ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE PRUEBA PARA UN SISTEMA DE SEGURIDAD RESIDENCIAL UTILIZANDO TECNOLOGÍA ZIGBEE CON UN INTERFAZ PARA MONITOREO VÍA INTERNET BAJO EL PROTOCOLO HTTPS CON ENVÍO DE ALERTAS AL CORREO ELECTRÓNICO Y SMS

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

ATIENCIA CONGACHA PAÚL DAVID

atieniciapaul@gmail.com

BASTIDAS CHÁVEZ JORGE ANDRÉS

Andres.bastidas8411@gamail.com

DIRECTORA: MSc. SORAYA MAITO SINCHE LUCIA

soraya.sinche@epn.edu.ec

Quito, Diciembre 2014

DECLARACIÓN

Nosotros, Atiencia Congacha Paúl David y Bastidas Chávez Jorge Andrés declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____ _____

Atiencia Congacha Paúl David Bastidas Chávez Jorge Andrés

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Atiencia Congacha Paúl David y Bastidas Chávez Jorge Andrés, bajo mi supervisión.

_____

MSc. SORAYA SINCHE

DIRECTORA DEL PROYECTO

AGRADECIMIENTO

A Dios, por habernos permitido llegar hasta este punto y habernos dado salud para lograr este objetivo, además de su infinita bondad y amor.

A nuestros padres, por habernos apoyado en todo momento, por sus consejos, por sus valores, por la motivación constante, por los ejemplos de perseverancia y constancia que los caracterizan y que nos han infundado siempre, por el valor mostrado para salir adelante que nos ha permitido ser personas de bien, pero más que nada, por su amor incondicional.

A nuestros amigos, que nos apoyamos mutuamente en nuestra formación profesional y que hasta ahora, seguimos siendo amigos “FULL NORTON” y que siempre han estado pendientes de la culminación de este proyecto de titulación brindándonos sus consejos y apoyo.

A nuestros maestros por su gran apoyo y motivación para la culminación de nuestros estudios, por su apoyo ofrecido, por su tiempo compartido y por impulsar el desarrollo de nuestra formación profesional.

A nuestra directora del proyecto de titulación MSc. Soraya Sinche, quien puso todo su conocimiento para que nosotros pudiésemos realizar esta investigación.

DEDICATORIA

El presente proyecto de titulación está dedicado a mi padre, a mi madrecita la mejor mujer del mundo, mis hermanos quienes estuvieron a mi lado en las buenas y malas, brindándome su apoyo incondicional.

Paul David Atiencia Congacha

Dedico este proyecto de titulación a Dios ya que permitió que mi familia siga completa y por la oportunidad de continuar aprendiendo de la vida junto a las personas que más quiero.

A mis padres y hermano por su apoyo y confianza en todo lo necesario para cumplir con mis objetivos como persona y estudiante.

Al resto de mi familia y amigos que de alguna u otra manera han sabido brindar de concejos y su sabiduría para la culminación de este proyecto.

Jorge Andrés Bastidas Chávez

CONTENIDO

ÍNDICE DE FIGURAS

CAPÍTULO 1: ÍNDICES DE INSEGURIDAD CIUDADANA Y TECNOLOGÍA APLICADA

CAPÍTULO 2: REQUERIMIENTOS Y DISEÑO DE LA SOLUCIÓN

ÍNDICE DE TABLAS

CAPÍTULO 1: ÍNDICES DE INSEGURIDAD CIUDADANA Y TECNOLOGÍA APLICADA

CAPÍTULO 2: REQUERIMIENTOS Y DISEÑO DE LA SOLUCIÓN

CAPÍTULO 3: IMPLEMENTACIÓN, PRUEBAS, VERIFICACIÓN DEL PROTOTIPO Y COSTOS

RESUMEN

El documento presenta una solución al problema de seguridad en los hogares, con la incorporación de equipos inalámbricos y vigilancia a través de la Web, donde en cada capítulo se desglosa la problemática y la manera en que se lo va a solventar.

En el capítulo 1 se presentan los índices de inseguridad en el Ecuador, de las viviendas que fueron víctimas de incidentes de robo. Además se hace una descripción de la tecnología ZigBee, así como, las topologías con las que puede trabajar, tipos de tráfico, servicios de seguridad que puede ofrecer, los posibles usos que se le puede dar y una comparación con respecto a otras tecnologías.

En el capítulo 2 se describe el desarrollo del aplicativo web de gestión del domicilio, encargado del control del sistema de seguridad domiciliario, junto a la configuración de los servidores necesarios para su funcionamiento.

El capítulo 3 trata sobre la implementación del prototipo de prueba, y se presentan los resultados de las pruebas, que incluye: el funcionamiento del mismo, cobertura e interferencia en la red de sensores, lectura y escritura en la base de datos, funcionamiento de la interfaz gráfica, notificación de alarmas por Mail y SMS. Adicionalmente se muestra el costo de implementación del prototipo de prueba, como también el costo referencial de la implementación en un domicilio tipo.

En el capítulo 4 se presenta información de los procedimientos de gestión que se establecen en ITIL, desarrollando cada uno de ellos y la relación que tiene con el sistema domiciliario.

En el capítulo 5 se expresan las conclusiones y recomendaciones obtenidas en la elaboración del presente proyecto de titulación.

PRESENTACIÓN

La creciente inseguridad por el incremento del crimen organizado ha llevado al desarrollo de formas de mantener la integridad física y psicológica de la ciudadanía, por este motivo se llegó a la elaboración de un sistema que permita incrementar el nivel de seguridad de los domicilios ante posibles robos.

Incorporar, en estos sistemas de seguridad, las diferentes tecnologías para un uso en beneficio de los usuarios finales, conlleva a un conocimiento de los protocolos de comunicación de las diferentes tecnologías existentes, así como, la manera de adecuar estos protocolos para la unificación de varias tecnologías en un solo conjunto.

Con la convergencia de servicios y la incursión del Internet en todas las áreas de tecnología, llevan al desarrollo de aplicaciones, como la que se presenta a continuación, que permite interactuar los usuarios e Internet, para el control y resguardo del hogar necesitado.

Por la importancia de ITIL, se hace necesario conocer los modelos de gestión propuestos para la prestación de servicios, y brindar al usuario alto nivel de calidad de servicio y soporte técnico óptimo.

El sistema desarrollado es una contribución en el campo de la seguridad familiar ante posibles robos o efectos dañinos a la salud de las personas, sin representar una inversión costosa; y de fácil implementación.

Adicionalmente, la interfaz de usuario tiene el propósito de ser amigable, con el fin de presentarle al usuario un ambiente cómodo para el control y monitoreo de su domicilio.

CAPÍTULO 1

ÍNDICES DE INSEGURIDAD CIUDADANA Y TECNOLOGÍA APLICADA

1.1 INTRODUCCIÓN

Sin duda las preocupaciones que genera la situación de inseguridad y violencia que se vive en el país no sólo inundan las conversaciones cotidianas, sino también se ha convertido en tema de discusión en fórums académicos y políticos. Una sección de este documento muestra una revisión de las investigaciones que se han realizado en el Ecuador sobre el tema de inseguridad residencial, enfocándose en ofrecer información sobre los diferentes casos en los que estos crímenes son perpetrados. También permitirá reconocer tendencias que conlleven a comprender el entorno de inseguridad en los hogares y generar soluciones que la enfrenten de forma efectiva.

En este esfuerzo, de buscar soluciones para la inseguridad domiciliaria, se enmarca la realización del presente proyecto de titulación con el fin de contribuir en el campo de la seguridad familiar, implementando un sistema de seguridad con características de estabilidad y robustez que impidan que el mismo pueda convertirse en un objeto de ataque, sin que esto implique una inversión muy costosa y difícil de realizar, al contrario, presentar una solución práctica, eficaz, que brinde control, y que no requiera de un gasto excesivo para el usuario final.

1.2 ÍNDICES DE INSEGURIDAD

En el país se han desarrollado una serie de diagnósticos de seguridad ciudadana[1] que permiten valorar la magnitud del problema de inseguridad, enfatizando en causas como: clase social, nivel cultural y del lugar del fenómeno.

[1] La seguridad ciudadana es referida como la garantía que deben tener todos los habitantes de las ciudades y del campo para que sus vidas y su integridad física, psicológica y sexual sean respetadas y protegidas, sin temores, a que sus objetos y pertenencias no les sean arrebatados, a no ser intimidados y a confiar en los demás seres humanos. (Concha Eastman)

La “Encuesta a Nivel Nacional de Percepción y Victimización de Inseguridad”, realizada como parte del Plan Nacional de Seguridad Ciudadana del Ecuador, así como estudios elaborados por el Observatorio Metropolitano de Seguridad Ciudadana del Municipio del Distrito Metropolitano de Quito (OMSC), y la empresa CIMACYT dedicada a la elaboración de estudios estadísticos revelan información significativa en base a los niveles de victimización e inseguridad en el país, esto permitirá aportar en el diseño de políticas públicas y privadas.

Los principales hallazgos de estas organizaciones permiten realizar un análisis de las necesidades de seguridad que puede tener un hogar, donde se da a conocer información estadística que permita avanzar en el diagnóstico de la problemática, para así identificar los niveles de victimización que ocurren en un determinado lugar por tipos de delitos, también reconocer la cifra negra o la cantidad de delitos que no son denunciados por las víctimas, y dar bases numéricas a la sensación de inseguridad o temor en la población.

1.2.1 ESTADÍSTICAS DE VICTIMIZACIÓN A HOGARES [1]

Una de las formas más comunes de agresión delincuencial es el robo a viviendas, por lo tanto, en la investigación se pregunta sobre robo o intento de robo a los hogares obteniendo los datos presentados en la Tabla 1.1 de estadística de robo.

ESTADÍSTICA DE ROBO A VIVIENDAS		
RESPUESTA	NÚMERO DE PERSONAS ENCUESTADAS	PORCENTAJE
SI	**289.243**	**14.60 %**
NO	**1’685.536**	**85.08 %**
NO SABE	**6.340**	**0.32 %**
TOTAL	**1’981.119**	**100 %**

Tabla 1.1: Estadísticas de robo a viviendas a Diciembre 2012 [1]

En donde se puede observar que el 14,6% de las viviendas en el país han sido víctimas de robo.

De igual manera se puede hacer una relación con los operativos realizados por la Policía Nacional en el mismo período. Figura 1.2

NACIONAL					
PERIODO	**2009**	**2010**	**2011**	**2012**	**2013**
ENERO	19.371	49.038	116.781	115.080	116.140
FEBRERO	20.181	78.805	148.983	152.987	154.890
MARZO	24.457	94.596	158.962	158.636	157.756
ABRIL	26.631	105.832	157.090	163.098	198.578
MAYO	26.121	125.213	167.804	168.334	167.934
JUNIO	27.601	118.560	159.374	159.093	160.815
JULIO	31.825	119.681	158.368	155.990	157.927
AGOSTO	39.366	126.681	186.774	189.728	192.889
SEPTIEMBRE	28.338	121.879	165.903	164.090	167.462
OCTUBRE	29.588	125.750	173.540	177.293	198.638
NOVIEMBRE	27.803	109.856	165.994	168.376	175.937
DICIEMBRE	30.114	117.976	187.039	190.152	198.637
TOTAL	**331.396**	**1’ 293.867**	**1’946.612**	**1’962.857**	**2.047.603**
INCREMENTO		**74,38%**	**33,53%**	**0,82%**	**4,32%**

Tabla 1.2: Estadísticas de operativos realizados por la Policía a nivel Nacional [1]

Los operativos realizados por la Policía Nacional en cada uno de los meses muestra una tendencia a incrementar, lo que significa un aumento del 74,38% en el año 2010 respecto al año 2009 mientras que entre los años 2010 y 2011 el número de operativos crece en un 33,53%, para el 2012 y 2013 se observa una estabilización del número de operativos comparados con el 2011. Otro aspecto a ser tomado en cuenta es la incidencia de robos a viviendas por día de la semana.

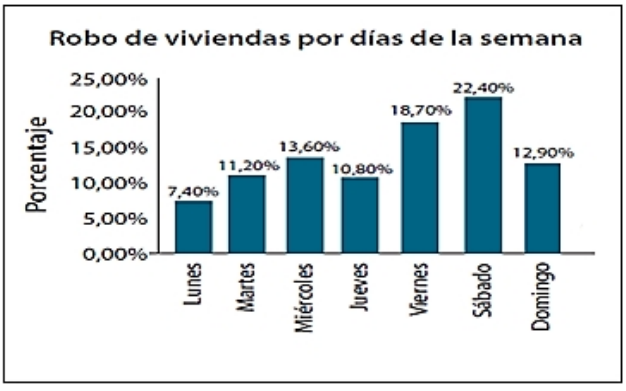


Figura 1.1: Robo a viviendas por día de semana a Diciembre 2013 [1]

El robo a las viviendas se ejecuta preferentemente mientras las casas están solas; por ello, los dos días de la semana de mayor ocurrencia del delito son viernes y sábado con porcentajes de 18,7% y 22,4%, respectivamente.

Todos los días en las dependencias de la Policía Judicial se receptan denuncias sobre robos a viviendas, cabinas telefónicas, tiendas y otros negocios, pero el nivel de denuncia de estos delitos no muestra el verdadero número de incidentes ocurridos en todo el país. La Figura 1.2 muestra la estimación de denuncia por el delito de robo a viviendas.

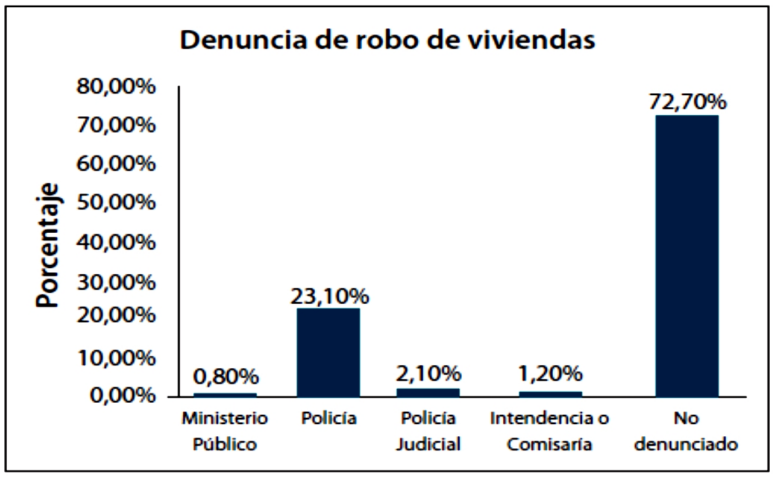


Figura 1.2: Nivel de denuncia por robo a viviendas a Diciembre 2012 y 2013 [1]

La denuncia de robo a viviendas es baja, pues se realiza apenas en la tercera parte de los casos según la Unidad de Ejecución Especializada de la Policía Nacional.

Uno de los factores que inciden en la falta de denuncias es la metodología que emplean los criminales para cometer los delitos, es decir, los integrantes de las bandas utilizan guantes para no ser implicados en la escena del delito. En las investigaciones también se ha determinado que quienes se dedican a esa actividad delictiva se han tecnificado, es decir, operan con equipos sofisticados de comunicaciones y vehículos rápidos de alto cilindraje.

A continuación en la Figura 1.3 se muestra un cuadro comparativo del nivel de denuncia del delito de robo a hogares donde se puede apreciar que las provincias con mayor índice de este problema son Guayas, Pichincha, Manabí y Azuay.

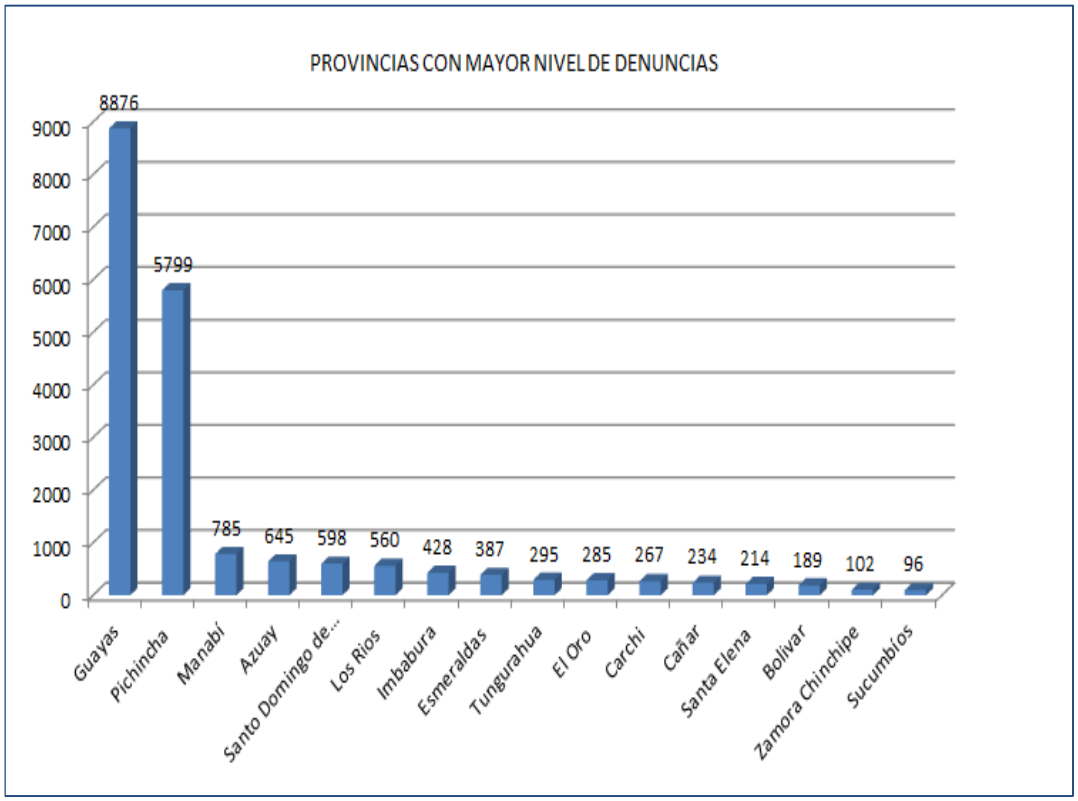


Figura 1.3: Denuncias a nivel provincial a Diciembre 2012 y 2013 [1]

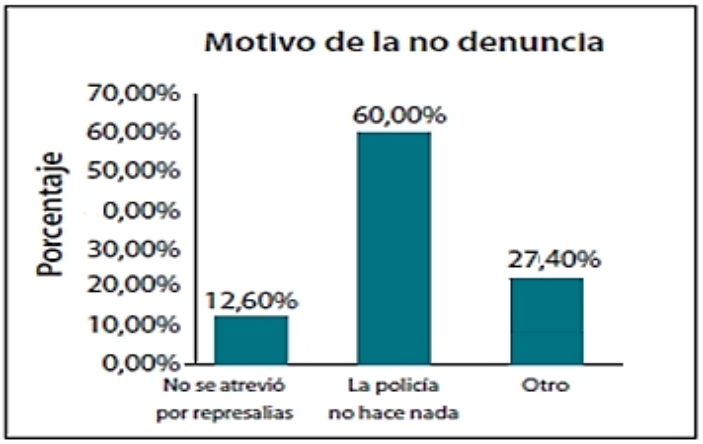


Figura 1.4: Distribución del motivo de la no denuncia a Diciembre 2012 y 2013 [1]

Como consta en la Figura 1.4, más de las dos terceras partes de las personas afectadas no denuncian por la percepción de que “la Policía no hace nada” con respecto a los robos ocurridos, también existe un 12,6% de personas que no denuncian por temor a represalias; mientras que un 27.4% no lo hace por otros motivos como desconocimiento o tiempo disponible para realizar la denuncia.

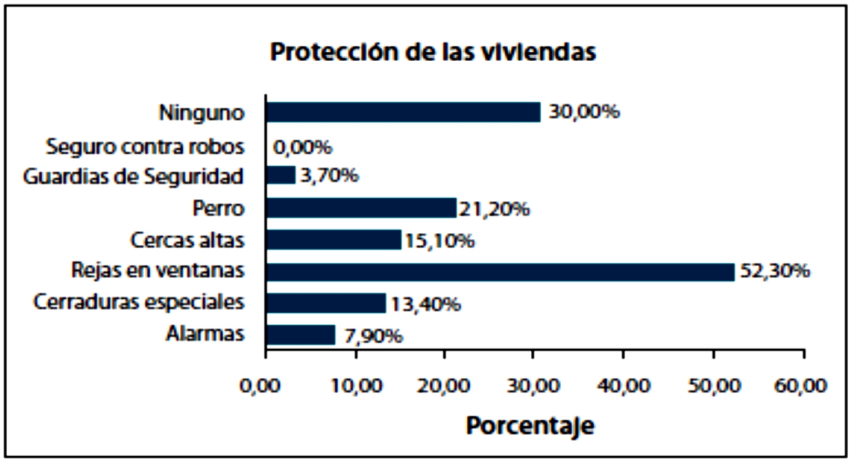


Figura 1.5: Distribución de protección a viviendas a Diciembre 2012 y 2013 [1]

La población opta por medidas de seguridad propias, unas de protección de los hogares (rejas en ventanas, perros, etc.) y otras de prevención organizacional, buscando con la organización barrial incrementar la seguridad.

NIVEL DE INSTRUCCIÓN DEL JEFE	ÍNDICE DE VICTIMIZACIÓN A HOGARES	
	NO	SI
NINGUNO	93,70%	6,30%
PRIMARIA	86%	14,00%
SECUNDARIA	83,80%	16,20%
SUPERIOR	79,30%	20,70%
OTROS	99,50%	0,50%

Tabla 1.3: Índice victimización a hogares por nivel de instrucción a Diciembre 2012 [1]

De la Tabla 1.3, el mayor índice de victimización según el nivel de instrucción del jefe o jefa de hogar corresponde a quienes tienen educación superior, y se muestra ascendente según el mayor nivel de instrucción; es decir, a mayor instrucción mayor victimización.

La Tabla 1.4 presenta una comparativa entre los años: 2010, 2011 y 2012, de denuncias correspondientes a delitos contra la propiedad en las provincias de mayor incidencia.

ROBO A DOMICILIO NACIONAL					
MES	2011	2012	2013	VARIACIÓN 11/12 RELATIVA %	VARIACIÓN 12/13 RELATIVA %
Diciembre	1078	1145	1322	5,85	15,45

Tabla 1.4: Comparativa de denuncias de robo a domicilios [1]

Las denuncias por robo a domicilios en Diciembre 2013 tuvieron un incremento del 15,45% en comparación al mismo mes del año 2012, lo que representa un aumento de 177 denuncias.

ROBO A DOMICILIO PROVINCIAL					
MES	2010	2011	2012	VARIACIÓN 10/11 RELATIVA %	VARIACIÓN 11/12 RELATIVA %
ROBO A DOMICILIO AZUAY					
Últimos 4 meses	**141,00**	**171,00**	**168,00**	**21,28**	**-1,79**
ROBO A DOMICILIO CHIMBORAZO					
Últimos 4 meses	**115,00**	**124,00**	**170,00**	**7,83**	**27,06**
ROBO A DOMICILIO ESMERALDAS					
Últimos 4 meses	**131,00**	**151,00**	**161,00**	**15,27**	**6,21**
ROBO A DOMICILIO GUAYAS					
Últimos 4 meses	**1089,00**	**1080,00**	**1104,00**	**-0,83**	**2,17**
ROBO A DOMICILIO LOS RÍOS					
Últimos 4 meses	**129,00**	**141,00**	**157,00**	**9,30**	**10,19**
ROBO A DOMICILIO MANABÍ					
Últimos 4 meses	**249,00**	**246,00**	**292,00**	**-1,20**	**15,75**
ROBO A DOMICILIO PICHINCHA					
Últimos 4 meses	**924**	**912**	**1008**	**-0,48**	**9,52**

Tabla 1.5: Comparativa de robo a domicilio Provincial [2]

Como se observar en la Tabla 1.5 para las provincias con mayor incidencia de robo a nivel nacional existe normalmente un incremento del delito hasta llegar al 21,28% en la provincia del Azuay en el año 2011, mientras que para el año 2012 el incremento más pronunciado lo muestra la provincia de Chimborazo con un 27,06%.

De la Tabla 1.5 se puede observar en algunas provincias una disminución del robo a hogares menor al 2% entre los años 2010, 2011 y 2012, porcentaje que no representa una rebaja significativa de la delincuencia.

Otro aspecto a destacar es que la provincia con mayor número de delitos es la del Guayas, sin embargo su nivel de delincuencia no ha crecido para los últimos cuatro meses de los años 2011 y 2012.

1.2.2 CARTOGRAFÍA DE VICTIMIZACIÓN A HOGARES

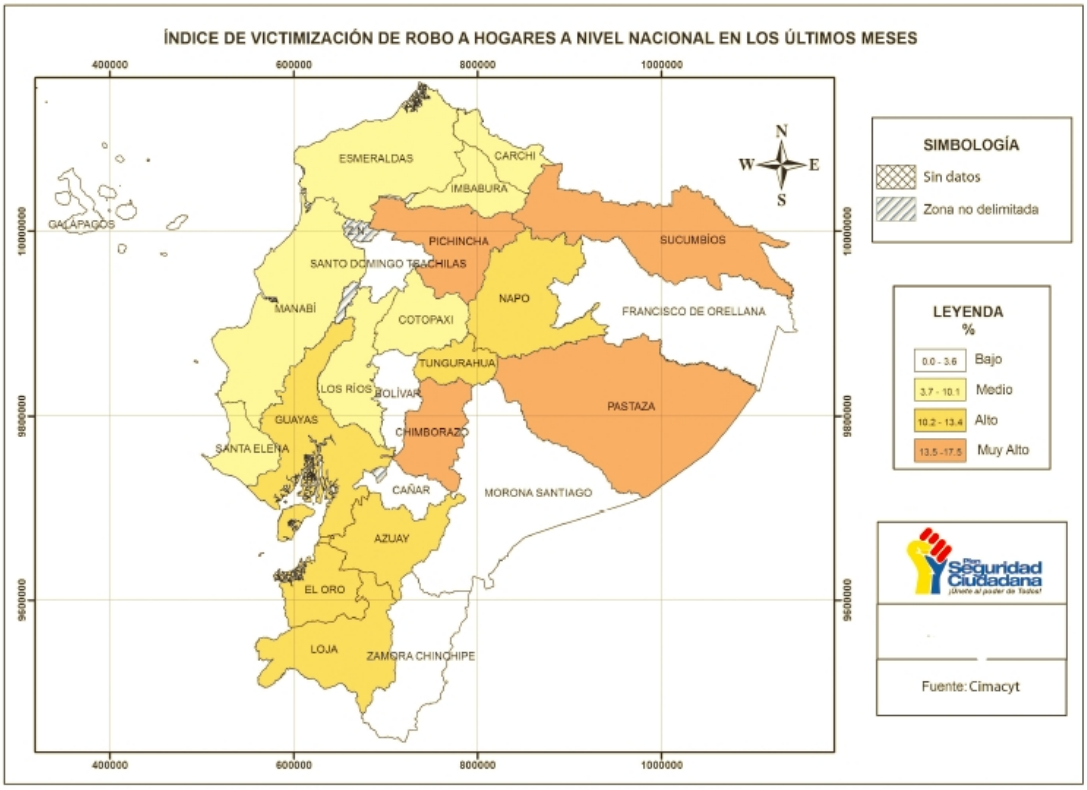


Figura 1.6: Índice victimización: robo hogares a nivel nacional a Diciembre 2012 [1]

En la Figura 1.6 se muestra que las provincias con mayor índice de robo a hogares.

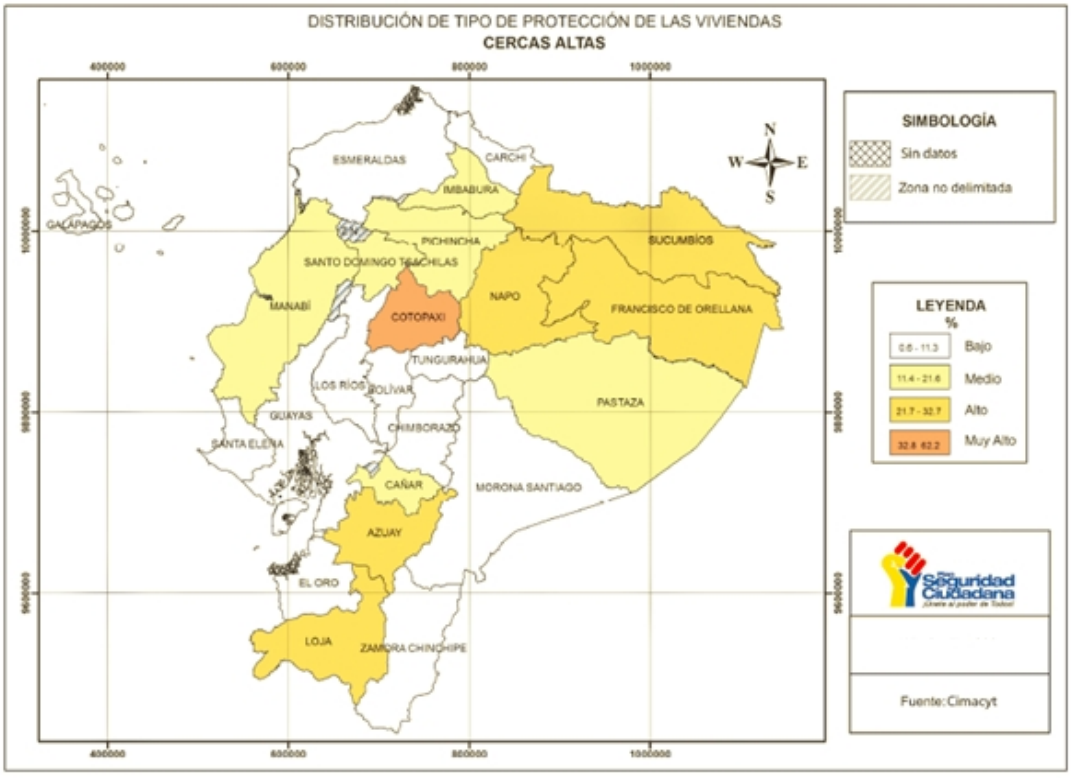


Figura 1.7: Seguridad con Cercas 2[m] de alto en las viviendas a Diciembre 2012 [1]

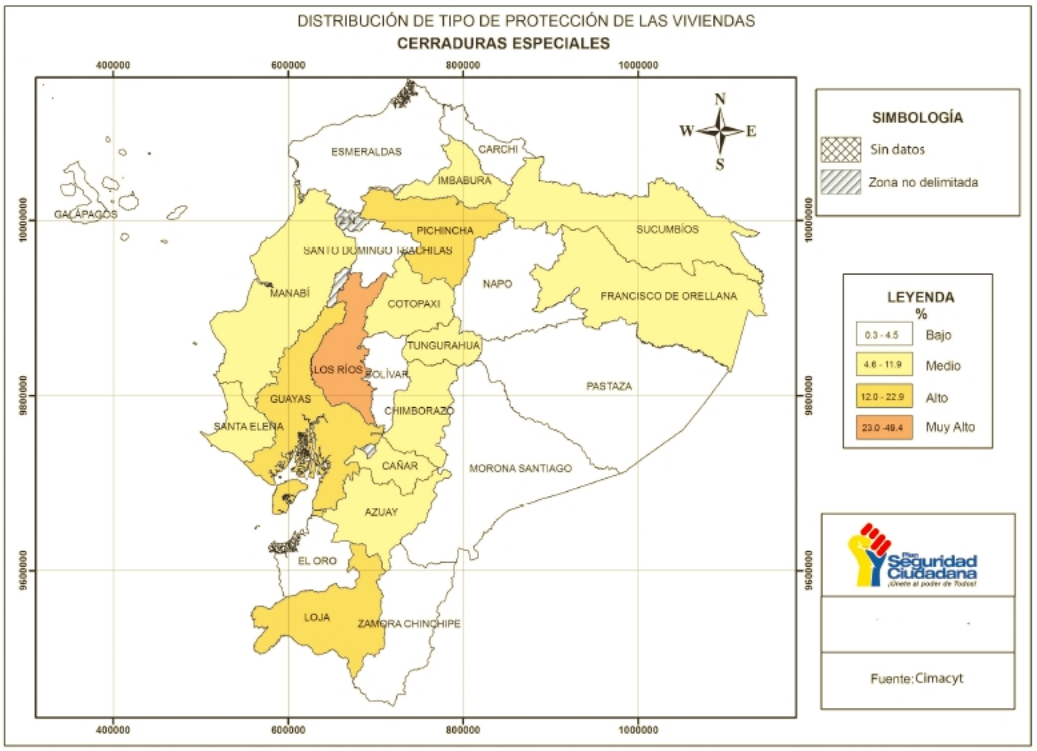


Figura 1.8: Seguridad Cerraduras varios tipos en las viviendas a Diciembre 2012 [1]

De las Figuras 1.7 y 1.8, se puede concluir que las personas buscan varias formas de defender sus hogares, dependiendo de sus posibilidades económicas.

A nivel de regiones se puede observar diferencias en la victimización, ya que, el robo a hogares es mayor en la Sierra y la Amazonía, mientras existe un mayor ataque a las personas en la región Costa. Además se puede decir que la pobreza constituye un aspecto discriminante en la preferencia de los y las atacantes, por la tendencia de que; a ingresos mayores y el pertenecer a estratos altos, hace más "apetecibles" y vulnerables a las personas y a los hogares para el ataque de la delincuencia.

Otro aspecto relevante es el hecho de la desconfianza en la institución policial ya que un alto porcentaje de delitos no son denunciados debido a la percepción ciudadana que la policía no podría resolverlo o por temor a las represalias. Ambos son problemas de expresa gravedad ya que demuestran una población que se siente en cierto sentido carente de un Estado que la proteja y por ende se abren las puertas para iniciativas de justicia por propia mano.

1.3 ESPECIFICACIÓN ZIGBEE [2]

ZigBee es diseñado y promovido por la *ZigBee Alliance*. No es una tecnología, sino un conjunto estandarizado de soluciones que pueden ser implementados por cualquier fabricante.

ZigBee está basado en el estándar IEEE 802.15.4 de redes inalámbricas de área personal (W*ireless Personal Área Network,* WPAN) cuyo objetivo es tener redes inalámbricas con capacidades de control y monitoreo confiables, de bajo consumo energético, bajo costo de transmisión bidireccional; todo basado en un estándar público global que permita a cualquier fabricante crear productos compatibles entre ellos.

1.3.1 CARACTERÍSTICAS GENERALES [2] [3] [4]

Se puede mencionar las siguientes características para el estándar ZigBee:

- ZigBee opera en las bandas libres ISM (*Industrial, Scientific & Medical*) de 2.4 GHz, 868 MHz (Europa) y 915 MHz (Estados Unidos).

- Velocidad de datos 250 kbps (2.4 GHz), 40 kbps (915 MHz), y 20 kbps (868 MHz).
- Método de acceso al canal es CSMA/CA.[2]
- A pesar de coexistir en la misma frecuencia con otro tipo de redes como *WiFi* o *Bluetooth,* su desempeño no se ve afectado, debido a su baja tasa de transmisión y, a características propias del estándar IEEE 802.15.4.
- Los dispositivos ZigBee, comparados con otras tecnologías inalámbricas, no consumen demasiada energía.
- Cada red ZigBee tiene un identificador de red único, lo que permite que coexistan varias redes en un mismo canal de comunicación sin ningún problema.
- Es un protocolo de comunicación multi - salto, es decir, que puede establecer comunicación entre dos nodos, siempre y cuando existan otros nodos intermedios que los interconecten.

1.3.2 FUNCIONES DEL ESTÁNDAR ZIGBEE [3]

- **Búsqueda de red** (*Network Scan*): La capacidad de un dispositivo de sondear canales dentro de su rango de comunicaciones. Este rango es llamado a menudo POS (*Personal Operating Space*).
- **Creación de una red PAN** (*Creating*): Construir una red, sobre canales sin utilizar el POS.
- **Descubrimiento de dispositivos** (*Device Discovery*): Permite identificar los dispositivos en una PAN.
- **Unión** (*Binding*): La comunicación a nivel de capa de aplicación con otros dispositivos en la red.

[2] CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*), mecanismo para acceder al canal de transmisión de datos evitando que se produzcan colisiones en el medio.

- **Asociación y desasociación de dispositivos** (*Joining and leaving a Network*): Permite agregar nuevos miembros en la red, así como también, separar miembros dentro de ella.
- **Configuración de un nuevo dispositivo** (*Configuring a new device*): Establece la configuración del *stack* para operaciones requeridas, por ejemplo el dispositivo puede ser configurado como coordinador ZigBee.
- **Direccionamiento** (*Addressing*): Permite a un dispositivo ZigBee asignar direcciones a dispositivos nuevos en la red.
- **Sincronización en una red** (*Synchronization within a network*): La sincronización de un dispositivo con otro mediante el envío de tramas *beacon* o poleo (*polling*).[3]
- **Asignación de ruta** (*Routing*): Enrutando las tramas a las direcciones establecidas.
- **Seguridad** (*Security*): Aplicando seguridad a las tramas transmitidas y recibidas.

1.3.3 TIPOS DE DISPOSITIVOS [2] [3] [4]

Se especifican tres tipos de dispositivos de acuerdo al rol que desempeñan dentro de la red:

- **Coordinador ZigBee** (*ZigBee Coordinator, ZC*): Es el dispositivo más completo. Puede actuar como director de una red en árbol *(cluster tree*), así como, servir de enlace a otras redes. Existe un coordinador por cada red.
- ***Router* ZigBee** (ZR): Además de ofrecer un nivel de aplicación para la ejecución de código de usuario, puede actuar como router interconectando dispositivos separados dentro de la red.
- **Dispositivo Final** (*ZigBee End Device, ZED*): Posee la funcionalidad necesaria para comunicarse con su nodo padre (coordinador o un router), pero no puede transmitir información destinada a otros dispositivos. De

[3] *Polling*: Sondeo de la red mediante el cual se solicita el envío de información.

esta forma, este tipo de nodo puede estar dormido la mayor parte del tiempo.

Se puede mencionar una segunda clasificación en base a la funcionalidad en la red:

- **Dispositivo de funcionalidad completa** (*Full Functionality Device,* FFD): Es capaz de recibir mensajes en formato del estándar IEEE 802.15.4, gracias a la memoria adicional y a la capacidad de procesar, puede funcionar como coordinador, *router* o puede ser usado como dispositivo de red que actúe de interfaz con los usuarios. También puede soportar los siguientes modos de operación:
  - ✓ **Dispositivo Simple:** Es un dispositivo que puede actuar como *router* o como dispositivo final.
  - ✓ **Coordinador PAN**: Es el controlador principal de la PAN, este dispositivo identifica a su red y permite a otros dispositivos asociarse, proveyéndoles una sincronización global.
- **Dispositivo de funcionalidad reducida** (*Reduced Functionality Device* RFD): Son los sensores/actuadores de la red y solo pueden asociarse a un FFD a la vez. Estos dispositivos no tienen la necesidad de enviar grandes cantidades de información ya que solo está previsto para aplicaciones simples.

1.3.4 TOPOLOGÍAS EN LA RED ZIGBEE [3] [4] [5]

En ZigBee existen tres tipos de topologías que pueden ser implementadas de acuerdo a la aplicación, y estas son: estrella, árbol (*cluster tree)*, y malla (*mesh network*).

1.3.4.1 Tipos de topologías

Dentro de la red ZigBee tenemos las siguientes topologías:

- **Topología en estrella**: Tiene un único dispositivo trabajando como coordinador PAN. La comunicación en esta topología es centralizada, cada

dispositivo (FFD o RFD) se une a la red y si desea comunicarse con otros dispositivos debe enviar la información al coordinador PAN, el cual enviará esta información al dispositivo correspondiente.

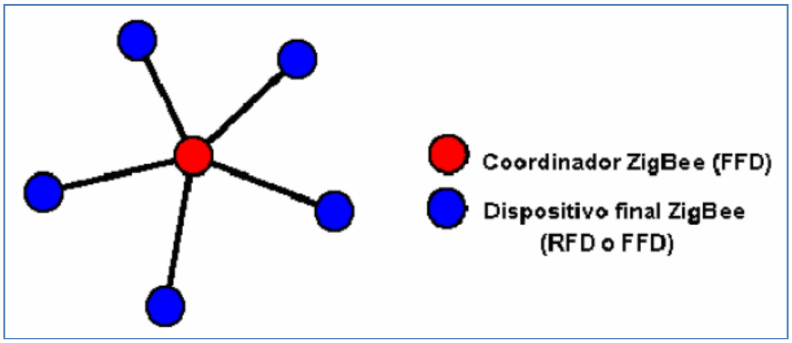


Figura 1.9: Topología en estrella [3]

- **Topología *clúster tree***: Tiene la asociación de varias redes (Figura 1.10) donde:

  El coordinador PAN:

  - Forma el primer *cluster* y se establece a sí mismo como *Cluster Head* (CH) con su respectivo *Cluster Identifier* (CID) igual a cero.
  - Elije un identificador PAN.
  - Envía tramas *beacon* a todos los dispositivos vecinos.

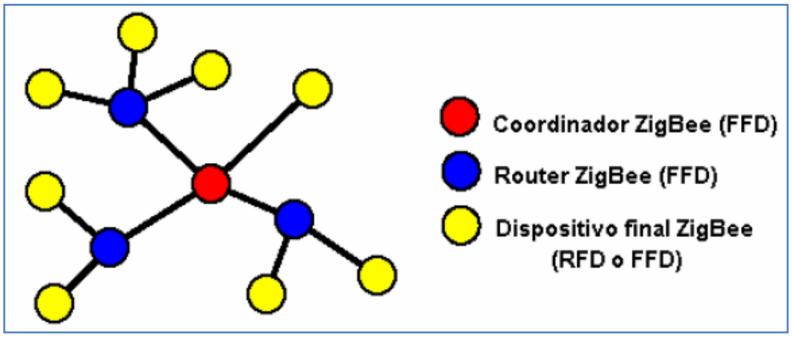


Figura 1.10: Topología *cluster tree* [3]

- **Topología *mesh***: En esta configuración hay conectividad total de todos los FFDs que conforman la red con el FFD que actúa como coordinador PAN, según muestra la Figura 1.11

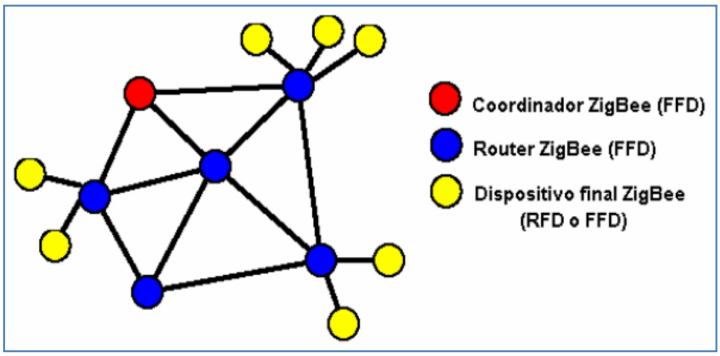


Figura 1.11: Topología *mesh* [3]

Las ventajas de esta topología es que es confiable y el rendimiento en el del envío de información en la red se debe a las múltiples trayectorias que pueden existir.

1.3.5 ARQUITECTURA [2] [3] [5]

La formación y la asociación de la red están basadas en algunas suposiciones:

- Los dispositivos son pre programados para su función de red.
- Los dispositivos finales siempre tratarán de asociarse a una red existente.
- Los coordinadores siempre tratarán de encontrar un canal sin usar de una red.

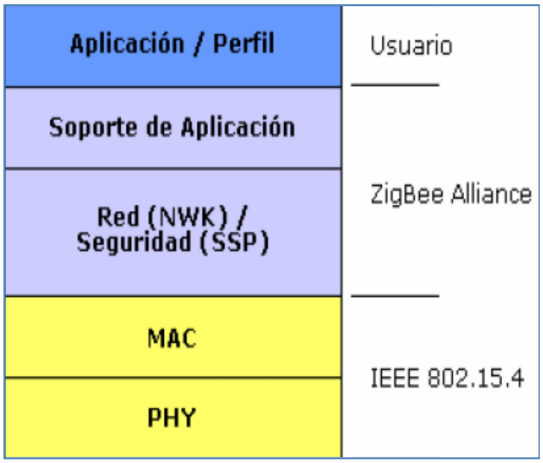


Figura 1.12: Capas de la pila de protocolos ZigBee [2]

En la Figura 1.12 se muestra la pila de protocolos ZigBee:

- La capa de más bajo nivel (IEEE 802.15.4), comprende la capa física (PHY) y la subcapa de acceso al medio (MAC).
- La capa definida por la ZigBee *Aliance* comprende la capa de red (NWK), y la capa de soporte de aplicación.
- La capa de aplicación.

1.3.5.1 Capa Física (Physical Layer PHY)

La capa física (PHY), en conjunto con la subcapa de acceso al medio (MAC), son las responsables de la transmisión y recepción de datos en un canal de radio.

El estándar IEEE 802.15.4 ofrece tres bandas de frecuencia:

- Frecuencia de 2.4 GHz, específica la operación en la banda Industrial, Médica y Científica (ISM), que prácticamente está disponible en todo el mundo.
- Frecuencia de 865 MHz opera en Europa.
- Frecuencia de 915 MHz opera en Estados Unidos.

El estándar IEEE 802.15.4 utiliza la técnica DSSS (*Direct Secuence Spread Spectrum*) para transmitir la información a través del medio.

Las características técnicas de cada frecuencia se resumen en la Tabla 1.6

PHY (MHz)	Banda de frecuencia (MHz)	Parámetros Spreading		Parámetros de Data		
		Chip rate (Kchip/s)	**Modulation**	**Bit rate (Kb/s)**	**Symbol rate (Ksymbol/s)**	**Symbols**
868/915	868-868.6	300	BPSK	20	20	Binary
	902-928	600	BPSK	40	40	Binary
868/915 (optional)	868-868.6	400	ASK	250	12.5	20-bit PSSS
	902-928	1600	ASK	250	50	5-bit PSSS
868/915 (optional)	868-868.6	400	O-QPSK	100	25	16-ary Orthogonal
	902-928	1000	O-QPSK	250	62.5	16-ary Orthogonal
2450	2400-2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

Tabla 1.6: Parámetros técnicos según las frecuencias [5]

El estándar IEEE802.15.4 define 49 canales de frecuencia entre las tres bandas.

- La banda de 868 MHz soporta 3 canales entre los 868 y los 868.6 MHz, de los cuales 2 canales son opcionales.
- La banda 915 MHz soporta 30 canales entre los 902 y 928 MHz, con un separación entre canales de 2 MHz, siendo 20 canales opcionales.
- La banda de 2.4 GHz soporta 16 canales entre 2.4 y 2.4835 GHz, con un separación entre canales de 5 MHz.

Gracias a los diferentes rangos de transición se puede obtener varias aplicaciones.. Por ejemplo, la capa física a 868/915 MHz se puede ocupar para lograr mayor sensibilidad y mayores áreas de cobertura, con lo que se reduce el número de nodos requeridos para cubrir una área geográfica, mientras que el rango superior de transmisión en la capa física a 2.4 GHz se puede utilizar para conseguir mayor velocidad de transmisión.

1.3.5.1.1 Características de la capa física

- **Activación/desactivación del *transceiver*:** El radio *transceiver* opera en tres estados: transmitiendo, recibiendo o en modo *sleeping*.
- **Detección de energía ED**: Es una estimación de la señal recibida, este valor es analizado con respecto a un valor umbral predeterminado (umbral ED). Esta medida es usada para la selección de canal, y por CCA (*Clear Channel Assessment*)[4] para determinar si el canal está libre u ocupado.
- **Indicador de calidad de enlace LQI** (*Link Quality Indication*): Indica la intensidad del enlace de comunicaciones. Es un valor calculado, basado en la intensidad de la señal recibida, así como el número de errores recibidos.
- ***Clear channel* Assessment CCA**: Esta operación es responsable de reportar el estado de actividad en el medio (libre u ocupado). EL CCA tiene tres modos de operación:

[4] CCA (*Clear Channel Assessment*): es una función lógica en la capa física (PHY) que determina el estado actual de uso del medio inalámbrico.

- ✓ Modo detección de energía**:** El CCA reporta que el canal está ocupado si el valor de la energía está sobre el umbral ED.
- ✓ Modo sondeo de portadora (*carrier)***:** El CCA reporta que el canal está ocupado solamente si detecta una señal con las técnicas de modulación establecidas por IEEE 802.15.4, sea que esta señal esté sobre o debajo del umbral ED.
- ✓ Sondeo de portadora (*carrier*) con detección de energía**:** Esta es una combinación de las técnicas ya mencionadas, el CCA reporta que el canal está ocupado solamente si detecta una señal con modo sondeo de portadora y que este valor de energía esté sobre el umbral ED.

- **Selección del Canal**: Seleccionar la frecuencia exacta en la cual el transceiver operará.
- **Transmisión y recepción de datos:** Datos que son enviados a través del canal de radio.

1.3.5.1.2 Servicios de la capa física PHY

La capa PHY proporciona dos tipos de servicios: el servicio de datos PHY y el servicio de gestión PHY.

- **Servicio de datos PHY**: Los datos a ser transmitidos son una unidad de datos de protocolo MAC (MAC *protocol data unit* MPDU). La subcapa MAC local genera la petición de transmisión y proporciona la MPDU.

  La PHY intenta la transmisión e informa del resultado del intento (con éxito o sin éxito) a la subcapa MAC. Las razones para un intento fallido de transmisión pueden ser:

  - ✓ El radio transceiver está deshabilitado.
  - ✓ El radio transceiver está en modo receptor. El radio no puede transmitir y recibir de forma simultánea.

- El radio transceiver está ocupado (en ese momento se encuentra transmitiendo).

- **Servicio de gestión PHY**: Los servicios que se proporcionan por medio de la PLME-SAP (*Physical Layer Management Entity* – SAP) son:
  - ✓ Activación y desactivación del radio transceiver.
  - ✓ Detección de Energía (ED)
  - ✓ *Clear Channel Assessment* (CCA)
  - ✓ Obtención de información desde la PHY PIB (*Información Base*)[5].

