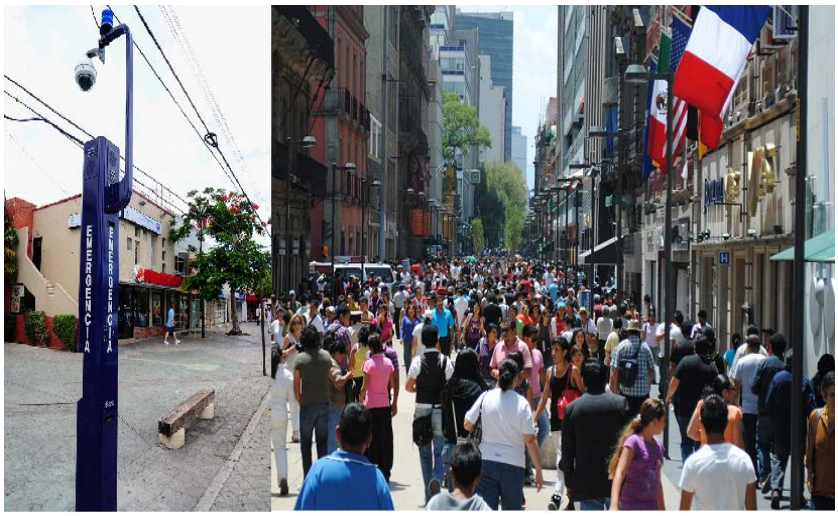


Figura 5.2 Terminales en sitios de interés.

5.2.3 Geo Posicionamiento Satelital.

Geo Posicionamiento Satelital (GPS) en los equipos de alerta, ya que con esto se pueden instalar en múltiples sitios móviles y seguir teniendo la posición exacta del dispositivo en el momento de ser requerido. Esta aplicación se puede separar a su vez en múltiples funcionalidades extra al sistema.

5.2.3.1 GPS en los servicios de transporte público

Es importante colocar equipos de GPS en los servicios de transporte público, ya que es un punto prácticamente olvidado en la actualidad con un alto índice de delitos.

Una instalación de un par de cámaras y botones de pánico dentro de los autobuses, para que en caso de un incidente se activen las cámaras mostrando la situación al interior del vehículo y ubicando el lugar exacto de la llamada de emergencia por medio del GPS, así la central de monitoreo ubicaría el incidente enviando a los cuerpos de seguridad necesarios y en caso de que el vehículo se moviera podrían rastrear la ruta que sigue el transporte.

Como se muestra en la Figura 5.3, los autobuses son un área olvidada en cuestión de seguridad interna, pero con un botón de pánico ligado a cámaras internas, se tendría una mayor seguridad para los usuarios del transporte.

Figura 5.3 Botón de pánico en transporte público.

5.2.3.2 GPS en terminales móviles

Sería de gran utilidad contar con equipos de GPS en terminales móviles montadas en las patrullas de Seguridad Pública. Con esto los cuerpos de seguridad podrían recibir una alarma de un incidente que se encuentre más cercano a su posición actual y así reducir aún más el tiempo de respuesta de los cuerpos de seguridad.

Al presentarse la alerta en un punto, si una patrulla se encuentra a unas cuantas calles del incidente, a esta se le desplegaría la alarma automáticamente; claro de manera paralela a la alerta que se genere en las centrales de monitoreo y podría asistir al incidente en caso de ser necesario, ya que se podría observar por las cámaras si es un asunto de su competencia o área.

La Figura 5.4 muestra un oficial utilizando un sistema de mapas portable, el cual le presenta las alertas al momento en la pantalla, permitiendo una respuesta más eficaz y rápida.

Figura 5.4 Terminales móviles.

5.2.3.3 GPS en botón de pánico portátil

Este dispositivo actualmente es de uso limitado por su poca promoción al público en general, lo cual hace que un pequeño número de personas conozcan de su existencia, pero es de gran funcionalidad y que permite el envió de la alerta y el audio en dos vías, así como de la ubicación del incidente.

Estos dispositivos pueden ser usados en vehículos que lleven algún tipo de carga de interés y después ser removidos, así como en personas que requieran algún tipo de auxilio o cierto tipo de monitoreo, se puede mencionar a manera de ejemplo: Menores de edad, personas de salud

delicada o personas de tercera edad que requieren asistencia. Cabe señalar, que en este tipo de suceso se omitiría la alarma a cuerpos de seguridad móviles cercanos y seria recibida solo por las centrales de monitoreo.