1.3.5.1.3 Paquete de la capa física PHY

La estructura de la trama de la capa física se muestra en la Figura 1.13

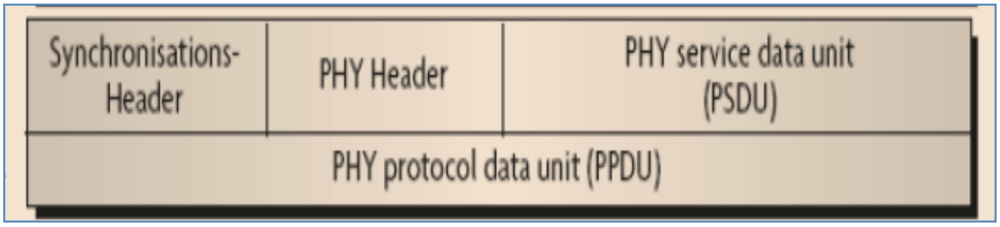


Figura 1.13: Estructura del paquete de capa física [3]

***Synchronization Header (SHR)*:** Campo de sincronización de la trama.

Phy Header (PHR): Especifica la longitud de la PHY *Service. Data Unit* PSDU.

Phy Service Data Unit*:* En el campo de datos de la capa física se encapsula a la trama MAC cuyo valor máximo es 127 bytes.

1.3.5.2 Subcapa de acceso al medio MAC

La subcapa MAC del protocolo IEEE 802.15.4 provee un interfaz entre la capa física y las capas superiores.

[5] La PHY PIB comprende los atributos necesarios para la administración de la capa física de un dispositivo. Cada uno de estos atributos pueden ser leídos o escritos empleando las primitivas PLME–GET.*request* y PLME–SET.*reques*t, respectivamente.

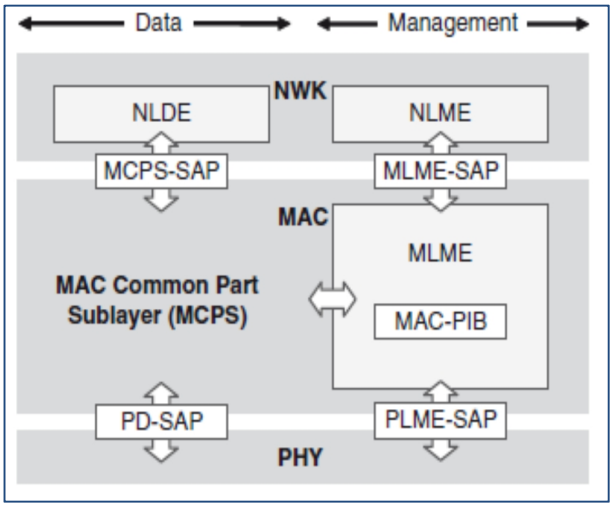


Figura 1.14: Modelo de referencia de la subcapa MAC [8]

- **Características de la subcapa MAC**:
  - ✓ Gestión de tramas *beacon*
  - ✓ Acceso al canal
  - ✓ Gestión de GTS (*Guaranteed Time Slots)*
  - ✓ Validación de la trama
  - ✓ Asociación y desasociación
- **Servicios de la subcapa MAC**

La subcapa MAC ofrece dos tipos de servicios: servicio de datos MAC y servicio de gestión MAC.

- ✓ **Servicio de datos MAC**: Los datos que necesitan ser transmitidos se proporcionan como *Network Protocol Data Unit* NPDU. El NPDU se coloca en la carga útil de MAC, que se llama el MSDU.
- ✓ **Servicio de gestión MAC**: Al servicio de gestión de MAC se accede a través de MAC *Layer Management Entity* SAP (SAP-MLME). Los comandos MAC normalmente incluyen parámetros tales como: direccionamiento, seguridad y reportar el resultado de una solicitud en la

forma de un estado a la capa superior. El estado puede ser de: ÉXITO o FALLA.

- **Estructura de las tramas MAC**

  El formato general de las tramas MAC está diseñado para ser flexible, que se ajuste a las necesidades de las diferentes aplicaciones con diversas topologías de red, al mismo tiempo que se mantenga un protocolo simple. **Estructura de la trama de Datos *(Data Frame):*** Usado para todas las transferencias de datos.

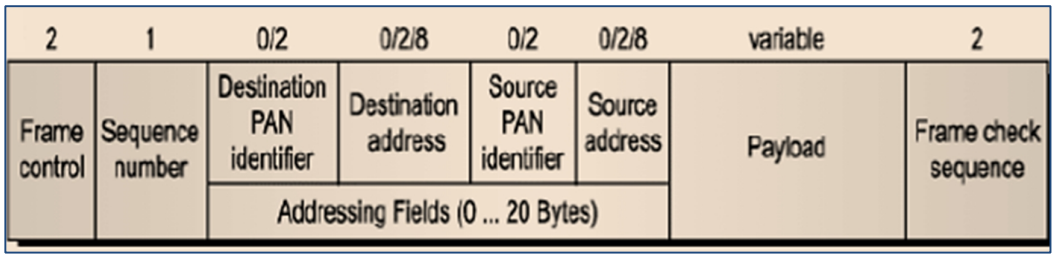


Figura 1.15: Formato general de la trama MAC [3]

- **Estructura de la trama *Beacon* (*Beacon Frame*):** Usada por un controlador para transmitir tramas *beacon.*

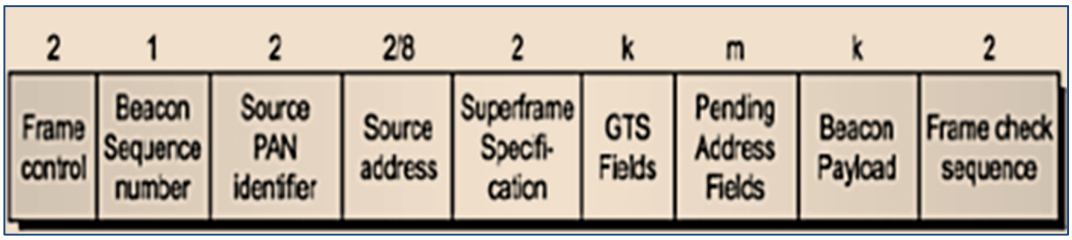


Figura 1. 16: Formato general de la trama *Beacon* [3]

- **Estructura de la trama ACK (*Acknowledgment Frame*):** Dado para confirmar la recepción exitosa de una trama.

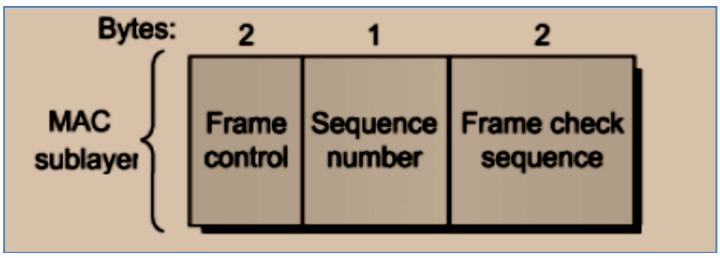


Figura 1.17: Formato general de la trama ACK [3]

- **Estructura de la trama Comandos MAC (*MAC Command Frame*):** Usado para manejar todo el control de la entidad MAC. Permite a un coordinador configurar a los dispositivos individualmente sin importar lo grande que sea la red.

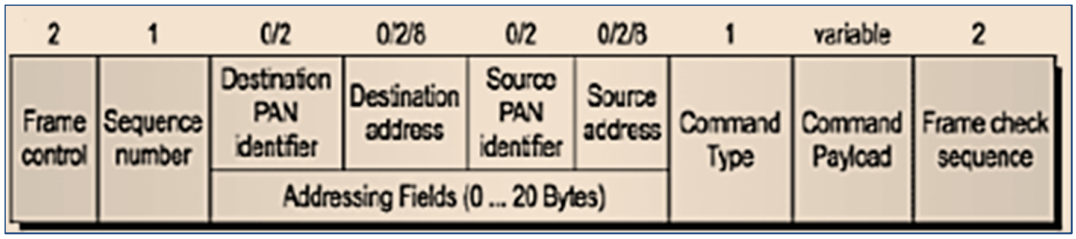


Figura 1.18: Formato general de la trama de comandos [3]

- **Estructura Superframes [5]**

El formato de la *superframe* se muestra en la Figura 1.19 y es definido por el coordinador.

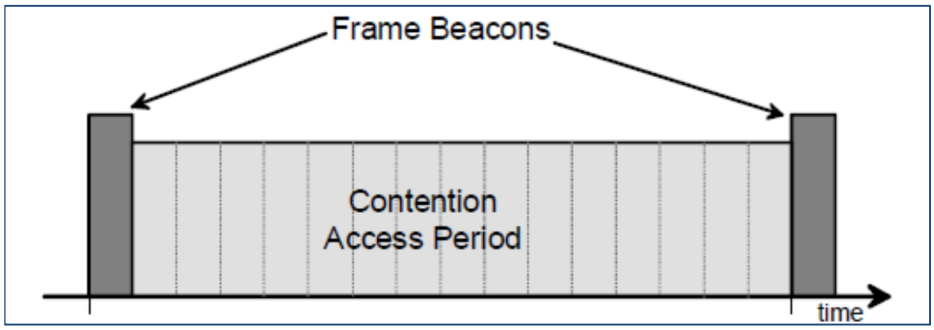


Figura 1.19: Estructura de la *superframe* [5]

La *superframe* puede contener una duración activa e inactiva. Durante el tiempo inactivo, el coordinador no interactúa con la PAN y puede entrar en modo de bajo consumo de energía.

Para aplicaciones de baja latencia o de ancho de banda específico, el coordinador PAN puede dedicar tiempo activo de la *superframe* para dicha aplicación. Este tiempo es llamado *guaranteed time slots* (GTSs), El GTSs forma el período libre de contención (*contention-free period* CFP). Figura 1.20

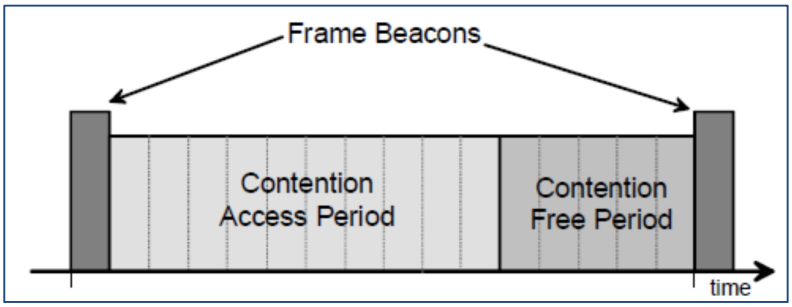


Figura 1.20: Estructura de la *superframe* con GTSs [5]

El *beacon* que se encuentra al inicio de una *Superframe*, es transmitido por el coordinador PAN en intervalos definidos. Estos intervalos pueden ser:

- Desde 15 ms hasta 245 seg en 2.4 GHz
- Desde 96 ms hasta 1573 seg en 915 MHz
- Desde 192 ms hasta 3146 seg en 868 MHz

1.3.5.2.1 Sondeo de canales [5]

El sondeo de canales es utilizado para identificar la existencia de redes PAN antes de la asociación o para crear una nueva PAN. El estándar define cuatro tipos de sondeo de canal:

- **Sondeo de canal ED (*Energy Detection*):** Este sondeo permite a un FFD (*Full Functionality Device*), obtener una medida de energía pico en un canal solicitado. Durante este proceso la subcapa MAC puede descartar tramas recibidas por la capa PHY.
- **Sondeo de canal activo**: Este sondeo permite a un FFD, localizar cualquier coordinador PAN, transmitiendo tramas *beacon* dentro de su área de operación. Durante este proceso la subcapa MAC descartará todas las tramas de la capa PHY que no sean tramas *beacon*.
- **Sondeo de canal *pasivo*:** Este sondeo permite a un dispositivo, localizar cualquier coordinador PAN, transmitiendo tramas *beacon* dentro de su área de operación. Durante este proceso la subcapa MAC descartará todas las tramas de la capa PHY que no sean tramas *beacon*.

- **Sondeo de canal *Orphan*:** Este sondeo permite a un dispositivo volver a intentar conectarse a un coordinador luego de perder sincronización. Durante este proceso la subcapa MAC descartará todas las tramas recibidas por la capa PHY que no sean tramas de comandos MAC de recuperación de conexión desde el coordinador.

1.3.5.2.2 Creación de una red ZigBee

Una PAN es creada solamente por un dispositivo FFD luego de elegir un canal y un identificador PAN. Una vez creada la PAN, el coordinador genera y envía tramas *beacon* para manejar la asociación y desasociación de otros dispositivos brindando servicios de sincronización, permitiendo la asignación y el manejo de GTSs.

- **Generación de *Beacons***: A un FFD le está permitido generar y enviar tramas *beacon* solo si previamente cumple al menos una de las siguientes condiciones:
  - ✓ El FFD es el coordinador PAN de una nueva red.
  - ✓ El FFD es un dispositivo asociado en una PAN previamente establecida.
- **Asociación de un dispositivo**: La asociación comienza con un sondeo activo o pasivo; luego de terminado el sondeo, el dispositivo selecciona el identificador PAN de la red a la que desea asociarse, entonces envía un paquete de datos al correspondiente coordinador solicitando la asociación.

  Si esta petición es recibida correctamente, el coordinador envía una trama ACK, para así confirmar la asociación. Sin embargo, el ACK de una petición de asociación no quiere decir que el dispositivo fue asociado; en efecto el coordinador necesita tiempo para procesar la petición y determinar si los actuales recursos de la PAN son suficientes para permitir otra asociación.
- **Desasociación de un dispositivo**: El proceso de desasociación puede ser iniciado por el coordinador o un dispositivo final.

- ✓ Coordinador inicia la desasociación: Si el coordinador quiere des asociar a uno de sus dispositivos, envía esta notificación; cuando el dispositivo recibe la notificación envía un ACK confirmando su recepción, si el ACK no es recibido por el coordinador, éste considera que el dispositivo está desasociado, y todas las referencias con respecto a él son borradas de la PAN.
- ✓ Dispositivo inicia la desasociación: Si un dispositivo quiere dejar la red envía una notificación al coordinador PAN. Una vez que el coordinador recibe esta notificación envía un ACK confirmando su recepción. Si el ACK no es recibido este se considerará des asociado, y todas las referencias acerca de la PAN serán removidas por el dispositivo.

- **Sincronización**: Se definen mecanismos para sincronizar el coordinador con sus dispositivos asociados, estos mecanismos de sincronización dependen del modo de operación de la PAN
- **Transmisión y recepción de datos**: La transmisión de datos depende del modo de operación de la PAN. En una PAN con *beacon* un dispositivo que desee transmitir información debe localizar tramas *beacon* de su coordinador.

1.3.5.2.3 Tipos de tráfico

- **Datos Periódicos:** Este tipo de tráfico se maneja con *beacon* donde el sensor se despertará debido a la recepción de una trama *beacon*, momento que utilizará para verificar cualquier tipo de mensaje y luego volverá a dormir.
- **Datos Intermitentes:** Esta información se maneja sin *beacon*. En este modo el dispositivo sólo se comunicará con la red cuando necesite enviar información.
- **Datos Repetitivos de baja velocidad:** Para estos datos de baja latencia se usa con *beacon* y se utilizan los GTSs, que permiten a cada dispositivo transmita datos sin realizar contención.

1.3.5.3 Capa de Red (Network Layer NWK) [3] [4] [7] [8]

La capa de red (NWK) se encarga de la topología de la red, añadiendo o eliminando dispositivos dentro de la misma; asignando direcciones de red y re-direccionando las tramas de información hacia el destinatario por el camino más adecuado. También se encarga de garantizar la fiabilidad y calidad de los datos recibidos en el nodo, mediante el control y corrección de errores, que pueden ser provocados por una mala comunicación de radio, congestión en la red, o colisión entre paquetes transmitidos. La capa de red proporciona una correcta funcionalidad a las capas inferiores (física y MAC), además de servir como interfaz de servicio para la capa de aplicación, tanto en datos, como en gestión.

1.3.5.3.1 Servicios de la capa de red

La capa de Red de ZigBee ofrece de un canal de comunicación directo entre los servicios en la misma capa, es decir, dispone de una interfaz para comunicar los servicios intermedios de datos y control. Dentro de cada uno de los servicios de la capa de Red, en las interfaces de comunicación se definen primitivas de comunicación entre las capas de; aplicación y MAC. De igual manera sucede en la comunicación entre los servicios de la propia capa. Figura 1.21

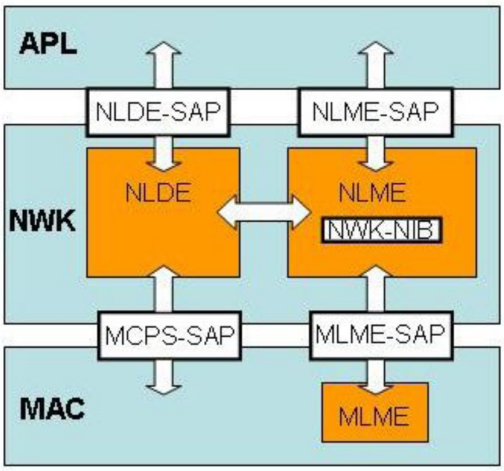


Figura 1.21: Capa de red ZigBee [4]

- **Servicio de Datos**: Conocido como NLDE (*Network Layer Data Entity*), provee de un servicio de datos, que permite a cualquier aplicación

comunicarse con las mismas unidades de datos, con dos o más dispositivos que deben estar en la misma red de interconexión.

- **Servicio de Control:** Conocido como NLME (*Network Layer Management Entity*), es un servicio que permite a la capa de Aplicación interactuar o comunicarse con la pila de protocolos directamente.

  El servicio de control de datos establece:

  - ✓ Configuración de un nuevo dispositivo.
  - ✓ Inicialización de una nueva red.
  - ✓ Integración y salida de una red.
  - ✓ Direccionamiento.
  - ✓ Descubrimiento de vecinos.
  - ✓ Recepción de control.
  - ✓ Enrutamiento.

1.3.5.3.2 Funcionalidades de la capa de red [10]

Las funcionalidades de esta capa son:

- **Inicialización de una red**: Es iniciado por dispositivos Coordinadores y que no se encuentren ya dentro de una red ZigBee. Un coordinador, sólo puede aparecer en una red.
- **Nuevos dispositivos en la red**: Iniciado por dispositivos Coordinadores o Router. En caso de que otro dispositivo iniciase este proceso, será cancelado por el servicio de control de la capa de red.
- **Unirse a la red**: Cuando se activa un dispositivo router o un dispositivo final, su primer objetivo es asociarse a una red ya existente, para ello realizan un escaneo de los canales que tienen previamente configurados en busca de un coordinador que responda.

- **Protocolos de Enrutamiento**: ZigBee permite varias topologías, utiliza diferentes algoritmos según la red esté estructurada en configuración estrella, árbol o malla.

  Para obtener la ruta óptima se realiza un cálculo del coste de cada camino en función del número de saltos que hay entre origen y destino y la calidad de los enlaces existentes entre ambos dispositivos.

  Dentro de los protocolos de enrutamiento se tienen:

  ✓ Proactivos: Aquellos que construyen las tablas de enrutamiento previo al envío de información.

  ✓ Reactivos: Descubren las rutas en función de la necesidad.

1.3.5.3.3 Formato del Paquete[7]

En la Figura 1.20, se muestra el formato del paquete de red.

Octets: 2	2	2	1	1	0/8	0/8	0/1	Variable	Variable
Frame control	Destination address	Source address	Radius	Sequence number	Destination IEEE Address	Source IEEE Address	Multicast control	Source route subframe	Frame payload
NWK Header									Payload

Figura 1.22: Formato del paquete de red [7]

- ***Frame Control***: **C**ontiene información que define el tipo de trama, direccionamiento, secuencia y control.

- ***Destination Address***: Si la bandera de *multicast* está en 0 en el *Frame Control*, la dirección de destino contiene la dirección de red del dispositivo de destino o una dirección de difusión. Si la bandera de *multicast* está en 1, será el ID de grupo *multicast* de destino.

- ***Source Address***: En este campo contiene la dirección de red de dispositivo que origina la trama.

- ***Radius***: Especifica el alcance de la transmisión, este campo se reduce en 1 por cada dispositivo receptor.

- ***Sequence Number***: Este valor se incrementa en 1 por cada trama transmitida.
- ***Destination* y *Source* IEEE *Address***: Tiene 64 bits de dirección IEEE, obtenidos en la dirección de la cabecera de Red.
- ***Multicast Control***: Está presente si el sub campo multicast del campo *Frame Control* tiene un valor de 1.
- ***Source Route Subframe***: Campo variable, y solo estará presente si el sub campo ruta origen del campo *Frame Control* tiene un valor de 1.
- ***Frame Payload***: Contiene la información del paquete de red.

1.3.5.4 Capa de aplicación (Aplication Layer APL) [8]

La capa aplicación (APL) es la más alta en la red inalámbrica ZigBee, y consta de tres secciones, como se muestra en la Figura 1.23: *Aplication framework,* subcapa *Aplication Support* (APS) y *ZigBee Device Objects* (ZDO).

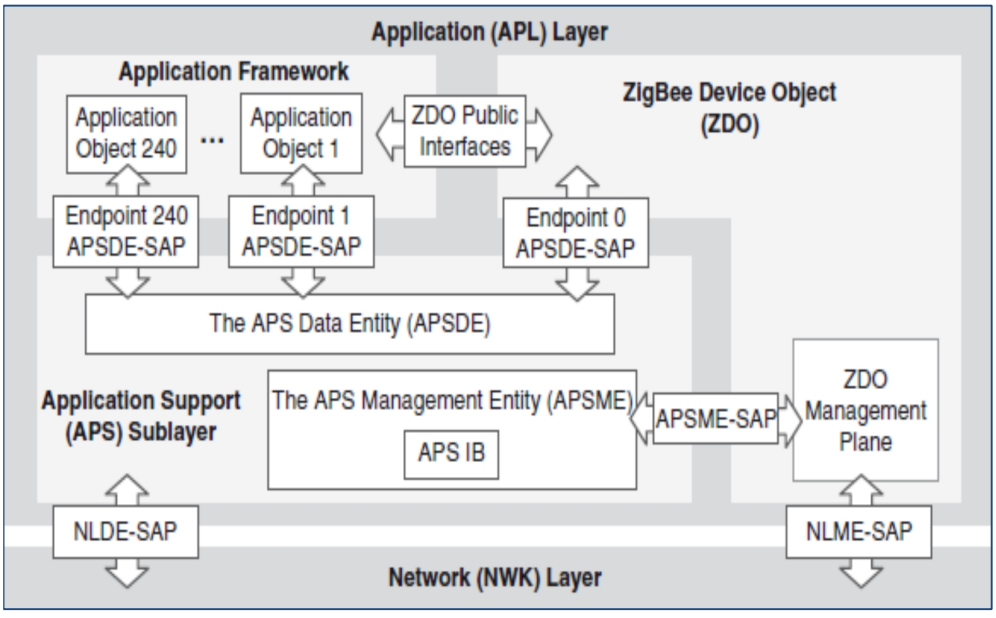


Figura 1.23: Capa Aplicación [8]

1.3.5.4.1 Aplication Framework

El *Aplication framework* es el ambiente en el cual los objetos de aplicación son organizados, para el control y gestión de los protocolos en los dispositivos ZigBee. Los objetos de aplicación son desarrollados por los fabricantes y adaptados para varias aplicaciones. Pueden existir 240 objetos aplicación por cada dispositivo.

Los objetos de aplicación utilizan el APS *Data Entity* – SAP (PAPSDE-SAP), para enviar y recibir datos entre los nodos. Cada objeto de aplicación tiene una única dirección de punto final. Para los mensajes de *broadcast* todos los objetos de aplicación establecen en 255 la dirección de punto final. Los puntos finales del 241 a 254 están reservados para uso futuro.

La dirección de punto final permite a múltiples dispositivos compartir el mismo canal de radio.

*1.3.5.4.2 ZigBee Device Object (*ZDO*)*

ZDO proveen un interfaz entre la subcapa APS y el *Aplication Framework*. El ZDO contiene las funcionalidades que son comunes en todas las aplicaciones que operan en la pila de protocolos ZigBee. Por ejemplo, ZDO es responsable de configurar el dispositivo en uno de tres posibles tipos lógicos: coordinador ZigBee, router ZigBee, o dispositivo final ZigBee. EL ZDO es responsable de:

- Inicializar el *aplication support sub-layer* (APS), la capa de red (NWK) y proveer servicios de seguridad (SSP).
- Ensamblar la información de configuración de las aplicaciones finales para determinar e implementar: gestión de seguridad, gestión de red y gestión de enlace.

Similar a los perfiles de aplicación definidos en el *Aplication Framework*, existe un perfil definido para ZDO, que se conoce como el perfil del dispositivo ZigBee (ZDP), o simplemente el perfil de dispositivo.

El perfil de dispositivo puede ser configurado como cliente o servidor. Un cliente es un dispositivo que solicita un servicio como; descubrimiento de dispositivos, el

dispositivo que responde a esta petición actúa como servidor. Los servicios que proporcionan los clientes como servidores se proveen en forma de comandos con identificadores únicos. Al dispositivo cliente se lo conoce como dispositivo local mientras que el dispositivo servidor se lo conoce como dispositivo remoto.

Existen dos grupos de comandos para: servicio de clientes y servidores, los cuales son divididos en tres categorías: servicio de descubrimiento de dispositivos, gestión de unión de dispositivos y gestión de red.

Los comandos de servicios de descubrimiento de dispositivos permiten solicitar información como: dirección de red, lista de descriptores de cualquier dispositivo en la red.

Los comandos de gestión de unión de dispositivos permiten a un dispositivo crear o eliminar relaciones de unión.

Los comandos de gestión de red son utilizados para: identificar vecinos en la red, solicitar tablas de enrutamiento, y administrar la unión y des unión de los dispositivos en la red.

1.3.5.4.3 Subcapa Aplication Support (APS)

La subcapa de soporte a la aplicación (APS) proporciona un interfaz entre la capa de red (NWK) y la capa de aplicación (APL) a través de un conjunto de servicios que utilizan los dispositivos objeto ZigBee ZDO y los objetos de aplicación, definidos por los fabricantes. Estos servicios son: servicio de datos y servicio de gestión.

- **Servicio de datos APS:** Es proporcionado por APS *Entity Data* (APSDE) y se accede a través APSDE *Service Access Point* (SAP). Permite la transmisión de datos de aplicación entre dos o más dispositivos dentro de la red.
- **Servicio de gestión**: Es proporcionado por APS *Management Entity* (APSME) y se accede a través de APSME-SAP, este servicio proporciona el descubrimiento y enlace de dispositivos, también mantiene una base de datos de los objetos llamado APS *Information Base* (AIB).

1.3.6 SEGURIDAD EN REDES ZIGBEE [4] [5] [6] [11]

ZigBee utiliza AES (*Advance Encryption Standard*) del NIST (*National Institute of Standards and Technology*) como técnica de encripción[6]. Este mecanismo se basa en forma presenta tres métodos de obtención de la clave para los dispositivos.

- **Preinstalación**: El fabricante embebe la clave en el dispositivo. Con un conjunto de mini llaves que el usuario puede seleccionar.
- **Transporte de clave**: El dispositivo pide a un centro de confianza la clave. En este caso hay un momento de vulnerabilidad cuando se envía la clave.
- **Establecimiento de clave sin comunicación**: Es un método que genera claves al azar para dos dispositivos sin necesidad de comunicarlos. Este servicio ZigBee se basa en el protocolo SKKE (*Symmetric-Key Key Establishment*)[7]. Los dispositivos destino de la clave deben tener una clave común llamada clave maestra que pudo haber sido pasada de acuerdo al método a) o b).

En la red ZigBee cada capa del protocolo (APS, NWK y MAC) es responsable de la seguridad de las tramas generadas en esa capa. Por simplicidad se usa una misma clave para todas las capas.

[6] Los detalles de AES se pueden encontrar en: FIPS Pub 197 [12]

[7] Los detalles del protocolo SKKE se pueden encontrar en: La especificación ZigBee [7].

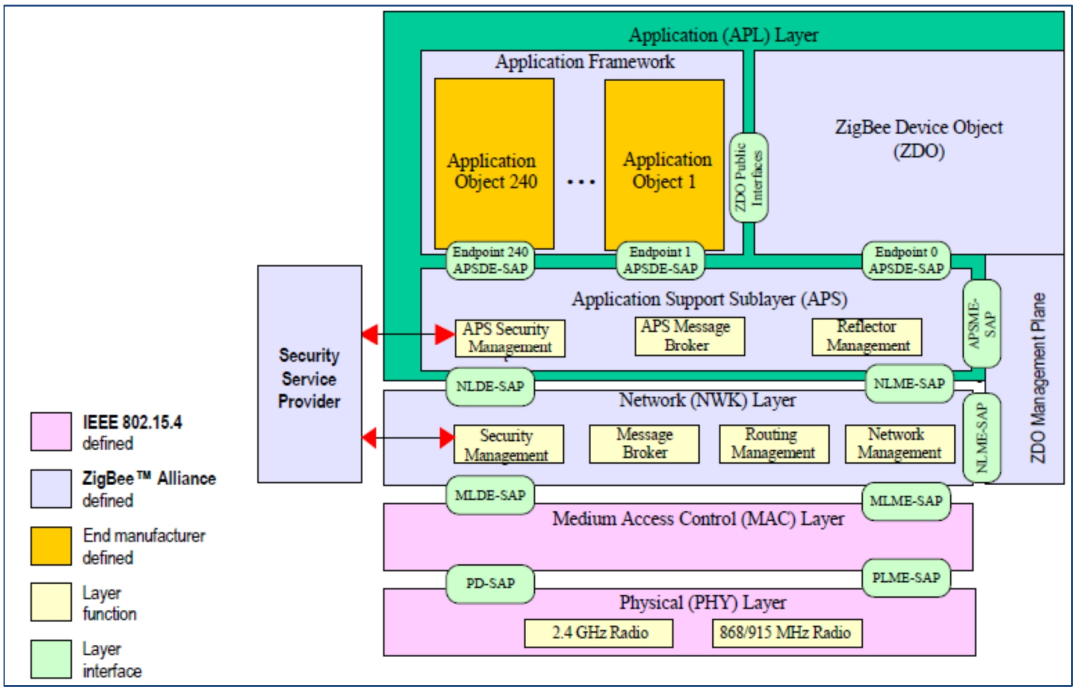


Figura 1.24: Protocolos de capas en ZigBee [8]

1.3.6.1 Centro de Confianza

Para brindar la funcionalidad de seguridad a una red ZigBee, un dispositivo debe permitir obtener claves confiables para el control de acceso a la red, conocido como el centro de confianza que cumple las siguientes funcionalidades.

- Almacenar las claves para la red.
- Utilizar servicios para configurar un dispositivo con claves del almacén.
- Manejar servicios para autorizar el ingreso a dispositivos dentro de la red.

1.3.6.2 Autenticación [8]

El procedimiento de autenticación de dispositivo se lleva a cabo en el centro de confianza. Cuando un dispositivo se conecta a una red segura, se une pero no autentica. Si el centro de confianza no decide autenticar el dispositivo que se unió, el centro de confianza solicitará la eliminación de dispositivo dentro de la red.

El estándar ZigBee soporta tanto la autenticación de dispositivos e integridad de datos.

- **Autenticación de dispositivos**: Permite confirmar que un nuevo dispositivo que se une a la red es quien dice ser a través de una clave de red y la configuración de atributos en un tiempo dado.

- **Integridad de datos**: El propósito de autenticación de datos es confirmar de que los datos no cambiaron durante la trasmisión. Para ello el transmisor acompaña al mensaje con un código especial llamado Código de Integridad de Mensaje (MIC, *Message Integrity Code*). El MIC se genera con un método que conocen tanto el emisor como el receptor. Un dispositivo no autorizado no deberá poder crear este MIC. El receptor al obtener el mensaje calcula el MIC y, si coincide con el cual envía el transmisor el mensaje se considera autentico.

1.3.6.3 Arquitectura de Seguridad [7]

La arquitectura de seguridad en ZigBee incluye mecanismos de seguridad en las capas de la pila de protocolos. Las capas NWK y APS son responsables del trasporte seguro de sus tramas. Por otra parte, la subcapa APS provee servicios de: establecimiento y mantenimiento de seguridad. Los dispositivos objeto de ZigBee ZDO, gestionan las políticas de seguridad y las configuraciones de seguridad de los dispositivos. Adicionalmente el estándar 802.15.4 implementa seguridad en la subcapa MAC de ZigBee.

1.3.6.3.1 Seguridad en MAC [3]

En la capa MAC el algoritmo de encriptación es AES (*Advanced Encryption Standard*) en las que se define una variedad de colecciones de seguridad. Estas colecciones protegen la confidencialidad, integridad, y autenticidad de las tramas MAC. La capa MAC brinda seguridad, pero las capas superiores son las que prepararán las claves y determinarán los niveles de seguridad. Cuando la capa MAC recibe una trama con seguridad, mira la fuente de la trama, recupera la clave asociada con esta fuente, y entonces usa esta clave para procesar la trama, según el tipo de seguridad asignada.

Al transmitir una trama, y es necesario mantener la integridad, los datos del MAC *Header* y el *payload* de MAC son usados para crear un MIC (*Message Integrity Code*), el cual puede ser de: 4, 8, o 16 octetos y es añadido al *payload* MAC. Para el uso de confidencialidad el *payload* de la trama MAC y el campo conteo de secuencia son usados para formar un *nonce* y éste es añadido al *payload* de la trama. Cuando la capa MAC recibe una trama y si el MIC está presente, se procede a descencriptar el *payload*.

1.3.6.3.2 Seguridad en la capa de red [3] [7]

El SSP (*Security Services Provider*) proporciona a la capa NWK una primitiva para aplicar seguridad a las tramas salientes y otra para verificar y quitar la seguridad de las tramas entrantes.

La capa NWK es responsable de la seguridad del proceso, pero las capas superiores controlan el proceso preparando claves. Similar al formato de la trama MAC, un conteo de secuencia de trama y el MIC pueden ser añadidos a la trama NWK.

1.3.6.3.3 Seguridad en la APL [7]

Al originar una trama en la capa APL, la seguridad es implementada en la subcapa APS mediante el uso de claves de enlace o claves de red.

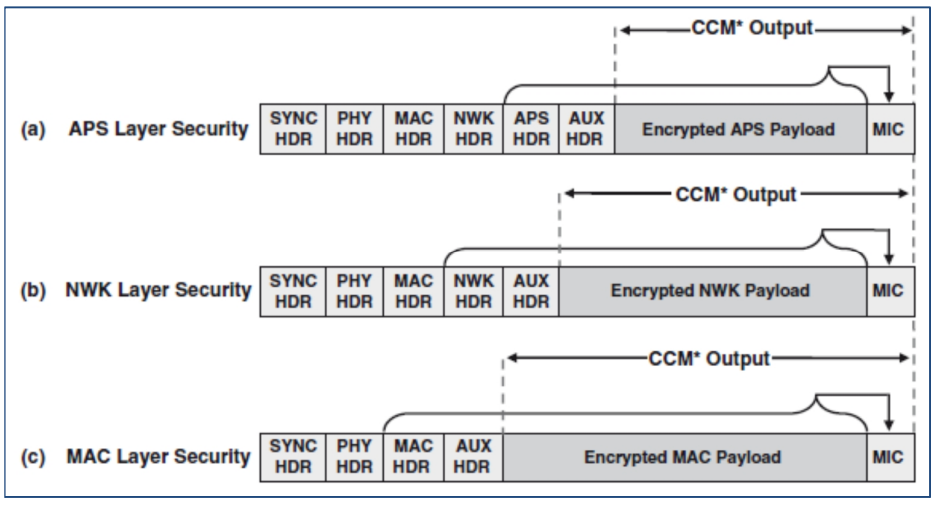


Figura 1.25: Tramas de seguridad en las capas NKK, APS y subcapa MAC [11]

- **Establecimiento de claves**: La subcapa APS provee servicio de establecimiento de claves. El establecimiento de claves involucra dos entidades; dispositivo iniciador y dispositivo receptor.

  La información de confianza (por ejemplo, la clave maestra), provee un punto de inicio para el establecimiento de claves de enlace mediante los siguientes pasos:

  - ✓ Intercambio de datos fugaces.
  - ✓ Uso de datos efímeros para obtener claves de enlace.
  - ✓ Confirmación que la clave de enlace fue procesada correctamente.

- **Transporte de claves**: Los comandos de transporte seguro de claves proveen un medio de transporte de claves: maestra, enlace o red desde una fuente segura (por ejemplo el Centro de Confianza) a otro dispositivo. Los comandos de transporte no seguro de claves proveen un medio para cargar a un dispositivo con una clave inicial, estos comandos no protegen con criptografía la clave al inicio de la carga, en este caso, la seguridad del transporte de clave puede ser realizado por un medio no criptográfico.

- **Actualización de dispositivos**: Proveen un medio seguro a un dispositivo (por ejemplo, un router), para informar a un segundo dispositivo (por ejemplo, el Centro de Confianza) que un tercer dispositivo ha tenido un cambio de estatus y debe ser actualizado (por ejemplo; un dispositivo sea unido o ha abandonado la red). Este es el mecanismo por el cual el Centro de Confianza mantiene una lista precisa de dispositivos de red activos.

- **Eliminar dispositivos**: Permite informar a un dispositivo que un dispositivo asociado a él debe ser eliminado de la red.

- **Petición de clave**: Solicita de forma segura una clave de red activa, o una clave maestra de aplicación extremo-extremo desde otro dispositivo (por ejemplo, su Centro de Confianza).

- **Cambio de clave**: EL servicio de cambio de clave provee un medio seguro a un dispositivo (por ejemplo, un centro de confianza), para informar a otro dispositivo que debe cambiar a una clave activa de red diferente.
- **Autenticación de entidades**: Permite sincronizar información con otro dispositivo, mientras que simultáneamente proporciona autenticidad basado en una clave compartida.

1.3.7 ÁREAS DE APLICACIÓN [2] [3] [4]

Actualmente un gran número de las empresas que forman parte de la *ZigBee Alliance* y se encuentran desarrollando productos que van desde electrodomésticos hasta teléfonos celulares, con control ZigBee. En la Figura 1.26 se presentan los grupos más dominantes de aplicaciones que están en la mira de ZigBee. Hay que tener en cuenta que ZigBee está diseñado para aplicaciones que transmiten baja tasa de datos, que es el caso de automatización. Al usar esta tecnología no habría la necesidad de cablear los interruptores, los cuales podrían ser cambiados de un lugar a otro con plena libertad, pudiendo por ejemplo, prender o apagar las luces de una casa a través de Internet o utilizando un teléfono celular en cualquier momento.

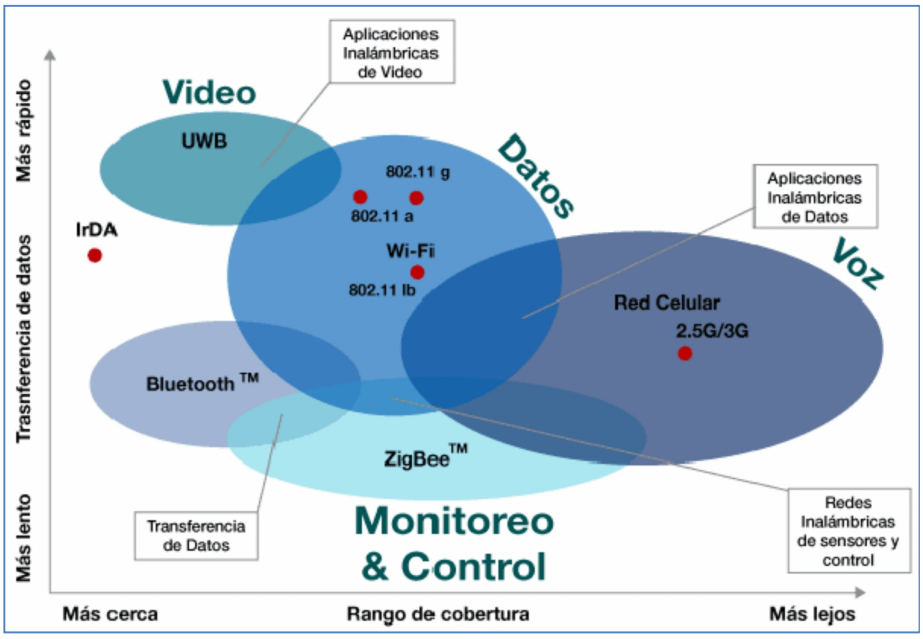


Figura 1.26: Grupos de aplicaciones que están en la mira de ZigBee [2]

El objetivo de ZigBee es adaptarse a redes estáticas, escalables y con muchos dispositivos, pocos requisitos de ancho de banda, uso infrecuente, y se requiera una duración muy prolongada de la batería.

Para aplicaciones de automatización es una buena alternativa en relación a otras tecnologías inalámbricas ya consolidadas en el mercado, como Wi-Fi y Bluetooth.

1.3.7.1 Hogares Automatizados

Los hogares automatizados permiten tener aplicaciones tales como:

- Control de luminarias: ZigBee habilita el encendido y apagado de luminarias por medio inalámbrico y automático.
- Los termostatos y controles de aire acondicionado pueden ser colocados en cualquier lugar libre de utilizar algún tipo de cableado.
- Sensores de movimiento, cerraduras electrónicas de seguridad con solo presionar un botón.
- Detectores de CO_2.

Comparación de Tecnologías Inalámbricas						
	Wi-fi 802.11 b/g	Bluetooth	ZigBee	UWB (Ultra Wide Band)	Wireless USB	IR Wireless
Tasa de Transferencia	11 & 54 Mbps	1Mbps	250 Kbps (2,4 Ghz) 40 Kbps (915 Mhz) 20 Kbps (868 Mhz)	100 - 500 Mbps	62,5 Kbps	20 - 40 Kbps 115 Kbps 4 & 16 Mbps
Rango de Nodos Internos	100m	10 - 100 m	10 - 100 m	< 10 m	10 m	< 10 m (linea de vista)
Topologías	Estrella	Estrella	Estrella, Árbol, mesh	Punto a punto	Punto a punto	Punto a punto
Frecuencias de Operación	2,4 Ghz	2,4 Ghz	2,4 Ghz 868/915 Mhz	3,1 - 10,6 Ghz	2,4 Ghz	800 - 900 nm
Consumo de Baterías	Horas de Batería	Días de Batería	Años de Batería	Meses	Meses	Meses
Acogimiento del Mercado	Alto	Medio	Bajo	Bajo	Bajo	Bajo
Aplicaciones	Edificio con Internet dentro	Computadores y teléfonos	Control de Bajo Costo y Monitoreo	Streaming de video Aplicaciones de entretenimiento de hogar	Conexiones de periféricos de PC	Control remoto, PC, PDA, phone enlaces para laptop
Número de Canales	11 - -14	79	16 (2,4 Ghz) 10 (915 Mhz) 1 (868 Mhz)	Alrededor de 14 canales dependiendo de la frecuencia central	De 4 - 16 canales	De 10 - 11 canles
Latencia	3 *seg*	10 *seg*	30 *mseg*	menor a 1 *mseg*	8 - 20 *mseg*	0,5 - 3,3 *mseg*
Numero de Dispositivos(teóricos)	32	8	255/6535	-------	127	2
Seguridad	128 AES plus aplicación layer security	64 y 128 bits encyption	Claves de cifrado de 128 bits	Compatible con protocolos de cifrado de 256 bits	Cifrado AES-128bits Autenticacion RSA SHA-256 bits	Norma ANSI 7,8
Consumo de Energía	400 mA transmitiendo 20 mA en reposo	400 mA transmitiendo 0,2 mA en reposo	30 mA transmitiendo 3 mA en reposo	es del orden de menos de 1/2 mW	20 dBm	9 Votios 30 - 350 mA
Precio	Costoso	Accesible	Bajo	Bajo	Accesible	Accesible
Complejidad de Dispositivos	Complejo	Complejo	Simple	Medio	Simple	Simple

Figura 1. 27: Comparación de tecnología ZigBee [4] [6] [13] [14]

CAPÍTULO 2

2.1 REQUERIMIENTOS Y DISEÑO DE LA SOLUCIÓN

El objetivo del Sistema es brindar un mecanismo de seguridad al domicilio, en lo que respecta a la prevención de robos, ahorro de consumo de energía ante otros sistemas y también a evitar problemas de salud provocados por gases nocivos dentro del hogar.

Para el desarrollo del Sistema de Seguridad, se toma como referencia una casa modelo de una planta de construcción (Figura 2.1), misma que tiene las siguientes características: Una sala, un comedor, una cocina, un baño, tres dormitorios (uno principal) y un patio delantero.

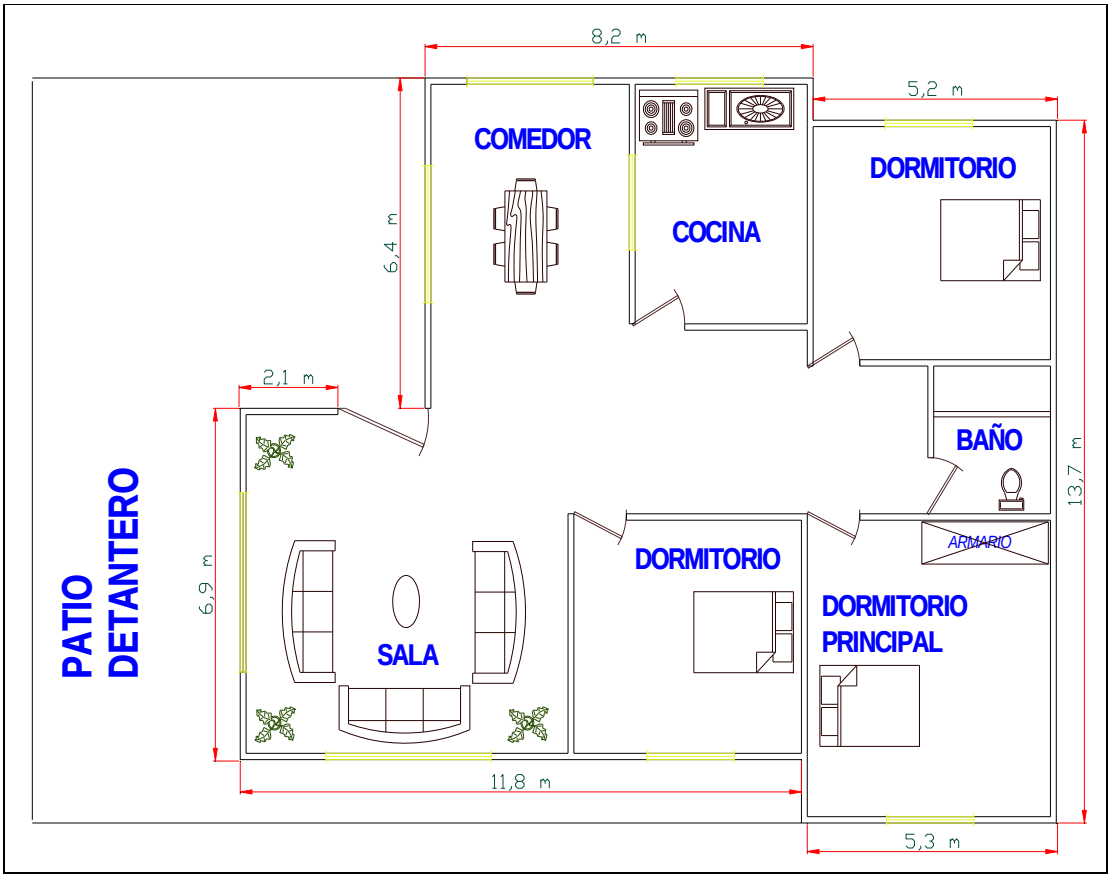


Figura 2.1: Plano estructural casa modelo

Dentro del domicilio modelo se establecerá un sistema de seguridad con video vigilancia que permita el para monitoreo en la noche y cuando los integrantes del hogar no se encuentren. Adicional se establecerá control de luminarias en el domicilio para ahorro del consumo de energía y con la intensión de simular presencia, encendiendo o apagando luces desde un sitio remoto, con acceso a internet.

El sistema de video vigilancia al monitorear el domicilio en la noche y cuando los usuarios no se encuentren en el hogar requiere de un mecanismo de alerta para grabar video activado por la presencia de movimiento, evitando grabaciones que no presenten información significativa. Al momento de detección de movimiento es necesario informar a las personas autorizadas sobre el acontecimiento, mediante un mensaje SMS y vía e-mail.

Se implementarán mecanismos de detección de gas nocivo para alertar a los integrantes de domicilio y evitar afecciones de salud que pueden presentarse.

El sistema hará uso de las instalaciones eléctricas del domicilio modelo para agilizar la implantación del mismo y abaratar costos.

La comunicación entre los dispositivos será inalámbrica, ya que se usará la tecnología ZigBee[29], puesto que esta utiliza bajo consumo de energía, opera en banda de frecuencia libre, alcance óptimo dentro del domicilio y su trasmisión no es muy afectada por otras tecnologías inalámbricas, debido al bajo volumen de datos.

Para el control del domicilio y alertas mediante el envío de e-mail es necesario que el sistema tenga acceso a Internet. Para el envío de alertas SMS se requiere contar con un dispositivo móvil de una operadora celular.

El acceso a Internet será ofrecido por un proveedor del servicio, el mismo que proporcionará el equipamiento para dicho acceso, pero se debe tomar en cuenta que el servicio prestado por el operado permita acceder al sistema desde la *web*.

[29] Ver Capítulo 1 sección 1.3

Para la administración del sistema de seguridad en el del domicilio se desarrollará una aplicación en la *web,* el mismo en el que se podrá realizar monitoreo de cámaras de video, gestión de usuario, así como, el control del encendido y apagando de luminarias para ahorro de consumo de energía y simulación de presencia.

El ingreso y transporte de datos contará con seguridad, debido a la confidencialidad de la información que manejará el sistema de seguridad.

Para el funcionamiento del sistema se consideran los siguientes bloques de elementos:

- Bloque de Adquisición de Datos (BAD)
- Bloque de Comunicaciones (BC)
- Bloque de almacenamiento y Gestión de la Información (BAGI)
- Bloque de Visualización de la Información (BVI)

En la Figura 2.2 se muestra un esquema básico del planteamiento global de la solución.

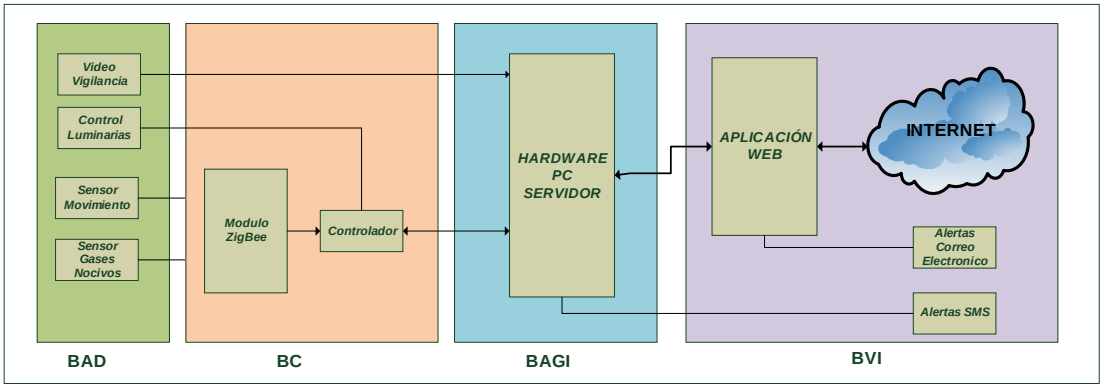


Figura 2.2: Diagrama básico del Sistema de Seguridad Domiciliario

2.1.1 BLOQUE DE ADQUISICIÓN DE DATOS (BAD)

Este bloque incluye todos los elementos capaces de generar información como: la visualización del sistema de video vigilancia, encendido y apagado de luminarias,

control de intrusos (sensores de movimiento) y prevención de problemas de salud (sensores de gas).

Los dispositivos y componentes requeridos para el funcionamiento del Sistema son:

a . Cámara de vigilancia

b . Sensores de movimiento

c . Sensores de gas

d . Luminarias.

2.1.2 BLOQUE DE COMUNICACIONES (BC)

Dentro de este bloque se establece el funcionamiento y elementos que permitirán el transporte de la información obtenida en el bloque anterior, es decir la información del video obtenido por las cámaras, la información de los sensores y control de luminarias.

El bloque de comunicaciones será el encargado de transportar la información de las cámaras, sensores y microcontrolador al sistema para gestionar los datos obtenidos en el BAGI

Dentro de este bloque se toma en cuenta los siguientes elementos.

a . Módulos ZigBee

b . Micro controlador

2.1.3 BLOQUE DE ALMACENAMIENTO Y GESTIÓN DE LA INFORMACIÓN. (BAGI)

En este bloque se especifica los requerimientos para el funcionamiento del aplicativo, que es el encargado de interpretar la información obtenida por los bloques anteriores

El aplicativo del Sistema de Seguridad Domiciliario permite la visualización de cámaras de video, control de luminarias, presentando un interfaz amigable y de fácil utilización.

El objetivo del Sistema es ofrecer un mecanismo de seguridad del domicilio, accesible, de libre acceso para desarrollar procesos y sin necesidad de adquisición de licencias razón por la que se considera el uso del Sistema Operativo Linux.

La implementación de este bloque comprende lo siguiente:

- Servidor del Sistema
- Desarrollo del aplicativo *web* del sistema.

2.1.4 BLOQUE DE VISUALIZACIÓN DE LA INFORMACIÓN (BVI)

Este bloque se encarga de entregar al usuario final la información gestionada por el bloque anterior por medio de mensajes SMS, y al correo electrónico de las personas autorizadas.

La implementación de este bloque tiene como objetivo:

- Visualización de alertas por SMS
- Visualización de alertas por correo electrónico

2.2 DISEÑO Y DESARROLLO DE LA SOLUCIÓN

Para el diseño y desarrollo de la solución se toma como referencia los bloques antes descritos:

- Bloque de adquisición de datos
- Bloque de comunicaciones
- Bloque de almacenamiento y gestión de la información
- Bloque de visualización de la información

2.2.1 DISEÑO DEL BLOQUE DE ADQUISICIÓN DE DATOS

Como se indicó con anterioridad dentro de este bloque se consideran cámaras, control de luminarias, sensores de movimiento y gas nocivo.

Para el uso de cámaras se debe considerar un sistema de vigilancia asociado al mismo. A continuación se describen los diferentes sistemas de video vigilancia que se aplicarían al sistema como también se analizara la mejor opción a ser aplicada al sistema.

2.2.1.1 Video Vigilancia *[15]*

El módulo de vigilancia tendrá como función el monitoreo del domicilio, a través de cámaras de video. La implementación del sistema de seguridad domiciliario puede realizarse con tecnología analógica o digital. A continuación se describe de manera general estas tecnologías.

a . Sistema analógico de video vigilancia

Los sistemas de vigilancia analógicos se basan en un circuito cerrado de televisión CCTV.

Figura 2.3: Video Vigilancia Analógico[30]

[30] Imagen de la web: Sistema de Vigilancia Analógico con DVR

- **Componentes:**

  El sistema de circuito cerrado de televisión consta de los siguientes componentes:

  - ✓ Medio de captación de imágenes (cámaras).
  - ✓ Equipos para visualización de imágenes (monitores).
  - ✓ Medio de transmisión (Cable coaxial).
  - ✓ Equipos de almacenamiento (DVR).

Características:

Dentro del sistema de video vigilancia analógica y los componentes que maneje se considera las siguientes características:

- DVR
  - ✓ 8 canales H.264 DVR de Vigilancia
  - ✓ MPEG4 de compresión de hardware
  - ✓ Video de entrada / salida: BNC 8 / BNC 1
  - ✓ Entrada / Salida de audio: RCA 4 / BNC 1
  - ✓ Salidas de vídeo: BNC y salida de monitor VGA PC
  - ✓ Sistema de señal: NTSC / PAL
  - ✓ Muestra: 240 fps[31]
  - ✓ Record: 240 fps
  - ✓ Acceso remoto: Internet Explorer
- Cables CCTV y de Video Cables (VGA) de envío de información
- Fuente individual de alimentación 12V/1500mA para cámaras de seguridad
- Características de la cámara
  - ✓ 480 líneas de TV, Horizontal
  - ✓ Lente de 3.6mm
  - ✓ Visión nocturna mínima de 0 Lux (IR On)

[31] Fps: Cuadros de imagen por segundo

- ✓ Temperatura de funcionamiento: -25 ° F a 122 ° F
- ✓ Energía: 12V DC
- ✓ Montaje: Pared
- ✓ Video Conector: BNC

La alternativa propuesta con un sistema de video vigilancia analógica en la casa modelo (Figura 2.1), considera la instalación de cámaras de vigilancia en sitios estratégicos del domicilio, donde permitan la visualización de los lugares de acceso al domicilio como son: puertas y ventanas. Tomando en consideración estos sitios se requiere la adquisición de 5 cámaras de seguridad para ser ubicadas en:

- ✓ 1 en la puerta principal
- ✓ 1 en la sala para monitoreo de las ventanas
- ✓ 1 en el pasillo para visualización de la entrada a los dormitorios
- ✓ 1 en la cocina
- ✓ 1 en el comedor

Lugares en los cuales se obtendrá imágenes de personas que ingresen al domicilio con intenciones de cometer un delito, adicional se debe tomar en cuenta que las cámaras de video deben contar con la resolución de imagen necesaria para el reconocimiento de los delincuentes.

Las cámaras de video vigilancia se ubicarán en el techo del domicilio. La instalación de las cámaras requiere de una conexión física de éstas hacia el DVR, lo que implica un cableado para video vigilancia, como también la conexión eléctrica para cada una de las mismas.

La conexión de las cámaras hacia el DVR debe establecerse con un cable CCTV o coaxial de 75 ohmios (requerimiento mínimo), para cumplir con el estándar ANSI/TIA/EIA 570-B grado 1, donde se provee servicios de: telefonía, satélite, CATV y datos.

En la Figura 2.4 se muestra la solución alternativa del sistema de video vigilancia con tecnología analógica.

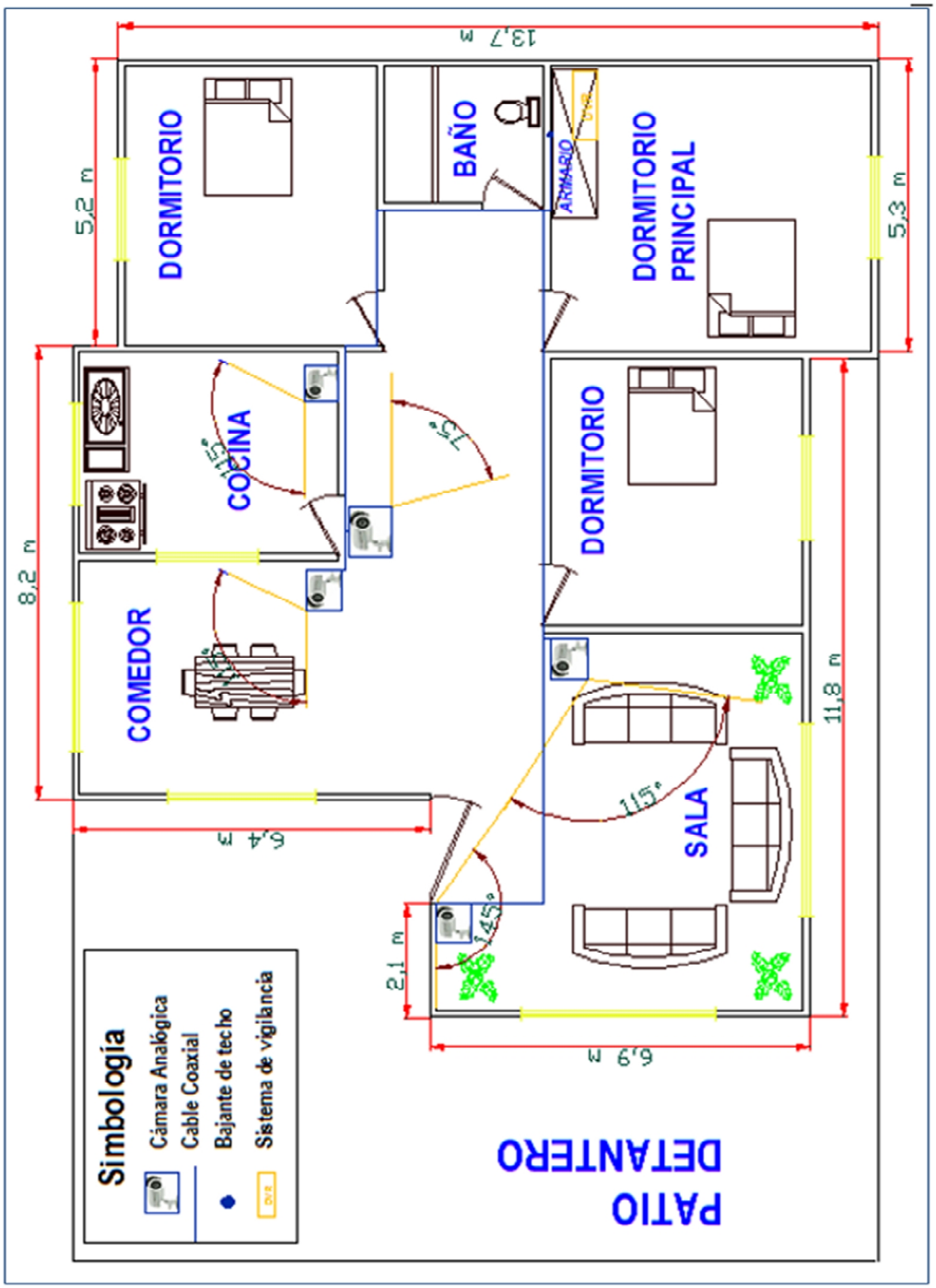


Figura 2. 4: Diseño Sistema Video vigilancia analógico

b . Sistemas Digitales de video vigilancia

El avance tecnológico ha conseguido combinar los beneficios de las cámaras inteligentes y de las imágenes digitales a través de una red, constituyendo un medio de vigilancia más efectivo que su antecesor CCTV. El video en la red ofrece todo lo que un sistema analógico proporciona, y

adicionalmente amplía su funcionalidad (escalabilidad, seguridad, conexión inalámbrica, entre otros).

El video se transmite a través de redes IP cableadas o inalámbricas, así como también el audio también hace uso de la misma infraestructura de red.

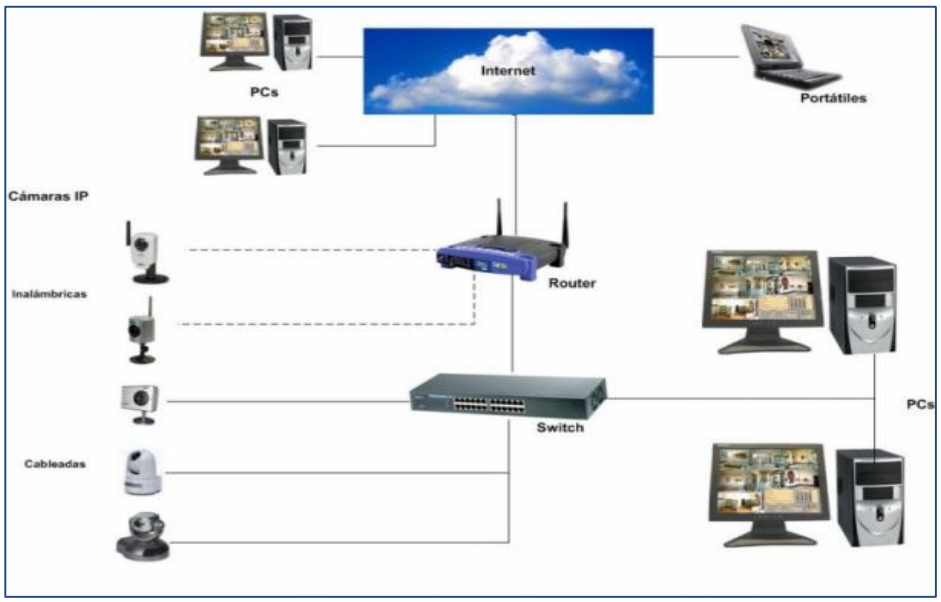


Figura 2.5: Video Vigilancia IP[32]

Esta tecnología utiliza una red IP para transportar video y audio digital, entre otros datos. Adicionalmente es posible proveer el suministro de energía a través del mismo cable de datos, por *Power Over Ethernet* (PoE)[33].

El sistema de vigilancia IP permite grabar video desde cualquier lugar de la red interna o remotamente.

- **Componentes:**

  Los componentes de un sistema de vigilancia digital son:

[32] Imagen de la web: Sistema de Vigilancia IP

[33] PoE permite a los dispositivos en una red recibir alimentación eléctrica por uno de los pares del cable UTP proporcionado directamente del equipo activo (*switch*), todo a través del cable Ethernet que transporta video.

- ✓ Cámara de red.
- ✓ Infraestructura de red (cableada o inalámbrica).
- ✓ Servidor (Almacenamiento de video).

- **Características:**

  Las principales características de un sistema de video vigilancia digital son:

  - ✓ Accesibilidad remota a cada cámara IP para vigilancia individualizada e iguales características a las solicitadas en la sección de video vigilancia analógica.
  - ✓ Posibilidad de integración con sistemas analógicos por si se necesita combinar con sistemas ya instalados.
  - ✓ Posibilidad de incrementar el número de cámaras, dependiendo de la capacidad del enlace ya existente en el hogar.
  - ✓ Seguridad en la información a través de codificación WPA
  - ✓ Almacenamiento seguro y mejorado por medio de bases de datos, con acceso restringido y con claves de usuario.
  - ✓ Dispositivos inalámbricos con alcances de 5 a 20 metros dependiendo de la necesidad requerida.

La propuesta alternativa con un sistema de video vigilancia IP considera dos escenarios: con medio de transmisión cableada (cable UTP) y medio de trasmisión inalámbrico.

i. <u>Utilizando medio de transmisión cableado</u>

Dentro de la implementación del sistema de video vigilancia, el medio físico de conexión de las cámaras utilizará cable UTP categoría 5e, para cumplir la norma ANSI/TIA/EIA 570-B grado 1, un servidor de almacenamiento. Además un switch de comunicaciones para la conexión física de las cámaras y el servidor.

El switch de comunicaciones debe contar con un mínimo de 7 puertos de red para: 5 cámaras IP, conexión del servidor de almacenamiento y acceso a la red.

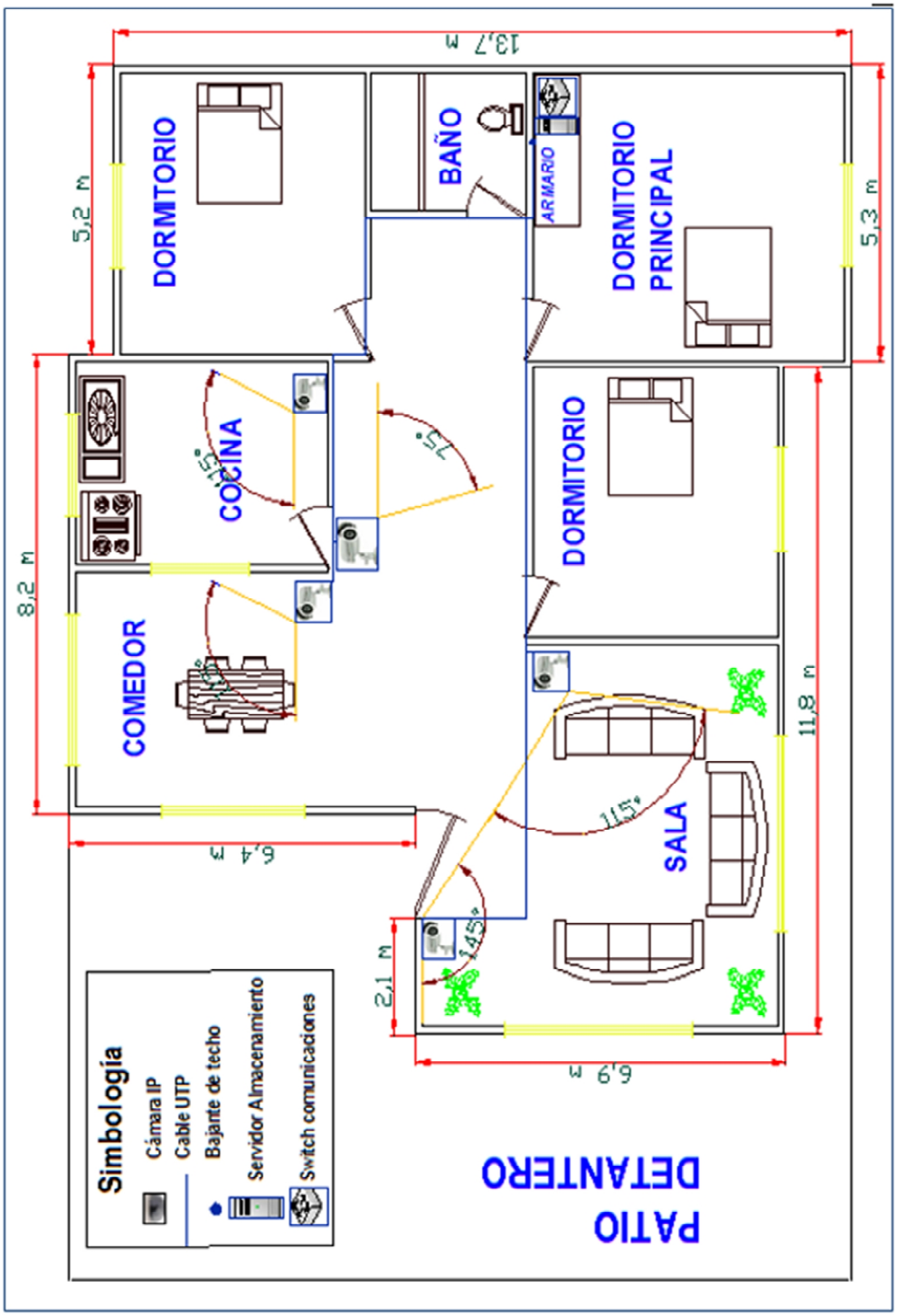


Figura 2. 6: Diseño Sistema de video vigilancia IP cableado

La implementación del sistema de vigilancia con tecnología IP cableada requiere los siguientes elementos:

- ✓ 5 cámaras IP.
- ✓ Cable UTP categoría 5e (cable de mínima categoría) para la conexión de las cámaras.
- ✓ Switch de comunicaciones con un mínimo de 5 puertos libres.
- ✓ Servidor de almacenamiento para las grabaciones.
- ✓ Alimentación eléctrica para las cámaras en caso de no soportar PoE.
- ✓ No se considera la instalación de un rack de comunicaciones ya que esto representaría un costo adicional al usuario final como también la adecuación de un sitio en el domicilio.

En la Figura 2.6 se muestra la solución alternativa del sistema de video vigilancia con un sistema IP cableado.

ii. Utilizando medio de transmisión inalámbrico

El planteamiento del sistema de video vigilancia IP con medio de transmisión inalámbrico considera; el diseño IP sin la instalación del cable UTP, adicional se reemplaza del switch de comunicaciones por un punto de acceso inalámbrico para conexión de las cámaras.

El punto de acceso inalámbrico trabajará con las cámaras IP inalámbricas en la bands de frecuencia libre 2,4 GHz.

El dispositivo de acceso inalámbrico debe considerar; seguridad en el transporte de información en el medio, evitando visualización y alteración de la información transmitida.

La ubicación del punto de acceso inalámbrico será en el dormitorio principal con el servidor de almacenamiento.

La implementación del sistema de vigilancia con tecnología IP inalámbrica difiere del sistema cableado en el medio de transmisión.

La solución del sistema de video vigilancia IP inalámbrico se muestra en la Figura 2.7

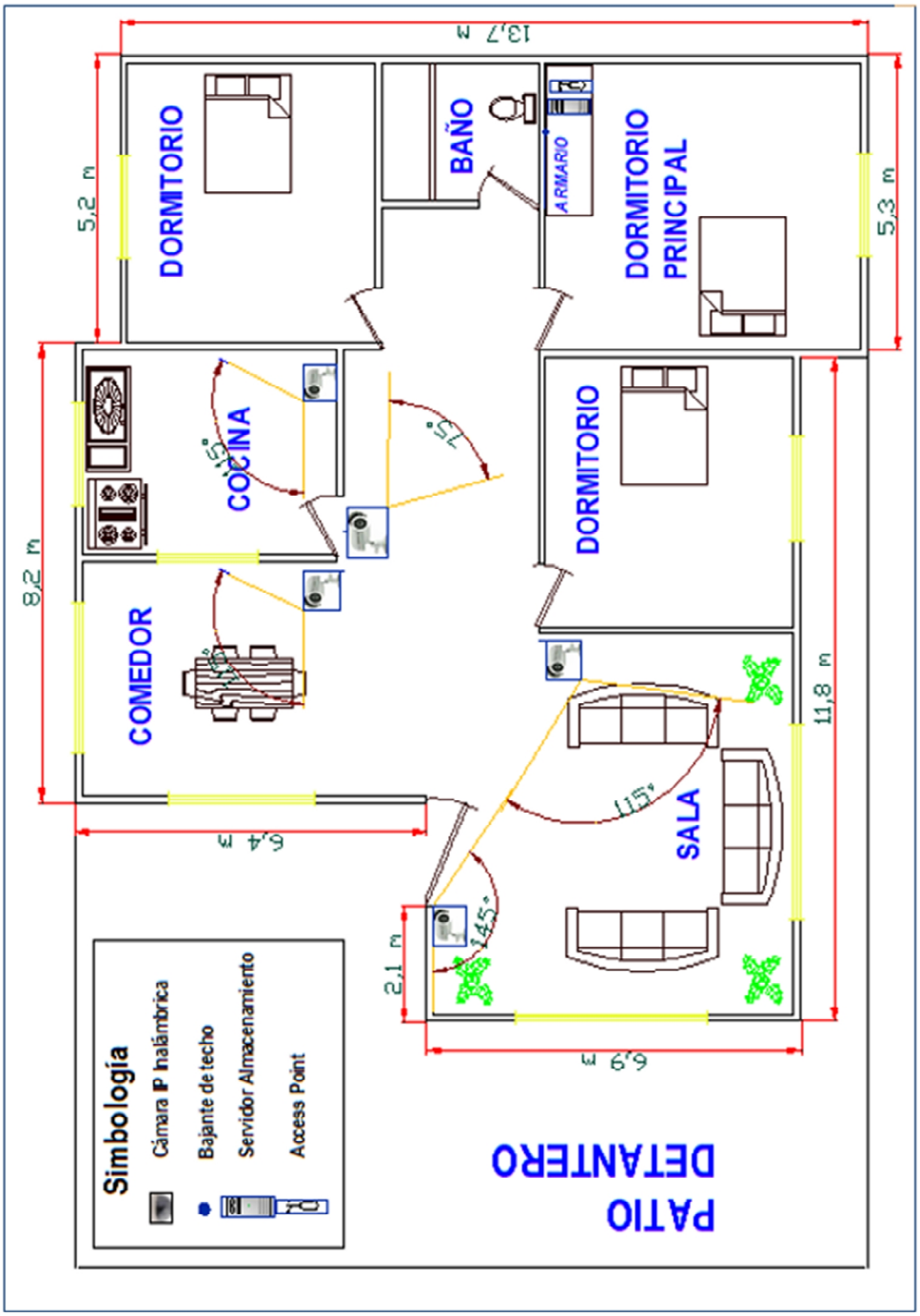


Figura 2. 7: Diseño Sistema de video vigilancia IP inalámbrico

- **Conclusión y elección de la solución**

  Por las ventajas que presenta un sistema de video vigilancia IP inalámbrico como:

  - ✓ Menor trastorno: al haber menos cableado que instalar, los plazos de los proyectos se acortan considerablemente y se reducen al mínimo las interrupciones en las actividades; adicional no se requiere instalaciones extras como tuberías o canaletas para cables.
  - ✓ Escalabilidad y migración: los sistemas de vigilancia anteriores pueden ampliarse fácilmente, utilizando vídeo por IP inalámbrico, lo que proporciona una solución rentable para la migración a sistemas totalmente digitales.
  - ✓ Costos: El costo de implementación de un sistema inalámbrico y un cableado son similares al comparar los gastos de instalación y equipos utilizados. Pero para un sistema cableado; se debe tomar en cuenta en el escenario planteado, el costo de cableado estructurado para puntos de red, necesarios para el funcionamiento del sistema. Ver Anexo I-1, lo que implica un aumento en los valores de implementación del sistema.

  Teniendo en consideración las ventajas mencionadas, se considera al sistema inalámbrico el más adecuado a ser implementado.

  Acorde a las consideraciones anteriores se selecciona al sistema con tecnología IP a ser implementado y con visión a futuro se establece el medio de transmisión inalámbrico para permitir escalabilidad sin instalaciones adicionales.

- **Dimensionamiento de *hardware de video vigilancia***

  Con la ayuda de la herramienta AutoCad, se construye el plano estructural de la casa modelo; considerando dimensiones reales de una casa. En función de estas medias se logra conseguir los ángulos de cobertura

requeridos por las cámaras IP, para visualizar los diferentes sitios del domicilio donde se consideró la ubicación de las cámaras.

Para la implementación del sistema de video vigilancia IP inalámbrico se consideran los dispositivos con las siguientes características.

- ✓ 3 cámaras IP inalámbricas indoor, con un ángulo mínimo de cobertura de 115°. Para visualización de: Sala, comedor, Cocina.
- ✓ 1 cámara IP inalámbrica indoor, con un ángulo mínimo de cobertura de 145°. Para visualización de la parte externa del domicilio.
- ✓ 1 cámara IP inalámbrica indoor, con un ángulo mínimo de cobertura de 75°. Para visualización del corredor de ingreso a los dormitorios.
- ✓ Conexión inalámbrica en la frecuencia 2,4 GHz.
- ✓ La resolución de las cámaras debe permitir distinguir las imágenes que se muestren, acorde a esto se presenta un ejemplo de resolución de cámaras en la figura 2.8.

  En base a las imágenes mostradas se tomó como valor mínimo de con resolucion 640x480 pixeles, con lo cual ser podrá distinguir las personas que ingresen al domicilio sin autorización.

Figura 2.8: Resolución de imágenes

- ✓ Luminiscencia mayor a 25(Lux), adecuada para un ambiente indoor en un domicilio (Dato obtenido de Consejo Superior de Investigaciones Científicas CSIC).
- ✓ Las cámaras IP deben contar con los protocolos: IPv4, DHCP, HTTP, para conexión y administración de las mismas dentro de la red.
- ✓ Las cámaras IP deben soportar protocolo RTSP[34] para visualización de video en tiempo real.
- ✓ Las cámaras IP deben manejar protocolos, FTP o cliente Samba, para grabación de video en un servidor centralizado.
- ✓ Las cámaras IP deben permitir seguridad en la trasmisión inalámbrica de datos, con lo cual ser obtendrá protección en los datos transmitidos. Dentro de la seguridad inalámbrica se tiene protocolos de seguridad como WEP (*Wired Equivalent Privacy*) y WPA (*WiFi Protected Access*)
- ✓ Detección de movimiento, con el objetivo de no llenar al servidor con grabaciones continuas de video las 24 horas del día, la cámara debe incluir activación de grabación por movimiento donde se muestren imágenes significativas de intrusiones al domicilio. Para esta característica se debe considerar al menos una distancia de 4,5 metros en función de los requerimientos del domicilio.

Para la elaboración del prototipo de prueba se emplearán dos cámaras IP inalámbricas que cumplan con los requerimientos mínimos del sistema de video vigilancia.

[34] RTSP *Real Time Streaming Protocol*: En un protocolo a nivel de aplicación para el control de la entrega de datos en tiempo real como audio y video. Basado en el RFC 1889.

CÁMARAS DE VIDEO VIGILANCIA			
Características mínimas	**Axis M1033-W**	**D'Link DCS 2121**	**TRENDnet TV-IP572W**
Alimentación Eléctrica 110 V	SI	SI	SI
Protocolos: IPV4, DHCP client, HTTP.	SI	SI	SI
Protocolos, RTSP, FTP, Samba	SI	SI	SI
Luminiscencia mayor 25 lux	SI	SI	SI
802.11 b/g/n	SI	SI	SI
Seguridad WPA	SI	SI	SI
Sensor de movimiento (Alcance mayor a 4,5m)	SI	SI	SI
Resolución mínima 8 KBytes	SI	SI	SI
Precio + IVA	$ 280	$ 120	$ 150

Tabla 2.1: Cámaras IP del mercado

De la Tabla 2.1; se selecciona la cámara D'Link DCS 2121 (Anexo A), por cumplir con los requerimientos mínimos necesarios para el sistema de video vigilancia y ser la de menor valor en el mercado.

2.2.1.2 Detección de Intrusos *[16] [17] [18]*

El Sistema de Seguridad Domiciliario tiene la funcionalidad de permitir la detección de intrusos evitando el robo del domicilio, mediante sensores de movimiento que se instalarán en el domicilio. Existen diferentes tecnologías de sensores de movimiento entre las que se puede mencionar:

- **Sensor de movimiento CMOS**

  Los sensores *Complementary-Metal-Oxide-Semiconductor* CMOS, captan cargas producidas por la luz, de tal manera, que cada píxel individual tiene se ve amplificado y se le asigna un valor digital.

  - **Características:**
    - ✓ Bajo consumo eléctrico.
    - ✓ Tecnología altamente desarrollada.
    - ✓ Económico (necesita pocos componentes externos).
    - ✓ Lectura simultánea de mayor número de pixeles.
    - ✓ El conversor digital puede estar integrado en el mismo chip.
    - ✓ Los pixeles pueden ser expuestos y leídos simultáneamente.

  Los sensores CMOS se basan en el cambio de luminosidad para la detección de movimiento, esto puede representar un inconveniente ya que se pueden producir falsas alarmas “disparadas” por el sensor, por ejemplo encender una luminaria al abrir la puerta, entre otros.

- **Sensores de movimiento PIR**

  Estos sensores no emiten radiación, solo reciben "pasivamente" la radiación infrarroja proveniente de cuerpos a temperatura superior al ambiente (todo cuerpo caliente emite radiación infrarroja). Este principio se aprovecha para detectar la presencia de personas sensando la radiación emitida por las mismas.

  Una variación térmica de todo el ambiente en su conjunto no indicaría la presencia de una persona como tampoco lo haría la variación de temperatura de un cuerpo. Para evitar disparos no deseados, los detectores en su interior poseen en realidad dos elementos sensibles, conectados en oposición de manera que su potencial se cancela cuando la variación térmica los afecta a ambos por igual.

- **Características:**
  - ✓ Bajo consumo de energía (5 Voltios DC)
  - ✓ Tecnología altamente desarrollada
  - ✓ Disuasión[35]

  El tipo de sensores PIR al detectar un cambio de calor evitará las falsas alertas provocadas por el cambio de luminosidad, aunque existirán falsas alarmas incitadas por mascotas dentro del domicilio.

- **Planteamiento de la solución**

  La implementación de sistema de detección de intrusos en la casa modelo considera la instalación de sensores de detección de movimiento en sitios estratégicos, por los cuales personas ajenas al domicilio circularían dentro del mismo.

  Tomando en cuenta estos sitios se requiere la adquisición de 8 sensores de movimiento para ser ubicados en:

  - ✓ 1 en la entrada principal.
  - ✓ 1 en la sala del domicilio.
  - ✓ 1 en el comedor del domicilio.
  - ✓ 1 en la cocina del domicilio.
  - ✓ 1 en el pasillo del domicilio.
  - ✓ 3 ubicados uno en cada dormitorio.

Teniendo en consideración los requerimientos de implementación del sistema de detección de movimiento para una casa modelo de: escalabilidad, rango de cobertura suficiente para abarcar el área del domicilio y detección de movimiento en base a calor evitando las falsas alarmas. Se establecerá el sistema de detección de movimiento con sensores PIR.

[35] El sensor se activa con independencia de que la persona detectada sea o no un intruso.

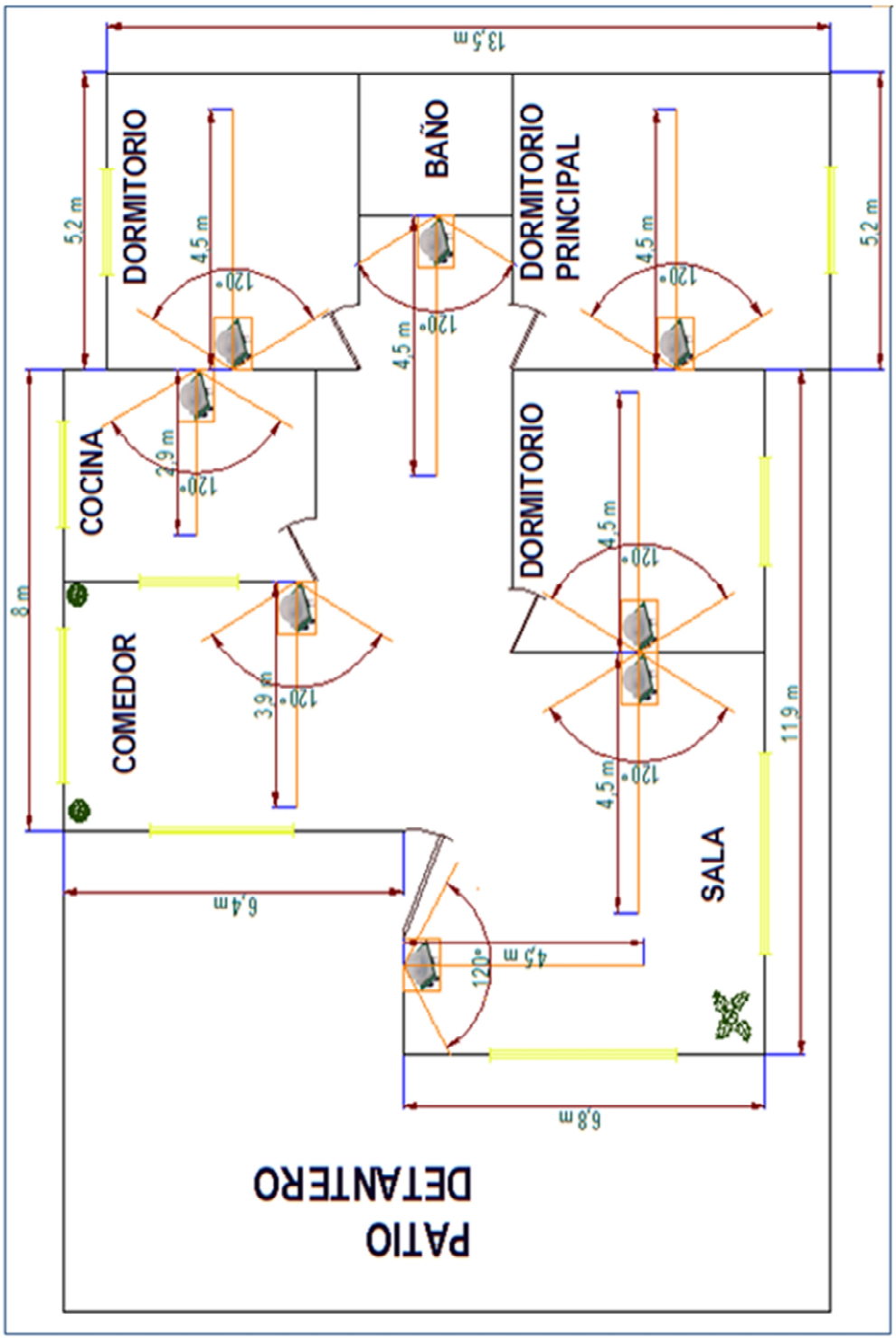


Figura 2.9: Diseño Sistema detección de intrusos

- **Dimensionamiento del *hardware* de detección de intrusos**

  Para la implementación del sistema de detección de movimiento se consideran los sensores PIR para evitar falsas alarmas producidas por

cambios en la luminiscencia, estos sensores deben cumplir los siguientes parámetros de distancia ángulos de cobertura obtenidos con la herramienta AutoCad.

- ✓ 6 sensores con un rango de cobertura mínimo de 4,5 metros y ángulo de 120°, para abarcar: la entrada al domicilio, las habitaciones, el pasillo de acceso a los dormitorios y la sala del domicilio.
- ✓ 1 sensor con rango de cobertura mínimo de 3.9 metros y ángulo de 120°, para controlar el acceso al el comedor del domicilio.
- ✓ 1 sensor con rango de cobertura mínimo de 2.9 metros y ángulo de 120°, con lo cual, ser cubre el acceso a la cocina del domicilio.
- ✓ Sensores alimentados por baterías, para no depender de la energía eléctrica y contar con fuente de alimentación independiente.
- ✓ Ambiente de operación indoor, los sensores es colocará en el interior del domicilio para la detección de intromisión.

En base al dimensionamiento de los sensores de movimiento se elige al sensor PIR 555 – 28027, por cumplir las características técnicas necesarias. (Anexo B) y si bien existen en el mercado otras opciones, la seleccionada es la más fácil de instalar y adecuada para las características necesitadas en función de su tamaño y adecuación con el resto de elementos a utilizarse.

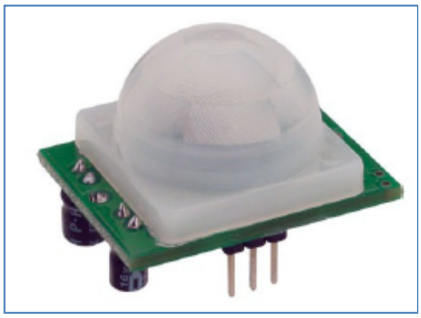


Figura 2.10: Sensor PIR 555 - 28027

Para la elaboración del prototipo de prueba se empleará un sensor de movimiento PIR, ubicado en la sala de la casa, lugar de tránsito obligatorio dentro del domicilio.

2.2.1.3 Detección de gases nocivos

Para evitar problemas de salud provocados por gases nocivos se implementará sensores de detección de gases.

Para la selección de los sensores de gas nocivo es necesario considerar los tipos de gases que se requiere detectar dentro del domicilio. El lugar donde se pueden generar gases nocivos para la salud es en la cocina. Adicional se debe considerar que en la casa modelo puede existir un calefón, razón por la cual también se ve la necesidad de ubicar un sensor en ese lugar.

Los gases comúnmente producidos en la cocina y calefón son:

- ✓ **CO**: En caso de incendio
- ✓ **H_2**: Concentración de ácidos grasosos (aceites comestibles)
- ✓ **LPG (*Liquid Petroleum Gas*):** Concentrado en los cilindros de gas doméstico.

- **Dimensionamiento del *hardware* de detección de gas nocivo**

  Para la implementación del sistema de detección de gas se consideran sensores que permitan evitar la concentración de los gases antes mencionados en concentraciones perjudiciales para la salud humana.

  - ✓ Detección de gas CO mayor a 50ppm (partes por millón) nivel de concentración máximo tolerable para el ser humano.[36]
  - ✓ Detección de gas H_2. mayor a 20ppm máximo nivel tolerable para el ser humano.[36]
  - ✓ Detección de gas LPG mayor a 28 ppm máximo nivel tolerable para el ser humano.[36]
  - ✓ Sensores alimentados por baterías, para no depender de la energía eléctrica y contar con fuente de alimentación independiente.

[36] Datos obtenidos de la Organización Mundial de la Salud

- ✓ Ambiente de operación indoor, el sensor se colocará en el interior del domicilio para la detección de gas.
- ✓ Tiempo de respuesta máximo de 60 segundos, ya que es el tiempo máximo necesario para que exista un problema de salud a causa de los gases nocivos.

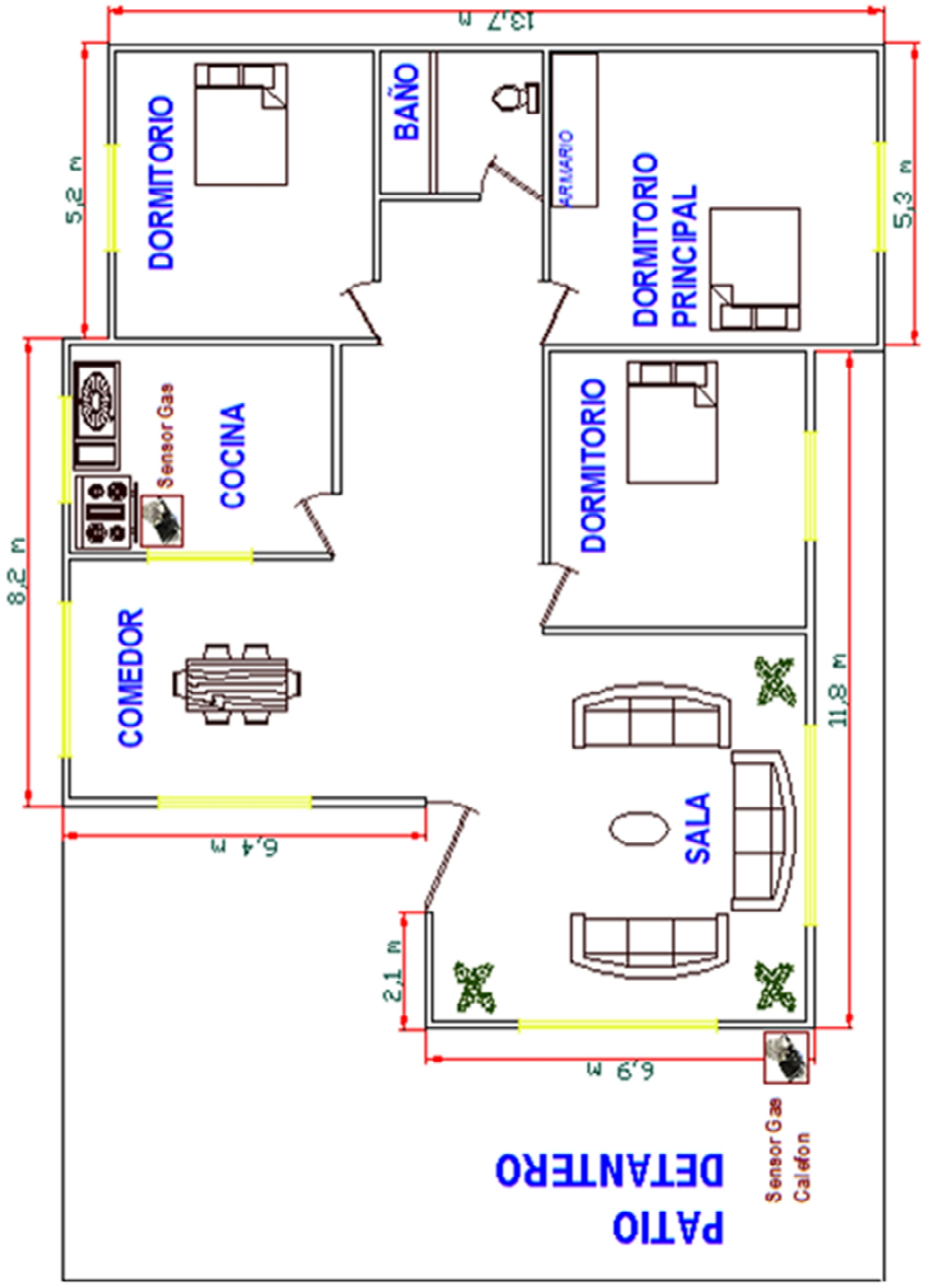


Figura 2. 11: Diseño Sistema detección de gas

En base al dimensionamiento de los sensores de gas se selecciona al sensor MQ5 por cumplir las características técnicas necesarias. (Anexo C).

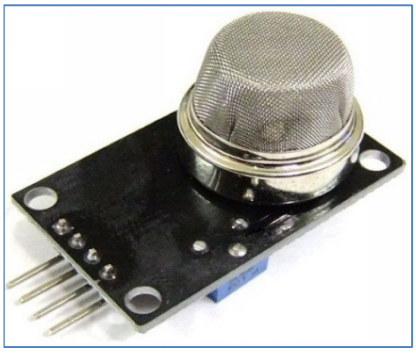


Figura 2.12: Sensor de gas MQ5

2.2.1.4 Control de Luminarias

El sistema gestionará el encendido y apagado de las luminarias del domicilio para ahorro de energía y simulación de presencia.

Este dispositivo de control se comunicará con el aplicativo del Sistema de Seguridad Domiciliario a través de un interfaz serial[37].

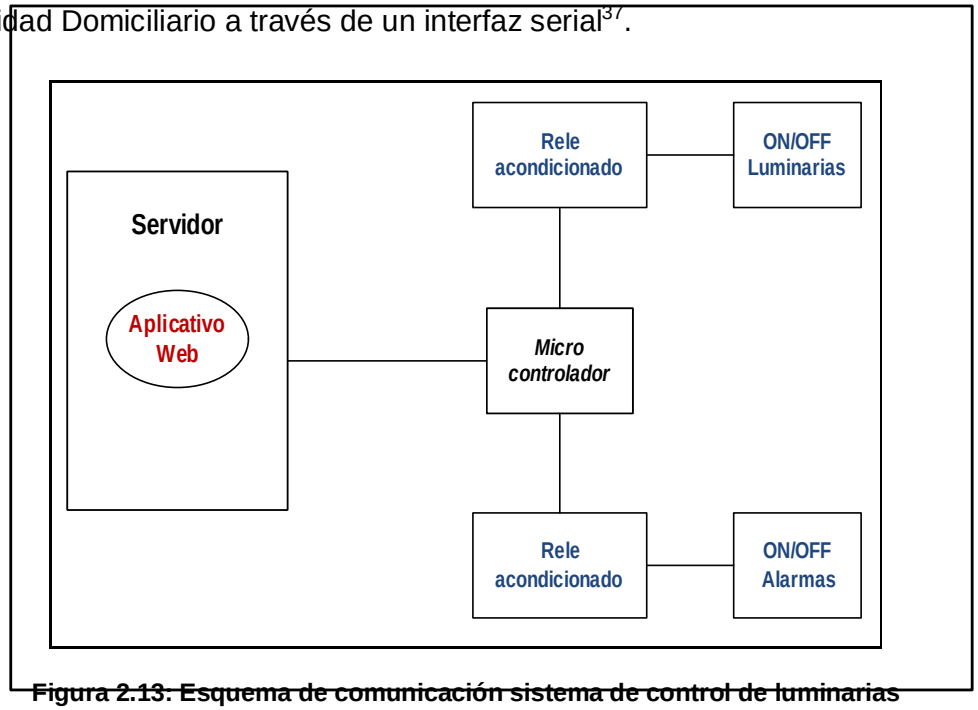


Figura 2.13: Esquema de comunicación sistema de control de luminarias

[37] Comunicación serial proporciona velocidad de transmisión idónea para distancias que no excedan los 15.2 metros. Ref: http://mundopc.net/el-puerto-serie-caracteristicas-y-funcionamiento/

En la Figura 2.14 se muestra la distribución de las luminarias en el domicilio, mientras que en la Figura 2.13 se observa la secuencia lógica del sistema de control de luminarias.

Este dispositivo de control debe permitir una fácil programación para implementar cambios en caso de ser necesario y no dificultar el funcionamiento del Sistema.

Adicional se debe considerar el equipo de potencia necesario para acondicionar las señales del dispositivo de control a la energía eléctrica del domicilio.