Al generarse un incidente, se presionaría el botón de este dispositivo, generando la alarma en la central, mandando al momento la ubicación GPS y se abren los canales de audio para comunicación dos vías, permitiéndole a la persona en la central de monitoreo escuchar a la persona que activó la alarma y su entorno con un micrófono omnidireccional montado en el equipo y a su vez, dar instrucciones o palabras de calma a la persona que activo el dispositivo, para que enseguida se le pueda enviar la ayuda pertinente.

La Figura 5.5 muestra un botón de radio frecuencia de pulsera, los que hay actualmente para sistemas de alarmas caseros, que bien podría ser sustituido, por uno con tecnología celular y operar con alguna telefónica para enviar la alerta.

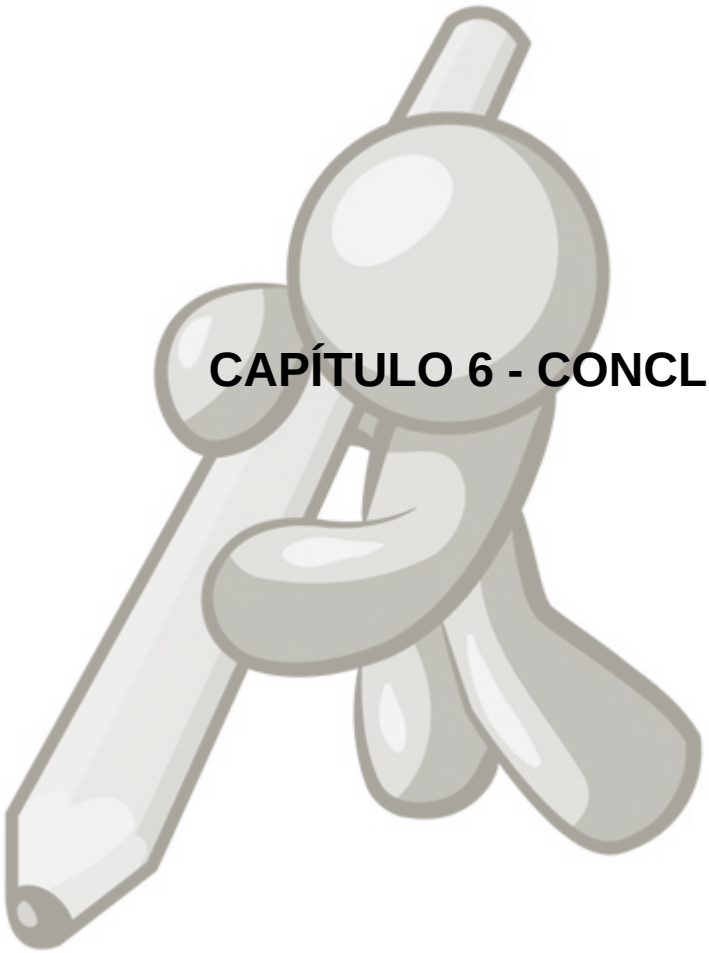
Figura 5.5 Botón de pánico portátil.

5.2.3.4 GPS en aplicación en celulares

Esta opción se le considera de gran utilidad y a la vez accesible, ya que en la actualidad, el uso de los celulares es muy común en la población. Esta portabilidad permitiría el envió de la alerta con una aplicación que ejecute el comando de enviar la alarma tras una combinación de botones de seguridad. Al igual que en el caso del botón de pánico portable se enviarían la ubicación y audio de dos vías.

La Figura 5.6 muestra un demo de la pantalla del desarrollo actual del sistema en celulares, que aún se encuentra en sus fases de prueba.

Figura 5.6 Aplicación para celulares.