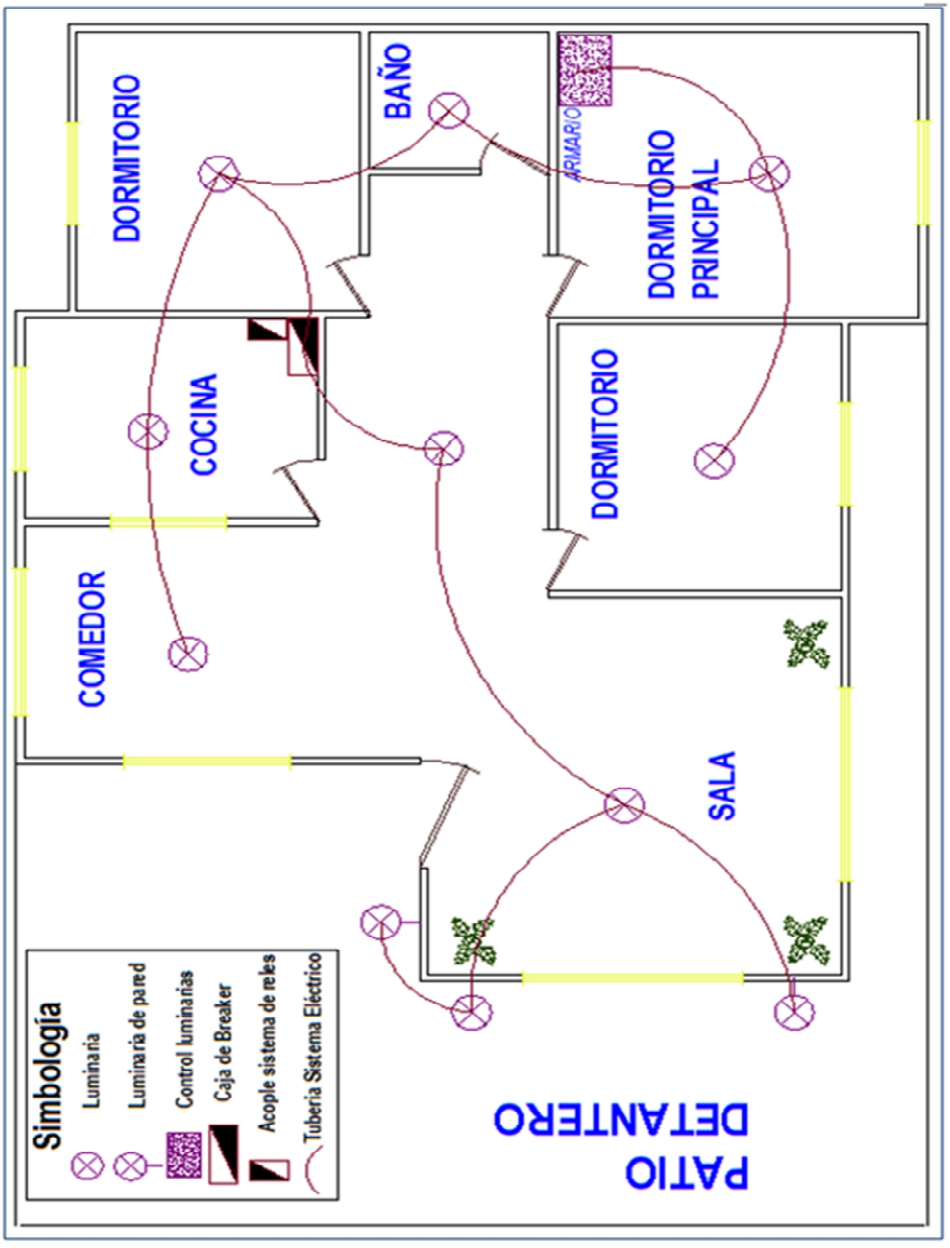


Figura 2. 14 Diseño Sistema control luminarias

- **Dimensionamiento del hardware de control**

  Para el sistema de control de luminarias se debe considerar un micro controlador, encargado de enviar las señales a cada una de las luces del domicilio (10 Luminarias), para las alarmas visual y sonora dentro del domicilio. Adicional este dispositivo es el encargado de recibir los datos obtenidos por los sensores (10 sensores) y enviar la información al aplicativo para gestionar las alertas por mensajes SMS o E-Mail.

  Para el sistema de luminarias se debe adaptar a las señales de control al sistema de energía eléctrico mediante un relé adecuado a 120 voltios. El número de relés depende del número de señales que se pretenda manejar. Con los requerimientos antes mencionados se requiere un micro controlador de las siguientes características:

  - ✓ Operatividad de los pines para entrada o salida de datos.
  - ✓ 10 pines de salida (ON/OFF luminarias), para la gestión de las luminarias del domicilio.
  - ✓ 2 pines de salida (alarmas dentro del domicilio), estos pines gestionaran las alarmas visuales dentro del domicilio.
  - ✓ 10 pines de entrada (datos de los sensores), la adquisición de datos depende del número de sensores que se instalen dentro del domicilio.
  - ✓ Interfaz serial de conexión hacia el servidor para comunicación con el aplicativo.

  El dispositivo de control de potencia:

  - ✓ Adecuar las señales de 5 voltios al sistema eléctrico de 120 voltios.

En la Figura 2.15 se presenta el diagrama de conexión a ser implementado en el prototipo.

Para la implementación del sistema de luminarias en el prototipo de prueba se incluirán 6 leds, que simularán el encendido de las luces dentro del domicilio, también se tomará en cuenta el encendido de un led y parlante que representara la alarma visual y sonora. Para el prototipo de prueba se elige el PIC 16F87XA (Anexo E).

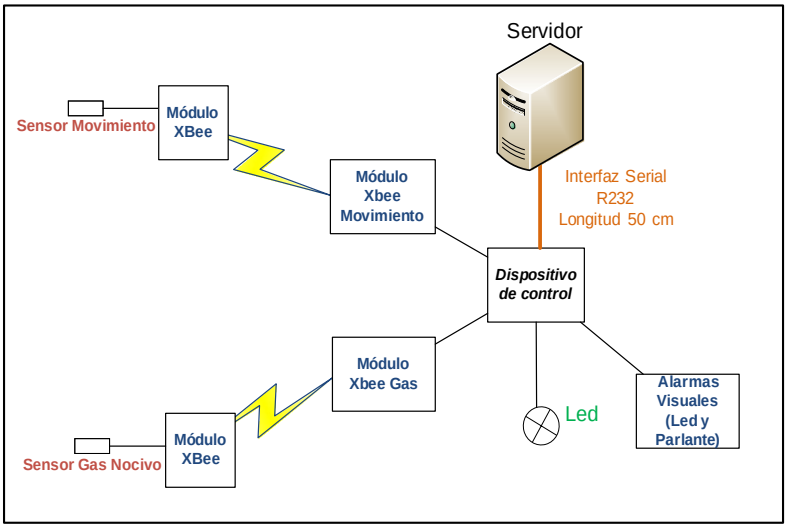


Figura 2.15: Conexión dispositivo de Control para el prototipo de prueba

2.2.2 DISEÑO BLOQUE DE COMUNICACIONES (BC)

La red de conectividad del Sistema de Seguridad Domiciliario tiene dos partes: la red interna del domicilio (LAN) y la red de acceso a Internet /WAN).

La implementación Sistema de Seguridad Domiciliario en la casa modelo cuenta con los siguientes elementos de red: cámaras IP inalámbricas, un punto de acceso AP para la conexión de las cámaras y el servidor del sistema. Como se indicó con anterioridad las cámaras IP se conectarán a la red inalámbricamente, para el servidor del sistema se contará con un punto de red del cableado, como también el AP (*Access Point*).

Para el prototipo de prueba se emplearán 2 cámaras IP, 1 sensor de movimiento y 1 sensor de gas.

La implementación de la red de conectividad comprende lo siguiente:

- Módulos ZigBee
- Transmisión de la información

2.2.2.1 Módulos ZigBee

La comunicación entre los sensores y el módulo de control del sistema se establecerá con dispositivos ZigBee. Los módulos ZigBee serán los encargados de transmitir la información obtenida por los sensores (movimiento y gas nocivo) al dispositivo de control, información que se manifestará en alarmas visual y sonora.

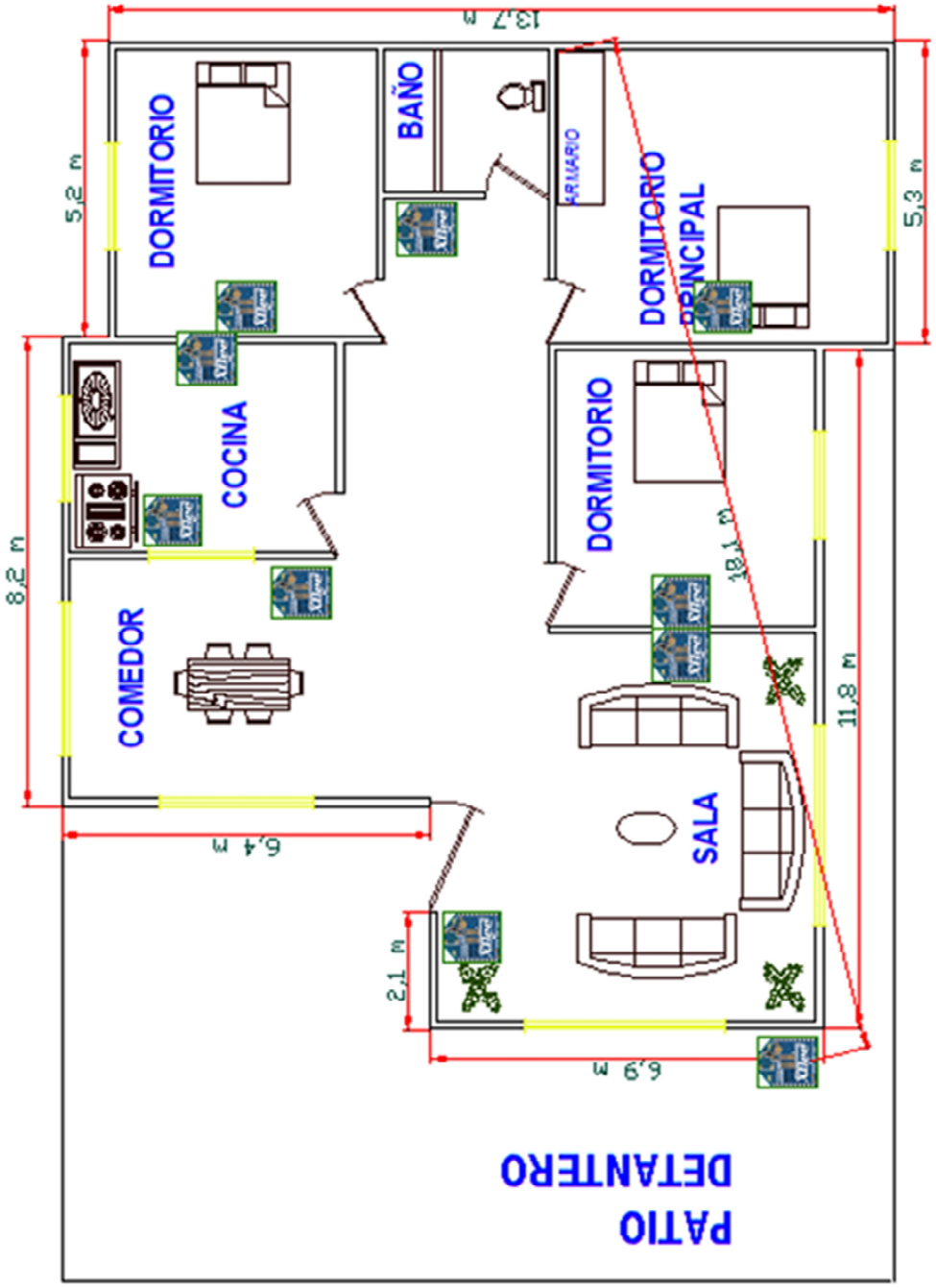


Figura 2. 17: Comunicación módulos ZigBee en la casas modelo

Para conocer el alcance necesario se toma como punto de referencia al sensor que se encuentre el sitio más distante del módulo de control

. Se debe considerar que los módulos ZigBee se alimentan por medio de baterías y también, que al ser un medio de comunicación inalámbrico se debe establecer seguridad en la información trasmitida.

La seguridad de la información se implementara con los módulos ZigBee con cifrado AES.

- **Dimensionamiento de *hardware* ZigBee**

  Los módulos ZigBee permitirán transportar la información proporcionada por los sensores de movimiento y gas, para ello, estos módulos deben cumplir con características como:

  - ✓ Alcance mínimo de 18 metros.
  - ✓ Los módulos ZigBee transportarán la información de los sensores, razón por la cual se requiere uno por cada sensor.
  - ✓ La información será transmitida en forma inalámbrica en banda de frecuencia libre 2.4 GHz.
  - ✓ Contar con seguridad en el medio inalámbrico, evitando que personas no autorizadas capturen paquetes y visualicen la información que se transmite.
  - ✓ Alimentación por baterías, para evitar la dependencia de la red eléctrica del domicilio.
  - ✓ Ambiente de operación indoor, los módulos ZigBee serán ubicados dentro del domicilio.

Establecidos los requerimientos mínimos de los dispositivos ZigBee se toma como referencia los siguientes modelos ZigBee:

MÓDULOS ZIGBEE		
Características mínimas	**XBee**	**XBee-PRO**
Alimentación 3- 12 V	2.8 - 3.4 VDC	3.0 - 3.6 VDC
Alcance mínimo 18 metros	Hasta 90m	Hasta 140 metros
Frecuencia de operación ISM	2.4 GHz	2.4 GHz
Seguridad AES	Cumple	Cumple

Tabla 2.2: Módulos ZigBee

De acuerdo a la Tabla 2.2, los dispositivos ZigBee cumplen con las condiciones mínimas requeridas. La selección del dispositivo es el XBee, por ser el más adecuado para el sistema.

Figura 2.17: Módulos ZigBee

La casa modelo contempla la red de sensores de movimiento para las siguientes localidades: entrada principal, sala, comedor, cocina, pasillo de acceso a las habitaciones y 3 habitaciones. La red de sensores de detección de gas contempla las siguientes localidades: cocina y ubicación de calefón (en caso de tenerlo).

Para el prototipo de prueba se considera 2 sensores. Los datos proporcionados por los sensores los adquieren los módulos XBee, los que a su vez transmiten esta información al módulo XBee de control.

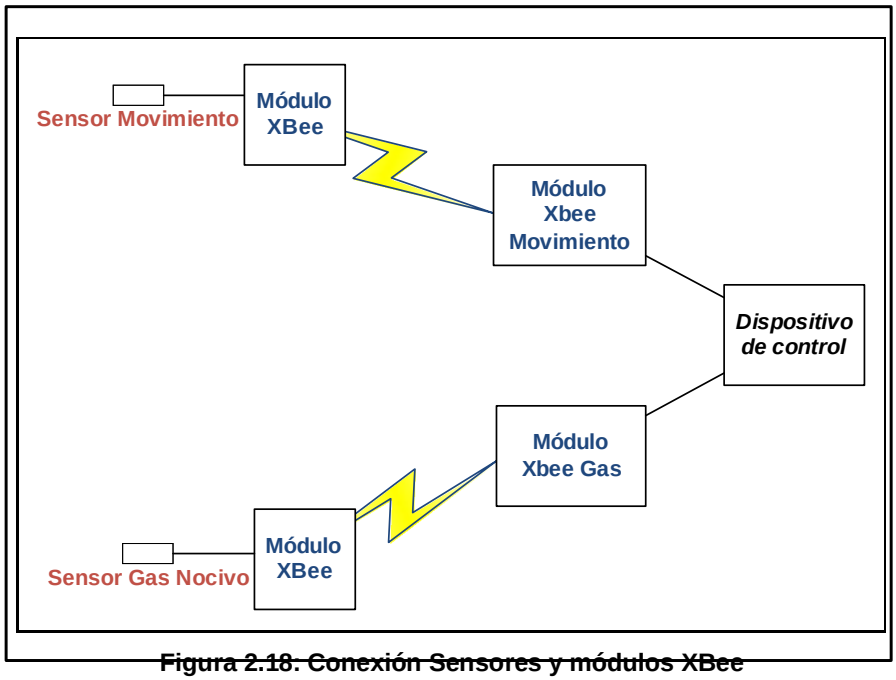


Figura 2.18: Conexión Sensores y módulos XBee

2.2.2.2 Diseño de la red de datos

El diseño de la red de comunicaciones contempla: el diseño, configuración, instalación y equipamiento requerido por el Sistema de Seguridad Domiciliario, no se consideran los equipos de red propios del domicilio (computadores de los usuarios y equipo de acceso a internet).

Se considera la implementación de cámaras IP en topología estrella a ser ubicadas en los puntos estratégicos del domicilio.

Dentro de la red de datos se considera un servidor de comunicaciones en el cual se concentrará la información del domicilio y albergará las grabaciones de las cámaras.

Como se indicó con anterioridad, en la red de comunicaciones se establecerán sensores de movimiento y detección de gases, mismos que enviarán la información obtenida en el domicilio por medio de los módulos ZigBee, los que se dispondrán en topología en estrella concentrado la información un Coordinador ZigBee, que será el encargado de enviar la información al micro controlador para gestionar los datos obtenidos.

Establecidos los elementos que conforman la red de comunicaciones, se establece:

- Los sensores se acoplan a los módulos XBee para una trasmisión en topología estrella hacia su coordinador ZigBee, conectado con el micro controlador que interactúa con el servidor a través de un interfaz serial
- El servidor del sistema se conecta a la red de datos por medio alámbrico.
- Las cámaras IP se conectan por medio inalámbrico, comunicándose con el servidor del sistema para la visualización del video desde el aplicativo *web*.
- La conectividad de las cámaras IP debe concentrarse en un Access Point que permita 5 conexiones inalámbricas mínimo, adicional debe contar con 2 puertos LAN para la conexión del servidor y el servicio de Internet.
- El equipo que permite el acceso al Internet será proporcionado por el proveedor del servicio.

En la figura 2.19 se presenta el diagrama de conexión del Sistema de Seguridad Domiciliario.

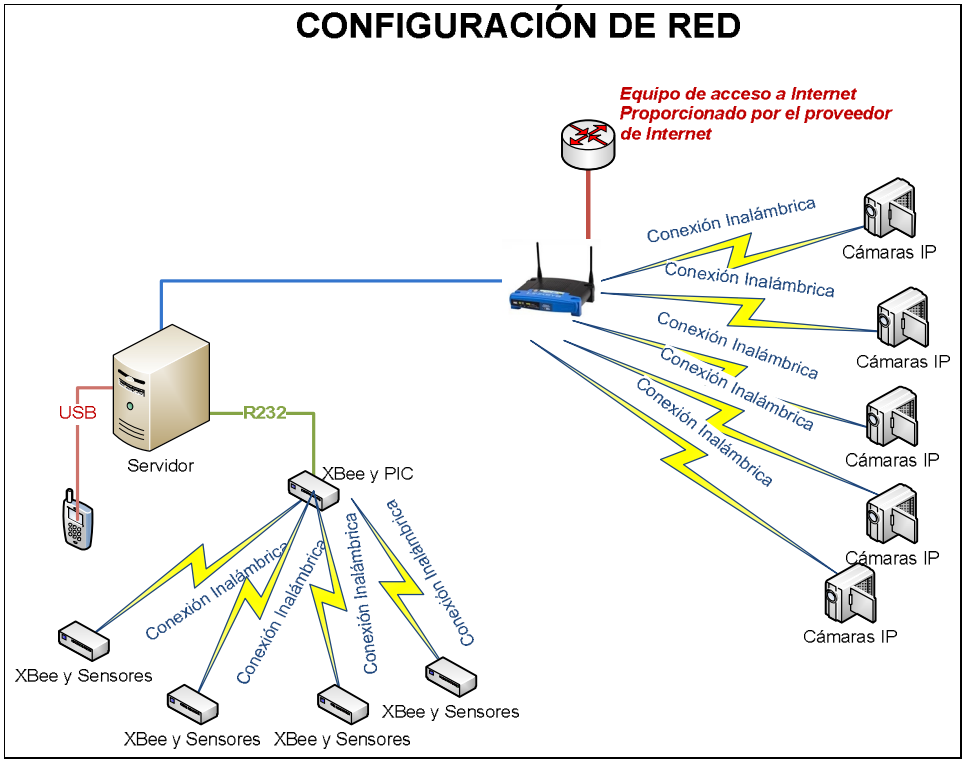


Figura 2.19: Red de Datos del Sistema

El micro controlado se conecta al servidor para enviar la información al sistema el mismo que será el encargado de gestionar los datos obtenidos.

Se establece una topología estrella para las cámaras IP conectadas hacia un Access Point, así como, para la red de sensores donde los dispositivos finales de conectan a un Coordinador ZigBee.

2.2.2.2.1 Plan de direccionamiento IP

Para el direccionamiento IP se toma en cuenta el número de dispositivos que interactúan dentro de la red de datos cámaras IP y servidor del sistema, bajo esta consideración se establece crear una subred privada clase C.

Los elementos de red requeridos por el Sistema de Seguridad Domiciliario son:

- Servidor del sistema: 1 dirección IP.
- Access Point: 1 Dirección IP.
- 5 Cámaras IP: 5 direcciones IP.
- Crecimiento en cámaras: Se reserva 4 direcciones.
- Dirección de Red, B*roadcast* y *Gateway*: 3 direcciones de configuración de red necesariamente a ser utilizadas.
- Equipo propios del domicilio: 10 direcciones para posibles conexiones.

De acuerdo a lo mencionado el número de direcciones requeridas son 24, adicionalmente se deben considerar direcciones para el crecimiento del Sistema de Seguridad, por lo tanto se tomarán 4 direcciones de crecimiento en base a lo expuesto, también se incluirá 10 direcciones para uso de los usuarios del domicilio. Acorde a este plan de direccionamiento IP, se plantea una red privada clase C, 192.168.10.0/27

En la Tabla 2.3 se establece el plan de direccionamiento IP de los dispositivos dentro de la red.

DIRECCIONAMIENTO IP	
Subred	**192.168.10.0/27**
Dispositivo	***IP Interna***
Servidor	192.168.10.30
Access Point	192.168.10.29
Cámara IP 1	192.168.10.20
Cámara IP 5	192.168.10.24
Reservado crecimiento de dispositivos	192.168.10.25 al 192.168.10.28
Disponible para red de usuario	192.168.10.2 al 192.168.10.19
Dirección de Gateway	192.168.10.1

Tabla 2.3: Direccionamiento IP

Dentro de la LAN del Domicilio se configuran las últimas direcciones IP de manera estática para el uso del Sistema de Seguridad Domiciliario ya que esto permitirá facilitar la administración de la red y de los elementos que se podrían conectar.

2.2.2.2.2 Disposición física de la red de comunicaciones

Dentro de la ubicación física de los equipos de comunicaciones se establece el dormitorio principal como punto central de la red, implementando seguridad física en el acceso a los equipos.

En este sitio se ubicarán los siguientes equipos:

- Servidor de comunicaciones.
- Access Point.
- Equipo de acceso a Internet.
- Coordinador ZigBee y micro controlador, por conexión serial hacia el servidor.
- Dispositivo móvil, por conexión USB hacia el servidor.

En el dormitorio principal donde se encontrarán los equipos de comunicaciones se implementará la red de datos, centralizando las comunicaciones en este sitio.

La red de datos contempla: el servicio de Internet brindado por un proveedor con su equipo de acceso; el equipo de comunicaciones que contempla: el *Access Point* y *switch* para conexión física del servidor y servicio de internet.

Para la conexión física del servidor hacia el switch de comunicaciones se establece un punto de cableado estructurado, la conexión hacia las cámaras se establece de forma inalámbrica con lo cual se debe configurar la red inalámbrica en el *Access Point,* tomado en cuenta parámetros de frecuencia y seguridad.

El celular y dispositivo de control de luminarias se conectan directamente al servidor por un cable USB.

Los sensores se instalarán en lugares altos para facilitar la capacidad de percepción de movimiento y gas, en la sala y cocina respectivamente; aprovechando sus cualidades de conexión inalámbrica.

Se debe tomar en cuenta que los sensores serán alimentados por baterías mientras que las cámaras IP requieren de alimentación eléctrica, los puntos eléctricos deberán ser adaptados para cada una de las cámaras de acuerdo a su disposición dentro de la casa y serán proporcionados por los residentes del hogar a ser protegido.

Otro aspecto a ser tomado en cuenta es el control en la casa gestionada por el micro controlador, para el encendido y apagado de las luminarias. Para el prototipo de prueba, el control de las luminarias es mediante la conexión directa a un pin del micro controlador.

2.2.2.2.3 Dimensionamiento del hardware de comunicaciones

Para el correcto funcionamiento de la red de comunicaciones se deben considerar los equipos activos que interactúan en ella.

El equipo de acceso a internet será proporcionado por el proveedor de servicio.

El equipo de conexión a la red de datos dentro del domicilio debe contar con las siguientes características:

- Contar con un mínimo de 2 puertos de red 10/100 Mbps para conexión del servidor y el proveedor de servicio de internet.
- Alimentación eléctrica 5 VDC 1.2 A y 6Watios, para evitar el consumo excesivo de energía.
- Temperatura de operación 0° - 40° C, temperatura Indor.
- Manejo de protocolos DHCP, direccionamiento Estático, rutas estáticas redirección de puertos.
- El equipo de comunicaciones debe permitir contar con la conexión inalámbrica (*Access Point*), para conexión de las cámaras IP.
- Manejo de estándares: IEEE: 802.11n, 802.11 b/g, 802.3, 802.3u.
- Banda de frecuencia 2,4 GHz
- Para la conexión inalámbrica permitir un nivel de seguridad mínimo de WPA[38]
- El equipo de comunicaciones de proveedor de Internet como el equipo de comunicación del domicilio deben permitir configurar NAT, para re-direccionar la conexiones de Internet hacia el servidor interno.

Para el prototipo de prueba se considera el equipo Dlin'k DIR 600, ya que cuenta con las funcionalidades antes descritas.

2.2.2.2.4 Configuración de los equipos de red

La configuración de la red de datos contempla: el servidor de comunicaciones, las cámaras IP, los sensores y módulos XBee, el equipo de comunicaciones del domicilio donde se considera la configuración de la red WLAN. Adicional en el equipo de comunicaciones se implementará el direccionamiento IP indicado en el ítem anterior.

En la configuración del equipo de comunicaciones se establecerá los siguientes parámetros:

- **SSID[39]:** ControlDomicilio

[38] http://www.cisco.com/web/LA/soluciones/comercial/proteccion_wireless.html

[39] SSID (*Service Set IDentifier)*: Es el nombre asignado a la red inalámbrica

- **Seguridad**: Se habilita WPA con cifrado TKIP[40] debido a este tipo de seguridad es el recomendado para pequeñas empresas y domicilios[41].
- **Direcciones IP**: Las cámaras contarán con un direccionamiento estático.

Dentro del equipo de comunicaciones se configura los siguientes parámetros para la red LAN:

- **DHCP**: Se habilita DHCP en el rango 192.168.10.2 - 192.168.10.19, para evitar el uso de las IP asignadas al Servidor y Cámaras IP.
- **Direccionamiento Server**: Como se indicó el servidor contará con una dirección estática, adicional dentro del equipo se establecerá una reserva de IP en función de la MAC para evitar conflicto de direcciones IP duplicadas con los equipos del Sistema de Seguridad Domiciliario.
- **Publicar el servidor en Internet**

  La configuración del NAT en el equipo de comunicaciones se efectuará en función de la tabla presentada a continuación:

Configuración de NAT				
Dispositivo	Puerto Externo	IP Pública	**IP Interna**	**Puerto Interno**
Servidor Web Https	18443	Dirección proporcionada por el proveedor de Internet	192.168.10.30	8443
Cámara IP 1	10554		192.168.10.20	554
Cámara IP 5	11554		192.168.10.25	554
Gateway	80		192.168.10.1	80

Tabla 2.4: Configuración de NAT

En la Tabla 2.4 se muestra la configuración de puertos utilizados para el uso de NAT. Esta configuración de puertos se la utilizó para evitar accesos no deseados y en base a su uso más común, por ejemplo el puerto 8443

[40] TKIP (*Temporal Key Integrity Protocol)*: Protocolo de inscripción de datos incluido como parte del estándar IEEE 802.11i, utilizado para implementar seguridad en redes inalámbricas

[41] http://www.cisco.com/web/LA/soluciones/comercial/proteccion_wireless.html

en servicios HTTPS, el 554 del protocolo RTSP de transmisión de datos en tiempo real y el 80 de HTTP.

2.2.2.2.5 Dimensionamiento de consumo de recursos de red.

Para poder contratar el servicio de internet es necesario conocer el consumo de ancho de banda que requerirá el sistema.

Para este cálculo se toma como referencia 2 herramientas que proporcionan un consumo de ancho de banda para un sistema de video vigilancia:

- Herramienta Axis tool V2[42]

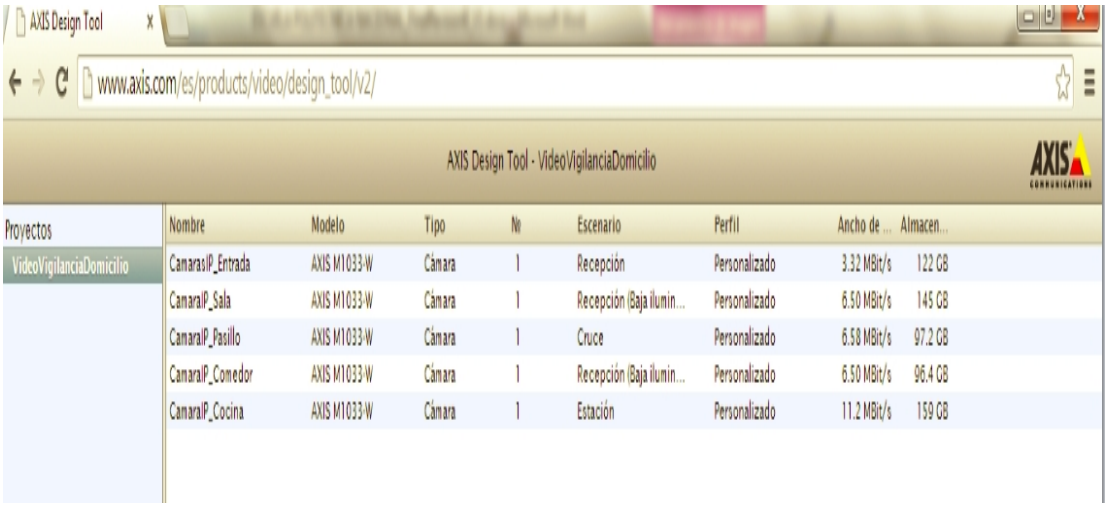


Figura 2.20: Herramienta Axis Tool

Estos valores se obtienen con las siguientes consideraciones:

- ✓ 5 Cámaras IP.
- ✓ Grabación por detección de movimiento.
- ✓ Resolución de video VGA

Con el uso de la herramienta indicada se tienen los valores de:

- ✓ Ancho de banda necesario: 34.1 Mbit/s

[42] http://www.axis.com/es/products/video/design_tool/v2/

- *Zavio Bandwidth and Storage Calculator*[43]: Herramienta que permite seleccionar los parámetros de grabación de la cámara sin especificar el modelo y marca.

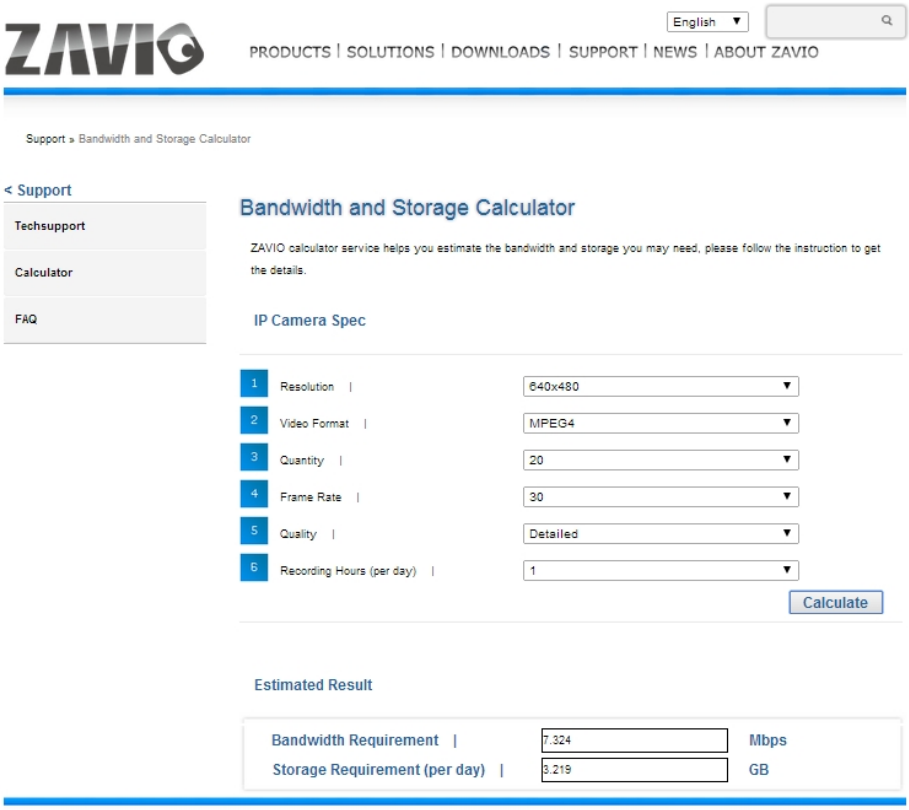


Figura 2.21: Herramienta *Zavio Bandwidth and Storage Calculator*

Para el uso de la herramienta de cálculo de ancho de banda se establecen los siguientes parámetros:

- ✓ Resolución del video: 640x480
- ✓ Formato del video: MPEG4
- ✓ Calidad de video: Detallada
- ✓ Grabación por día: 1 hora

En función de los parámetros descritos se tienen los siguientes datos.

- ✓ Almacenamiento necesario: 3,219 GB
- ✓ Ancho de banda necesario: 7,324 Mbps

[43] http://www.zavio.com/support-calculator.php

Trasladando los valores a 5 cámaras y grabación por 3 meses se tiene:

- ✓ Almacenamiento necesario: 1.448,55 GB
- ✓ Ancho de banda necesario: 36,62 Mbps

Se debe tener en cuenta que la herramienta considera un período de grabación de 1 hora al día, lo que no se aplica, se debe considerar un periodo de grabación de 25 min por día lo que representa un 42% de la duración de la grabación con lo que se tiene un espacio de almacenamiento de: 608,391 GB

En base a los cálculos indicados se considera necesario un disco de almacenamiento aproximado de 600 GB y el ancho de banda aproximado para el uso de video vigilancia de 35 Mbps.

El consumo de ancho de banda del sistema de video vigilancia dentro del domicilio se considera con el estándar 802.11g/a que permite tener un ancho de banda de 54 Mbps, suficiente para el uso del sistema.

Para poder visualizar el sistema desde internet se debe considerar el uso promedio de ancho de banda de los usuarios del domicilio al Internet, ya que esto implica consumo en el servicio.

Para conocer los recursos necesarios para observar las cámaras mediante internet, es necesario interpretar el consumo de ancho de banda que cada cámara requiere:

AB = Cuadros por segundo * Tamaño de imagen * % de ocupación[44]

Las imágenes de las cámaras serán de resolución 640x480 píxeles, tomado un promedio en el tamaño de dichas imágenes tenemos 8 KBytes de tamaño. Estableciendo en las cámaras el parámetro de 15 cuadros por segundo.

[44] http://noticias.alas-la.com/version_anterior/index.php/tutoriales-anteriores/279-tutorial-ed44.html

Tomando en cuenta que las cámaras serán para un sistema de video vigilancia donde se estima que durante el día se observará 12 horas en caso de encontrarse solo el domicilio, se tienen un porcentaje de ocupación de 50%.

Con los parámetros antes mencionados se tiene:

$$AB = 15\ fps * 8\ KBytes * \frac{8\ bits}{1\ byte} * 0{,}5$$

$$AB = 480\ Kbps\ (por\ cámara)$$

Considerando que en el Sistema se contará con 5 cámaras tenemos:

$$AB = 2400\ Kbps\ (por\ 5\ cámaras)$$

Dónde:

$$AB = 2400\ Kbps * \frac{1M}{1024\ K}$$

$$AB = 2{,}34\ Mbps$$

El ancho de banda de 2,34 Mbps, es el mínimo valor que debe ser contratado por el cliente a su ISP, para el correcto funcionamiento del sistema dentro del domicilio.

No se toma en cuenta el consumo de ancho de banda de los usuarios, ya que cuando los mismos se encuentren en casa el sistema de video vigilancia no será utilizado; por ser una medida de seguridad en caso de ausencia de los integrantes del domicilio.

2.2.2.2.6 Red de acceso a Internet

El servicio de Internet del domicilio depende del proveedor del servicio que es contratado por los usuarios del hogar. Al existir varios proveedores de Internet en el mercado se debe establecer requerimientos mínimos que permitan implementar el aplicativo *web* en Internet.

Para el acceso al aplicativo *web* desde Internet el proveedor del servicio debe brindar la posibilidad de publicar servidores, es decir, manejar NAT[45] en sus equipos de acceso a Internet, adicionalmente debe permitir el envío de correo electrónico con el protocolo SMTP (*Simple Mail Transfer Protocol*)[46], para las alertas generadas en caso de presentarse detección de movimiento, gases nocivos o daño de una cámara IP.

En el país existen varios proveedores de Internet con diferentes tecnologías de acceso y cobertura. Para implementar el Sistema de Seguridad Domiciliario se requiere que el proveedor del servicio cumpla con los siguientes:

- Dirección IP pública estática: Para el control del domicilio desde Internet
- Equipo de acceso a Internet que permita configurar NAT: Este equipo es proporcionado por el proveedor del servicio.

Los proveedores de servicio de Internet en la ciudad de Quito se presentan a continuación en la Tabla 2.5

PROVEEDOR	SERVICIO RESIDENCIAL	TECNOLOGÍA ALÁMBRICA	TECNOLOGÍA INALÁMBRICA
ANDINATEL S.A	Fast Boy	XDSL /GPON	WIMAX, CDMA
MEGADATOS S.A.	NetLive	GPON	WIMAX, CDMA
OTECEL S.A.	Movistar	-	3.5G/HSPA*/EDGE/GPRS
CONECEL S.A.	Claro	Cablemodem (No permite Acceso Remoto	3.5G/HSPA*/EDGE
PUNTONET S.A.	Puntonet	ADSL/Dial-UP (No asigna IP)	WIMAX
Grupo TV Cable	TV Cable	Cablemodem (No permite Acceso Remoto)	WIMAX

Tabla 2.5: Proveedores Internet [19] [20] [21] [22] [23] [24]

[45] NAT: *Network Address Translation* es un método por el cual las direcciones IP son mapeado de una subred a otra. NAT se utiliza para conectar un dominio de direcciones aisladas con direcciones privadas no registradas a un dominio externo con direcciones registradas globalmente únicas.

[46] *Simple Mail Transfer Protocol* (SMTP): Protocolo de la capa de aplicación, basado en texto, utilizados para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet.

Acorde a la tecnología de acceso a Internet del proveedor, los concesionarios que permiten al acceso al aplicativo *web* de control del domicilio se muestran en la Tabla 2.6

PROVEEDOR	SERVICIO RESIDENCIAL	TECNOLOGÍA MEDIO ALÁMBRICO	TECNOLOGÍA MEDIO INALÁMBRICO
ANDINATEL S.A	Fast Boy	XDSL	WIMAX, CDMA
MEGADATOS S.A.	NetLive	GPON	WIMAX, CDMA

Tabla 2.6: Proveedores Recomendados

2.2.3 DISEÑO BLOQUE DE ALMACENAMIENTO Y GESTIÓN DE LA INFORMACIÓN. (BAGI)

En este bloque se especifica el funcionamiento del aplicativo, que es el encargado de interpretar la información obtenida por los bloques anteriores

La implementación de este bloque comprende lo siguiente:

- Servidor del Sistema
- Desarrollo del aplicativo *web* del sistema.

2.2.3.1 Servidor del Sistema

Este servidor es el medio de comunicación entre los sensores – módulos XBee, dispositivo móvil y el aplicativo del Sistema (instalado en el servidor), adicionalmente en este servidor se almacenará las grabaciones obtenidas por las cámaras IP. También permitirá la comunicación con: la red de datos, micro controlador y dispositivo móvil razón por la cual requiere los interfaces que permitan esta integración. Para ello el servidor debe contar un puerto de conexión serial para el micro controlador, puertos USB para comunicación con el dispositivo móvil y tarjeta de red para conexión a la red de datos.

En el servidor del Sistema se debe implementar el Sistema Operativo con los servicios necesarios para cumplir con las necesidades que el aplicativo del sistema lo requieran.

Para el almacenamiento de la información en el servidor se debe considerar:

- ✓ El tamaño promedio del video grabado por las cámaras.
- ✓ El número de grabaciones en caso de robo en un día determinado.
- ✓ El tiempo que se mantendrán las grabaciones.
- ✓ Número aproximado de incidencias al mes.
- ✓ Espacio necesario para el Sistema Operativo.
- ✓ Servicios necesarios para el aplicativo

En consideración a los requerimientos antes mencionados se tiene:

- ✓ Tamaño promedio de las grabaciones: 200 MB
- ✓ Numero de grabaciones 10 por cada cámara (5 cámaras instaladas).
- ✓ Duración de las grabaciones 3 meses mínimo.
- ✓ Número de incidencias por mes 20.
- ✓ 200 MB x 10 grabaciones x 5 cámaras = 10 GB promedio.
- ✓ 10 GB x 20 incidencias x 3 meses = 600 GB promedio de almacenamiento
- ✓ Espacio para el Sistema operativo 20 GB
- ✓ Servicio necesarios para el aplicativo 10 GB
- ✓

- **Dimensionamiento del hardware del servidor**

  Las consideraciones más relevantes para un PC que tendrá las funciones de servidor son:

  - ✓ Interfaz serial R232 para comunicación con el micro controlador.
  - ✓ Interfaz USB 2.0 para comunicación con el dispositivo móvil.
  - ✓ Interfaz de red 10/100 Mbps, para acceso a la red de datos.
  - ✓ Disco Duro de 600 GB, tomando en cuenta las consideraciones anteriores.
  - ✓ Memoria RAM 1024 MB para la ejecución de los servicios y aplicativo *web*.

2.2.3.2 Diseño del Aplicativo Web del Sistema

EL aplicativo *web* es el encargado de gestionar todas las funcionalidades del Sistema de Seguridad Domiciliario: manejo de alertas, control del domicilio y visualización de las cámaras IP, así como también, administración de usuarios. Adicionalmente el aplicativo *web* permitirá el control del domicilio desde Internet.

Como se mencionó el control del domicilio será por medio de Internet y debido a ello este aplicativo debe ofrecer confidencialidad y confiabilidad en la información transmitida.

2.2.3.2.1 Requerimientos del aplicativo web

Para el correcto funcionamiento del aplicativo *web* del Sistema este debe cumplir con los objetivos propuestos: acceso desde Internet, ofrecer seguridad en la información transmitida, acceso a usuarios permitidos, visualización de video de las cámaras IP instaladas, control de luminarias del domicilio, envío de alarmas en caso de: detección de movimiento o gas nocivo y alertas del estado de las cámaras IP mediante mensajes SMS y E-Mail.

El Sistema Operativo donde residirá el Aplicativo debe cumplir con funcionalidades de servidor: *web* para publicar al sistema en Internet, servidor de almacenamiento de datos para guardar los videos obtenidos por las cámaras IP, servidor de base de datos para gestionar los usuarios del sistema.

Para brindar seguridad en el intercambio de información dentro de Internet, se implementará certificados digitales dentro del protocolo https. El acceso al Sistema será por usuarios validados dentro de una base de datos.

Tomando en cuenta los requerimientos de *software* y Sistema Operativo que deben cumplir, se ha seleccionado el Sistema Operativo Linux en la distribución Centos, ya que cuenta con las funcionalidades de servidor y es una distribución libre de Linux ampliamente difundida en el mercado y con gran soporte técnico.

Para acceso desde Internet al Sistema de Seguridad Domiciliario, el Sistema Operativo Linux distribución Centos debe contar con un servidor *web* (apache-tomcat).

La seguridad de la información se implementará con certificados digitales generados por la Herramienta Open SSL, herramienta sin licenciamiento, compatible con el Sistema Operativo y de gran aceptación en el mercado.

El servidor de base de datos encargado del manejo de usuarios del Sistema debe ser compatible con el Sistema operativo Linux distribución Centos, libre de licenciamiento y con amplio soporte técnico.

Dentro del servidor se almacenara el video grabado por las cámaras IP, razón por la cual se implementará un servidor Samba encargado de almacenar las grabaciones de video.

En el Servidor se debe configurar la inicialización de los servicios al momento del arranque del Sistema Operativo, para ello se emplea el comando *"chkconfig",* donde se activan los servicios: httpd, smb, mysqld y tomcat.

Tomando en cuenta los servicios previos que requiere el aplicativo *web* para su correcto funcionamiento se implementarán los siguientes servidores, dentro de la misma PC destinada a ser Servidor:

- Servidores Web
- Servidor de Gestión de Bases de Datos SGBD

2.2.3.2.2 Servidores Web

A continuación se presenta una comparativa de los posibles servidores *Web* a ser utilizados en el sistema.

SERVIDOR	DISPONIBILIDAD	PRECIO
Apache	Unix/Linux, Windows 95/98/NT/2000	Libre
Enhydra	Windows NT/2000, Unix/Linux	Libre
Jigsaw	Unix/Linux, Windows 95/98/Millenium y NT/2000	Libre
NCSA HTTPd	Unix/Linux, Windows 3.x,NT	Libre

Tabla 2.7: Comparativa Servidores Web

Por conocer el servicor apache-tomcat, facilidad de uso, difusión de la herramienta se escogió al Servidor Apache-Tomcat como el que mejor se ajusta a los requerimientos del aplicativo Web

2.2.3.2.3 SGBD Disponibles en el Mercado

SGBD de código abierto (libres)

- ✓ MySQL Licencia Dual, depende el uso. Sin embargo, existen 2 versiones. una gratuita que sería equivalente a la edición "*express*" SQL server de Windows y otra más completa de pago.
- ✓ PostgreSQL (http://www.postgresql.org Postgresql) Licencia BSD
- ✓ Firebird basada en la versión 6 de InterBase, Initial Developer's PUBLIC LICENSE Versión 1.0.
- ✓ SQLite (http://www.sqlite.org SQLite) Licencia Dominio Público
- ✓ DB2 Express-C (http://www.ibm.com/software/data/db2/express/)
- ✓ Apache Derby (http://db.apache.org/derby/)

SGBD de propietario (no libres)

- ✓ Advantage Database
- ✓ dBase
- ✓ FileMaker
- ✓ Fox Pro
- ✓ IBM DB2 Universal Database (DB2 UDB)
- ✓ IBM Informix
- ✓ Interbase de CodeGear, filial de Borland
- ✓ MAGIC
- ✓ Microsoft Access
- ✓ Open Access
- ✓ Oracle

- Sistema operativo que pueden utilizar

SGBD	WINDOWS	MAC OS X	LINUX	UNIX
Adaptive Server Enterprise	Sí	Sí	Sí	Sí
DB2	Sí	No	Sí	Sí
Firebird	Sí	Sí	Sí	Sí
HSQLDB	Sí	Sí	Sí	Sí
Informix	Sí	Sí	Sí	Sí
InterBase	Sí	No	Sí	Sí
MySQL	Sí	Sí	Sí	Sí
Oracle	Sí	Sí	Sí	Sí
PostgreSQL	Sí	Sí	Sí	Sí

Tabla 2.8: Comparativa SGBD Sistema Operativos

Debido a que se trata de disminuir costos para el funcionamiento del sistema de seguridad, se empleará el sistema operativo CentOS de distribución Linux. Y la base de datos MySql por ser nativa del sistema operativo.

2.2.4 DISEÑO BLOQUE DE VISUALIZACIÓN DE LA INFORMACIÓN (BVI)

A continuación se describe el proceso de gestión de la información para ser visualizada por medio de SMS y correo electrónico.

Para la visualización de SMS se enviarán alertas por un dispositivo móvil.

2.2.4.1 Dispositivo Móvil

El dispositivo móvil permitirá el envío de SMS en caso de detectar un evento en los sensores de movimiento y gas

El dispositivo móvil se conectará al servidor para la integración con el Sistema de Seguridad Domiciliario.

El manejo de alarmas es por medio de la integración del PIC – aplicativo del sistema – dispositivo móvil, por esta razón quien es el encargado del envío de alarmas es el aplicativo del sistema y para conseguirlo es necesario que el aplicativo pueda interactuar con el dispositivo móvil.

- **Características del Dispositivo Móvil**

  La funcionalidad del dispositivo móvil es el envío de SMS alertando a los usuarios en caso de detección de movimiento o detección de gas nocivo.

  EL dispositivo móvil debe permitir la conexión con el servidor para poder interactuar con el aplicativo del sistema. Esta conexión debe ser por medio cableado evitando errores en la transmisión y mayor confiablidad de la misma.

DISPOSITIVO MÓVIL	
REQUERIMIENTOS MÍNIMOS	**CARACTERÍSTICA**
Funcionalidad	Envío SMS
Conexión cableada al Servidor	Interfaz USB 2.0
Integración al Sistema de Seguridad Domiciliario	Permitir recepción de comandos AT
Cobertura	En el sector del domicilio

Tabla 2.9: Requerimientos Dispositivo Móvil

Para el prototipo de prueba se considera al equipo móvil Nokia C1 con el SIM de la operadora CLARO.

2.2.4.2 Correo Electrónico

Mediante mensajes de correo electrónico se alertará de incidencias dentro del domicilio, la cuenta de correo electrónico se establece con servidores ampliamente difundidos ya que se creará una cuenta dedicada a la alerta de incidentes.

Para el uso de esta cuenta de correo electrónico el servidor debe tener acceso a Internet y poder conectarse a cualquiera de estos servidores de Mail.

El sistema de seguridad realizará el proceso automático de envío de un mail en caso de detección de una alarma.

2.3 SERVIDORES Y DISEÑO DEL SISTEMA DE SEGURIDAD DOMICILIARIO

Los servicios requeridos por el sistema para el correcto funcionamiento del aplicativo son:

- Servidor Web: Acceso al interfaz de visualización de las cámaras IP e ingreso al sistema desde internet.
- Servidor de archivos compartidos: Almacenamiento de los videos correspondientes a las cámaras IP.
- Servidor de Base de Datos: Almacenamiento de usuarios, SMS y banderas de control para el encendido – apagado de luminarias, así como también, gestión de alertas.