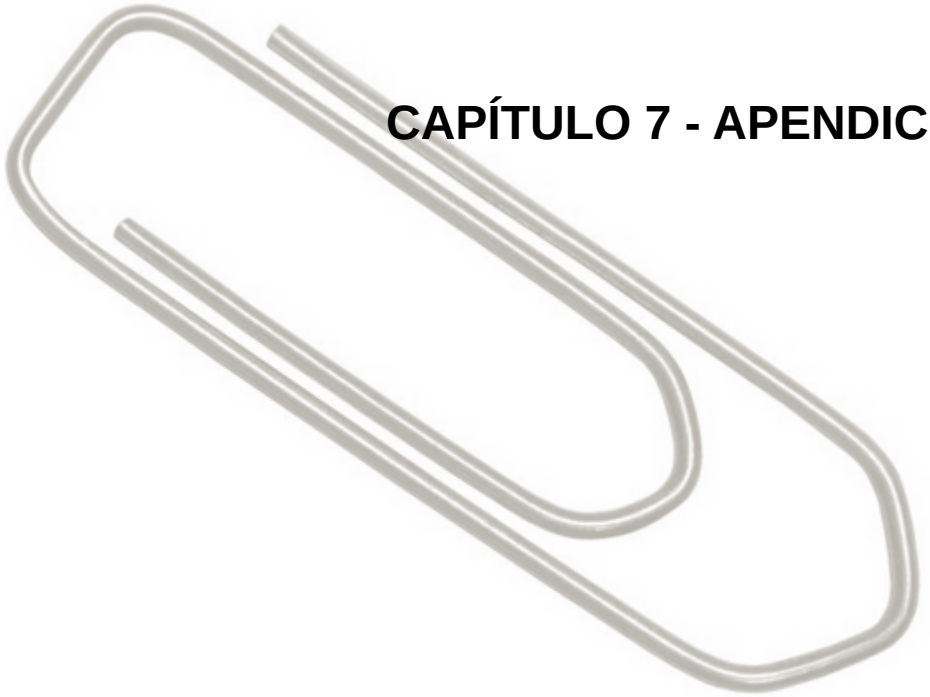


CAPÍTULO 6 - CONCLUSIONES

De la presente investigación se desprende que la implementación del Sistema de Monitoreo en Tiempo Real mejora notablemente los tiempos de respuesta de los cuerpos de Seguridad Pública para la atención de las incidencias en las escuelas, lo que crea un mejor ambiente de seguridad para los estudiantes y por consecuencia, disminuyen los índices de criminalidad que aquejan el sector educativo.

Cabe mencionar que, tomando en cuenta los resultados exitosos de las pruebas, la versatilidad y portabilidad del sistema de monitoreo en tiempo real, permitirá su uso en otros sectores independientes del área educativa, es decir, el sistema podrá implementarse dentro del transporte público, en zonas residenciales, lugares de interés social, o cualquier lugar que necesite monitoreo para la atención a incidencias, proporcionando de esta manera, un ambiente con mayor tranquilidad y seguridad para los ciudadanos, que es lo que se pretende al proponer la implementación de este sistema.

Por lo tanto la hipótesis se valida, ya que se ven claramente reducidos los tiempos de respuesta de los cuerpos de Seguridad Pública, usando el Sistema de Monitoreo en Tiempo Real, los botones de pánico y cámaras de circuito cerrado que se proponen, las cuales, facilitan su llegada al lugar de la emergencia.



CAPÍTULO 7 - APENDICES

7.1 DIAGRAMAS DE USO (UML)

La Figura 7.1 muestra el Diagrama de Uso que sigue el proceso de emergencia visto por el operador en la pestaña Monitor.