2.3.1 SERVIDOR WEB

El servidor *web* permitirá el acceso mediante Internet al control del domicilio, dentro de las funcionalidades requeridas por el sistema se consideran los siguientes aspectos:

- ✓ Usuarios que ingresaran simultáneamente al sistema.
- ✓ Seguridad en transporte de información.
- ✓ Compatibilidad con el Sistema Operativo.
- ✓ Compatibilidad con el sistema de control de luminarias a implementarse con JAVA.

- **Dimensionamiento del servidor**
  - ✓ El servidor tendrá mínimo 5 sesiones concurrentes.
  - ✓ Implementación con el protocolo SSL y TLS para implementar seguridad en la información.
  - ✓ Compatibilidad con el Sistema Operativo Linux.
  - ✓ Desarrollo en lenguaje JSP, logrando compatibilidad con JAVA.

Para el Sistema de Seguridad Domiciliario se considera al Servidor apache-tomcat.

2.3.2 SERVIDOR DE ARCHIVOS COMPARTIDOS

El servidor de archivos compartidos permitirá transportar las grabaciones obtenidas por las cámaras IP hacia un disco de almacenamiento. La implementación de este servidor debe considerar las siguientes funcionalidades.

- ✓ Uso libre
- ✓ Compatibilidad con el sistema operativo.
- ✓ Autenticación en los archivos compartidos.

- **Dimensionamiento del servidor**
  - ✓ Servidor libre de licenciamiento.
  - ✓ Compatibilidad entre sistema Linux y Windows.
  - ✓ Permitir autenticación a nivel de usuario (cámaras IP)

Para el Sistema de Seguridad Domiciliario se considera al Servidor Samba.

2.3.3 SERVIDOR DE BASE DE DATOS

El servidor de base de datos permitirá gestionar usuarios del sistema, que tendrán atributos como: Nombre, Apellido, Numero Celular, Correo electrónico, Notificación de alertas. También gestionara la tabla de envío de SMS, e-Mail, como también permitirá la gestión de las luminarias mediante el uso de banderas de estado. Para el almacenamiento de esta información se debe considerar las siguientes características:

- ✓ De uso libre.
- ✓ Compatibilidad con el sistema operativo.
- ✓ Interconexión con lenguaje JAVA.
- ✓ Proporcionar sistemas de almacenamiento transaccional y no transaccional.

- **Dimensionamiento del Servidor**
  - ✓ Servidor libre de licenciamiento.
  - ✓ Compatibilidad con el sistema operativo Linux y Windows.

- ✓ Conexión con lenguaje JSP y JAVA.
- ✓ Permitir transacciones con las bases de datos.
- ✓ Seguridad con el manejo de usuarios y contraseñas.
- ✓ Permitir el incremento de tablas en caso de requerirlo.

Para el Sistema de Seguridad Domiciliario se considera al Servidor MySql.

2.4 SERVIDOR TOMCAT

Al aplicativo *web* se tendrá acceso desde Internet para ello es necesario un Servidor *Web*, se considera el Servidor Apache-Tomcat, por las características que ofrece:

- Compatibilidad con tecnología JSP y JAVA
- Compatibilidad con el Sistema Operativo Linux distribución Centos
- Fácil administración
- Servidor de código abierto
- Soporta seguridad SSL y TLS
- Servidor ampliamente difundido

El Servidor Tomcat a utilizarse en el proyecto es la versión apache-tomcat 6.0.35

Como requisitos previos para la instalación del Servidor son necesarios los repositorios de Java y JDK[47].

2.4.1 INSTALACIÓN DE TOMCAT [24]

1. Descargar la versión apache-tomcat 6.0.35 para Linux en el link http://tomcat.apache.org/
2. Descomprimir el archivo en un directorio del sistema
3. Para iniciar el servicio se requiere correr el script "*startup.sh",* localizado en la carpeta /*bin* del servidor tomcat, mediante la instrucción *"./startup.sh"*

[47] Java *Development Kit*: Es un entorno de desarrollo para construir aplicaciones, applets y componentes utilizando el lenguaje de programación java.

2.4.2 CONFIGURACIÓN DE TOMCAT

Como primer paso luego de la instalación de Tomcat, se requiere configurar el acceso a usuarios para la administración del Servidor, para ello se debe modificar el archivo *"tomcat-users.xml"* añadiendo las instrucciones mostradas en la Figura 2.22

```
    <role rolename="tomcat"/>
    <role rolename="role1"/>
    <role rolename="manager-gui"/>
    <user password="tomcat" roles="tomcat" username="tomcat"/>
    <user password="tomcat" roles="tomcat,role1" username="both"/>
    <user password="tomcat" roles="role1" username="role1"/>
    <user password="puul" roles="manager,admin" username="puul124"/>
    <user password="puul124" roles="manager-gui,manager,admin" username="puul"/>
</tomcat-users>
```

Figura 2.22: Configuración Usuarios en Servidor Tomcat

Como se observa en la Figura 2.22, se añade usuarios con un *password* de acceso y se establece los roles de administración.

Luego de configurar el acceso para la administración del Servidor Tomcat, se implementa seguridad en el intercambio de la información, habilitando el protocolo https con seguridad SSL/TLS[48], ésto se logra modificando el archivo *"server.xml"*. Adicionalmente el acceso al Sistema de Seguridad Domiciliario mediante el protocolo https se configura en el puerto estándar 8443, como se muestra en la Figura 2.23

```
    <!-- Define a SSL HTTP/1.1 Connector on port 8443
         This connector uses the JSSE configuration, when using APR, the
         connector should be using the OpenSSL style configuration
         described in the APR documentation -->

    <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
               maxThreads="150" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS"
               keystorePass="changeit"
               keystoreFile="/etc/tomcat6/apache-tomcat-6.0.35/CertSeguridad/CertSeguridad-
keystore"
    />
```

Figura 2.23: Seguridad en Servidor Tomcat

[48] *SSL Secure Socket Layer:* Protocolo que proporción servicio de seguridad de cifrando los datos intercambiados entre el servidor y Cliente, utilizando algoritmo simétrico, típicamente el RC4 o IDEA, y cifrando la clave de sesión de RC4 o IDEA mediante un algoritmo de cifrado de clave pública, típicamente el RSA.

Para habilitar seguridad SSL/TLS, se añaden certificados digitales colocados en el "*keystoreFile*".

2.5 CERTIFICADOS DIGITALES

Los certificados digitales se los puede adquirir de dos maneras:

1. Comprar los certificados digitales a una entidad reconocida en la *Web*
2. Generar certificados digitales propios

Para el proyecto se opta por la generación de certificados propios, con la finalidad de no incurrir en un costo adicional.

Para la generación de certificados digitales se implementó la herramienta OpenSSL la cual presenta las siguientes características:

- Compatibilidad con el Sistema Operativo Linux distribución Centos
- Herramienta de código abierto
- Certificados compatibles con el Servidor Tomcat
- Herramienta ampliamente difundida
- Licencia de estilo apache para fines comerciales y no comerciales

2.5.1 HERRAMIENTA OPEN SSL [25] [26]

El proyecto OpenSSL es un esfuerzo de colaboración para desarrollar un Sistema robusto, con todas las funciones de criptografía y de código abierto.

OpenSSL se basa en una biblioteca SSLeavy desarrollada por Eric A. Young y Tim J. Hudson. El kit de herramientas OpenSSL utiliza una licencia estilo Apache, que básicamente significa que es libre de obtener y utilizar para fines comerciales y no comerciales.

OpenSSL es una librería que ofrece funcionalidades de criptografía para aplicaciones tales como Servidores Web seguros.

A continuación se describe la simbología de OpenSSL:

- CA: Gestión de una autoridad certificadora
- CRL: Gestión de revocación de certificados
- pkcs12: Gestión de certificados PKCS#12
- req: Gestión de solicitudes de certificados X.509
- RSA: Gestión de llaves RSA
- x509: Gestión de certificados de tipo X.509

Creación de Certificados Digitales [27] [28] [29]

Para la creación de certificados digitales es necesario seguir los siguientes pasos:

- **Paso1**: Creación de una autoridad certificadora CA

  La Autoridad de Certificación CA (*Certification Authority*) es la entidad encargada de firmar y revocar los certificados digitales.

  El proceso para crear una autoridad certificadora es el siguiente:

  1. Crear los directorios "*certs*, *newcerts* y *private*" en el directorio /etc/pki/CA del Servidor, mediante el comando "*mkdir",* como se muestra a continuación en la Figura 2.24

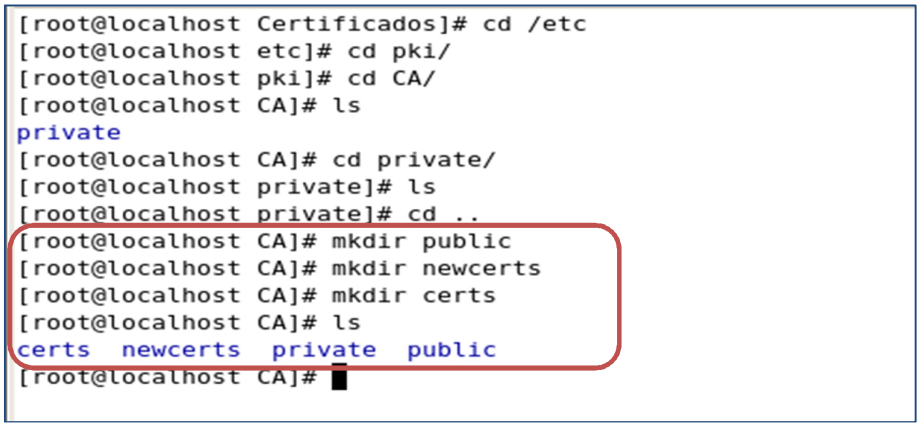


Figura 2.24: Creación directorios Autoridad Certificadora

2. Creados los directorios se procede a generar la autoridad de certificación con la instrucción *"./CA -newca"*, en el directorio *"/etc/pki/tls/misc"*.

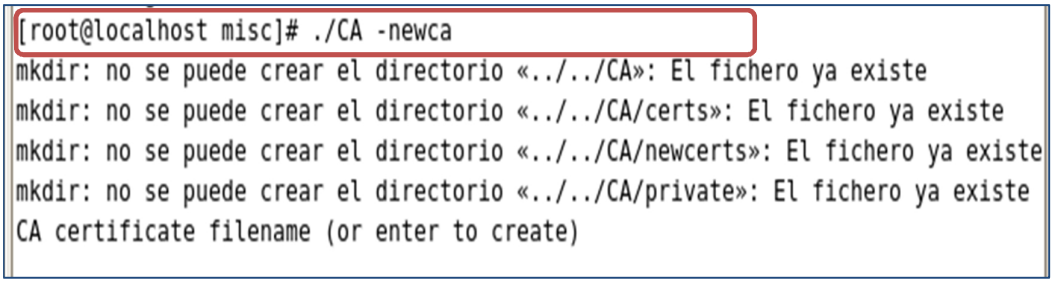


Figura 2.25: Creación Autoridad Certificadora

En La Figura 2.25, se muestra creación de la Autoridad Certificadora, esta Autoridad solicitará la siguiente información:

- ✓ Una frase de seguridad: SeguridadDomiciliaria
- ✓ Código de país: EC
- ✓ Provincia: Pichincha
- ✓ Cuidad: Quito
- ✓ Organización: Seguridad
- ✓ Campania: fullredes
- ✓ Nombre del Host: fullredes.net
- ✓ Email: atienciapaul@gmail.com

Con la información solicitada se genera la Autoridad Certificadora.

- **Paso 2**: Generar certificado auto firmado

Con la autoridad certificadora (CA) generada, se puede crear los certificados digitales para el Sistema de Seguridad Domiciliario, mediante el protocolo https; para lo cual se realiza el siguiente procedimiento:

1. Crear una llave privada

   Para crear la llave privada y la solicitud de firmado del certificado se requiere ejecutar el comando mostrado en la Figura 2.26

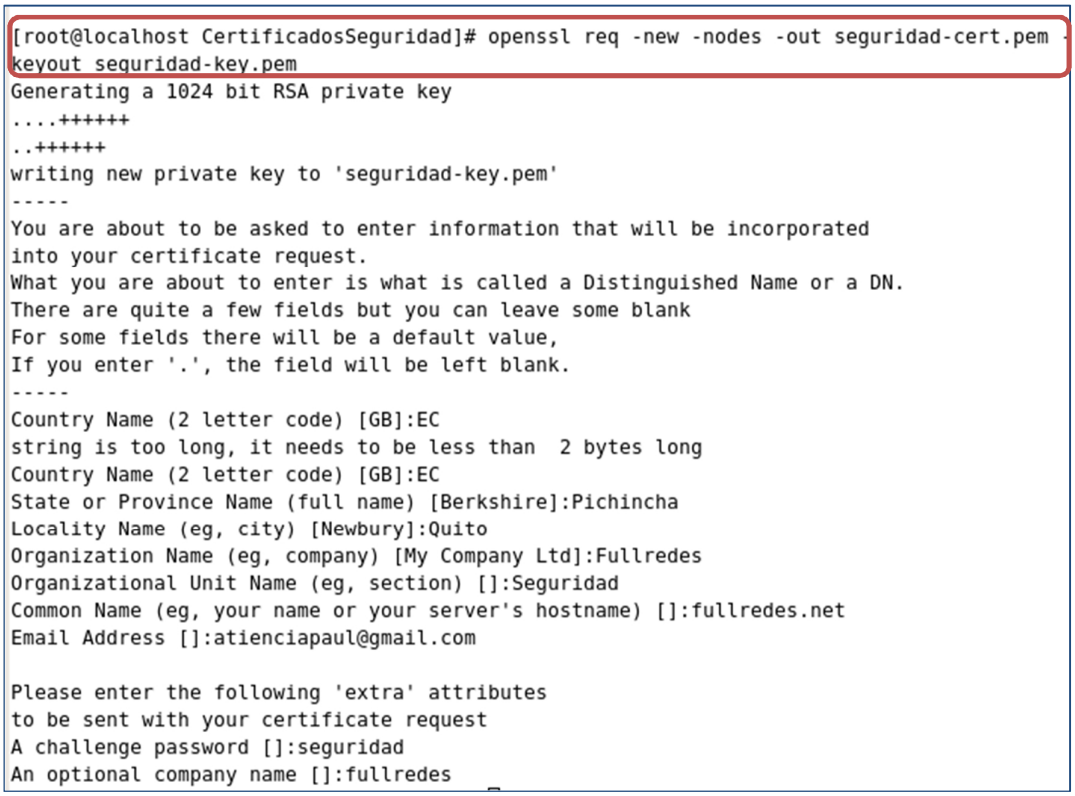


Figura 2.26: Generación llave privada y solicitud de firmado del certificado

Con la ejecución de la instrucción de la Figura 2.26 se obtienen los archivos:

- ✓ seguridad-key.pem
- ✓ seguridad-cert.pem

Donde “seguridad-key.pem”, es la llave privada con la cual se codifica la información mediante un algoritmo de cifrado. Mientras que “seguridad-cert.pem”, es la solicitud de firmado del certificado.

2. Firmar la solicitud para generar un certificado auto firmado

Para generar el certificado auto firmado se ejecuta el comando mostrado en la Figura 2.27 donde se solicita la frase de seguridad generada en la Autoridad Certificadora (SeguridadDomiciliaria), así como también el tiempo de vigencia del certificado.

```
[root@localhost private]# openssl ca -out seguridad.pem  -days  365  -infiles se
guridad-cert.pem
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for ../../CA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: May 29 06:26:07 2012 GMT
            Not After : Apr 10 23:57:51 1926 GMT
        Subject:
            countryName               = EC
            stateOrProvinceName       = Pichincha
            organizationName          = Fullredes
            organizationalUnitName    = Seguridad
            commonName                = fullredes.net
            emailAddress              = atienciapaul@gmail.com
```

Figura 2.27: Auto firmado del certificado

El tiempo de validez para el certificado es de 365 días (1 año), pasado este tiempo se deberá renovar el certificado digital acorde a los avances de tecnología y bibliotecas de criptografía.

- **Paso 3**: Exportar el certificado a formato PKCS 12

El PKCS 12 especifica un formato portátil para almacenar y transportar certificados, claves privadas y otra información secreta. Es el formato preferido para el manejo de muchas operaciones con certificados, adicionalmente es compatible con la mayoría de navegadores y versiones recientes de la familia de Sistemas Operativos Windows. Tiene la ventaja de ser capaz de almacenar el certificado y la clave correspondiente en un solo archivo en el directorio raíz del sistema.

```
[root@localhost private]# openssl pkcs12 -export -in seguridad.pem -inkey seguri
dad-key.pem  -out seguridad.pkcs12 -name seguridad -CAfile ../cacert.pem -caname
 seguridadca
Enter Export Password:
Verifying - Enter Export Password:
[root@localhost private]#
```

Figura 2.28: Exportación del certificado a formato pkcs12

En la Figura 2.28, se muestra la instrucción para cambiar el certificado digital a formato PKCS 12. Adicionalmente requiere una clave de exportación para proteger la integridad del certificado.

- **Paso 4**: Instalar el certificado de la Autoridad Certificadora

  Creado el certificado, firmado por la autoridad certificadora y exportada a formato PKCS 12, es necesario colocar éste certificado en un repositorio llamado *keystore*, mediante la instrucción que se presenta en la Figura 2.29

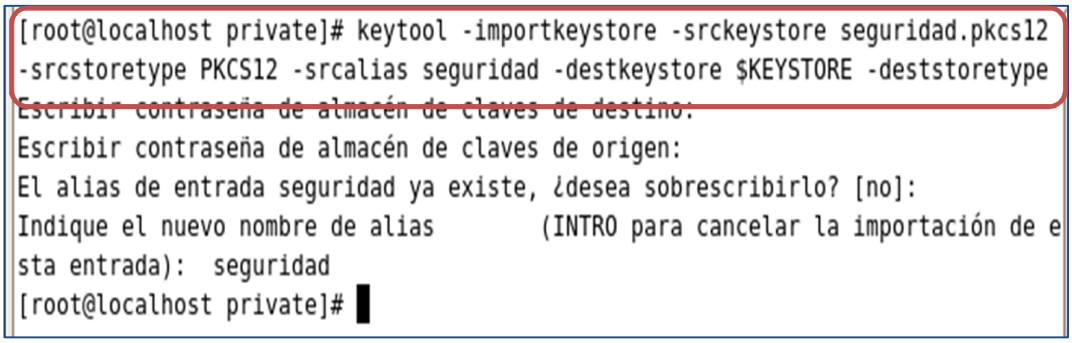


Figura 2.29: Guardar certificado en repositorio *keystore*

En este caso es necesario establecer una contraseña para el almacén de claves (clave asignada en el cambio de formato PKCS 12)

Por ultimo ya instalado el certificado en el repositorio *keystore* se establece una contraseña mediante la siguiente instrucción:

keytool -list -keystore $KEYSTORE -storepass changeit

El navegador Mozilla permite la conexión sin establecer configuraciones adicionales, los navegadores como Internet Explorer, Chrome, Opera y Safari no reconocen el certificado generado en el Sistema de Seguridad Domiciliario, para el reconocimiento del certificado digital se debe agregar la autoridad certificadora generada en la herramienta OpenSsl.

2.6 SERVIDOR APACHE HTTPD [24]

Para poder visualizar el historial de videos obtenidos por las cámaras IP en la *web* se configuró el servidor *web* http.

Se selecciona al Servidor http por presentar las siguientes características:

- Compatibilidad con el Sistema Operativo Linux distribución Centos
- Servidor de código abierto

- Servidor ampliamente difundido
- Servidor de configuración sencilla
- No requiere licencia de operación
- Permite la trasferencia de archivos multimedia
- Cada petición al servidor por el cliente no depende de una transacción anterior

La instalación del Servidor Apache se realiza con la siguiente instrucción ejecutada en el terminal:

yum install httpd

Se debe tomar en cuenta que para ejecutar la instrucción antes mencionada es necesario tener acceso a Internet.

Para habilitar del Servidor Apache (httpd), es necesario configurar el Servidor Apache, modificando el archivo *"httpd.conf"* ubicado en la carpeta "/etc/httpd/conf".

En este archivo se establecerán los siguientes parámetros:

- Puerto de acceso al Servidor Apache; (Figura 2.30)
- Establecer carpetas de ubicación de los archivos de video; (Figura 2.31)

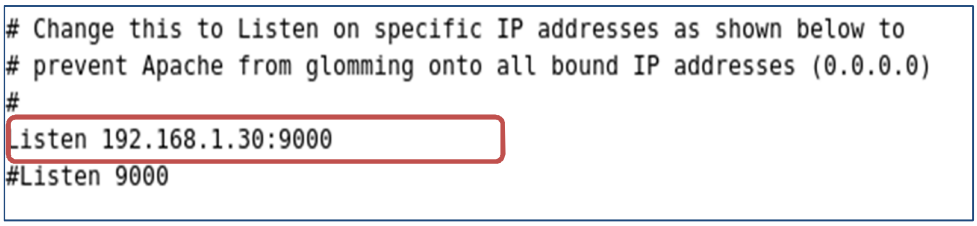


Figura 2.30: Puerto de acceso al Servidor Apache

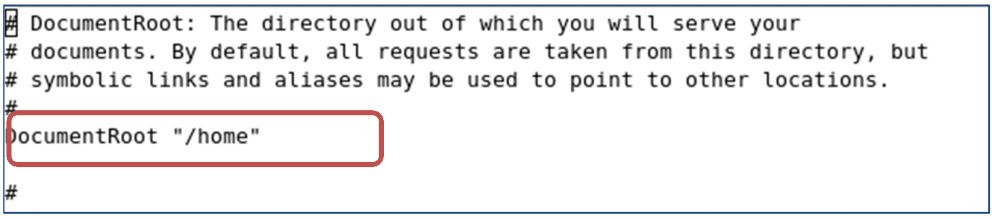


Figura 2.31: Carpeta raíz de videos cámaras IP

Por último para iniciar el servicio se requiere ejecutar la siguiente instrucción en un terminal:

service httpd start

2.7 SERVIDOR SAMBA [30]

Las cámaras IP, requieren de un Servidor Samba para guardar los archivos de video generados al momento de detectar movimiento.

Samba es una implementación libre, de protocolo de archivos compartidos de Microsoft Windows para sistemas de tipo UNIX. De esta forma, es posible que ordenadores con Linux o Mac actúen como clientes en redes de Windows.

Samba configura directorios Unix-Linux (incluyendo sus subdirectorios) como recursos para compartir a través de la red. Para los usuarios de Microsoft Windows, estos recursos aparecen como carpetas normales de red. Los usuarios de Linux pueden ubicar los archivos en estas unidades de red como si fueran dispositivos locales.

2.7.1 INSTALACIÓN DEL SERVIDOR SAMBA

Para instalar el Servidor Samba se requiere ejecutar las siguientes instrucciones en un terminal:

yum install -y samba samba-client samba-common

yum install -y samba-swat

Se debe tomar en cuenta que para ejecutar estas instrucciones es necesario tener acceso a Internet.

2.7.2 CONFIGURACIÓN DEL SERVIDOR SAMBA

1. La configuración del Servidor Samba requiere modificar el archivo *"smb.conf"* ubicado en la carpeta *"/etc/samba/"*, estableciendo los siguientes parámetros:

- Ubicación del recurso compartido, así como también, el usuario y permiso de acceso al recurso (Figura 2.32)

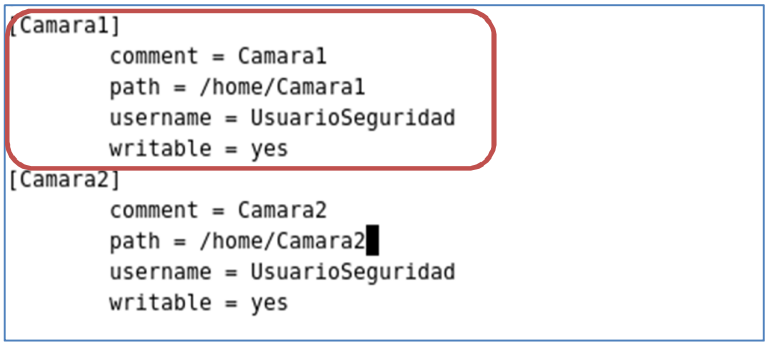


Figura 2.32: Ubicación de recursos compartidos

Como se muestra en la figura 2.32, se establecen dos carpetas compartidas, por la existencia de dos cámaras IP.

2. Creación de usuarios samba

Para la creación de usuarios es necesario realizar las instrucciones que se muestran en la figura 2.33

Figura 2.33: Creación usuarios samba

2.8 SERVIDOR MYSQL [31] [32]

El Sistema de Seguridad Domiciliario gestionará usuarios, datos de los sensores y luminarias, para ello se ha seleccionado al gestor MySQL como motor de base de datos, por cumplir con las siguientes características:

- Servidor incorporado en el Sistema Operativo Linux distribución Centos

- Servidor de código abierto
- Base de Datos relacional, multiplataforma y multiusuario
- Compatible con tecnología Java, Servlets y JSP
- No requiere el uso de licencias
- Servidor ampliamente difundido

2.8.1 CONEXIÓN AL SERVIDOR MYSQL

Para conectarse al Servidor MySQL, se necesita de un nombre de usuario (*login*) y una contraseña (*password*).

Para establecer la conexión con el servidor MySQL se debe ejecutar el siguiente comando en un terminal:

mysql -u root -p

Al ejecutar el comando, el servidor solicita una contraseña de acceso.

2.8.2 CREACIÓN Y USO DE BASE DE DATOS

Para crear la base de datos llamada *"seg_domiciliaria",* se debe ejecutar la siguiente instrucción:

mysql> CREATE DATABASE seg_domiciliara;

En el Sistema Operativo Linux, los nombres de las bases de datos son sensibles al uso de mayúsculas y minúsculas, por lo tanto se debe tener cuidado al escribir correctamente el nombre de la base de datos y tablas.

Al crear una base de datos, ésta no se selecciona de manera automática; se debe hacer de manera explícita, para ello se usa el comando USE.

mysql> USE seg_domiciliara

La base de datos se crea una sola vez, pero se debe seleccionar cada vez que se inicia una sesión en MySQL.

2.8.3 CREACIÓN DE TABLAS Y RELACIONES

Para la gestión de usuarios en el Sistema de Seguridad Domiciliario se necesita una tabla que permita el registro de usuarios admitidos, así como, el tipo de acceso a los datos; para cumplir este requerimiento, se crea dos tablas, una llamada Usuario en la que se deberán ingresar todos datos como son: Nombre, Apellido, Clave (de ingreso al Sistema), e-mail (para próximas notificaciones) y el número celular, como se muestra en la Figura 2.34

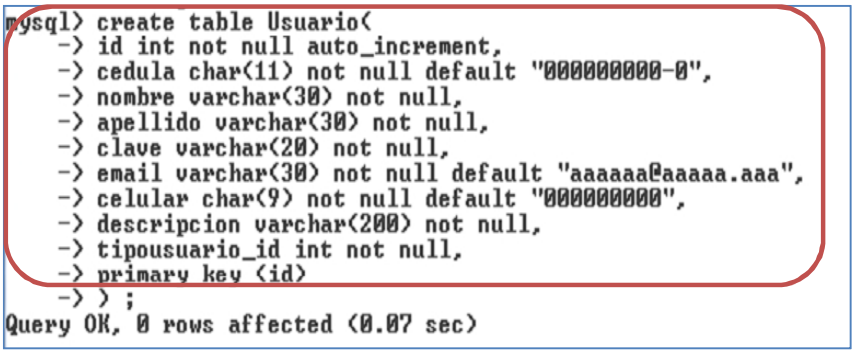


Figura 2.34: Creación Tabla Usuario

Una tabla que contenga los tipos de Usuarios que van a manejar el Sistema de Seguridad Domiciliario, y así poder asignar permisos. Solo serán dos tipos de usuarios: Administrador y Usuario Registrado. En la Figura 2.35 se muestra la tabla Usuario y en la Figura 2.36 se presenta la tabla Tipo Usuario.

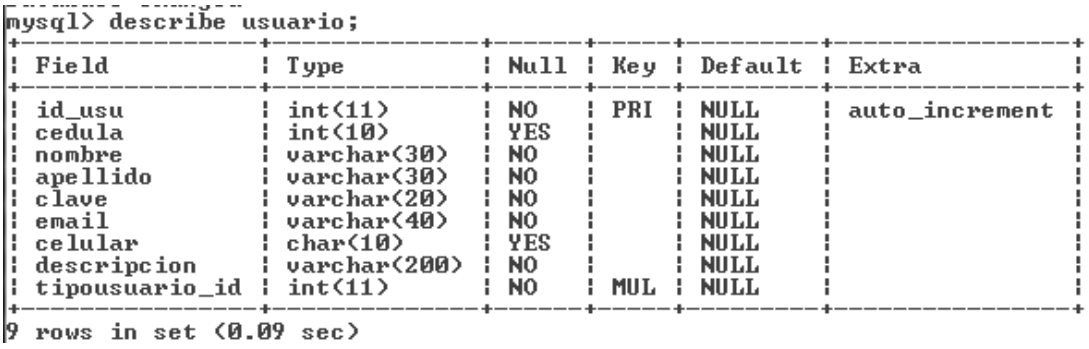


Figura 2.35: Descripción Tabla Usuario

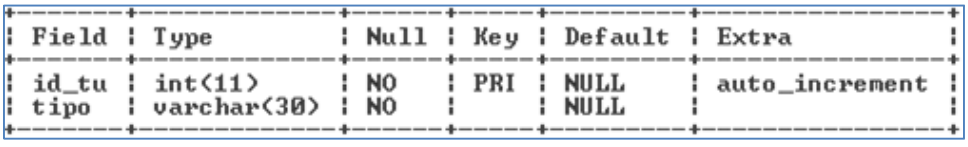


Figura 2.36: Descripción Tabla Tipo Usuario

2.8.4 BACKUP DE LA BASE DE DATOS

Para tener respaldo en la base de datos en lo que respecta a los usuarios u tablas de los dispositivos se puede establecer respaldos. En el terminal se ejecuta la siguiente instrucción para realizar un *backup*.

mysqldump --opt -u root -p seg_domiciliara > seg_domiciliara_backup

Una vez ejecutado esta instrucción se solicitará el *password* del usuario y creará el archivo de *backup* en el directorio en el cual se ejecute la instrucción antes mencionada.

2.9 DESARROLLO DEL APLICATIVO WEB DEL SISTEMA

Un Sistema informático está compuesto por *hardware* y *software*. Donde el *hardware* se analizó con anterioridad. Sin embargo, respecto del *software*, su construcción y resultados han sido históricamente cuestionados debido a los problemas asociados, entre ellos podemos destacar los siguientes:

- Los Sistemas no responden a las expectativas de los usuarios.
- Los programas “fallan” con cierta frecuencia.
- Los costes del *software* son difíciles de prever y normalmente superan las estimaciones.
- La modificación del *software* es una tarea difícil y costosa.
- El *software* se suele presentar fuera del plazo establecido y con menos prestaciones de las consideradas inicialmente.

A continuación se presenta el proceso de desarrollo del aplicativo del Sistema de Seguridad Domiciliario, donde se describe; la herramienta de programación y el desarrollo del interfaz gráfico.

La programación del Sistema de Seguridad Domiciliario se realiza con la herramienta NetBeans en lenguaje Java, JSP y Servlets.

2.9.1 HERRAMIENTA NETBEANS [33]

Netbeans es una herramienta de programación que permite el desarrollo de:

- Aplicaciones Java de Escritorio
- Aplicaciones Móviles
- Aplicaciones *WEB*

Adicional NetBeans ofrece las siguientes características:

- Herramienta de licencia gratuita
- Herramienta de código abierto
- Herramienta fácil y eficiente para la administración de proyectos
- Herramienta de programación en múltiples lenguajes
- Herramienta de interfaz amigable
- Herramienta de fácil uso
- Herramienta con idioma en español
- Soporte JavaScript
  - ✓ Ayuda en la sintaxis del lenguaje de programación
  - ✓ Completación de código y análisis de tipeo
  - ✓ Verificación de sintaxis
- Mejoras de Desempeño
  - ✓ Inicio 40%masrapido a las versiones anteriores
  - ✓ Menor consumo de memoria
- Soporte para los APIs *Web*
  - ✓ Fácil creación de aplicaciones
  - ✓ Compatible con lenguaje Java y Servlets

La herramienta de programación NetBeans se muestra a continuación en siguiente la Figura 2.37

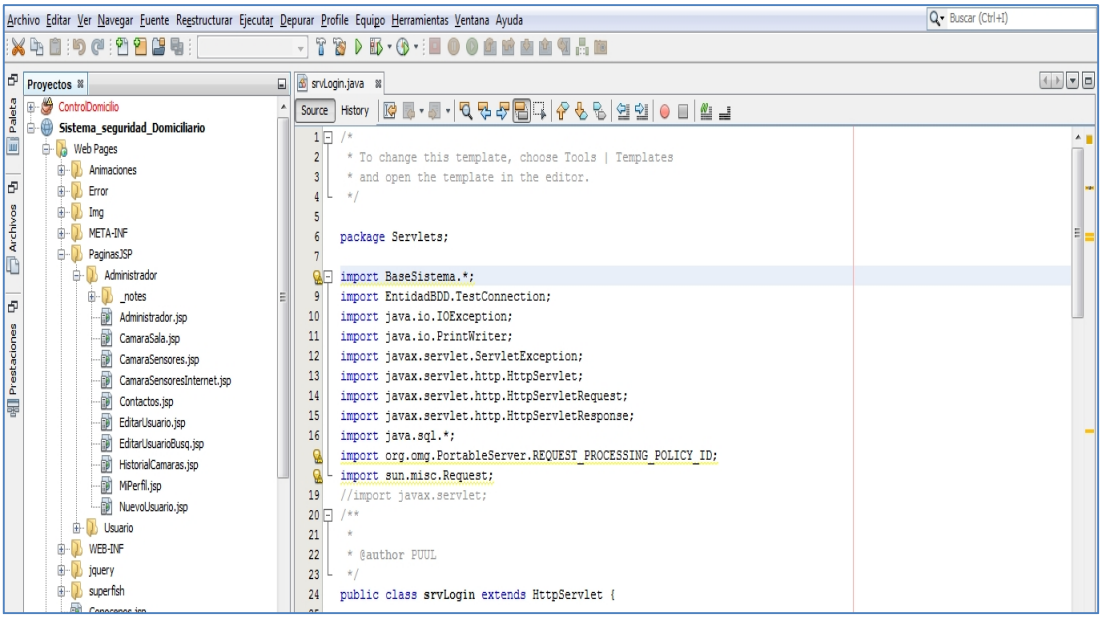


Figura 2.37: Herramienta NetBeans

2.9.2 DESARROLLO DEL INTERFAZ GRÁFICO

A continuación se presentan los procesos seguidos para el desarrollo del aplicativo *web* de Sistema de Seguridad Domiciliario.

2.9.2.1 Procesos de desarrollo del Software [34]

El proceso de desarrollo de *software* tiene como propósito la producción eficaz y eficiente de un producto *software* que reúna los requisitos del cliente. Dicho proceso, en términos globales se muestra en la Figura 2.38

Figura 2.38: Proceso desarrollo de *software* [34]

Adicionalmente el *software* es intangible y por lo general muy abstracto, esto dificulta la definición del producto y sus requisitos. Esto hace que los requisitos sean difíciles de consolidar tempranamente.

Para el desarrollo del Sistema de Seguridad Domiciliario se tomará como base el Proceso Unificado *Rational* (RUP)[49].

2.9.2.2 Proceso de Unificado Rational [35]

El Proceso Unificado de Rational (RUP) es una metodología de desarrollo de *software* orientada a objetos creada por *Rational Software Corporation*. Como toda metodología de desarrollo *software* su finalidad es convertir las especificaciones que da el cliente en un sistema *software*. Las características que tiene el RUP son:

- Dirigido por casos de uso
- Centrado en la arquitectura
- Ciclo de vida iterativo e incremental

2.9.2.2.1 Dirigido a casos de uso [36]

Las actividades de: especificación, análisis, diseño, verificación y mantenimiento son guiados por los casos de uso que describen la funcionalidad de la aplicación.

Los casos de uso definen la funcionalidad de la aplicación, adicionalmente constituyen guías transversales que dirigen todas las fases del proceso:

- Especificación
- Análisis
- Diseño
- Verificación y prueba

[49] RUP *(Rational Unified Process*): Es un proceso de desarrollo de *software* desarrollado por la empresa Rational *Software*. Junto con el Lenguaje Unificado de Modelado UML, constituye la metodología estándar más utilizada para el análisis, diseño, implementación y documentación de sistemas orientados a objetos.

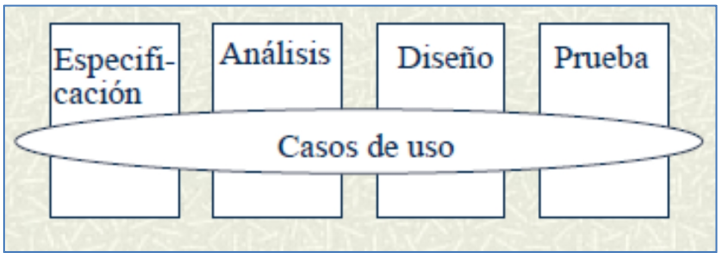


Figura 2.39: Caso de Uso [36]

Por último, los casos de uso sirven de base para establecer las pruebas funcionales que validan la operatividad de la aplicación.

2.9.2.2.2 Centrado sobre la Arquitectura [36]

La arquitectura se formula desde el inicio del proyecto y se toma como referencia central del proceso. Ésta se introduce para satisfacer no solo las necesidades de la funcionalidad, sino también para conseguir flexibilidad frente a la evolución posterior.

2.9.2.2.3 Iterativo e Incremental [37] [38] [39]

Este permite construir un proyecto en etapas incrementales, donde cada etapa agrega funcionalidad. Las iteraciones hacen referencia a pasos en el flujo de trabajo y los elementos, al crecimiento del *software*. Para seleccionar una iteración, se lo hace en base al tratamiento de un grupo de casos de uso, de tal modo que se amplía la utilidad del Sistema y se pueden apreciar acertadamente los riesgos de mayor relevancia.

Figura 2.40: Modelo de desarrollo iterativo incremental [34]

Entre las ventajas del modelo incremental se encuentran:

- Los elementos son integrados progresivamente.

- Los riesgos pueden ser descubiertos en etapas tempranas.
- Resulta un producto más robusto ya que los errores se corrigen en cada iteración.
- Los clientes no esperan hasta el fin del desarrollo para utilizar el sistema. Pueden empezar a usarlo desde el primer incremento.
- Los clientes pueden aclarar los requisitos que no tengan claros conforme ven las entregas del sistema.
- Las partes más importantes del sistema son entregadas primero, por lo cual se realizan más pruebas en estos módulos y el riesgo de encontrar fallos disminuye.

2.9.2.3 Fases del Proceso Unificado Rational [34]

El proceso unificado consiste en una serie de ciclos, donde al final de cada ciclo se tiene una versión del producto. Las fases de cada ciclo son: Inicio, Elaboración, Construcción y Transición. Cada fase termina con un hito[50] (Figura 2.41), que se determina por la disponibilidad de un conjunto de artefactos (modelos o documentos desarrollados hasta cierto punto)

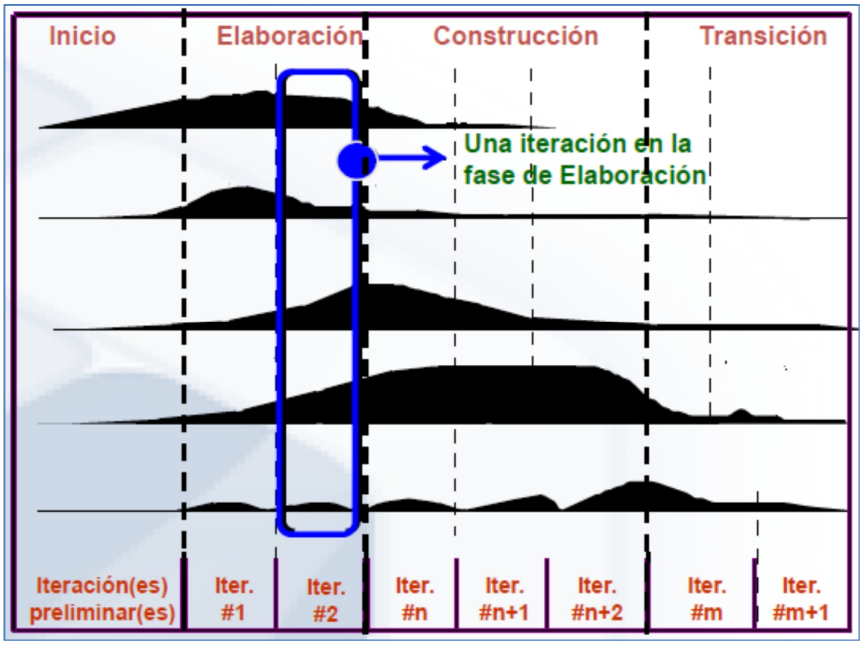


Figura 2.41: Fases del Proceso Unificado Rational [34]

[50] Hito: Punto límite entre fases o iteraciones

- **Inicio**: Establece la oportunidad y alcance del proyecto, se identifican todas las entidades externas y con las que se trata (actores) y se define al iteración a un alto nivel de abstracción.
- **Elaboración**: Se analiza el dominio del problema, establece una arquitectura, desarrolla un plan del proyecto y elimina elementos de mayor riesgo para el desarrollo exitoso del proyecto.
- **Construcción**: Se tiene énfasis en la producción eficiente y no en la creación intelectual.
- **Transmisión**: El objetivo es traspasar el *software* desarrollado a los usuarios; ya instalado, surgirán nuevos elementos que implicarán nuevos desarrollos.

2.9.2.4 Flujos de Trabajo del Proceso Unificado Rational

En cada iteración existen los siguientes flujos de trabajo:

1. Requisitos: Capturar lo que el Sistema debe saber (Casos de Uso).
2. Análisis: Depurar y estructurar los requisitos.
3. Diseño: Definir las actividades de implementación del sistema.
4. Implementación: Construir el *software.*
5. Pruebas: Verificar que la implementación funcione de manera adecuada.

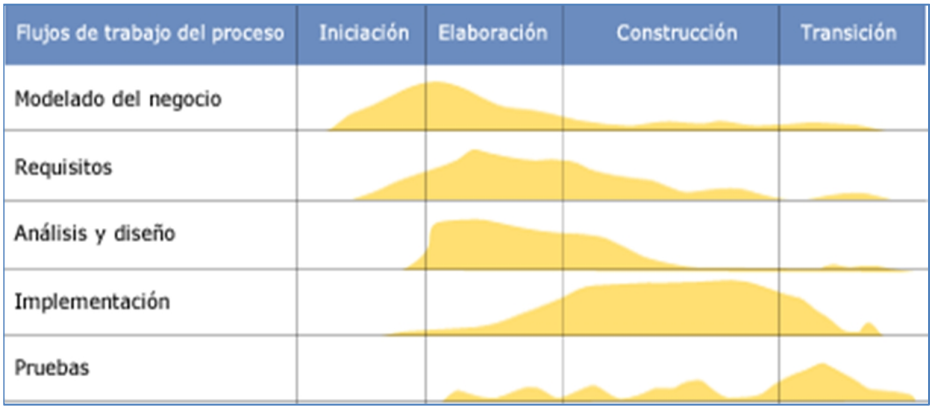


Figura 2.42: Flujos de Trabajo del Proceso Unificado Rational [34]

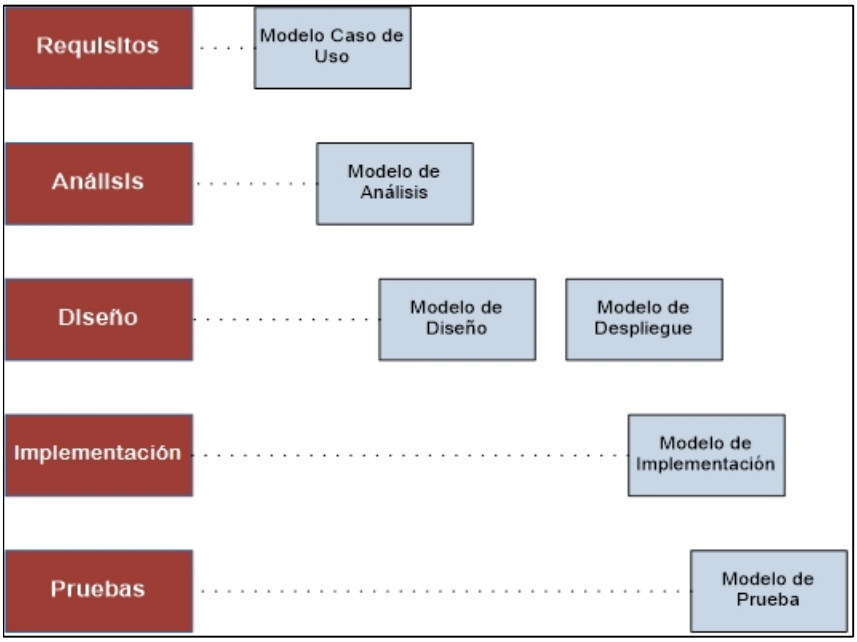


Figura 2.43: Flujos del Proceso Unificado [36]

2.9.2.5 Casos de Uso

Los casos de uso ha sido adoptados universalmente para la captura de requisitos de sistemas de *software* en general, adicionalmente estos dirigen el proceso de desarrollo en su totalidad.

Los casos de uso implican el diseño del modelo de negocio, modelo del dominio.

2.9.2.6 Análisis del Sistema

El Sistema de Seguridad Domiciliario es un aplicativo que proporciona un mecanismo de seguridad a la casa mediante Video Vigilancia, detección de intrusos, gas nocivo y control de luminarias del hogar. Con estas consideraciones se pretende desarrollar un *software* para la gestión de los ítems antes mencionados por parte de los integrantes del domicilio, así como, también por el personal autorizado.

Para este análisis se toma en cuenta el personal que tendrá acceso al Sistema como son: Administradores y Usuarios.

Acceso Administradores:

- Administración de usuarios del Sistema

- Control total del Sistema de Seguridad Domiciliario: Video vigilancia, luminarias, mensajes SMS.
- Gestión de los contactos a los que se enviará las alertas generadas el Sistema de Seguridad Domiciliario.

Acceso Usuarios

- Control de su perfil de usuario
- Control parcial del Sistema de Seguridad Domiciliario: Video vigilancia, mensajes SMS.

Adicionalmente el Sistema de Seguridad Domiciliario, estará disponible desde Internet por esta razón se considera:

- Permitir el acceso al sistema por medio de un *login* y *password*.
- Proporcionar información del Sistema.
- Proporcionar información de los servicios que brinda el Sistema.
- Proporcionar un medio de contacto con los administradores del Sistema.

2.9.2.7 Modelos de Caso de Uso

2.9.2.7.1 Definición de Actores

ACTORES	FUNCIONALIDAD
Invitado	Visualizar información del Sistema Realizar consultas acerca del sistema
Usuario	Visualizar información del Sistema Control del perfil de usuario Acceso a video vigilancia del domicilio Envío de mensajes SMS
Administrador	Visualizar información del Sistema Administración de usuarios Acceso a video vigilancia del domicilio Control de luminarias del domicilio Envío de mensajes SMS

Tabla 2.10: Definición de Actores

2.9.2.7.2 Diagrama de Caso de Uso

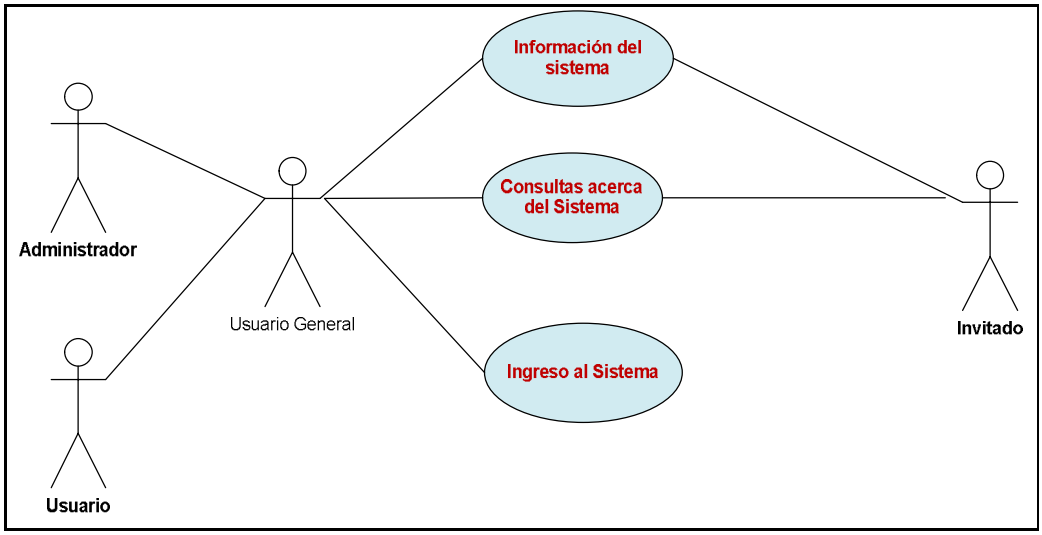


Figura 2.44: Diagrama Caso de Uso Ingreso al Sistema

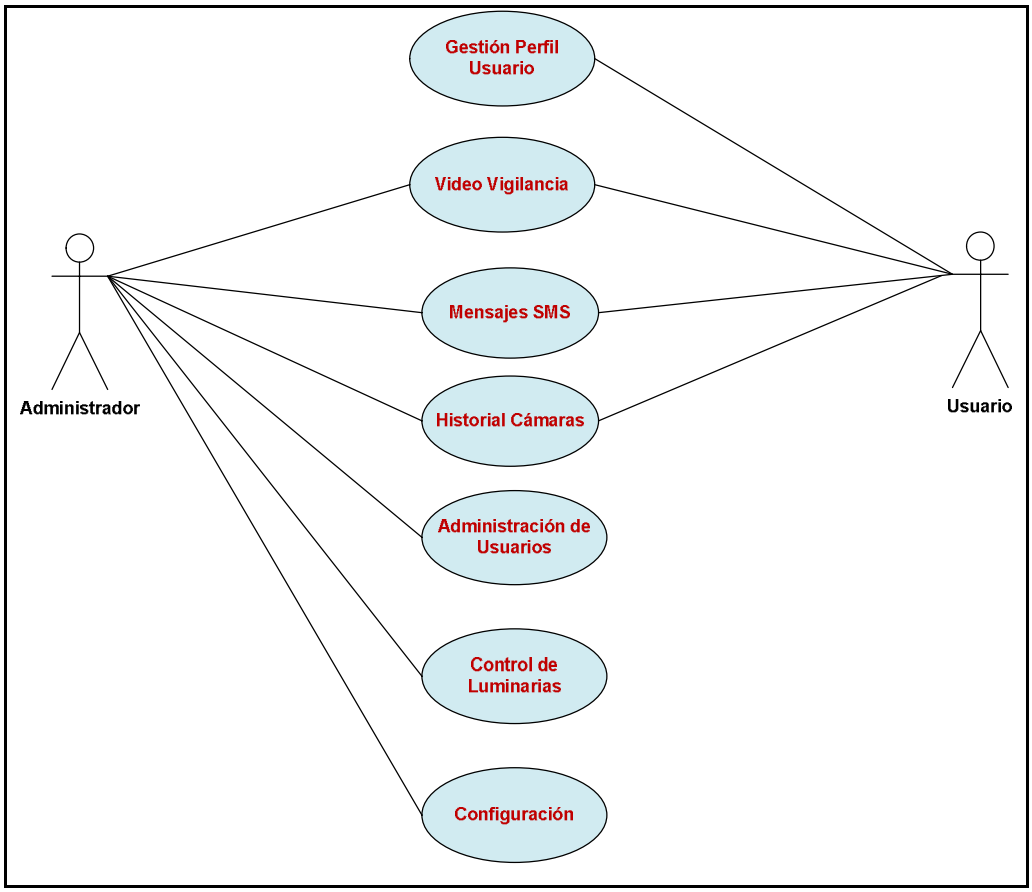


Figura 2.45: Diagrama Casos de Uso Manejo Sistema

2.9.2.7.3 Especificación de los Casos de Uso

CASO DE USO	DESCRIPCIÓN
Ingreso al Sistema	El Actor Administrador y Usuario ingresa al Sistema con un *login* y *password*.
Información del Sistema	El Sistema permite la visualización de la razón y misión.
Servicios del Sistema	El Sistema permite la visualización de los servicios que se ofrece: Video vigilancia, protección contra intrusos y gas nocivo, control de luminarias y mantenimiento de equipos.
Consultas del Sistema	El Sistema permite la formulación de preguntas y sugerencias a los administradores por medio del envío de un e-mail.
Gestión Perfil Usuario	El Sistema permite la gestión del perfil de usuario. Cambio de los datos personales y contraseña de ingreso al Sistema.
Video vigilancia	El Sistema permite la visualización de cámaras instaladas en el domicilio a usuarios autenticados en el sistema.
Mensajes SMS	El Sistema permite el envío de mensajes SMS por medio de la página web a usuarios autenticados en el sistema.
Historial Cámaras	EL Sistema permite la visualización de videos grabados con anterioridad por las cámaras IP
Administración de Usuarios	El Sistema permite la administración de usuarios: Añadir usuarios, editar usuarios (Cambio de datos personales y contraseña) y eliminar usuarios.
Alertas Sistema	Los sensores de movimiento y gas nocivo envían alertas al sistema para alertar al usuario en caso de algún incidente.

Tabla 2.11: Especificación Diagrama de Casos de Uso

2.9.2.7.4 Especificación de Casos de Uso

ANÁLISIS CASO DE USO: Ingreso del Sistema	
ID	Ingreso del Sistema
Descripción	El Actor ingresa al Sistema.
Actividades: 1. El Actor: Ingresa al Sistema con *login* y *password*. 2. El Sistema Comprueba la identidad del usuario 3. El Sistema permite al acceso al actor y otorga los privilegios.	
Alternativas: 1. Comprobada la identidad del Actor se permite el acceso. 2. No comprobada la identidad se carga nuevamente la página web principal del Sistema.	

Tabla 2.12: Caso de Uso Ingreso Sistema

ANÁLISIS CASO DE USO: Video Vigilancia	
ID	Video Vigilancia
Descripción	El usuario autenticado accede a la página *web* de video vigilancia y observa en tiempo real las cámaras IP.
Precondición	El Actor Administrador o Usuario ingresa al Sistema.
Actividades: 1. El Actor Administrador y Usuario accede a la página *web* de video vigilancia. 2. El Sistema permite la visualización de las cámaras IP instaladas en el Domicilio.	
Alternativas: 1. El actor puede visualizar las cámaras IP y estado de sensores en caso de estar habilitadas. 2. El sistema presenta una alerta gráfica de desconexión de cámaras IP o sensores.	
Pos condición	El actor observa el video proporcionado por las cámaras IP.

Tabla 2.13: Caso de Uso Video Vigilancia

ANÁLISIS CASO DE USO: Mensajes SMS	
ID	Mensajes SMS
Descripción	El usuario autenticado accede al módulo de envío de mensajes SMS en una página *web* del Sistema.
Precondición	El Actor Administrador o Usuario ingresa al Sistema.
Actividades: 1. El actor ingresa al módulo de envío mensajes SMS. 2. El actor ingresa el número y mensaje a ser enviado. **3.** El Sistema con un proceso envía el mensaje.	
Alternativas: 1. En caso de envío satisfactorio el Sistema carga nuevamente la página *web* de envío de mensajes. 2. En caso de envío fallido un proceso del Sistema genera un error de envío y carga la página *web* de envío de mensajes.	
Pos condición	El Receptor del mensaje revisa el contenido.

Tabla 2.14: Caso de Uso Mensajes SMS

ANÁLISIS CASO DE USO: Control de Luminarias	
ID	Control de Luminarias
Descripción	El Actor Administrador: Gestiona el encendido o apagado de las luminarias del domicilio desde la página *web*.
Precondición	El Actor Administrador ingresa al Sistema.
Actividades: 1. El Administrador ingresa al módulo de control de luminarias del domicilio. Enciende o apaga luminarias en la página *web*. 2. El Sistema cambia el estado de luminarias en la base de datos. 3. Un proceso del Sistema se comunica con el micro controlador conectado el servido por medio serial. **4.** El Sistema cambia el estado gráfico de la luminaria en la página *web*.	
Pos condición	Se visualiza en el prototipo del prueba el encendido o apagado de las luminarias.

Tabla 2.15: Caso de Uso Control Luminarias

ANÁLISIS CASO DE USO: Alertas Sistema	
ID	Alertas Sistema
Descripción	El Actor Sensor: Envía alertas al Sistema en caso de incidentes
Precondición	Generación de incidencia.
Actividades: 1. El Sensor envía una señal a sistema en caso de incidencia. 2. La incidencia cambia un parámetro en la base de datos. 3. Un proceso del Sistema genera las Alertas para el Usuario.	
Pos condición	Generación de alertas vía e-mail o SMS.

Tabla 2.16: Caso de Uso Alertas Sistema

2.9.2.8 Modelo de Análisis

2.9.2.8.1 Diagramas de Clases de Análisis

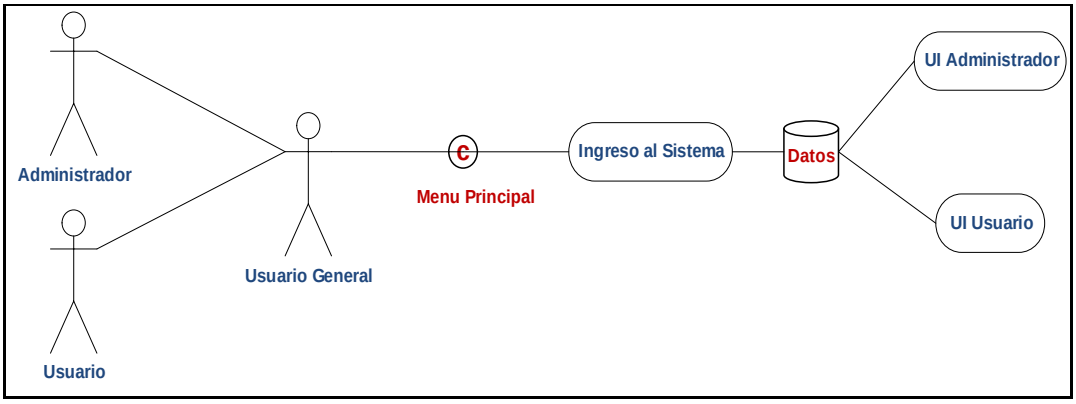


Figura 2.46: Diagrama Ingreso al Sistema

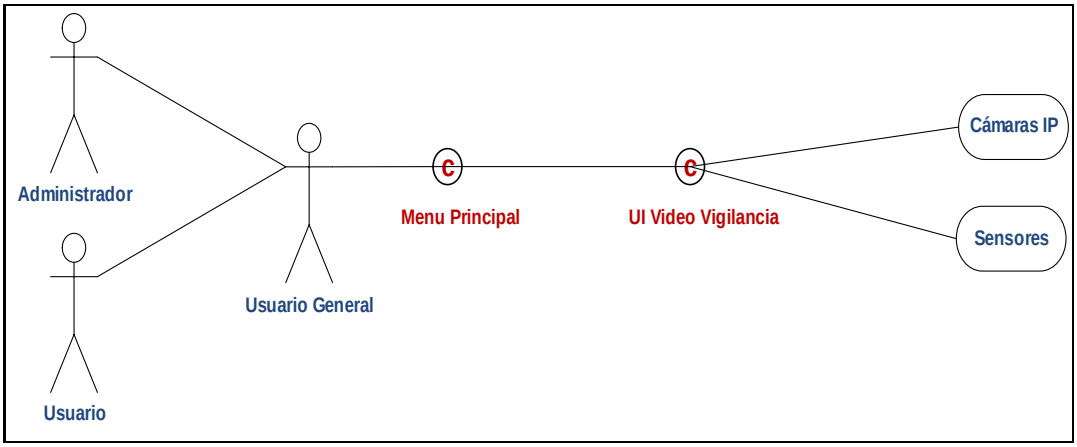


Figura 2.47: Diagrama Video Vigilancia

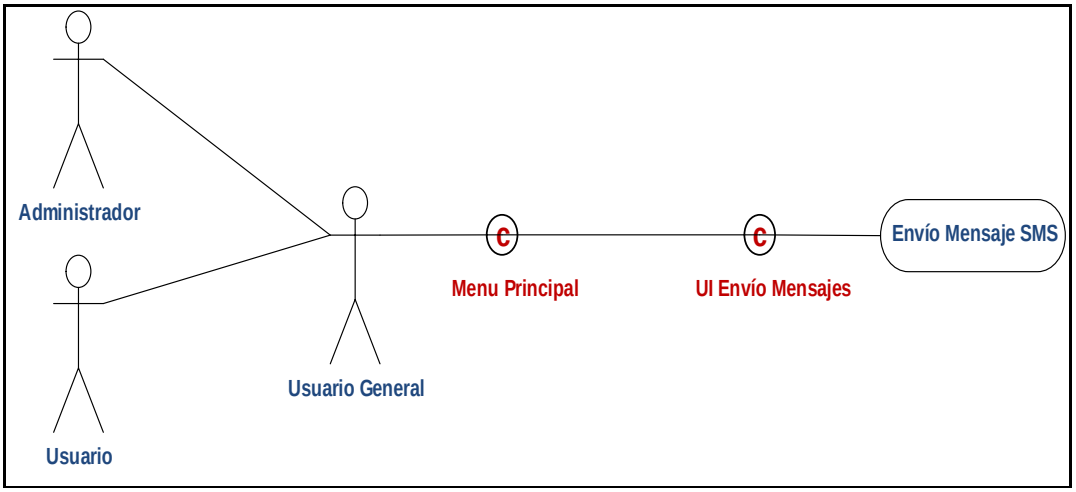


Figura 2.48: Diagrama Mensajes SMS

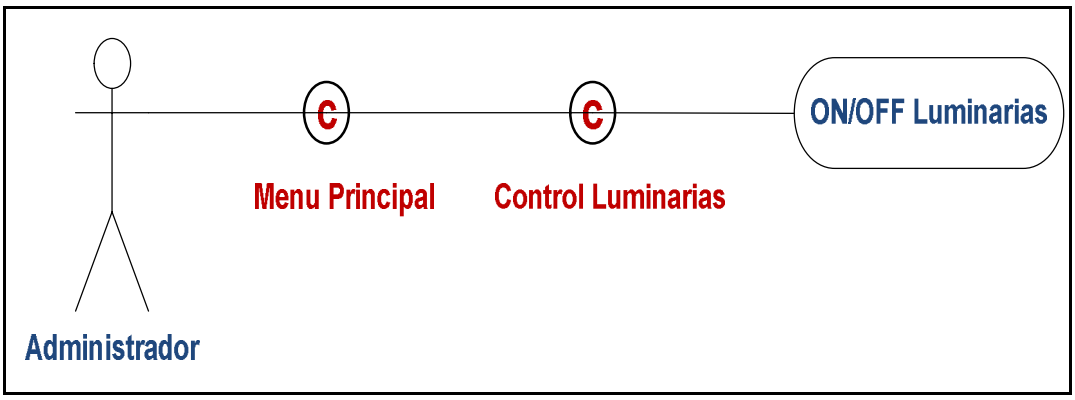


Figura 2.49: Diagrama Control Luminarias

2.9.2.8.2 Diagramas de Secuencia [30]

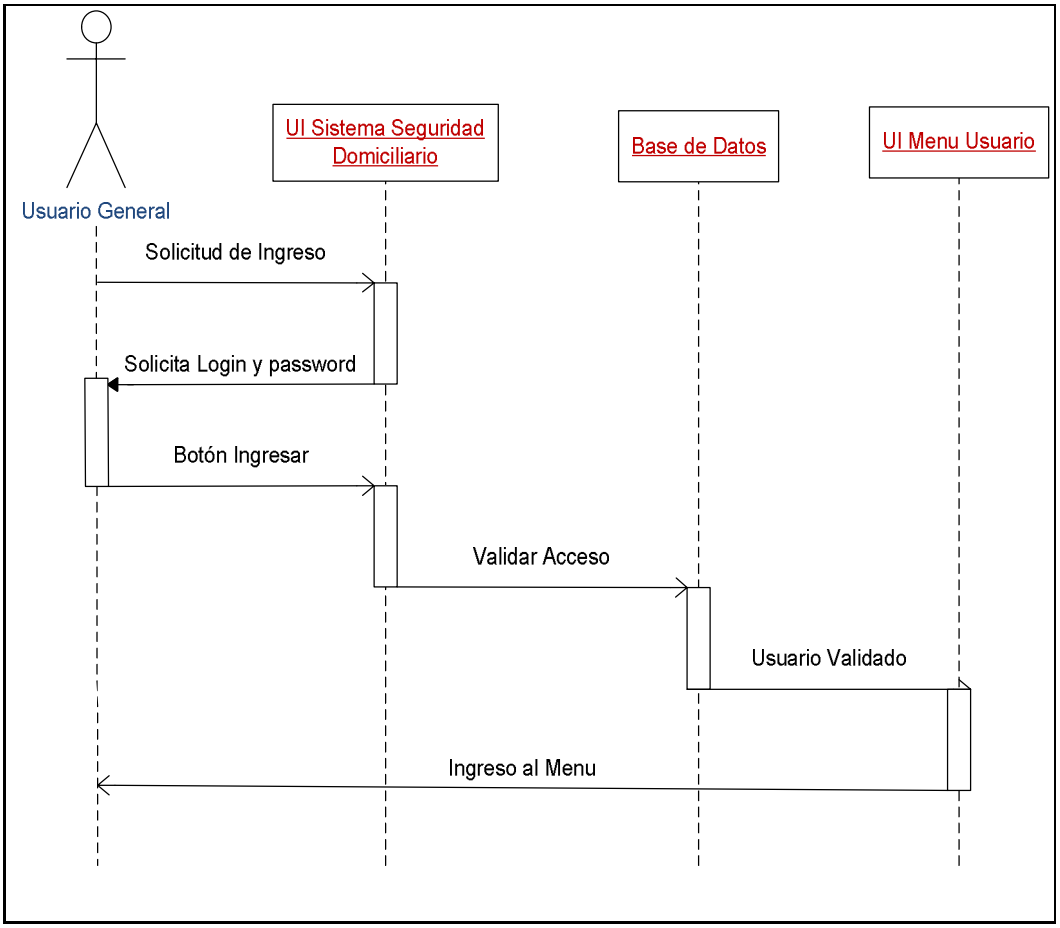


Figura 2.50: Secuencia Ingreso Sistema

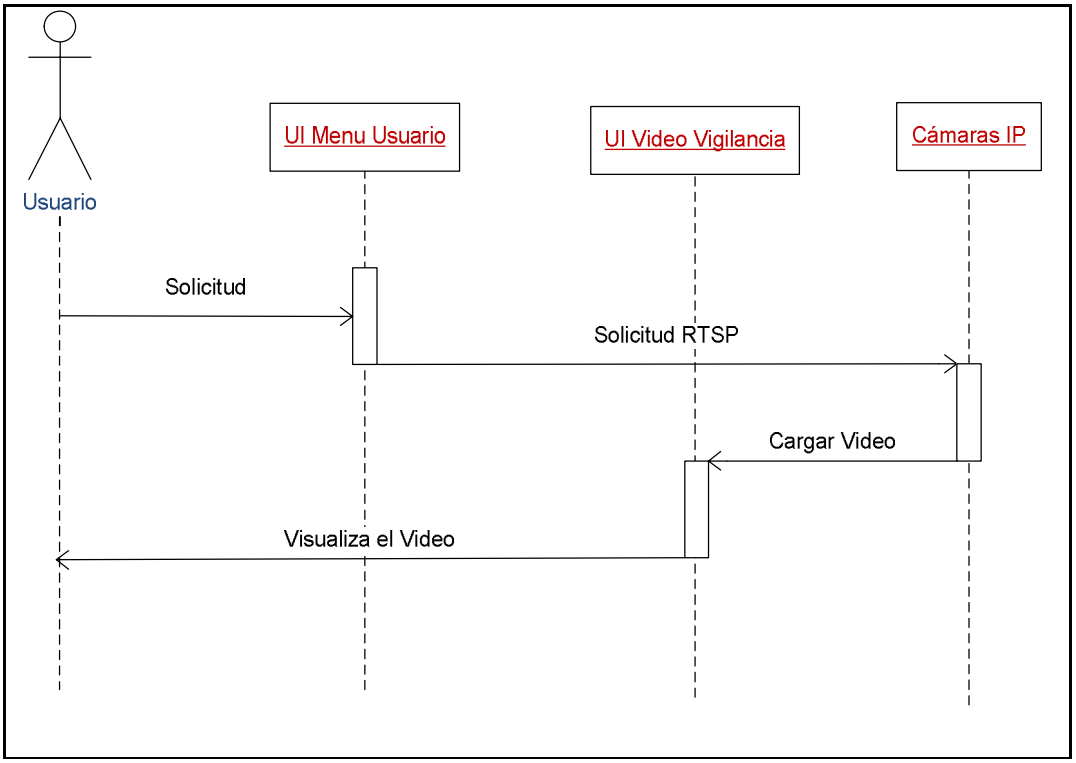


Figura 2.51: Secuencia Video Vigilancia

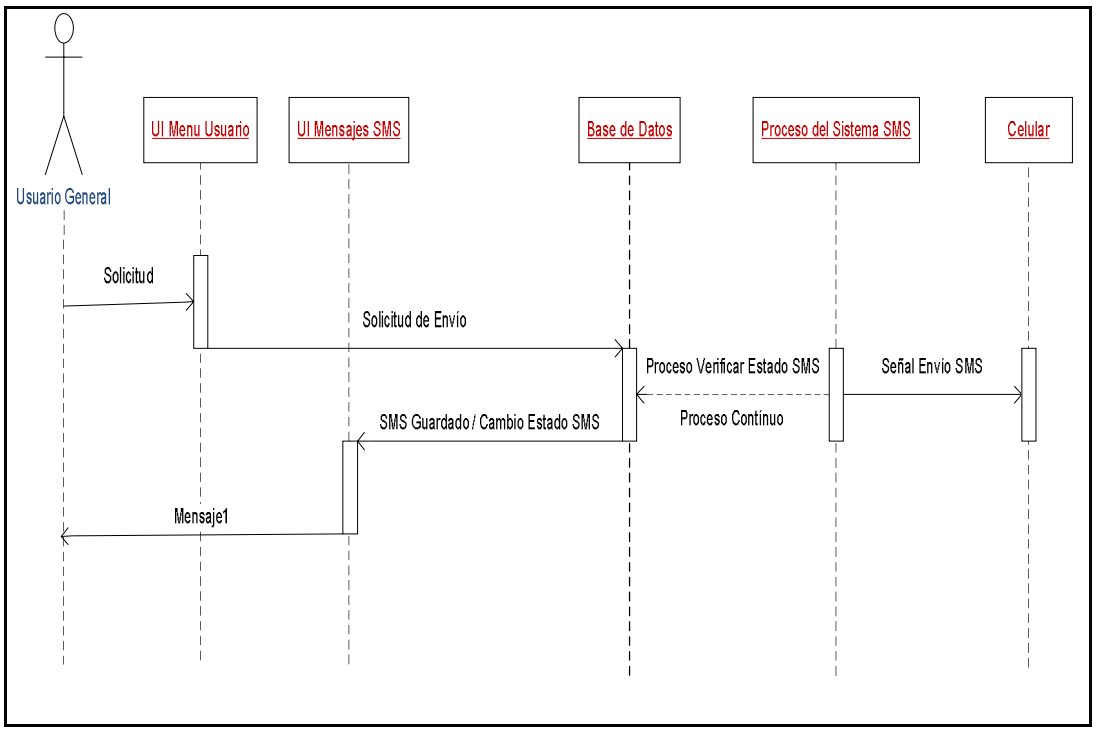


Figura 2.52: Secuencia Mensajes SMS

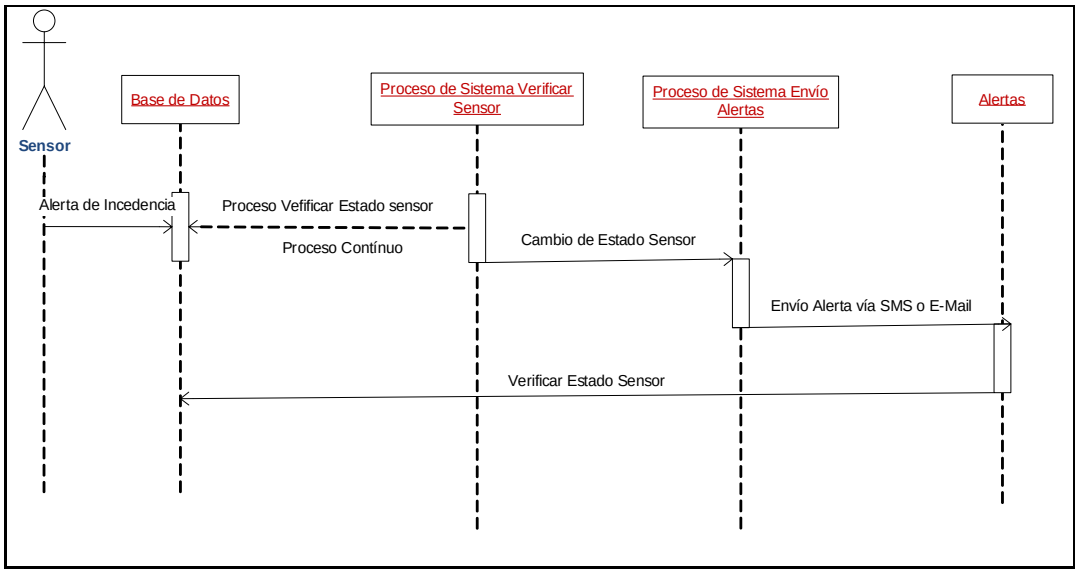


Figura 2.53: Secuencia Control Luminarias

2.9.2.9 Diseño del interfaz de Usuario

2.9.2.9.1 Diagrama de Navegación

Para el diseño del interfaz se toma un modelo estándar para todo el Sistema como se muestra en las Figuras 2.54, 2.55 y 2.56

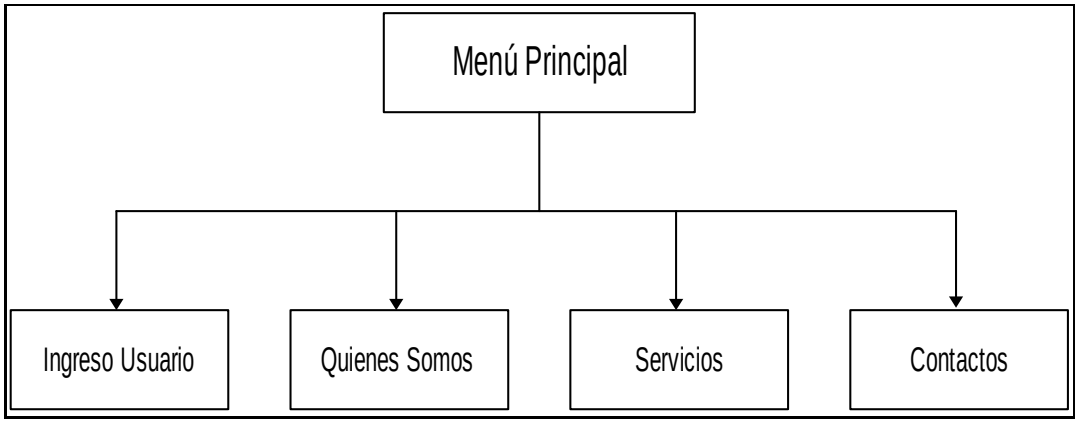


Figura 2.54: Diseño Menú Principal

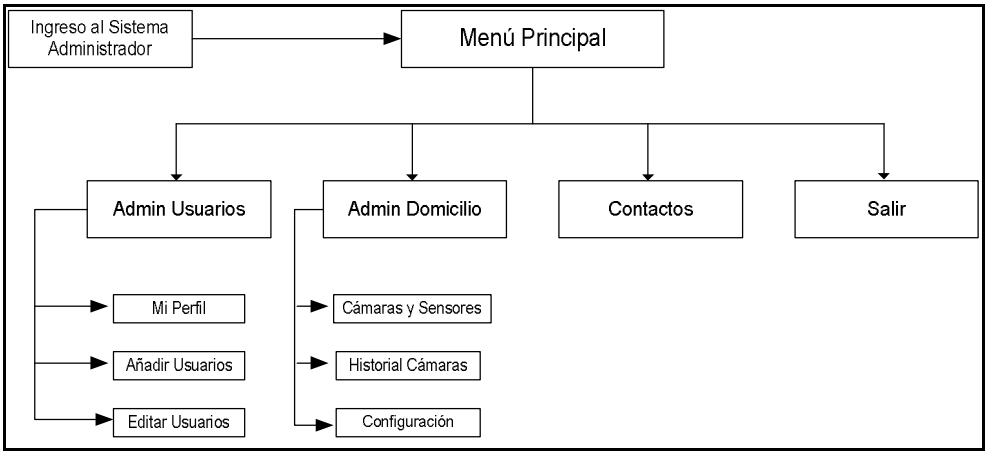


Figura 2.55: Diseño Menú administrador

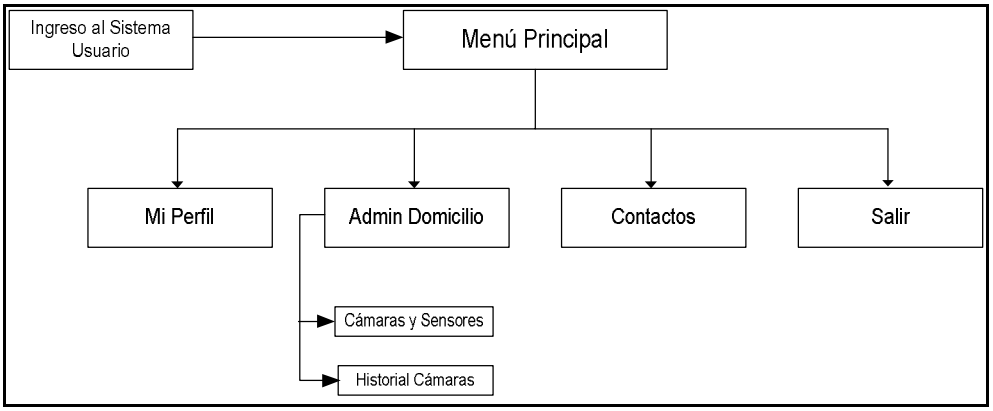


Figura 2.56: Diseño Menú Usuario

2.9.2.9.2 Descripción de Interfaz de Administrador y Usuario

La distribución de elementos en el interfaz gráfico se presenta en la Figuras 2.57

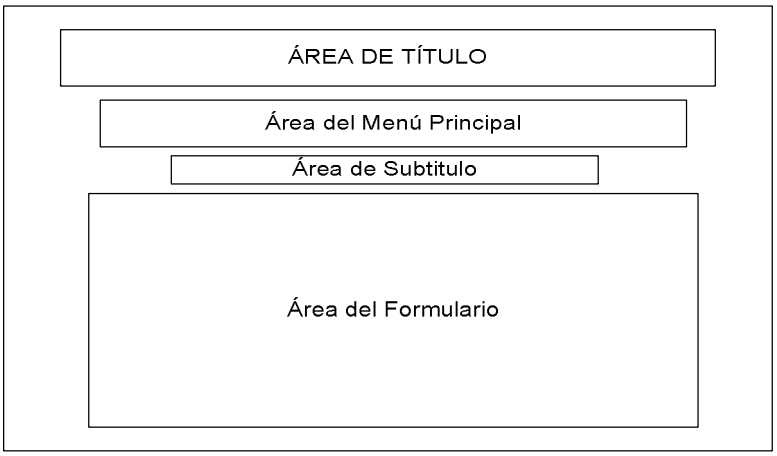


Figura 2.57: distribución Interfaz Gráfico

- **Área de Título:** Presenta el nombre del Sistema.
- **Área Menú Principal:** Presenta los diferentes módulos de trabajo que proporciona el Sistema.
- **Área de Subtítulo:** Presenta el nombre del usuario ingresado.
- **Área de Formulario:** Presenta el área de trabajo del Sistema

2.9.3 DESARROLLO DE LAS PÁGINAS WEB

Las páginas *web* se encargarán de ser el enlace entre la aplicación y los usuarios de sistema de seguridad domiciliario. Como inicio de la aplicación se tienen las siguientes paginas JSP:

- Index.jsp
- Conócenos.jsp
- Servicios.jsp
- Contactos.jsp

Adicionalmente por el nivel de acceso se tiene dos tipos de páginas *Web* según el nivel de privilegios (usuario o administrador), de acuerdo a esto se tiene las siguientes páginas:

- Administrador
    - ✓ Administración Usuarios
        - ❖ MiPerfil.jsp
        - ❖ AñadirUsuarios.jsp
        - ❖ EditarUsuarios.jsp
    - ✓ Administración Domicilio
        - ❖ CamarasSensores.jsp
        - ❖ HistorialCamaras.jsp
        - ❖ Configuracion.jsp
    - ✓ Contactos.jsp

- Usuario
  - ✓ Miperfil.jsp
  - ✓ Administración Domicilio
    - ❖ CamarasSensores.jsp
    - ❖ HistorialCamaras.jsp
  - ✓ Contactos.jsp

2.9.3.1 Página web índex

La página *index.jsp* es el inicio del aplicativo de Sistema de Seguridad Domiciliario, la página básicamente está desarrollada en lenguaje JSP, como se muestra en la Figura 2.58

Esta página presenta el "*login"* de usuario para ingreso al sistema y los diferentes módulos del mismo. Se debe tomar en cuenta que el Sistema de Seguridad Domiciliario tiene dos niveles de acceso, uno con nivel de administrador, mismo que brinda todos los privilegios que el sistema otorga y el segundo nivel es de usuario el cual tiene acceso restringido a varios módulos del Sistema *Web*.

Figura 2.58: Página *index.jsp*

Para poder gestionar el acceso de usuarios mediante el "*login"*, se estableció un servlet, mostrado a en la Figura 2.59

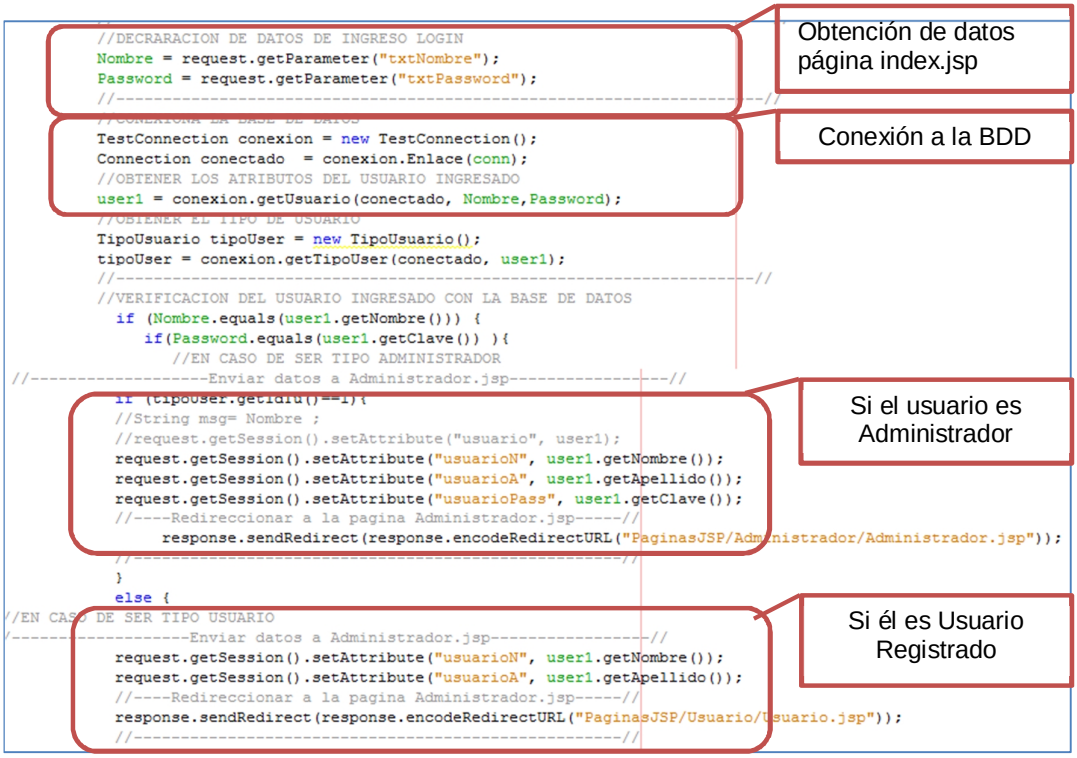


Figura 2.59: Servlet srvlogin

Como se muestra en la Figura 2.60 el servlet "*srvlogin"* se adquiere los datos de usuario y contraseña de la página *index.jsp*, con los cuales se realiza una consulta a la base de datos, obteniendo un objeto usuario con los atributos: nombre, apellido, contraseña, email, teléfono y tipo de usuario (usuario o administrador). Adquiridos estos parámetros, el servlet en primera instancia verifica la existencia del usuario y la contraseña introducida, en caso de ser correctos los valores, verifica el tipo de usuario para otorgar el nivel de acceso al Sistema de Seguridad domiciliario, en caso de error en los datos ingresados se regresa a la página *index.jsp*.

2.9.3.2 Página *web* Conócenos

La página *Conocenos.jsp* describe la razón social del Sistema de Seguridad Domiciliario, es decir se presenta la Misión y Visión del Sistema *Web*.

Figura 2.60: Página *Conócenos.jsp*

2.9.3.3 Página web Contactos

La página *Contactos.jsp*, tiene dos modalidades de funcionamiento, una para usuarios del sistema *web* y la otra para usuarios visitantes:

- Usuarios Visitantes: La página *Contactos.jsp"* para estos usuarios se muestra en la Figura 2.61

Figura 2.61: Página *Contactos.jsp*

Para este tipo de usuarios es obligatorio el ingreso de los siguientes parámetros para realizar una consulta al administrador del Sistema Web: Nombre, Apellido, E-mail, Dirección, Teléfono, Ciudad y Comentario.

La página toma los datos antes mencionados y crea un e-mail dirigido a la cuenta de administrador con el mensaje escrito por un usuario visitante.

Este e-mail es construido en un servlet con los datos obtenidos de la página *Contactos.jsp*, la programación de envío email se muestra en la Figura 2.62

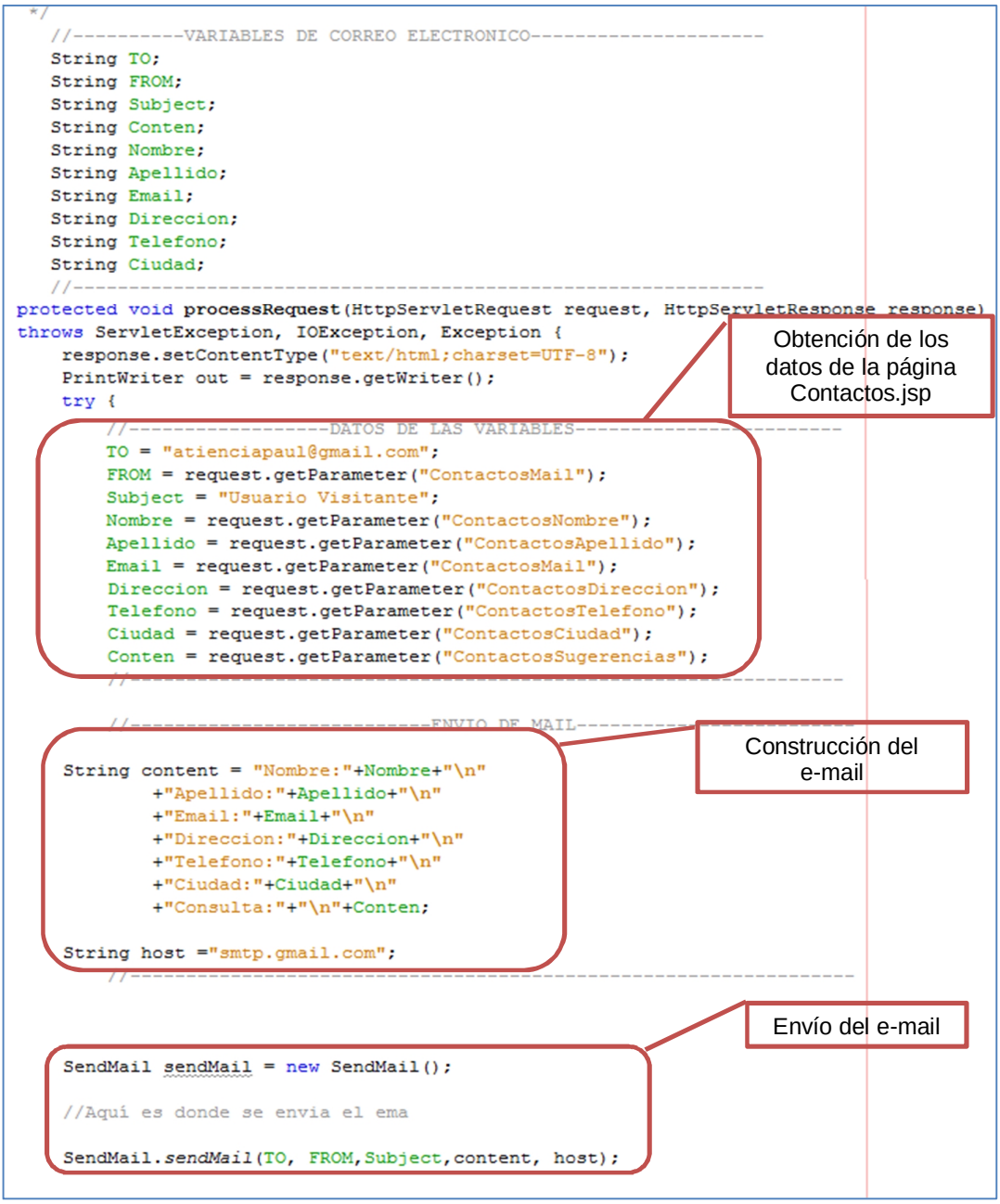


Figura 2.62: Programación Envío e-mail

Como de observa en la Figura 2.62; para el uso de la instrucción*:*

" SendMail sendMail = new SendMail();" se requiere la librería: "*javax.mail"*.

La librería "*javax.mail"*, se la pude descargar de la siguiente dirección:

http://www.oracle.com/technetwork/java/javamail/index.html

Para el uso de la librería "*javax.mail"*, no se requiere ninguna licencia.

Enviado el e-mail generado en la página contactos el Sistema *Web* regresará a la página de inicio "*index.jsp"*.

- Usuarios Logeados: La página *"Contactos.jsp"* para usuarios validados en el Sistema de Seguridad Domiciliario se muestra en la Figura 2.63

Figura 2.63: Usuario logeados *Contactos.jsp*

Esta página envía un e-mail al administrador, con los valores de asunto y mensaje, ya que los datos de nombre, apellido y e-mail son obtenidos al momento de ingreso al Sistema de Seguridad Domiciliario, utilizando la estructura de la figura 2.62.

2.9.4 DESARROLLO PÁGINAS WEB ADMINISTRADOR

El Sistema de Seguridad Domiciliario tiene dos tipos de ingreso como: administradores y usuarios registrados, a continuación se describen las páginas JSP para administradores.

La página "*Administrador.jsp*", se muestra en la Figura 2.64, y se puede observar que ésta página presenta información del Sistema *Web* dirigido a usuarios administradores.

En página *Administrador.jsp* se identifica al usuario que ha ingresado en la sesión de administrador.

La página contiene el siguiente menú de opciones:

- Administración de Usuarios
- Control Domiciliario
- Contactos
- Salir

Figura 2.64: Administrador.jsp

2.9.4.1 Administración de Usuarios

El menú de Administración de Usuarios se muestra en la Figura 2.65:

El menú de administración de Usuarios presenta las siguientes opciones:

- ✓ Mi Perfil
- ✓ Añadir Usuarios
- ✓ Editar Usuarios

Figura 2.65: Administración Usuarios

2.9.4.1.1 Página web Mi Perfil

La página *"Mi Perfil.jsp"* como se muestra en la Figura 2.66, permite la modificación de los datos del usuario administrador como son: Nombre, Apellido, Cedula, E-mail y Celular.

Figura 2.66: *MiPerfil.jsp*

La página JSP también permite el cambio de contraseña de inicio de sesión del Sistema de Seguridad Domiciliario.

2.9.4.1.2 Página web Añadir Usuarios

La página "*AñadirUsuarios.jsp*" Figura 2.67, permite a un administrador ingresar nuevos usuarios para acceso al Sistema *Web*. En esta modalidad el administrador gestiona dos tipos de privilegios que se otorgará a los nuevos usuarios.

Figura 2.67: *AñadirUsuarios.jsp*

Para la creación de nuevos usuarios es necesario el servlet *AñadirUsuarios*, que se muestra en la Figura 2.68

Figura 2.68: Servlet AñadirUsuario

Como se muestra en la Figura 2.68, se realiza una llamada a *"setUsuario"* (instrucción SQL), encargada de añadir un nuevo usuario en la base de datos, Figura 2.69

```
try {
   System.out.println("Ingresando Usuario espere...");
   Usuario user = new Usuario(0, cedula, nombre, apellido, clave, email, celular, descripcion);

      PreparedStatement psmt = connn.prepareStatement("insert into usuario "
              + "(id_usu,cedula,nombre,apellido,clave,email,celular,descripcion,tipousuario_id) "
              + "values(?,?,?,?,?,?,?,?,?)");
      psmt.setInt(1,0);
      psmt.setString(2,user.getCedula());
      psmt.setString(3,user.getNombre());
      psmt.setString(4,user. getApellido());
      psmt.setString(5,user.getClave());
      psmt.setString(6,user.getEmail());
      psmt.setString(7,user.getCelular());
      psmt.setString(8,user.getDescripcion());
      psmt.setInt(9,tipo);
      psmt.executeUpdate();
      psmt.close();

      System.out.println("Usuario ingresado exitosamente");
   } catch (SQLException e) {
  System.out.println("Error de MySQL: " + e.getMessage());
```

Instrucción SQL para Añadir Usuarios

Figura 2.69: Función SQL Añadir Usuario

2.9.4.2 Control del Domicilio

El Menú de Administración del Domicilio permite la gestión del domicilio, así como, la visualización del historial de las cámaras y configuración de los equipos de red, como se muestra en la figura 2.70

Figura 2.70: Menú administración Domicilio

2.9.4.2.1 Páginas web Cámaras y Sensores

La página "*CamarasSensores.jsp",* mostrada en la Figura 2.71; presenta los videos en tiempo real de las cámaras IP del domicilio, permite el control de las luminarias instaladas en diferentes lugares de un domicilio y alerta el estado de los sensores en caso de movimiento o detección de gas en el domicilio, también se puede visualizar el estado de conexión de las cámaras IP.

Adicionalmente se puede realizar el envío de mensajes SMS desde la interfaz *web*, indicando el número del destinatario.

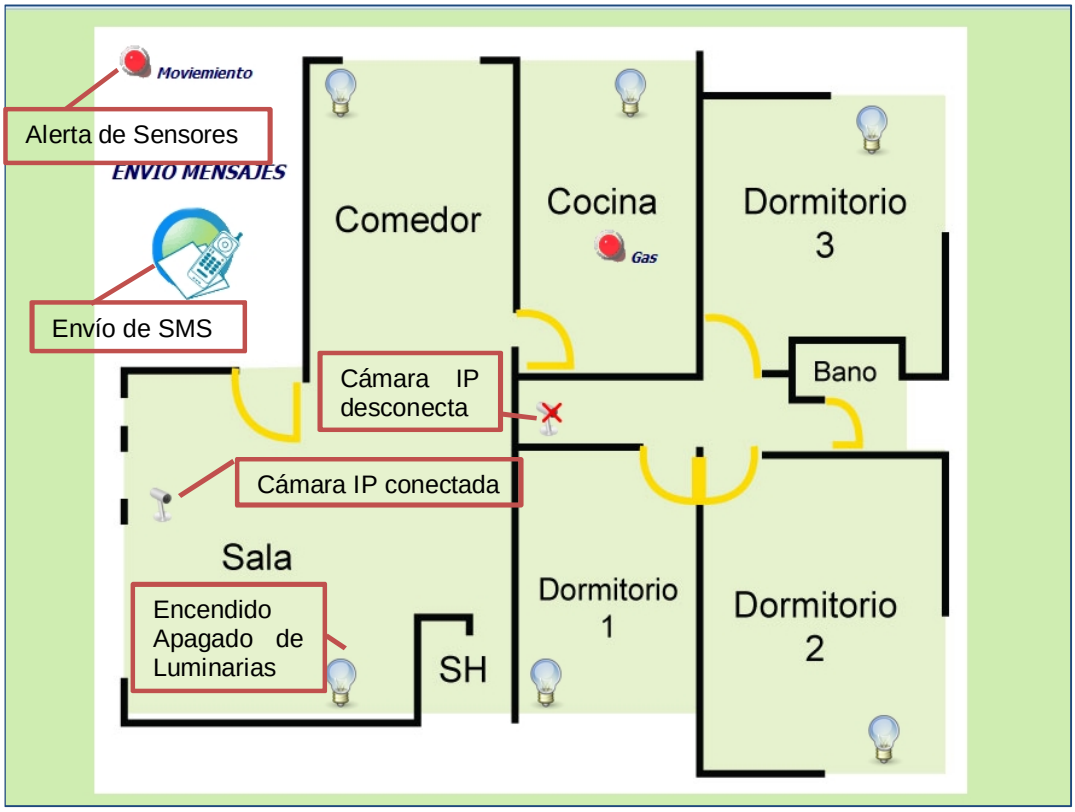


Figura 2.71: *CámarasSensores.jsp*

En la Figura 2.71; se muestra el control del domicilio al cual se tiene acceso:

- Encendido Apagado de Luminarias: Para el control de las luminarias se emplea la tabla "Datos" de la base de datos, al momento de encender o apagar una luminaria se actualiza un valor en la columna "datos".

Adicionalmente, se desarrolló un programa que se ejecuta como demonio[51], este programa tiene la función de revisar la tabla "Datos" y si existe una actualización de un valor ejecuta el proceso de comunicación serial al microprocesador encendiendo o apagando una luminaria según sea el caso.

- Alerta de sensores: En la tabla *"Datos",* existe un campo donde se recopila la información proporcionada por los sensores, de igual manera al control de luminarias se ha desarrollado un demonio, para las alertas de los sensores vía e-mail; y alerta SMS.

- Cámaras IP: Para verificar la conexión de las cámaras ha desarrollado un demonio, que ejecuta un comando *"ping",* a las cámara IP y verificar el estado de conexión.

- Envío Mensajes: Para el envío de los mensajes se hace uso de la tabla SMS de la base de datos donde se almacena el número de celular, el mensaje y un estado que indica si existe un nuevo mensaje.

  Adicionalmente se tiene un demonio, encargado de verificar el estado de nuevos mensajes, y en caso de tener un nuevo mensaje se ejecutan comandos AT a un teléfono celular conectado al servidor, donde se realiza el envío del nuevo mensaje al número indicado.

Los demonios indicados con anterioridad para el Sistema de Control Domiciliario, se han creado de manera independiente para su mejor administración y control en caso de presentar algún problema de funcionamiento.

[51] Proceso informático que se ejecuta en segundo plano y se ejecuta de forma continua.