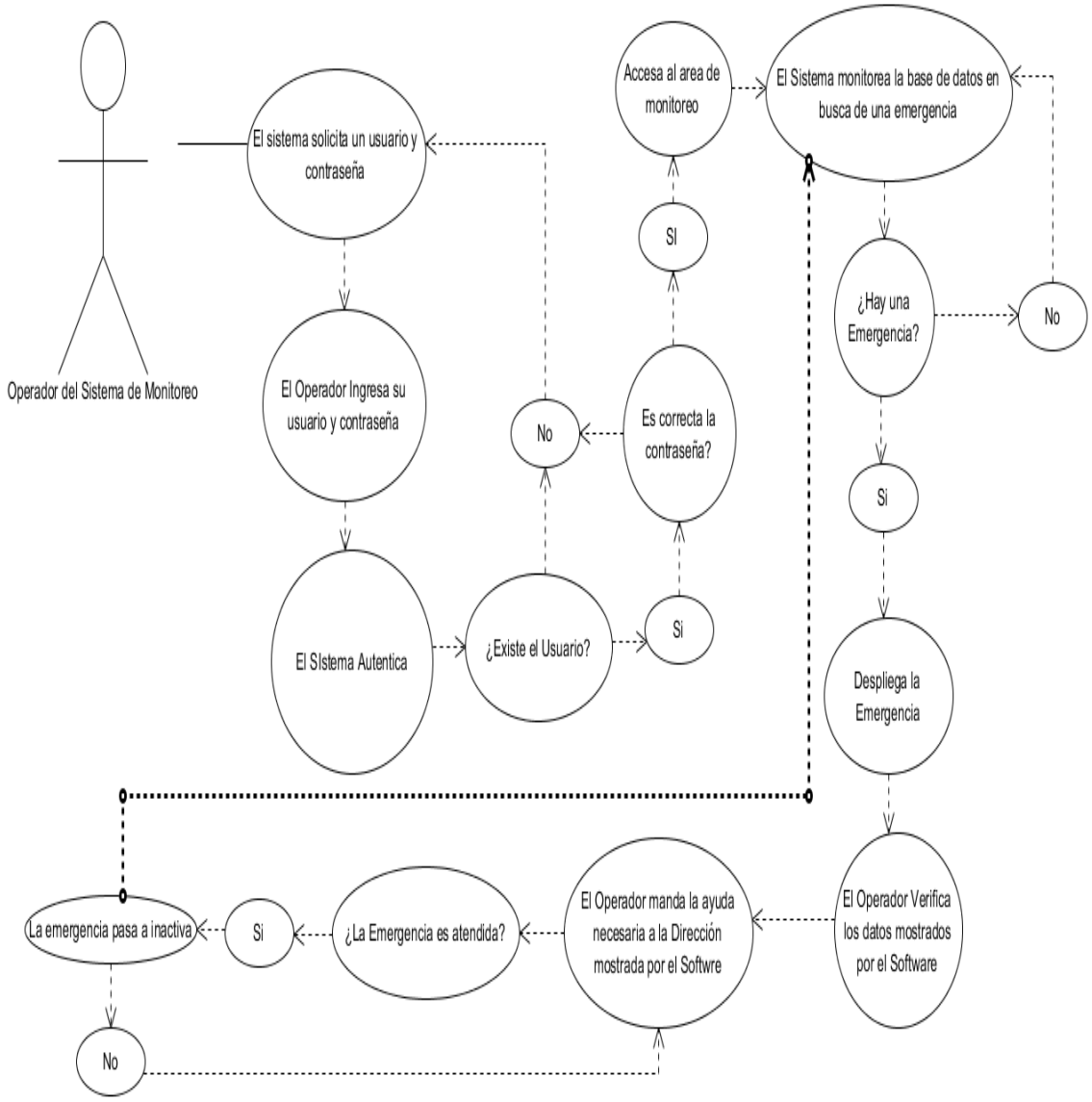


Figura 7.1 Diagrama de Uso (UML) del operador en pestaña Monitor.

La Figura 7.2 muestra el Diagrama de Uso que sigue el proceso de emergencia visto por el Usuario