Figura 2.72: Manejo Luminarias

Figura 2.73: Envío Alertas vía e-mail

Figura 2.74: Envío alertas vía SMS

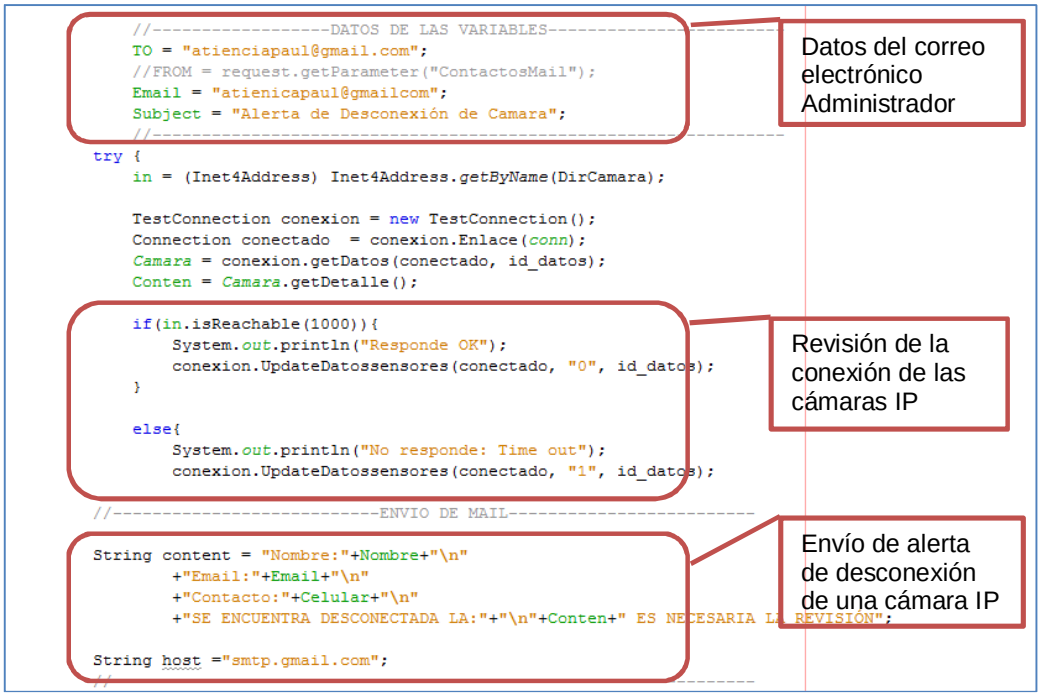
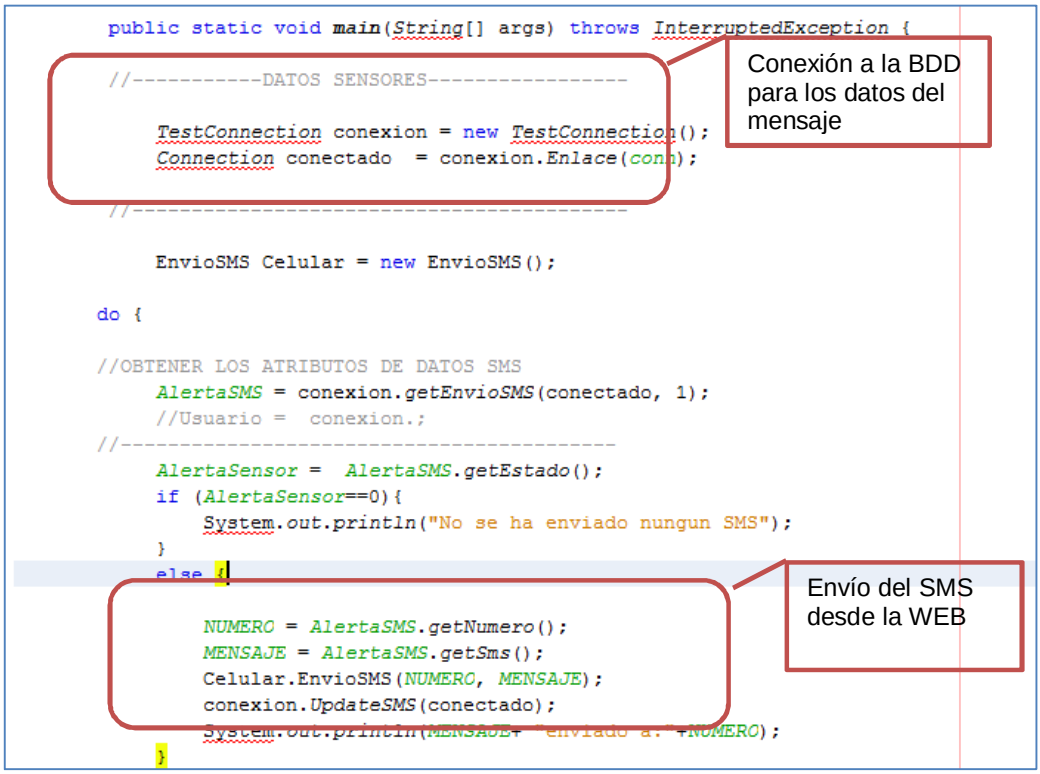


Figura 2.75: Envío Alertas Desconexión Cámaras IP




```
public static void main(String[] args) throws InterruptedException {
//----------DATOS SENSORES----------------

    TestConnection conexion = new TestConnection();
    Connection conectado  = conexion.Enlace(con);

//-----------------------------------------

    EnvioSMS Celular = new EnvioSMS();

do {

//OBTENER LOS ATRIBUTOS DE DATOS SMS
    AlertaSMS = conexion.getEnvioSMS(conectado, 1);
    //Usuario =  conexion.;
//-----------------------------------------
    AlertaSensor =  AlertaSMS.getEstado();
    if (AlertaSensor==0){
        System.out.println("No se ha enviado nungun SMS");
    }
    else {

        NUMERO = AlertaSMS.getNumero();
        MENSAJE = AlertaSMS.getSms();
        Celular.EnvioSMS(NUMERO, MENSAJE);
        conexion.UpdateSMS(conectado);
        System.out.println(MENSAJE+ " enviado a: "+NUMERO);
    }
```

Figura 2.76: Envío SMS desde la Web

2.9.4.2.2 Página web Historial Cámaras

La página *"HistorialCamaras.jsp"*, muestra los videos obtenidos por las cámaras IP al momento de detección de movimiento.

2.9.4.2.3 Página web Configuración de equipos

La página *"Configuracion.jsp"*, permite el acceso a la configuración de cámaras IP y la configuración del router de internet se establece un link de acceo a la pantalla de administracion del sispositivo.. Se debe tomar en cuenta que para acceder al módulo de configuración del Sistema *Web* es necesario encontrarse dentro de la red LAN, para el módulo de configuración no se tiene acceso mediante internet para establecer seguriadad en la información.

2.9.5 DESARROLLO PÁGINAS WEB USUARIO

Las páginas a continuación presentadas son para usuarios con restricciones, las mismas que no tendrán todos los privilegios de administrador.

2.9.5.1 Página web Usuario

Figura 2.77: *Usuario.jsp*

2.9.5.2 Página web Mi Perfil

En esta página *web* el usuario tiene el privilegio de editar solo su perfil, la página es igual a *MiPerfil.jsp* de administrador.

2.9.5.3 Página web Administración Domicilio

El Menú de Administración del Domicilio permite la visualización de las cámaras IP.

2.9.5.3.1 Páginas web Cámaras y Sensores

La página "*CamarasSensores.jsp",* para los usuarios registrados es similar a la de administradores, por el nivel de privilegios los usuarios registrados no tienen acceso al menú de configuración, así como, no tienen permiso de control de luminarias.

2.9.5.3.2 Página web Historial Cámaras

La página de "*HistoriarCamaras.jsp",* es igual a la de usuario administrador.

CAPÍTULO 3

IMPLEMENTACIÓN, PRUEBAS, VERIFICACIÓN DEL PROTOTIPO Y COSTOS

A continuación se detalla el proceso de construcción del prototipo de prueba del Sistema de Seguridad Domiciliario, que permite la simulación del control de una casa modelo. En el prototipo se realizarán las pruebas que determinen la funcionalidad del sistema como: control de las luminarias, alertas y visualización del sistema de video vigilancia por medio de internet. Del resultado de estas pruebas se realizarán los ajustes correspondientes en la implementación de un domicilio real.

3.1 CONSTRUCCIÓN DEL PROTOTIPO DE PRUEBA

El prototipo de prueba se implementará en una maqueta que representa un domicilio tipo, compuesto de: 3 dormitorios, sala, comedor, cocina y baño.

Con la finalidad de verificar el funcionamiento de detección de intrusos y gas nocivo se construirán placas con los sensores y los dispositivos XBee para la trasmisión de la información obtenida.

Para el sistema de control de luminarias se implementará un circuito con Led's, conectados directamente a un micro controlador, que simularán el encendido y apagado de las luminarias dentro del domicilio.

El sistema de video vigilancia se implementará con las cámaras IP DCS 2121, que mostrarán la maqueta construida.

Para el envío de alertas SMS se implementará un celular Nokia C1, mientras que las alertas vía E-MAIL se la realizará con la cuenta de correo electrónico atienciapaul@gmail.com.

3.1.1 CONSTRUCCIÓN DE LA MAQUETA

La maqueta de prueba se construirá en base a un domicilio tipo con las características antes mencionadas.

En la Figura 3.1 se muestra el plano de la maqueta que se construirá para el prototipo de prueba.

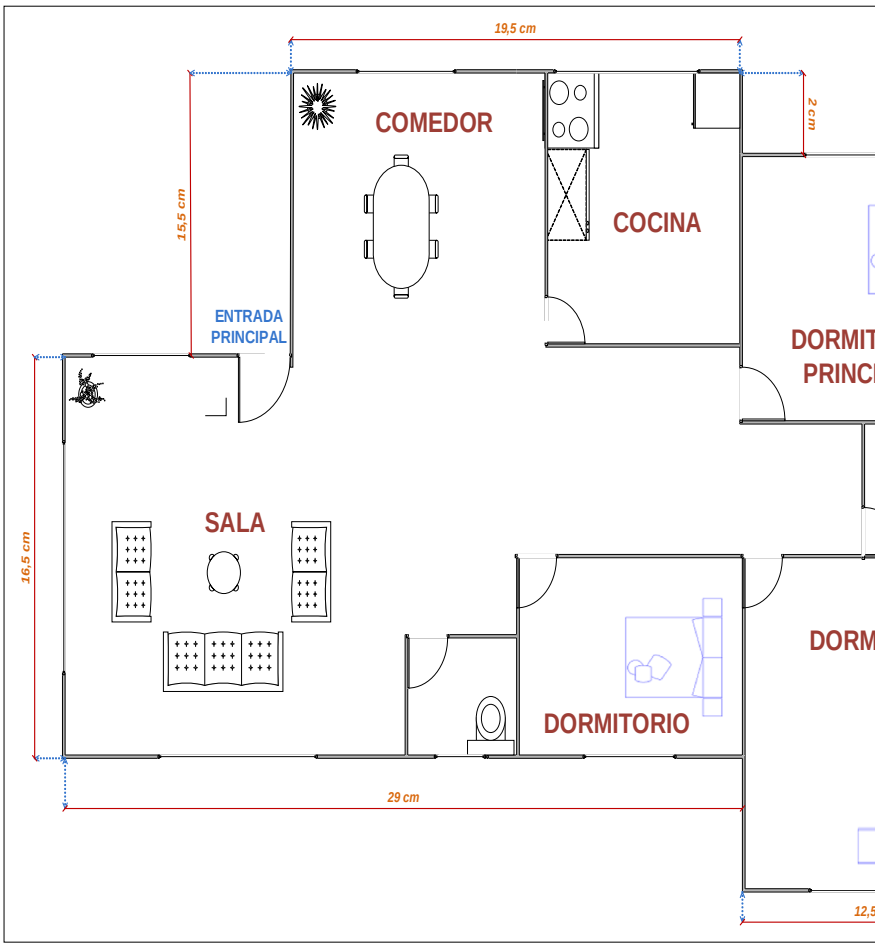


Figura 3.1: Plano estructural de la maqueta

Con el plano estructural se construye la maqueta de la Figura 3.2, en la que se coloca un circuito de potencia para simular las luminarias del domicilio. Adicional se colocan un Led color rojo y un parlante en la sala para contar con alarma visual y sonora dentro del domicilio en caso de detección de intrusos o gases nocivos.

Figura 3.2: Maqueta de una casa tipo

3.1.2 SISTEMA DE SENSORES Y MÓDULOS XBEE

La detección de intrusos y gases nocivos dentro del domicilio, como se indicó en el capítulo anterior, se establecerá con un sensor de movimiento PIR 555 - 28027 y la detección de gas nocivo con un sensor MQ5.

La información obtenida por los sensores será transmitida por dispositivos XBee, hacia el micro controlador, que se comunicará con el aplicativo *web* por medio de un interfaz serial R232, conectado al servidor.

La conexión entre el sensor y el módulo XBee se llamará nodo. En el Sistema de Seguridad Domiciliario se implementarán 2 nodos; Sensor de movimiento –

módulo XBee y Sensor de gas - módulo XBee, cada uno transmitirá la información a su nodo par XBee.

3.1.2.1 Nodo detección de intrusos

El nodo de detección de intrusos transmitirá los datos obtenidos por el sensor de movimiento, a su nodo receptor. En caso de detección de movimiento el nodo receptor comunicará esta nueva información al aplicativo *web* a través de micro controlador para la gestión de alarmas de detección de movimiento.

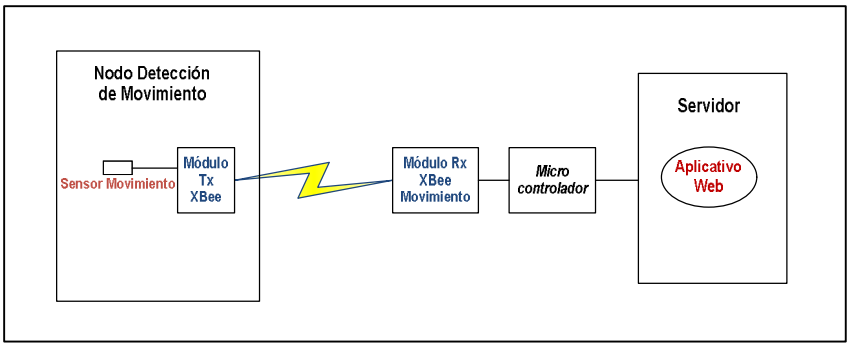


Figura 3.3 Comunicación Nodo Movimiento

En la Figura: 3.4 se puede observar el diseño de la placa correspondiente al nodo detección de movimiento, basado en las especificaciones del Data Sheet del sensor y del módulo de transmisión ZigBee.

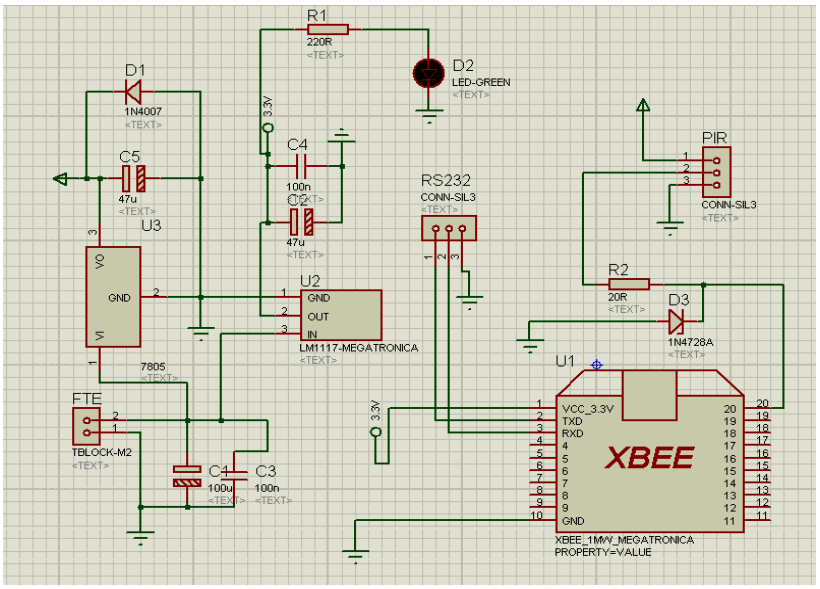


Figura 3.4: Diagrama de la placa nodo movimiento

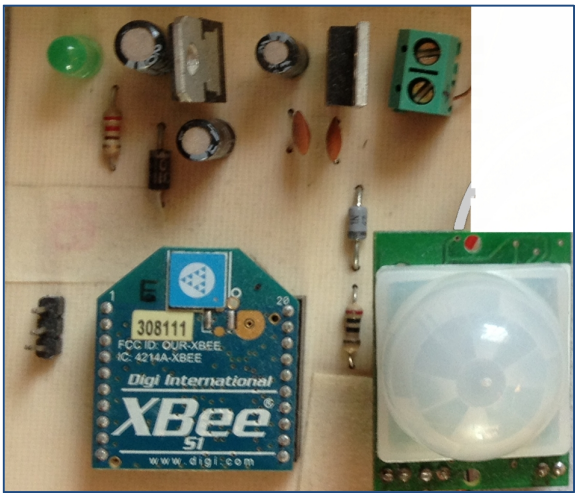


Figura 3.5: Placa nodo movimiento

Como se muestra en la Figura 3.5, el módulo XBee y Sensor PIR se encuentran colocados en zócalos, lo que permite su fácil reemplazo en caso que el sistema lo requiera. También se puede observar un led color verde que indica que el circuito se encuentra alimentado por energía. El nodo de movimiento será alimentado por baterías, con la finalidad que el sistema de detección sea independiente del sistema eléctrico del domicilio.

3.1.2.2 Nodo detección de gas nocivo

El nodo de detección de gas transmitirá datos obtenidos por el sensor de gas, a su nodo receptor. En caso de detección de gases como: CO, H_2, LPG, el nodo receptor comunicará esta nueva información al aplicativo *web* a través de micro controlador para la gestión de alarmas de detección de gases.

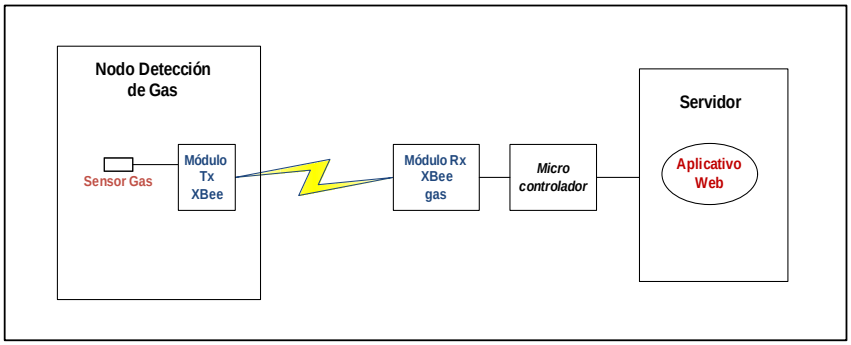


Figura 3.6: Comunicación Nodo Gas

En las Figuras: 3.7 y 3.8 se puede observar el diseño de la placa, y una foto del *hardware* correspondiente al nodo detección de gases, basado en las especificaciones del datasheet de los modulos XBee y el sensor de gas. Diagrama circuito impreso (ver Anexo L)

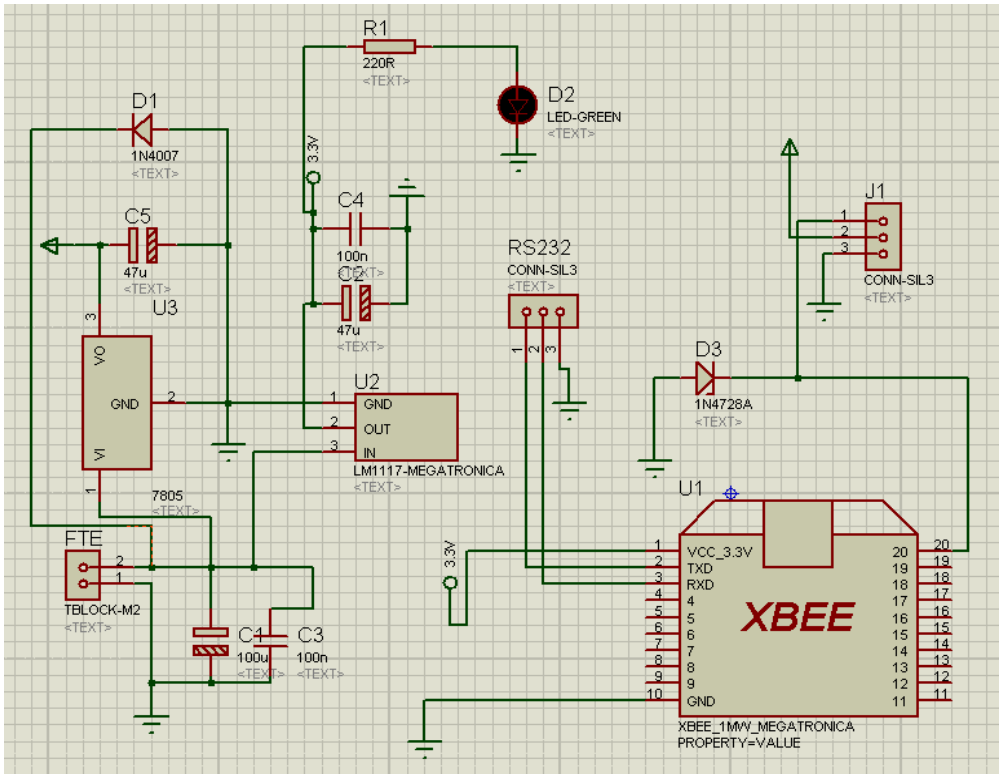


Figura 3.7: Diagrama de la placa nodo gas

Figura 3.8: Placa nodo gas

Como se muestra en la Figura 3.8, el módulo XBee y Sensor MQ5 se encuentran colocados en zócalos lo que permite su fácil reemplazo en caso que el sistema lo requiera. También se puede observar un led color verde que indica que el circuito se encuentra alimentado por energía. El nodo de movimiento será alimentado por baterías, con la finalidad que el sistema de detección sea independiente del sistema eléctrico del domicilio.

3.1.3 SISTEMA DE CONTROL

Para el prototipo de prueba de control de luminarias se construirá una placa con el micro controlador PIC 16F87XA, mismo que gestionará el encendido y apagado de led's de la maqueta en función del aplicativo *web*. Adicionalmente se obtendrá los datos proporcionados por el nodo de movimiento y gas para presentar las alarmas visuales dentro de la maqueta (led rojo ubicado en la sala) y enviar esta información al aplicativo *web* para el envío de alertas SMS y correo electrónico. También se presentará una alarma visual en la placa del PIC (led´s amarillos). Estos led's se encenderán en función del cambio de estado de un nodo. Como se observa en la Figura 3.9.

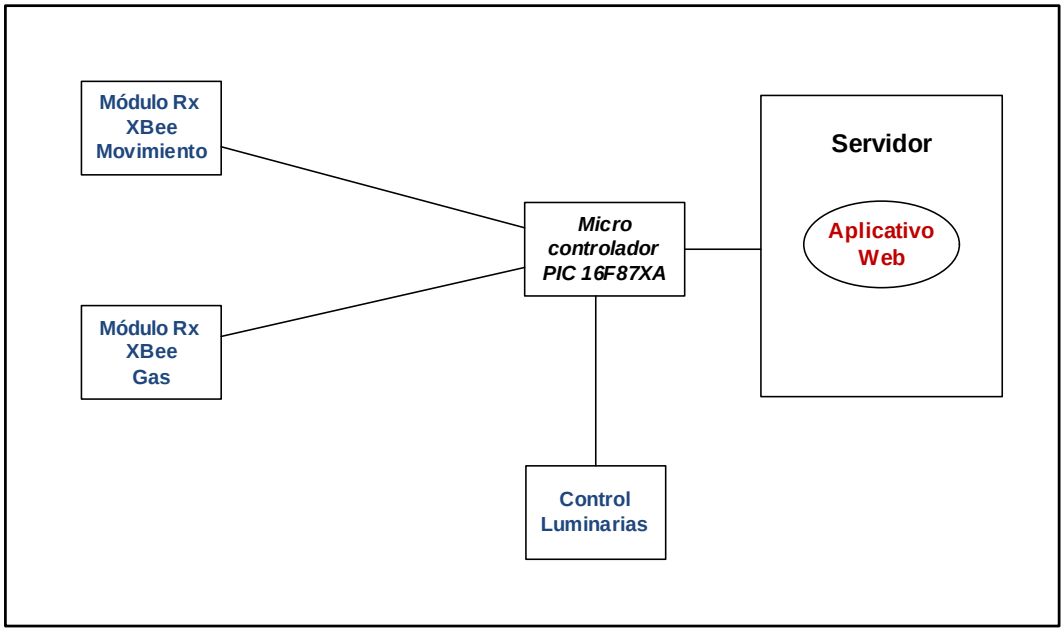


Figura 3.9: Diagrama de control de luminarias y sensores

En las Figuras: 3.10, 3.11, 3.12, se puede observar el diseño de la placa, y el *hardware* correspondiente al control de luminarias y nodos de movimiento y gas.

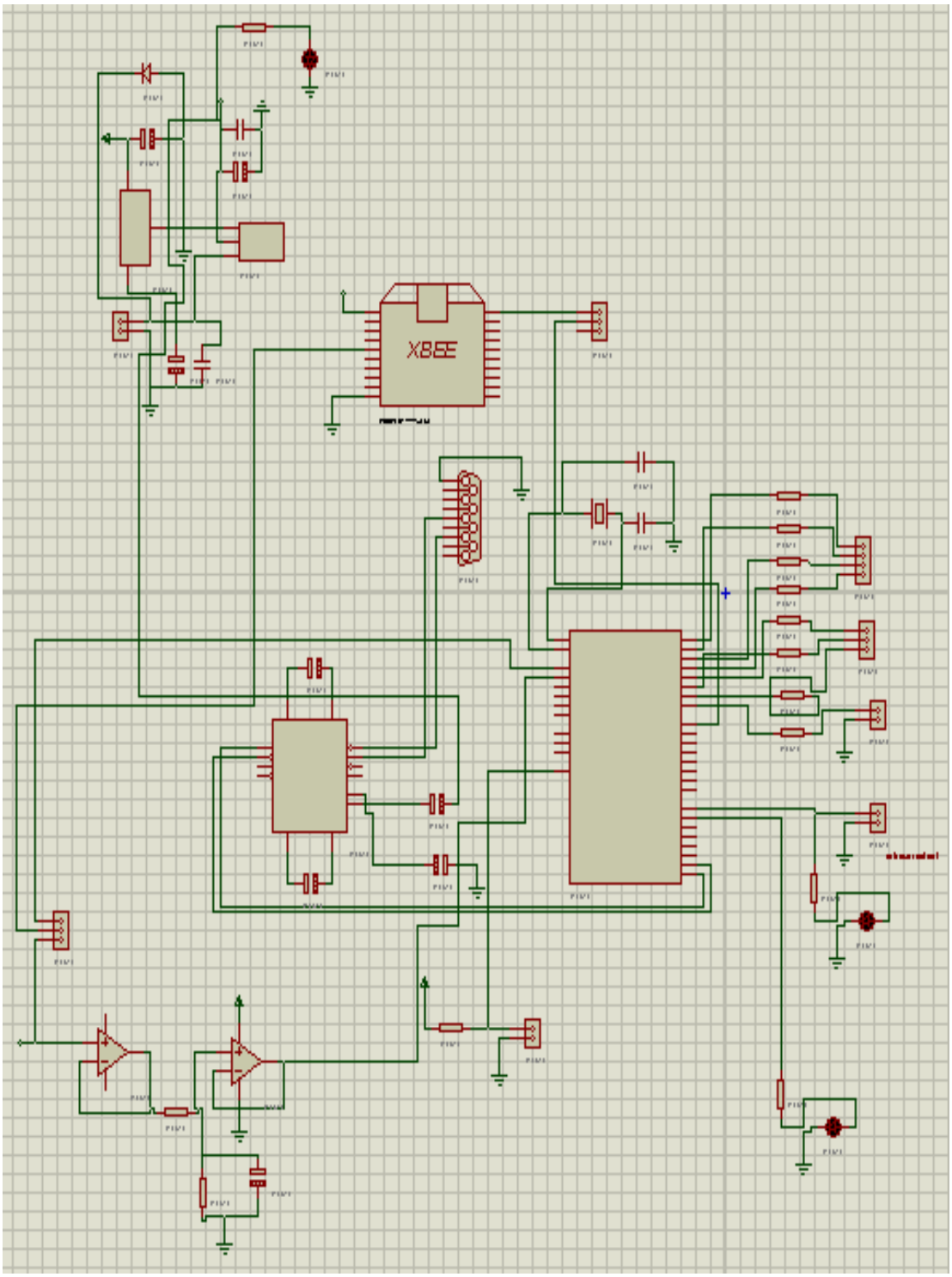


Figura 3.10: Placa de control luminarias y receptor nodo gas

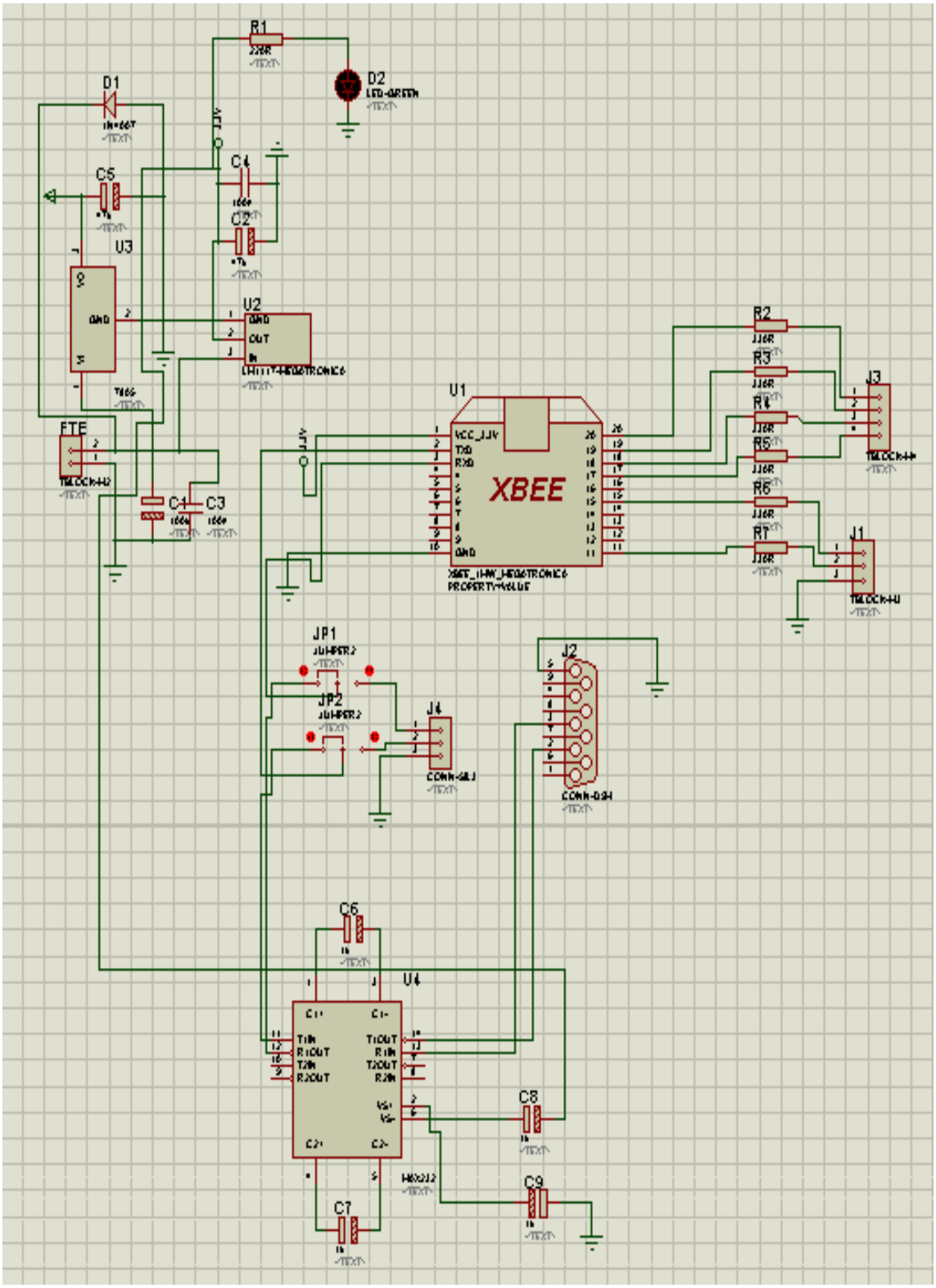


Figura 3.11: Placa receptor nodo movimiento

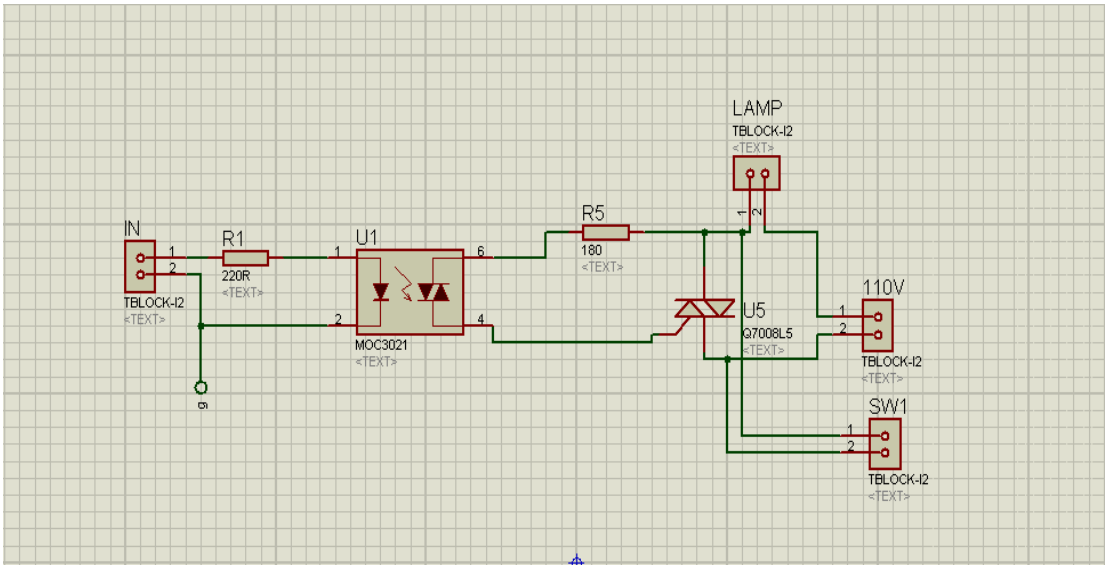


Figura 3.12: Placa circuito de potencia para luminarias

En la figura 3.10, se puede observar como componentes: un puerto RS232 a utilizarse para el intercambio de información entre la PC y el dispositivo XBee receptor de información (datos en hexadecimal) lo cual permitirá, el encendido y apagado de las luminarias y enviar alertas del cambio de estado de los sensores; también se hace uso de un microcontrolador PIC 16F87XA el cual dependiendo de la seña recibida se encargará de gestionarla y enviarla por los puertos correspondientes. Se muestra foto del circuito en la figura 3.13.

En la figura 3.11 se hace uso de un circuito similar al de la figura 3.10, con la diferencia que no existe procesamiento de la información a través del PIC, y más bien, la información es retransmitida al nodo principal. Se muestra foto del circuito en la figura 3.14.

La figura 3.12 muestra el circuito que se utilizaría para controlar las luminarias de una casa real alimentada con un voltaje de 110 [V].

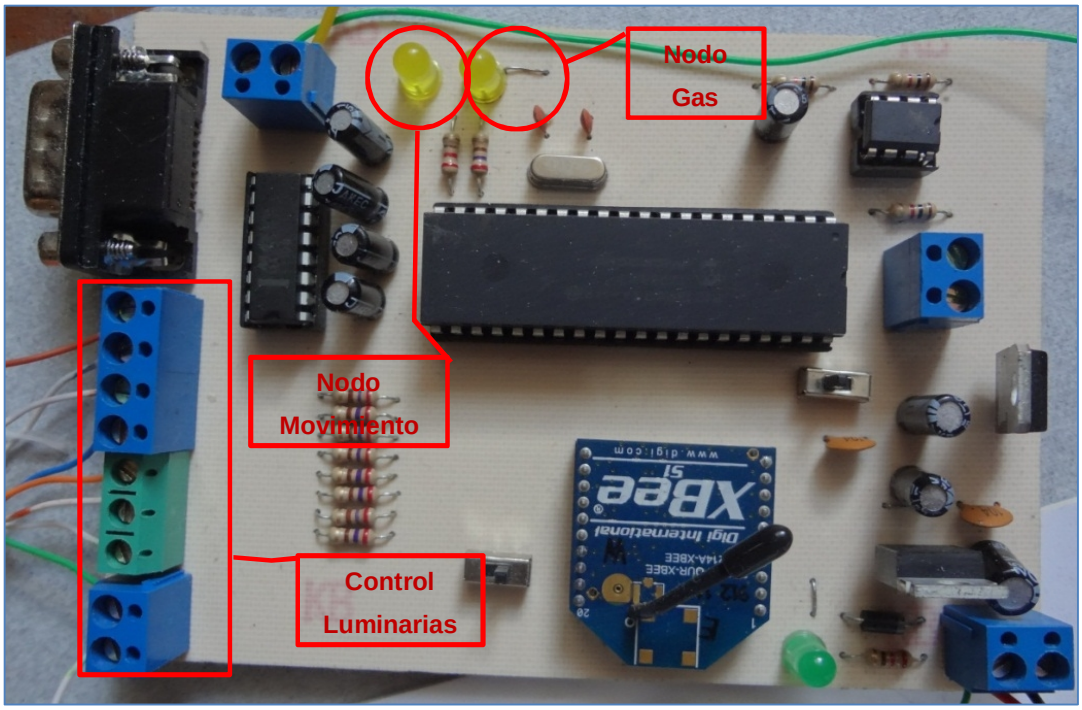


Figura 3.13: Placa de control del domicilio y receptor nodo gas

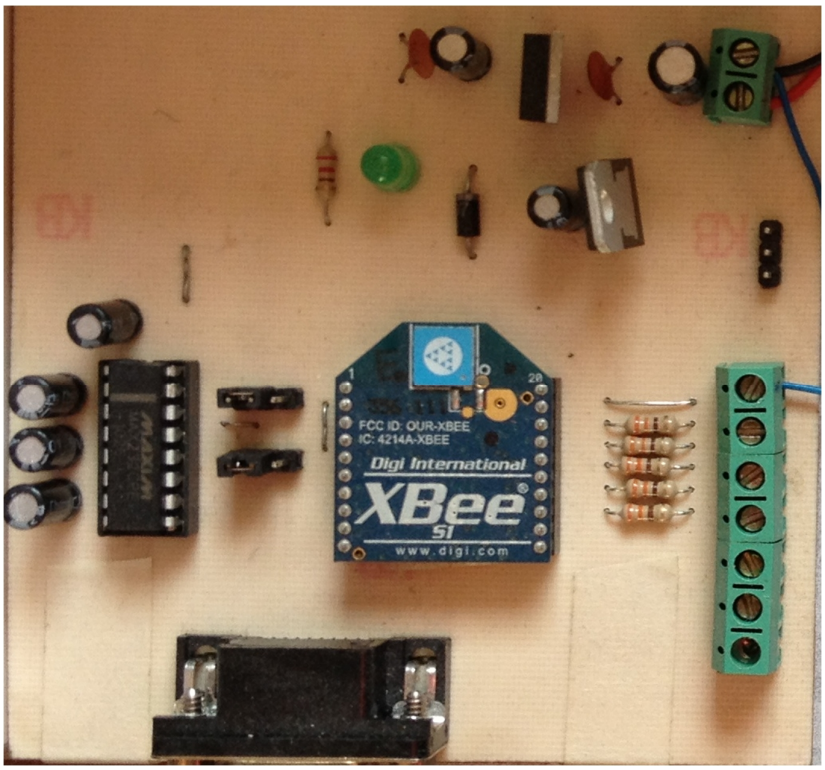


Figura 3.14: Placa receptor nodo movimiento

Las placas de control de luminarias y receptor del nodo de movimiento cuentan con un led color verde que indica que el circuito se encuentra alimentado por

energía. Se debe considerar que estas placas de conectaran el sistema eléctrico que alimenta al servidor del Sistema de Seguridad Domiciliario.

El diseño de las placas se basó en las recomendaciones de los fabricantes, especificadas en los datasheet de los módulos Xbee, el micro controlador PIC 16F87XA, además se puede observar el diseño de los circuitos impresos en el Anexo L

3.1.4 SERVIDOR DEL SISTEMA DE SEGURIDAD DOMICILIARIO

La configuración del servidor para el prototipo de prueba se realizará en una PC de las siguientes características mínimas:

SERVIDOR	
Ítem	**Características**
Mainboard	P21G V3.1
Procesador	Intel Pentium IV
Memoria	2 GB
Entradas USB	4 entradas
Puerto Serial	1 R232
Disco Duro	IDE 500 GB

Tabla 3.1: Características Servidor

En el servidor se instalará el Sistema Operativo Linux distribución Centos, con los con los servicios necesarios (Tomcat, MySQL, SAMBA), para el correcto funcionamiento del aplicativo *web*.

Al servidor se conectará el micro controlador por medio del interfaz serial R232, las cámaras IP se comunicarán con el servidor a través de la LAN.

Adicionalmente se conectará al servidor, por medio de un interfaz USB, un dispositivo móvil (celular) para el envío de alertas SMS. El celular seleccionado para el envío de alertas es un Nokia C1 de características básicas, capaz de cumplir con el trabajo necesitado.

3.2 IMPLEMENTACIÓN DEL PROTOTIPO DE PRUEBA

La implementación del Sistema de Seguridad Domiciliario se realizó en una maqueta prototipo (Figura 3.18), donde se implementó el cableado eléctrico y los módulos ZigBee conectados a los sensores de movimiento y gas nocivo, con el propósito de verificar el correcto funcionamiento del Sistema. Adicionalmente la maqueta se conecta por interfaz serial al Servidor del Sistema.

Como se indicó con anterioridad se establecieron led´s en la maqueta para simular Luminarias del domicilio, en la sala de la maqueta se colocó un led color rojo y un parlante para establecer alarmas visual y sonora en caso de detección de movimiento o gas nocivo.

Figura 3.15: Maqueta prototipo de prueba

Las pruebas consideradas para la verificar funcionamiento del Sistema de Seguridad Domiciliario son las siguientes:

- Funcionamiento, Cobertura e Interferencia de los Sensores.
- Funcionamiento de la interfaz gráfica en la *Web*.
- Funcionamiento de Alarmas.

Adicionalmente se presentará un análisis de costos para la implementación del Sistema de Seguridad Domiciliario.

3.3 PRUEBAS DE FUNCIONAMIENTO DEL SISTEMA

A continuación se presenta las pruebas realizadas al Sistema de Seguridad Domiciliario.

3.3.1 Funcionamiento, Cobertura e Interferencia nodos: movimiento y Gas

La verificación del funcionamiento del sistema consistirá en realizar pruebas a los nodos de movimiento y gas, tomando en cuenta los siguientes parámetros generales:

- El área física de toma de datos no varía. Se hará uso de una casa (modelo para la elaboración del prototipo) con obstáculos propios (paredes, puertas y ventanas).
- Los datos se obtendrán a partir lecturas del tiempo que le toma a la señal ser percibida por el sistema colocando los dispositivos ZigBee a distancias fijas de prueba. Se registrarán las medidas cada 5 metros de separación, hasta llegar al máximo alcance especificado por el fabricante de 30 metros para los sensores en un ambiente *Indoor,* ya que para este documento no se considerará distancias mayores por el hecho de que cada uno de los sensores se utilizará para una casa modelo de máximo esa dimensión.
- Con la finalidad de establecer errores en las transmisiones de los nodos, se establecerán 3 repeticiones[31] en el envío de la información obtenida por los sensores.

[31] Se considera que la detección de intrusos y gas debe ser confiable en caso de detección se debe disparar la alarma, se toman 3 muestras para establecer una la confiabilidad de los datos.

Acorde a los parámetros antes mencionados se establecen los siguientes escenarios:

- Pruebas de cobertura, de los dispositivos ZigBee, sin interferencia

  En este escenario se tomará datos de tiempo de respuesta en función de la distancia. Sin considerar interferencia en el ambiente.

  Acorde a este escenario se obtienen los siguientes datos.

NODO MOVIMIENTO		
Distancia [m]	**Tiempo respuesta [s]**	**Errores Nro. intentos**
5	1	-
10	2	-
15	3	-
20	3	-
25	no percibe señal	3
30	no percibe señal	3

Tabla 3.2: Cobertura Sin Interferencia Nodo Movimiento

NODO GAS		
Distancia [m]	**Tiempo respuesta [s]**	**Errores Nro. intentos**
5	1	-
10	2	-
15	2	-
20	3	-
25	no percibe señal	3
30	no percibe señal	3

Tabla 3.3: Cobertura Sin Interferencia Nodo Gas

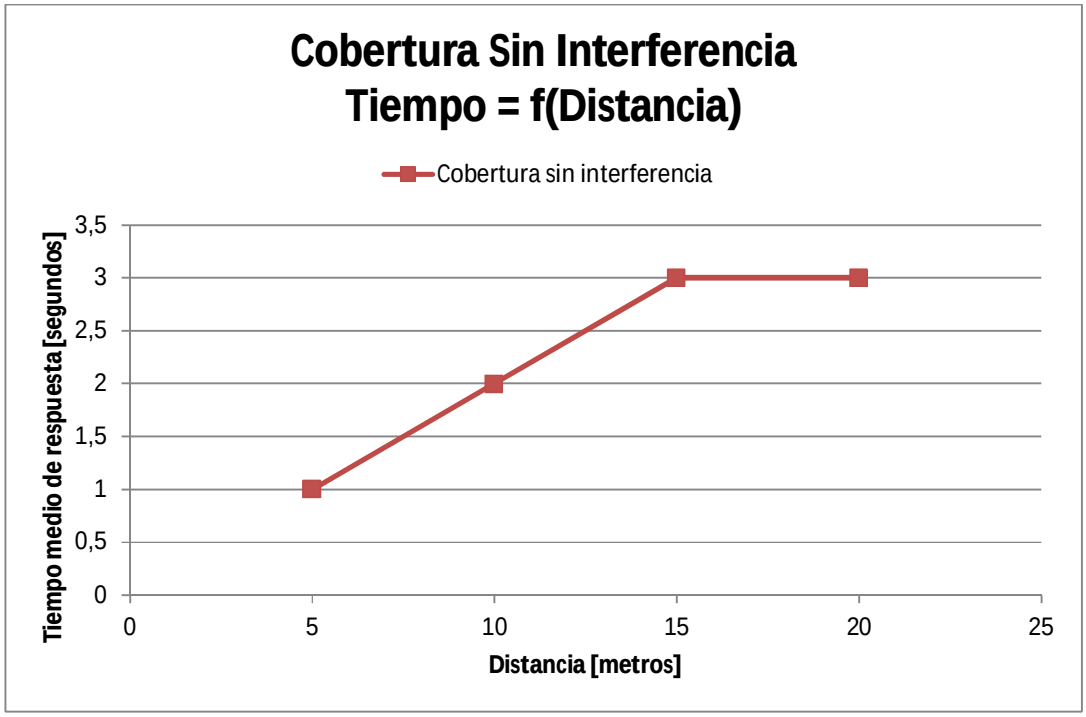


Figura 3.16: Cobertura Sin Interferencia Nodo Movimiento

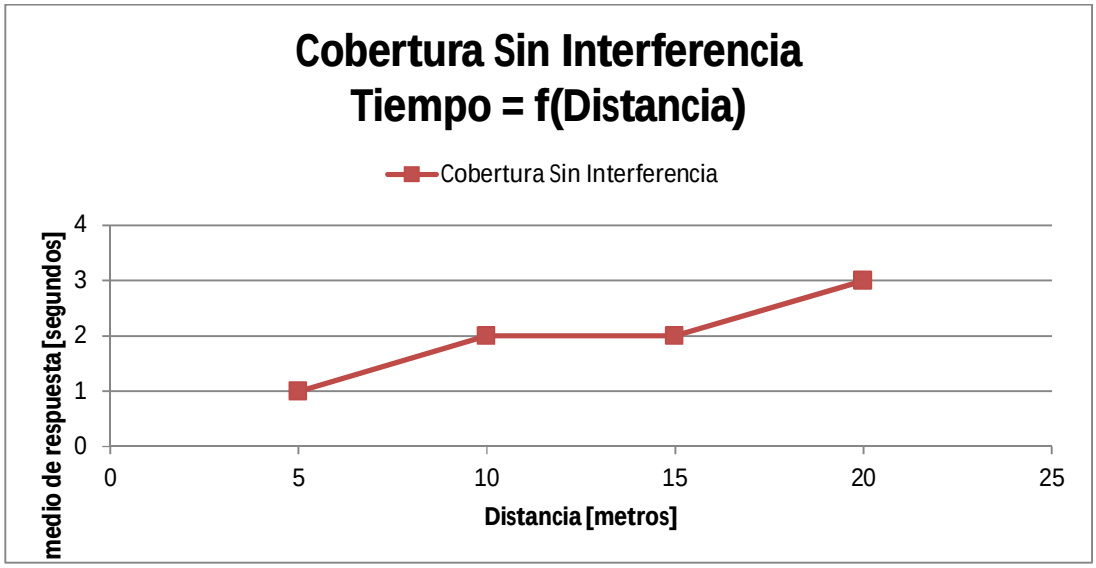


Figura 3.17: Cobertura Sin Interferencia Nodo Gas

De los datos se puede concluir que el alcance máximo de la transmisión de datos para un ambiente sin interferencia es de 25 metros, con un máximo de tiempo de detección de señal de 3 segundos, estas mediciones se la hicieron verificando la señal recibida en el micro – controlador y enviada a la base de datos.

- Pruebas de cobertura, de los dispositivos ZigBee, con interferencia media

  En este escenario se tomará datos del tiempo de respuesta en función de la distancia. Para considerar interferencia media se utilizará para ello el uso de un equipo Wi-Fi, con potencia máxima de -20 dBm, que será ubicado a lado del receptor ZigBee.