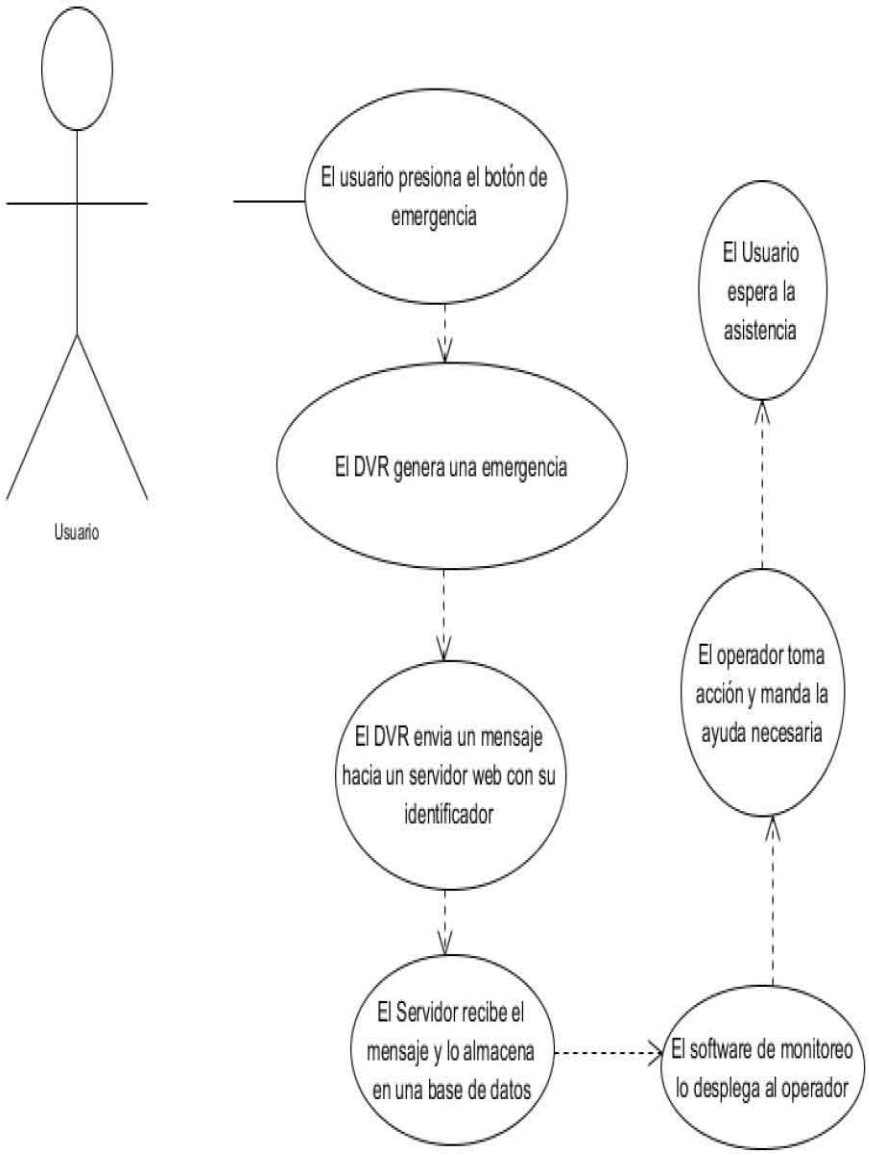


Figura 7.2 Diagrama de Uso (UML) visto por el usuario que reporta la emergencia.

La Figura 7.3 muestra el Diagrama de Uso que sigue el proceso de Obtención de datos para la elaboración de informes y estadísticas visto por el operador en la pestaña Archivo.

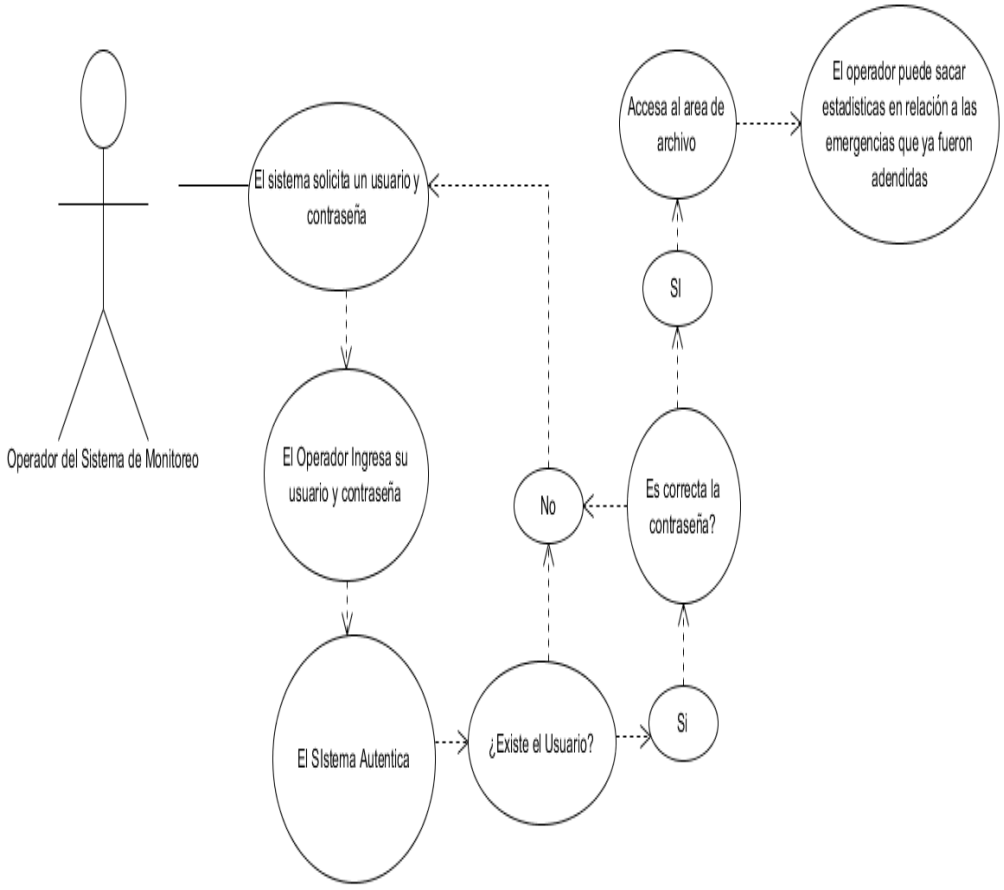
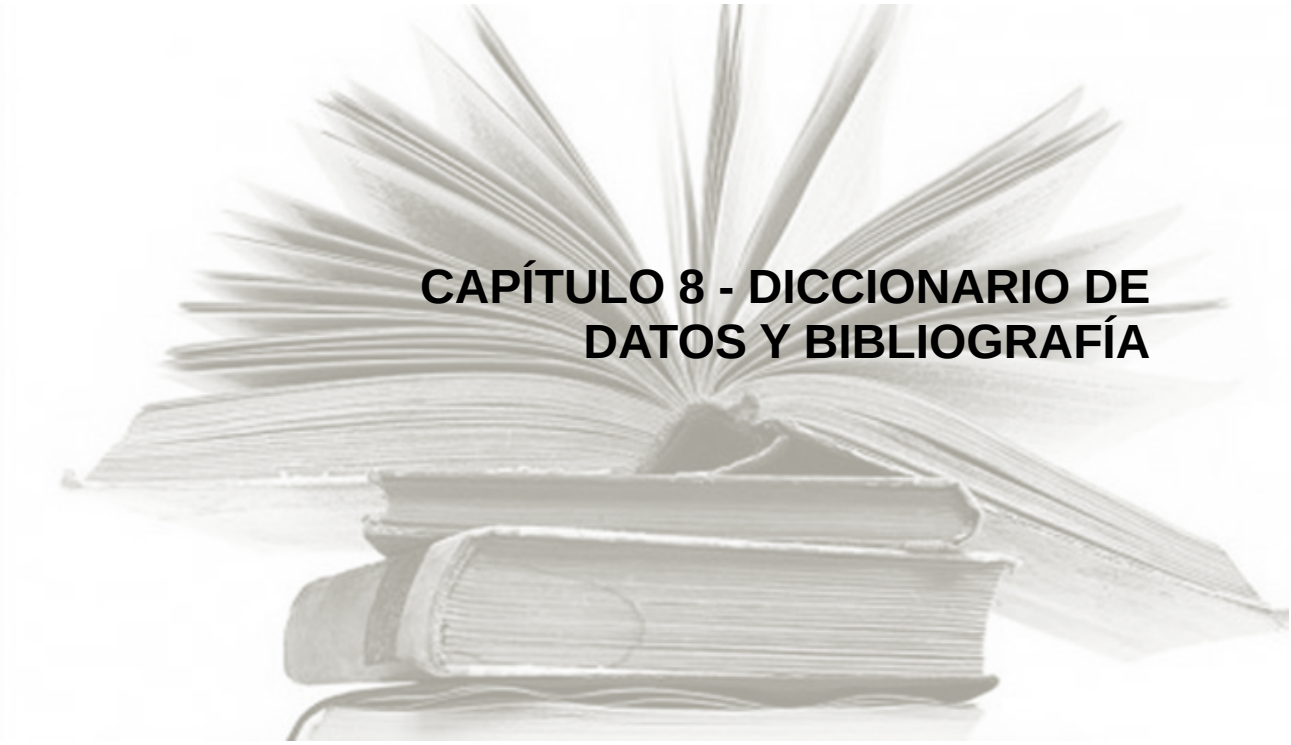


Figura 7.3 Diagrama de Uso (UML) visto por el operador en la pestaña archivo.



CAPÍTULO 8 - DICCIONARIO DE DATOS Y BIBLIOGRAFÍA

8.1 Diccionario de Datos

En el presente apartado se muestra la estructura de la base de datos usada en el proyecto, así como las tablas y su estructura.

Base de Datos: Seguridad

Estructura de la tabla Catálogo

Columna	Comentarios
Id	Id
nombre_dependencia	Nombre de la Dependencia
direccion_dependencia	Dirección de la Dependencia
tel_dependencia	Teléfono de la Dependencia
email_contacto	Email del contacto
nombre_contacto	Nombre del contacto
url_dvr	Dirección web del DVR
coord_dvr	Ubicación GPS del DVR
Dvr	No. Del DRV

Estructura de la tabla Dependencia

Columna	Comentarios
Id	Id
tipo_dependencia	Tipo de la Dependencia (escuela, hospital, condominios, etc.)
clase_dependencia	Clase Dependencia (privada, pública, primaria, secundaria, etc.)

Estructura de la tabla Emergencia

	Comentarios
Id	Id
Dvr	No. Del DRV
tipo_dependencia	Tipo de la Dependencia (escuela, hospital, condominios, etc.)
Status	Active o inactive
fecha_insercion	Fecha de Ingreso de Emergencia
fecha_supervisado	Fecha de atención

Estructura de la tabla Opción

Columna	Comentarios
Id	Id
significado	Activa = 1 e Inactiva = 0

Estructura de la tabla Usuarios

Columna	Comentarios
Id	Id del Usuario
Usuario	Quick Login del Usuario
password	Contraseña

8.2 Referencias

Adriana Covarrubias. 2011. Instalan botones de pánico en escuelas en Guerrero. 2012, de El Universal México. Sitio web: http://archivo.eluniversal.com.mx/estados/82007.html

Apache Software Foundation. 1998. Apache HTTP SERVER PROJECT. 2013, de httpd.apache. web: https://httpd.apache.org/ org Sitio

APR. 2010. Qué es un servidor y cuáles son los principales tipos de Servidores. 2013, de aprenderaprogamar.com. Sitio web: http://aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftppop3-y-smtp-dhcp&catid=57:herramientas-informaticas&Itemid=179

Brian21. 2007. Refresh page after Inline Edit. 2013, de ASP Runner Sitio web: http://www.asprunner.com/forums/topic/20275-refresh-page-after-inline-edit/

Brittani Sponaugle. 2013. Best Linux OS: A Comparison of Twenty Popular Linux Distributions. 2014, de udemy blog. Sitio web: https://blog.udemy.com/best-linux-os/

courier-mta.org. 1998. Courier Mail Server. 2012, de courier-mta.org Sitio Web: http://www.courier-mta.org/

C.S. 2013. Retrieve Linux local mailbox with command lines non-interactively. 2013, de CS Notes Sitio web: http://notes-cs.blogspot.mx/2013/04/use-command-line-to-read-linux-local.html

debían.org. 2001. ¿Qué es Bind9?. 2012, de wiki.debian.org Sitio Web: https://wiki.debian.org/Bind9

Diario Oficial de la Federación 2009. Ley general del Sistema Nacional de Seguridad Pública. Sitio Web http://dof.gob.mx/nota_detalle.php?codigo=5076728&fecha=02/01/2009

Diccionario de la lengua española. 2005, 2014, de Wordreference Sitio web: http://www.wordreference.com/definicion/hardware

Diccionario de la lengua española. 2005. 2014, de Wordreference Sitio web: http://www.wordreference.com/definicion/software

Dointech. 2010. Video Vigilancia IP: Sistemas de Seguridad con Cámaras IP. 2013, Sitio web: http://www.dointech.com.co/video-vigilancia-ip.html

Elías Hidalgo. 2012. Crea tu propio servidor de correo en GNU/Linux. 2014, de Linux Zone España Sitio web: http://linuxzone.es/2012/02/20/crea-tu-propio-servidor-de-correo-en-gnulinux/

Eliza Witkowska. 2011. Auto refresh content after changes in database - AJAX. 2013, de Blog Code Busters Sitio web: http://blog.codebusters.pl/en/auto-refresh-content-after-changes-in-database-ajax

Gerardo Cabrera Hernández. 2011. Variables between bash and php-cli. 2012, de Stackoverflow Sitio web: http://stackoverflow.com/questions/5940639/variables-between-bash-and-php-cli

GNU Operating System. 2007. GNU Bash. 2012, de gnu.org Sitio web: http://www.gnu.org/software/bash/

HOSPEDAJE-WEB, 2010. ¿Cómo funciona el Sistema DNS (Domain Name Server)?. 2012, de hospedaje-web.com Sitio web: http://hospedaje-web.com

howtoforge.com, 2012. Installing Apache2 With PHP5 and MySQL Support On Ubuntu 12.01 LTA (LAMP). 2012, de howtoforge.com Sitio web: https://www.howtoforge.com/installing-apache2-with-php5-and-mysql-support-on-ubuntu-12.04-lts-lamp

Instituto Nacional de Estadística y Geografía. 2011. Panorama socio demográfico de Guerrero. 2014. Sitio web: http://www.inegi.org.mx/prod_serv/contenidos/espanol/bvinegi/productos/censos/poblacion/2010/panora_socio/gro/Panorama_Gro.pdf

Imágenes extraídas de www.nosolounix.com

Hikvision. 2012. Specifications and Key features of DS-7204/7208/7216HVI-ST/SN. 2013. Sitio web: http://www.hikvision.com/UploadFile/image/20120614142113650 30.pdf

Leidy Reyes R., María del Carmen Ruiz, Mónica Vivanco E. 2009. Prototipo Informáticos. 2014, de Universidad Nacional de Loja, Ecuador. Sitio web: https://sistemas2009unl.wordpress.com/prototipos-informaticos/

Maria DB. 2010. ¿Qué es Maria DB 5.1?, 2012, de mariadb.com Sitio web: https://mariadb.com/kb/es/what-is-mariadb-51/

MidiSec. 2010. Introducción a los Sistemas de Vigilancia IP. 2014, Sitio web: http://www.midisec.com/index.php?option=com_content&view=article&id=64:introduccion-a-sistemas-vigilancia-ip&catid=42:introduccion-a-las-tecnologias&Itemid=67

PHP: Hypertext Preprocessor. 2001. ¿Qué es PHP?. 2012, de php.net Sitio web: http://php.net/manual/es/intro-whatis.php

postfix.org, 1998. The Postfix Home Page. 2012, de postfix.org Sitio Web: http://www.postfix.org/

Programa de las Naciones Unidas para el Desarrollo, PNUD-Cuba. 2003. Debate acerca del papel de la ciencia y la tecnología en el desarrollo humano. 2014, de Centro de Documentación sobre Desarrollo Humano Sitio web: http://www.centrodesarrollohumano.org/pmb/opac_css/doc_num.php?explnum_id=924

RAHUL. 2012. How to Install MariaDB 5.5 in Ubuntu 12.04 LTS. 2012, de tecadmin.net Sitio web: http://tecadmin.net/install-mariadb-5-5-in-ubuntu/#

Secretaría de Educación Guerrero. 2011. Escuelas Particulares Incorporadas Departamento de Incorporación y Revalidación. 2012, de Secretaría de Educación Guerrero. Sitio web: http://i.guerrero.gob.mx/uploads/2011/12/Instituciones-Particulares-Incorporadas-a-la-SEG-fraccion-XVI.pdf

Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. 2012. Estadísticas de Seguridad Pública de Estado de Guerrero, Mpio. de Acapulco de Juárez. 2014. Sitio web: www.secretariadoejecutivo.gob.mx

squirrelmail.org, 1999. SquirrelMail – WEBMAIL FOR NUTS. 2012, de squirrelmail.org Sitio Web: http://squirrelmail.org/

Tuxradar. 2011. The best linux distro of 2011. 2014. Sitio web: http://www.tuxradar.com/content/best-distro-2011

Ubuntu flavours, 2012. Ubuntu flavours. 2013. Sitio web: http://www.ubuntu.com/download/ubuntu-flavours

Ubuntu Server, 2012. Scale out with Ubuntu Server. 2012. Sitio web: http://www.ubuntu.com/server

Wed. 2012. Triggering a PHP script when your Postfix server receives a mail. 2014, de The Coding Machine Sitio web: http://blog.thecodingmachine.com/content/triggering-php-script-when-your-postfix-server-receives-mail