  Acorde a este escenario se obtienen los siguientes datos.

NODO MOVIMIENTO		
Distancia [m]	**Tiempo respuesta [s]**	**Errores Nro. intentos**
5	2	-
10	4	-
15	4	-
20	5	-
25	no percibe señal	3
30	no percibe señal	3

Tabla 3.4: Cobertura Interferencia Media Nodo Movimiento

NODO GAS		
Distancia [m]	**Tiempo respuesta [s]**	**Errores Nro. intentos**
5	2	-
10	3	-
15	4	-
20	4	-
25	no percibe señal	3
30	no percibe señal	3

Tabla 3.5: Cobertura Media Nodo Gas

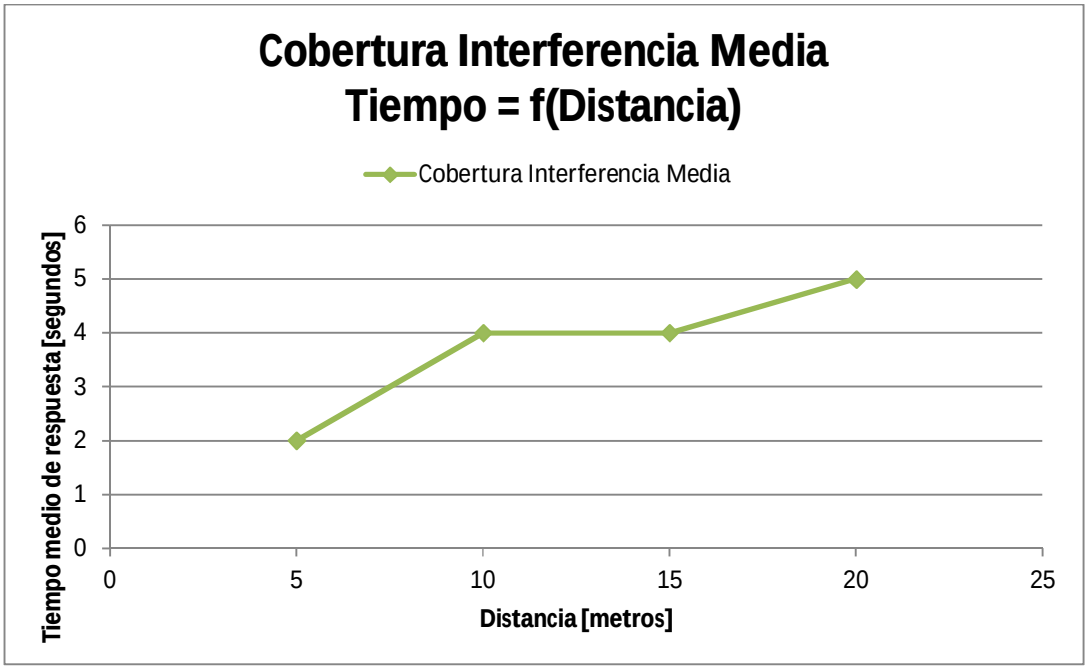


Figura 3.18: Cobertura Interferencia Media Nodo Movimiento

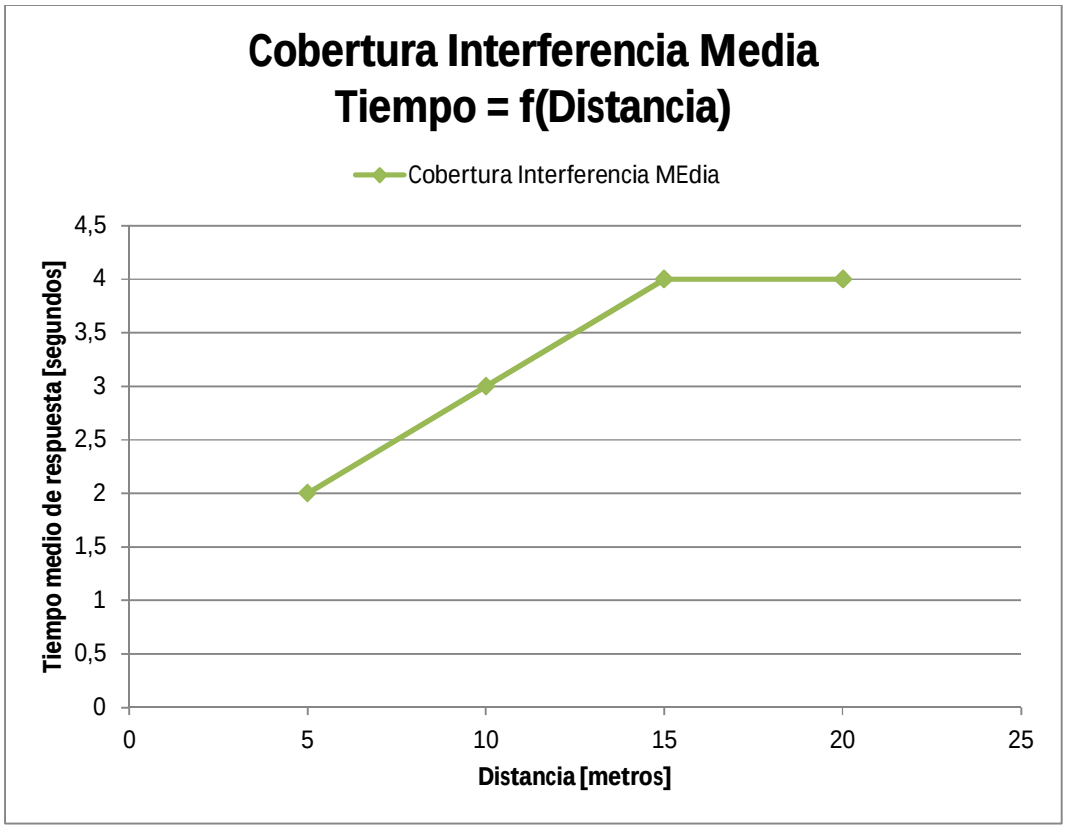


Figura 3.19: Cobertura Interferencia Media Nodo Gas

Al tener un ambiente con interferencia baja, la distancia de recepción de la señal se redujo con respecto a las pruebas anteriormente realizadas y el tiempo de percepción de señal aumento.

- Pruebas de cobertura, de los dispositivos ZigBee, con interferencia alta

  En este escenario se tomará datos del tiempo de respuesta en función de la distancia. Considerando interferencia alta, para ello el módulo XBee receptor se ubicará junto al equipo Wi-Fi, teléfono inalámbrico y una computadora portátil transmitiendo datos con el dispositivo Wi-Fi.

  Acorde a este escenario se obtienen los siguientes datos.

NODO MOVIMIENTO		
Distancia [m]	**Tiempo respuesta [s]**	**Errores Nro. intentos**
5	2	-
10	3	-
15	5	-
20	5	1
25	no percibe señal	3
30	no percibe señal	3

Tabla 3.6: Cobertura Interferencia Alta Nodo Movimiento

NODO GAS		
Distancia [m]	**Tiempo respuesta [s]**	**Errores Nro. intentos**
5	3	-
10	4	-
15	5	-
20	6	1
25	no percibe señal	3
30	no percibe señal	3

Tabla 3.7: Cobertura Interferencia Alta Nodo Gas

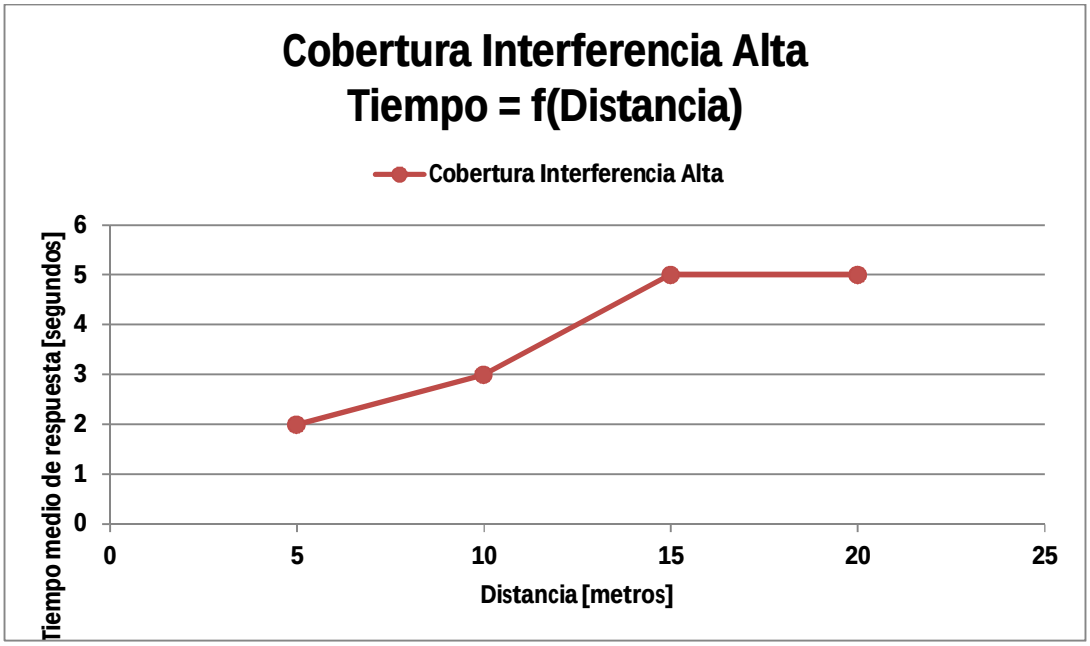


Figura 3.20: Cobertura Interferencia Alta Nodo Movimiento

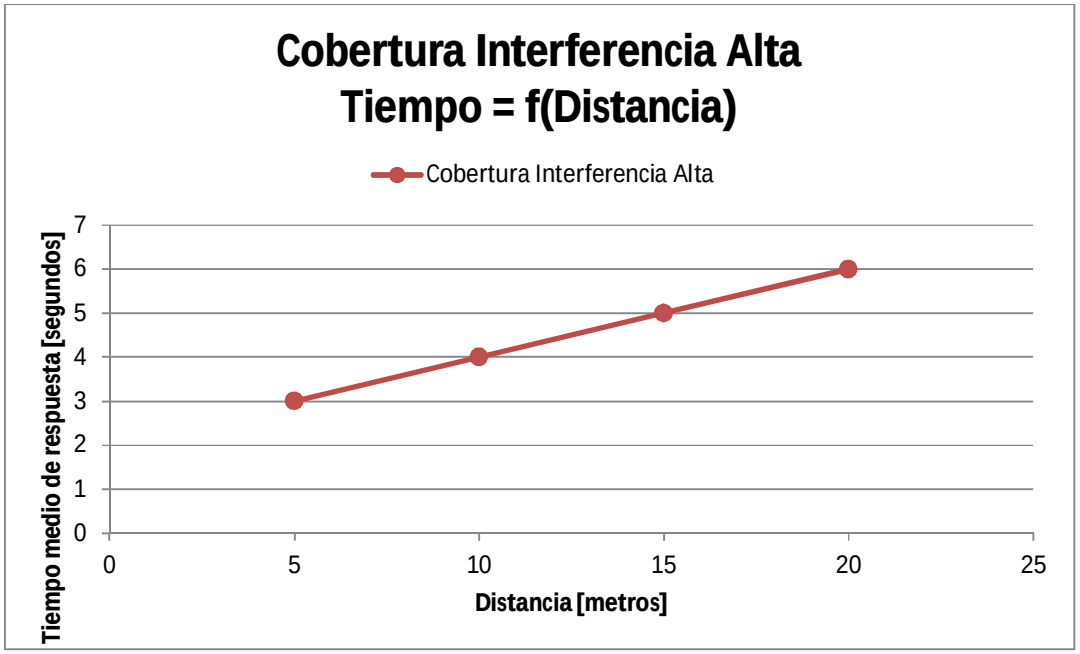


Figura 3.21: Cobertura Interferencia Alta Nodo Gas

Con los datos antes indicados se establece una comparativa entre los diferentes tiempos de respuesta y los escenarios de pruebas.

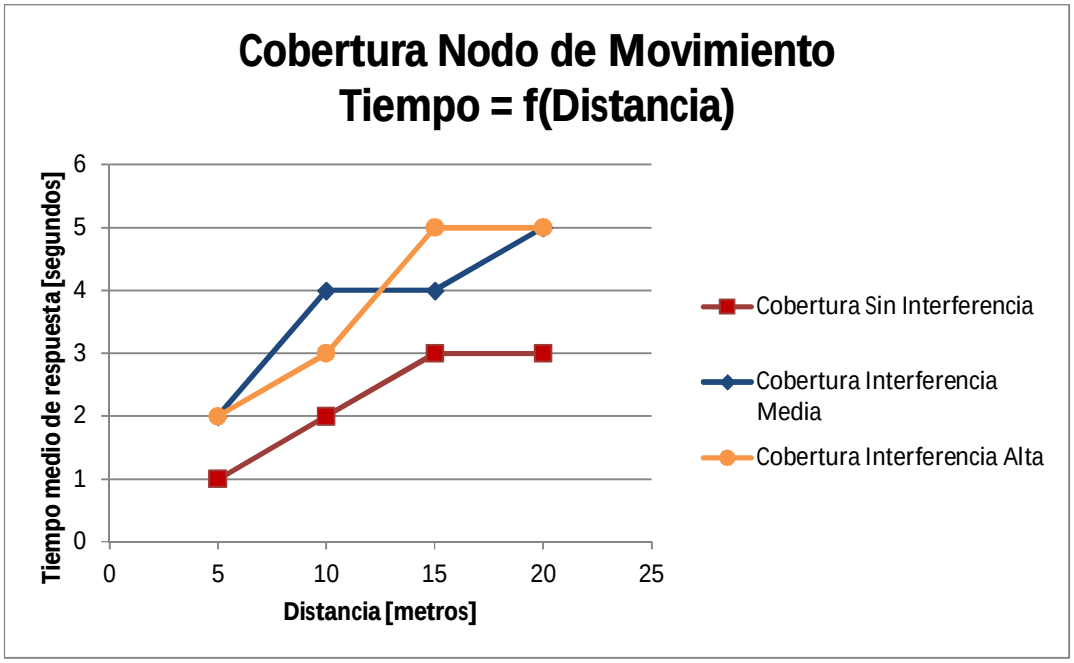


Figura 3.22: Comparativa Tiempo de respuesta Nodo Movimiento

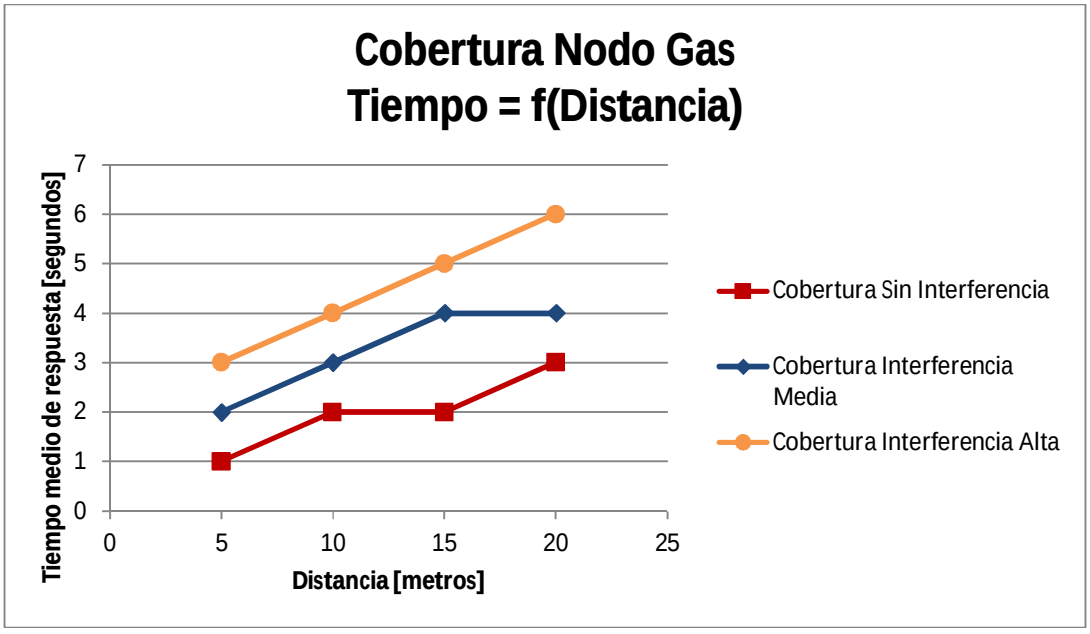


Figura 3.23: Comparativa Tiempo de respuesta Nodo Gas

De las medidas obtenidas por los nodos de movimiento y gas se puede indicar que en un ambiente de interferencia alta los tiempos de recepción de señal crece, pero la distancia sigue siendo comparable al caso anterior. En la práctica no se presentará ya que los nodos transmisores y los módulos receptores no se ubicarán en lugares cercanos a dispositivos que provoquen interferencia.

Se debe tomar en cuenta que la distancia máxima alcanzada en las pruebas es de 20 metros en un ambiente *Indoor*, los datos teóricos de alcance son de 30 metros en un ambiente *Indoor*, la cobertura máxima alcanzada se debe a los obstáculos presentados en el domicilio

3.3.2 Funcionamiento de los nodos

A continuación se muestra figuras de las placas de detección de movimiento y detección de gas, con las alarmas visuales en funcionamiento:

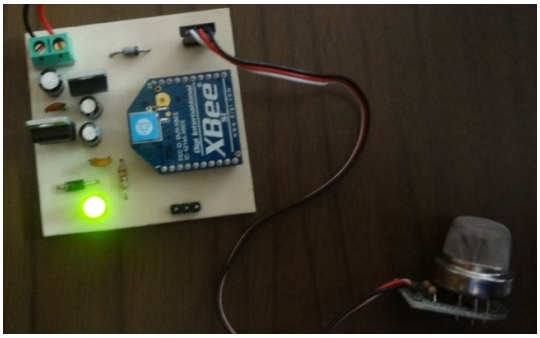


Figura 3.24: Nodo de Gas

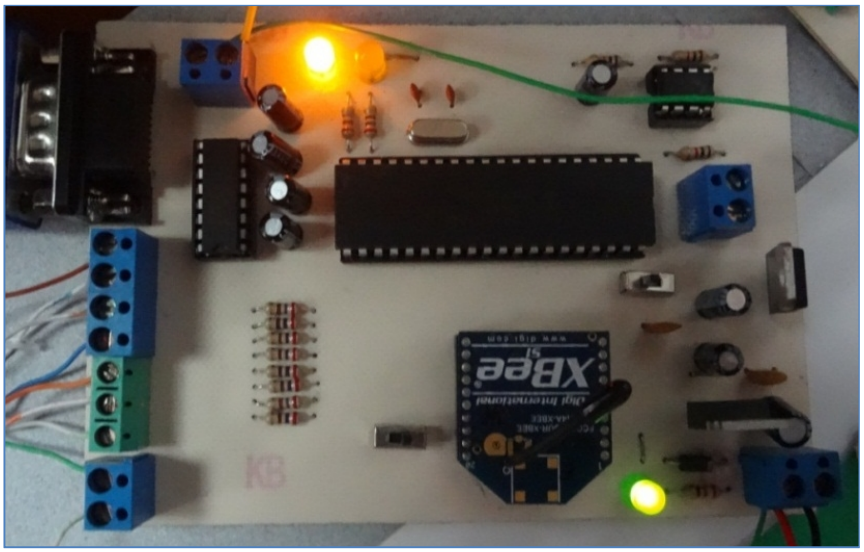


Figura 3.25: Alarma detección de movimiento

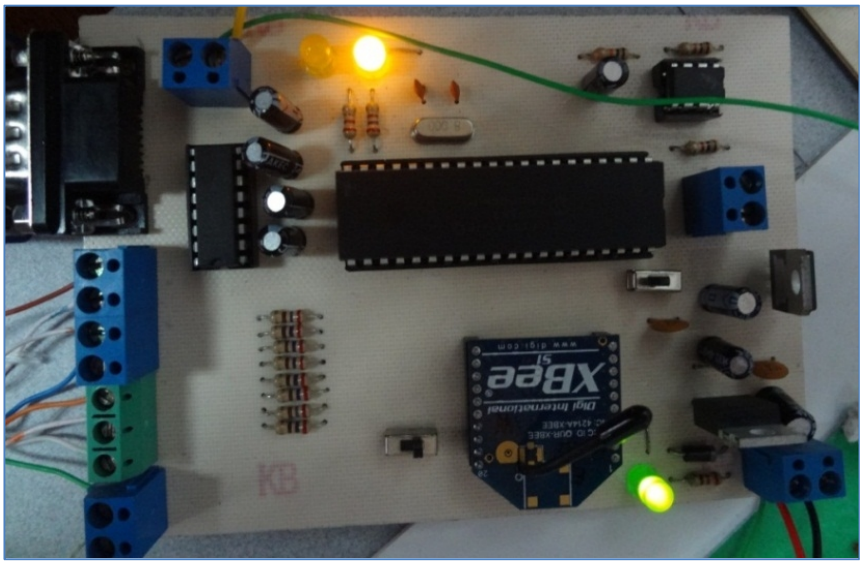


Figura 3.26: Alarma detección de gas nocivo

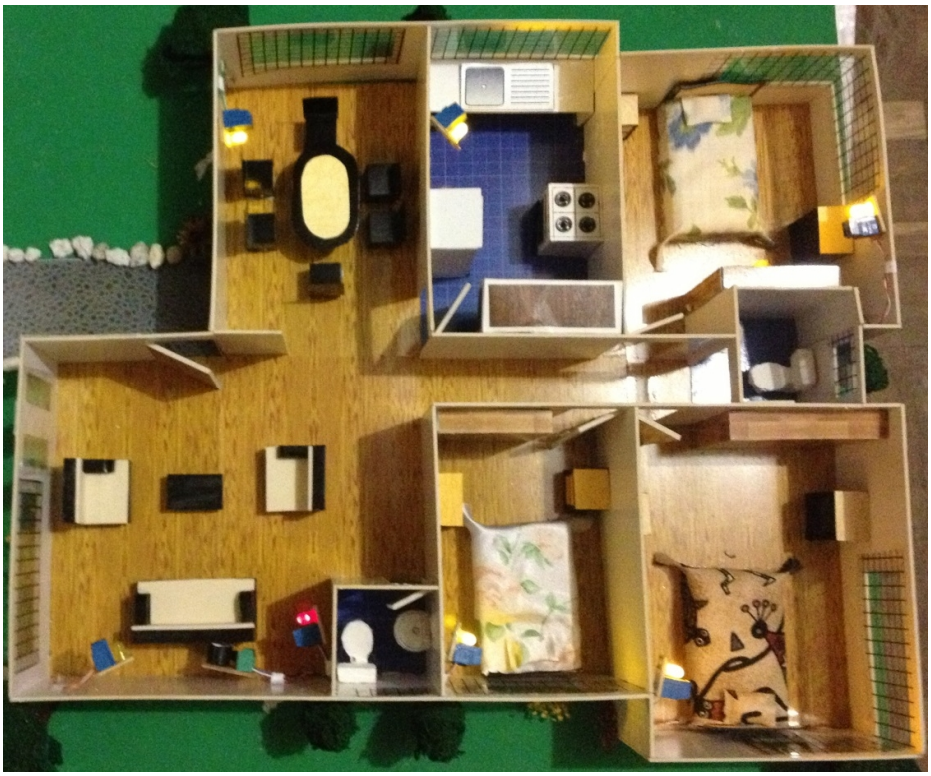


Figura 3.27: Alarma detección de movimiento y gas nocivo en la maqueta

3.3.3 Funcionamiento del Interfaz Gráfico

Las pruebas que se realizarán pretenden determinar la percepción de la población del aplicativo *web*. Para estas pruebas se define una matriz en base al nivel de

cumplimiento de la prueba de cada una de las operaciones más importantes en el sistema. Estas pruebas serán realizadas por un usuario promedio sin grandes conocimientos de operación de programas computacionales y con un nivel de instrucción medio.

También se estableció un sistema de calificación de tres niveles donde:

- **5**: El usuario se toma un tiempo aceptable para comprender el sistema y ejecutar la prueba
- **3:** El usuario no comprende inmediatamente el sistema, pero al final realiza la prueba establecida
- **1**: El usuario no logra cumplir con la prueba.

Para estas pruebas se tomarán 10 personas a las que les pide que ingresen al sistema a través del internet pidiéndoles que cumplan con los siguientes objetivos:

- Validación de ingreso de usuario.
- Cambio de clave de Usuario.
- Actualización de datos del usuario.
- Envío de mensaje SMS.
- Acceso al video de las cámaras de seguridad.
- Encendido y apagado de luminarias.

Luego de haber cumplido estos objetivos el usuario evaluará su experiencia en el uso del sistema.

De los datos arrojados en la prueba se obtiene la siguiente tabla, tomando como dato el promedio de las opiniones brindadas:

ASPECTO A PROBAR	DESCRIPCIÓN DEL CASO	PRE-REQUISITOS	RESULTADO ESPERADO	RESULTADO OBTENIDO	OBSERVACIÓN
VALIDACIÓN DE INGRESO USUARIO	Cada uno de los usuarios debe probar su propia clave para el ingreso al sistema de seguridad	El usuario debe tener una clave asignada por el administrador del sistema.	Ingreso al sistema	5	El usuario deberá luego de haber ingresado al sistema cambiar su clave de acceso por una clave privada.
CAMBIO DE CLAVE DE USUARIO	El usuario debe cambiar su clave acceso por una propia	El usuario debe tener una clave asignada por el administrador del sistema.	Cambio de la clave por una diferente	5	El sistema muestra información del Usuario adicional a la de la clave
ACTUALIZACIÓN DE DATOS DEL USUARIO	Cambiar los datos de un usuario por otros diferentes	El usuario debe tener una clave asignada por el administrador del sistema.	Actualización de la información del usuario	5	El usuario puede cambiar cualquiera de sus datos personales
ENVIO DE MENSAJE	Acceso y envío de un mensaje de alerta por medio de la aplicación en el sistema	El usuario debe tener una clave asignada por el administrador del sistema.	Envío y recepción del mensaje propuesto por el usuario	3	La primera vez que el usuario entra al sistema le tomo un poco de tiempo encontrar el icono de envío de mensajes. El mensaje enviado puede ser escrito según su criterio del usuario.
ACCESO A VIDEO DE LA CAMARA DE SEGURIDAD	El usuario deberá poder observar las imágenes enviadas por la cámara de seguridad a través de la interfaz Web.	El usuario debe tener una clave asignada por el administrador del sistema.	Visualización de las imágenes captadas por las cámaras de seguridad	3	Las imágenes obtenidas tienen un retraso muy pequeño dependiendo de la distancia y calidad del enlace de internet.
ENCENDIDO Y APAGADO DE LUMINARIAS	Ingreso a la sección de luminarias y control de cada una de ellas	El usuario debe tener una clave asignada por el administrador del sistema.	Encendido y apagado de las luminarias deseadas por el usuario	5	Los usuarios deben esperar alrededor de 5 a 8 segundos para que su cambio se realice.
NAVEGACIÓN DEL SISTEMA	Ubicar en el sistema la información requerida	El usuario debe tener una clave asignada por el administrador del sistema.	Navegación fluida por el sistema	5	El usuario al ingresar al sistema no demuestra mayor inconveniente en ubicar la información que necesita

Tabla 3. 8: Pruebas de Interfaz Gráfico

De las pruebas se concluye que la interfaz gráfica de administración con un promedio de 4,43 sobre 5 puntos posibles, lo que implica que la aplicación está diseñada con menús de navegación fáciles de interpretar, con la finalidad de brindar al usuario del domicilio un ambiente amigable para la administración de su domicilio, ya que como se puede ver en la tabla 3.8 se consideró solo 2 aspectos que causaron dificultad de manipulación para los usuarios que puede ser solventado con algo de capacitación.

Los campos de ingreso de datos son corregidos a nivel de aplicación para evitar que los usuarios ingresen datos erróneos.

Se muestran figuras con pantallas de ingreso al aplicativo *web* en el Anexo M.

Las pruebas que se realizan al interfaz gráfico son de escritura y lectura en la base de datos, revisión del estado de las alarmas, envío de SMS desde la página web y control de luminarias del domicilio desde el interfaz de administración.

PRUEBAS INTERFAZ GRÁFICO				
ACCESO	***PRUEBA***	***PÁGINA WEB***	***DESCRIPCIÓN***	***FIGURA***
Administrador	*Mi Perfil*	Editar Perfil	El administrador edita sus datos personales	3.28
	Administración Usuarios	Añadir Usuarios	Creación de un nuevo usuario estableciendo los niveles de acceso	3.29
		Editar Usuarios	Edición de usuarios existentes cambiando: permisos, claves o datos personales. Adicionalmente se puede eliminar un usuario	3.30
	Control Domicilio	Visualización Estado Sensores	Página en la cual es muestra la detección de: movimiento o gas nocivo	3.31
		Visualización Estado Cámaras	Página en la que se muestra el video de las cámaras así como también el estado de conexión	3.32
		Control Luminarias	El administrador tiene el control de las luminarias del domicilio	3.33 3.34
	Configuración *ANEXO N*	Configuración Cámaras	Página que brinde el acceso a configuración de las cámaras instaladas	N-1
		Configuración Router	Página que brinde el acceso a configuración del router	N-2
		Configuración Servidor	Página que brinde el acceso a configuración del Servidor tomcat	N-3
	Mensajes SMS	Envío SMS	Página que permite el envío de mensajes SMS	3.35 3.36

	Contactos	Contactos	Página que permite enviar e-mail al administrador del sistema	3.37
Usuario	*Mi Perfil*	Editar Perfil	El usuario edita sus datos personales	3.28
	Control Domicilio	Visualización Estado Sensores	Página en la cual es muestra la detección de: movimiento o gas nocivo	3.31
		Visualización Estado Cámaras	Página en la que se muestra el video de las cámaras así como también el estado de conexión	3.32
	Mensajes SMS	Envió SMS	Página que permite el envío de mensajes SMS	3.35 3.36
	Contactos	Contactos	Página que permite enviar e-mail al administrador del sistema	3.37

Tabla 3.9: Pruebas de funcionamiento interfaz gráfico

Figura 3.28: Editar Perfil

Figura 3.29: Añadir Usuario

Figura 3.30: Editar Usuario

Figura 3.31: Estado Sensores

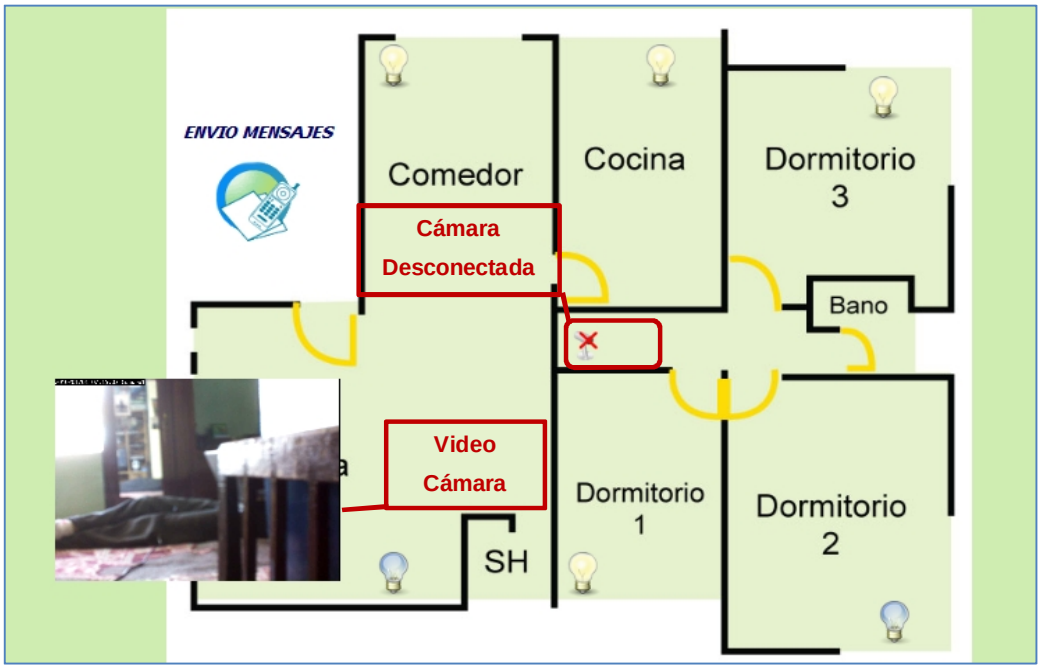


Figura 3.32: Cámaras IP

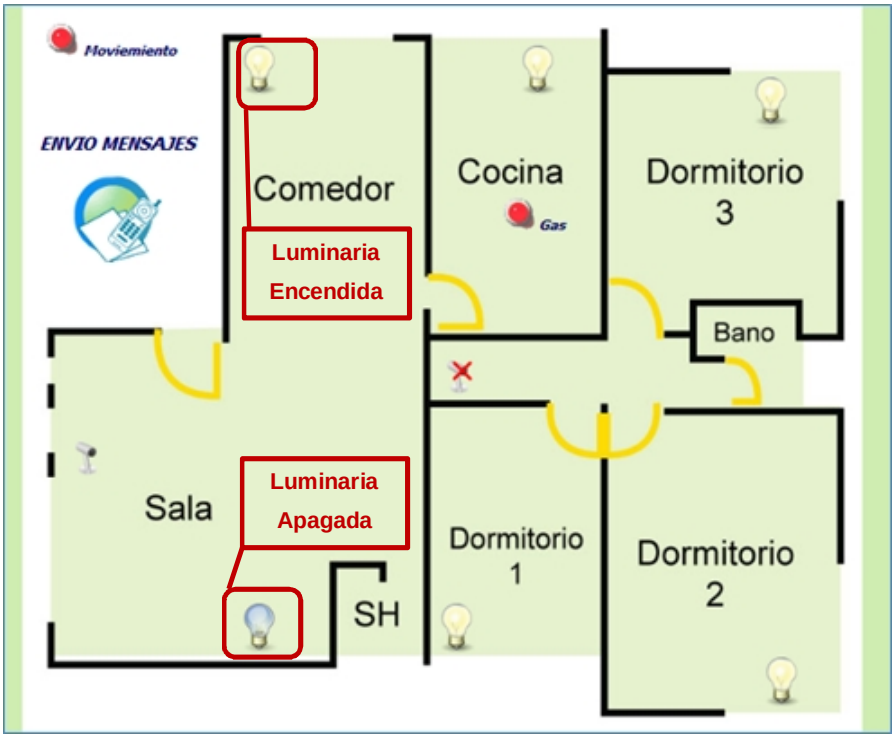


Figura 3.33: Control Luminarias

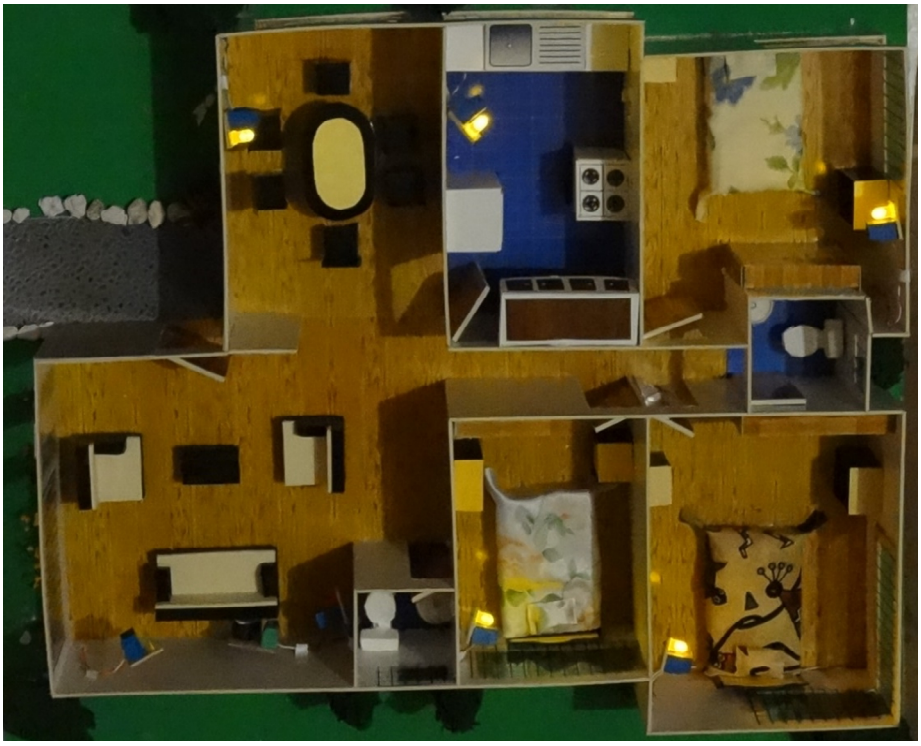


Figura 3.34: Control Luminaria Maqueta

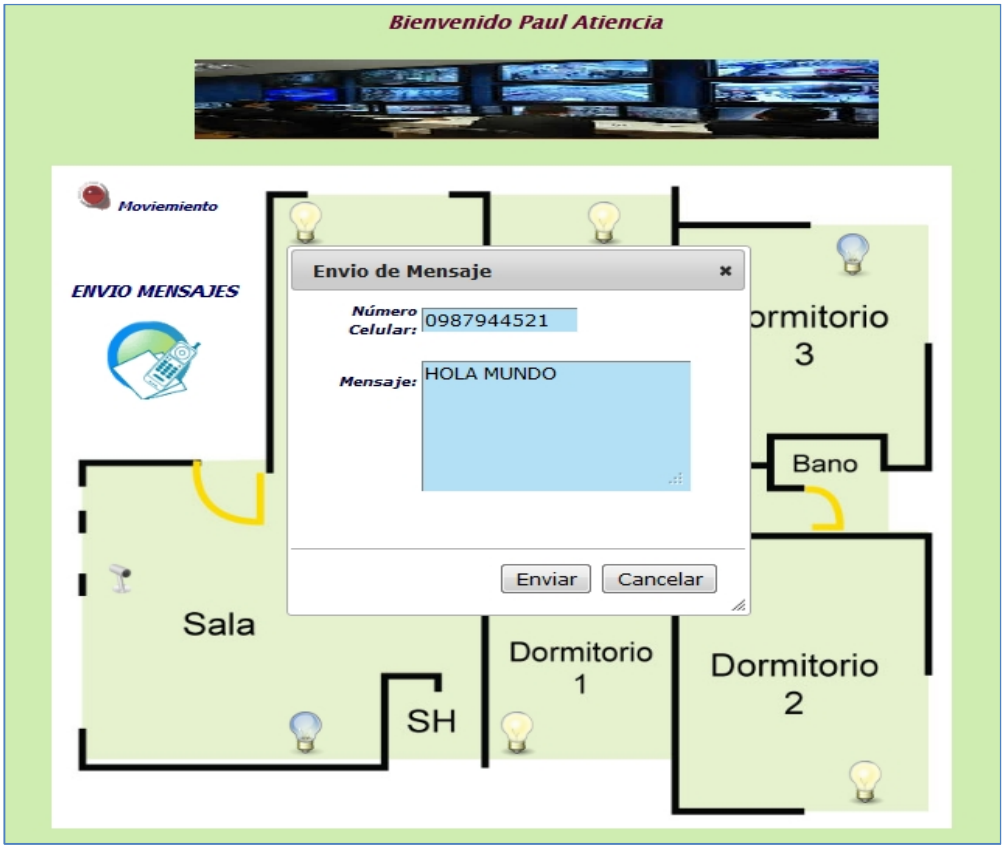


Figura 3.35: Envío SMS desde Interfaz Web

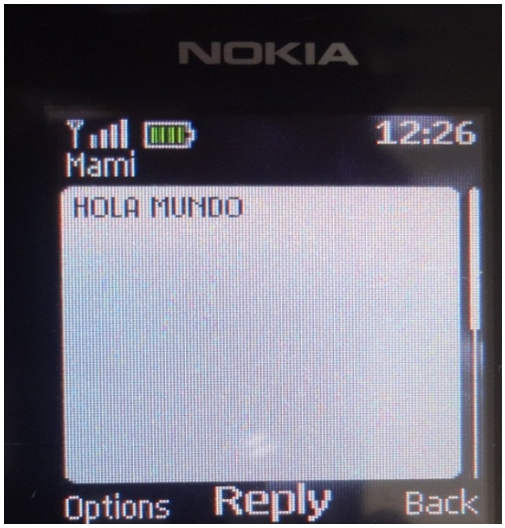


Figura 3.36: Recepción SMS

Figura 3.37: Contactos

3.3.4 Funcionamiento de Alarmas

Las alarmas del sistema de seguridad domiciliario consisten en encender una bocina y luminaria en caso de: detección de movimiento o gas nocivo dentro del domicilio, adicional se presentan aletas con el envío de SMS o correo electrónico indicando el evento suscitado. Las pruebas a realizarse consisten en accionar los sensores de movimiento y gas para verificar el envío de SMS y correo electrónico.

También se presentará un alerta enviando un correo electrónico en caso de desconexión de una cámara IP para su revisión.

Las alarmas que proporciona el Sistema de Seguridad Domiciliario se presenta en la Tabla 3.10

ALARMAS DE SENSORES Y CÁMARAS			
Tipo Alarma	***Alerta***	***Descripción***	***Figura***
Movimiento	Envío SMS	Alerta de detección de movimiento en el domicilio	3.48
	Envío E-Mail	Alerta de detección de movimiento en el domicilio	3.49
Gas	Envío SMS	Alerta se ha detectado gas en el domicilio	3.50
	Envío E-Mail	Alerta se ha detectado gas en la cocina del domicilio	3.51
Desconexión Cámara	Envío E-Mail	Se encuentra desconectada la cámara es necesario su revisión	3.52

Tabla 3.10: Funcionamiento Alarmas

Figura 3.38: Alerta SMS por detección de movimiento

Figura 3.39: Correo electrónico, alerta de detección de movimiento

Figura 3.40: Alerta SMS por detección de gas

Figura 3.41: Correo electrónico, alerta de detección de gas nocivo

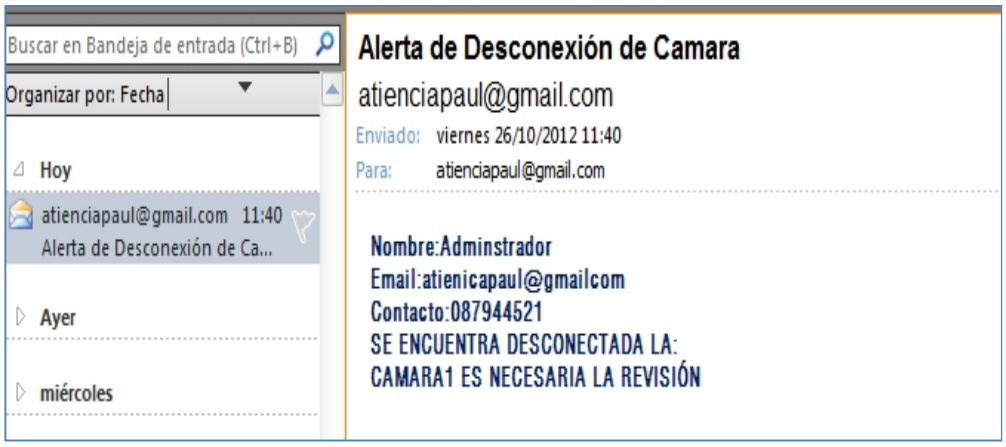


Figura 3.42: Correo electrónico cámara desconectada

3.4 COSTO SISTEMA DE SEGURIDAD DOMICILIARIO

A continuación se detallan los costos de los elementos utilizados en la implementación del prototipo de prueba, como también los costos que se generarían en la implementación de un domicilio tipo.

Cabe indicar que los costos varían con el incremento de nodos de movimiento que se desee implementar dentro de un domicilio.

3.4.1 COSTO IMPLEMENTACIÓN DEL PROTOTIPO DE PRUEBA

Los elementos que se consideran en el prototipo son: un nodo de detección movimiento, un nodo de detección de gas, el micro controlador para gestión de luminarias, la implementación de dos cámaras IP para el sistema de video vigilancia y la maqueta de prueba. No se considera el servidor y el dispositivo móvil, por ser implementado el servidor en una PC de escritorio y el dispositivo móvil un celular.

ÍTEM	CANTIDAD	PRECIO UNITARIO $	PRECIO TOTAL $
Aplicación del sistema de seguridad	1	1.116	1.116
Cámaras IP	2	120	240
Sensor Movimiento	1	50	50
Sensor Gas	1	50	50
Módulos XBee	4	80	320
PIC 16F87XA	1	20	20
Construcción Placas	4	5	20
Maqueta	1	100	100
Accesorios varios	1	40	40
SUBTOTAL			**$ 1.956,00**
IVA 12%			**$ 234,72**
TOTAL			**$ 2.190,72**

Tabla 3.118: Costos Prototipo de Prueba

En el costo de desarrollo de interfaz gráfico se tomó en cuenta el costo / hora de programación tomando como referencia la remuneración mínima vigente al 2013 y la el sueldo de un programador:

Remuneración Mínima Vigente al 2013: $318,00 [32].

Sueldo mensual de un Ingeniero programador: 5.9 x Salario mínimo [33].

Costos hora programación: $\frac{5{,}9\ x\ 318}{(21\ días\ laborables\ por\ mes)(8\ horas)} = 11.16\ dolares/h$

Horas de programación de aplicativo *web*: 100.

El costo de desarrollo del aplicativo es: $ 1116 Dólares.

En el costo de accesorios varios se consideran elementos como: resistencias, baterías, Led's entre otros.

3.4.2 COSTO IMPLEMENTACIÓN EN UNA CASA MODELO

En los costos considerados en la implementación del sistema se debe añadir los siguientes elementos:

- Servidor del sistema.
- Dispositivo móvil.
- Instalación de 1 punto de red categoría 5e(para el servidor del sistema).
- Dispositivos de potencia para adaptar las señales del micro controlador a la red eléctrica.
- Mano de obra de instalación de dispositivos de potencia incluido materiales[34].

[32] Remuneración mínima vigente al 2013 Fuente: Ministerio de relaciones laborales

[33] PROYECTO DE REGLAMENTO DE ESCALAFÓN Y SUELDOS DE LOS INGENIEROS ELÉCTRICOS Y ELECTRÓNICOS DEL ECUADOR, Comisión de Defensa y Ejercicio Profesional CIEEPI

[34] http://www.cconstruccion.net/estadistica/rubros_unitarios.xls (pagina revisada al 05 Septiembre del 2013)

ÍTEM	CANTIDAD	PRECIO UNITARIO $	PRECIO TOTAL $
Aplicación del sistema de seguridad	1	1.116	1.116
Instalación dispositivos de potencia	12	42,13	505,56
Cámaras IP	5	150	750
Dispositivos de potencia	12	20	240
Servidor	1	600	600
Celular	1	70	70
Sensor Movimiento	8	50	400
Sensor Gas	2	50	100
Módulos XBee	12	80	960
PIC 16F87XA	1	20	20
Construcción Placas	12	5	60
Punto de red Cat 5e	1	80	80
SUBTOTAL			**$ 4.911,56**
IVA 12%			**$ 589,39**
TOTAL			**$ 5.500.95**

Tabla 3.9: Costos Domicilio Tipo

CAPÍTULO 4

ITIL *(*INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY*)*

4.1 DESCRIPCIÓN DE ITIL [40]

Information Technology Infrastructure Library ITIL. Es un estándar desarrollado en los años 80 por el Reino Unido dentro del departamento llamado OGC con sus siglas traducidas Oficina de Comercio Gubernamental.

ITIL se puede considerar como el estándar de facto que ha sido adoptado como base por grandes compañías de gestión de servicios como: HP, IBM y Microsoft, dando como resultado nuevos modelos, como para consultoría, educación y herramientas de *software* para el soporte.

ITIL se ha extendido a nivel mundial para la gestión de Servicios TI. Las razones para este éxito se deben a las características de ITIL, desde su comienzo ha estado disponible a todo el público. Esto significa que cualquier organización puede utilizar este marco en sus publicaciones. ITIL documenta las mejores prácticas de la industria.

ITIL describe el comportamiento de las organizaciones de Gestión de Servicios. Los modelos muestran las actividades generales, los objetivos, las entradas y salidas de los varios procesos que pueden incorporarse dentro de las estructuras IT. ITIL no pretende establecer de forma obligatoria los pasos que deben hacerse a diario, debido a que cada organización es diferente.

4.2 BENEFICIOS DE USAR ITIL [41] [42]

La implementación de los servicios TI ofrecida por ITIL brinda beneficios como:

- Mejora la percepción de satisfacción de los usuarios con los servicios TI.
- Incrementa la capacidad de encontrar los requisitos de negocio para los servicios TI.

- Reducción de costos en el desarrollo de prácticas y procedimientos dentro de una organización.
- Establecimiento de estándares y guías para el personal TI.
- Mejor comunicación entre el personal de TI y los clientes.
- Mejora de calidad de los servicios TI.
- Mayor productividad y mejor uso de la experiencia del personal TI.

Los beneficios para los clientes de los servicios TI, son:

- Seguridad de que los servicios TI son dados por procedimientos documentados que pueden ser auditados.
- Conocimiento de las formas de pedir asesoramiento por los puntos de contacto o foros sobre requerimientos de cambio.
- Soluciones registradas listas para que el personal de TI brinde un servicio más rápido y un control de acuerdos de niveles de servicio.

Diversas organizaciones TI se orientan hacia sus clientes, para demostrar su compromiso con el negocio. ITIL enfatiza en la importancia de proveer los servicios TI para cubrir las necesidades del negocio de una manera eficiente y efectiva, con respeto a sus costos, ayudando a reducirlos.

El uso de ITIL en una organización permite un acercamiento a la gestión de servicios, usando un lenguaje común de términos que permite una mejor comunicación entre TI y los clientes.

4.3 VERSIONES ITIL

La diferencia entre las versiones v2 y v3 de ITIL, es que esta última versión basa su estructura sobre la modalidad denominada Ciclo de Vida de los Servicios.

El Ciclo de Vida del Servicio tiene cinco fases que se retroalimentan entre ellas de la manera mostrada en la Figura 4.1

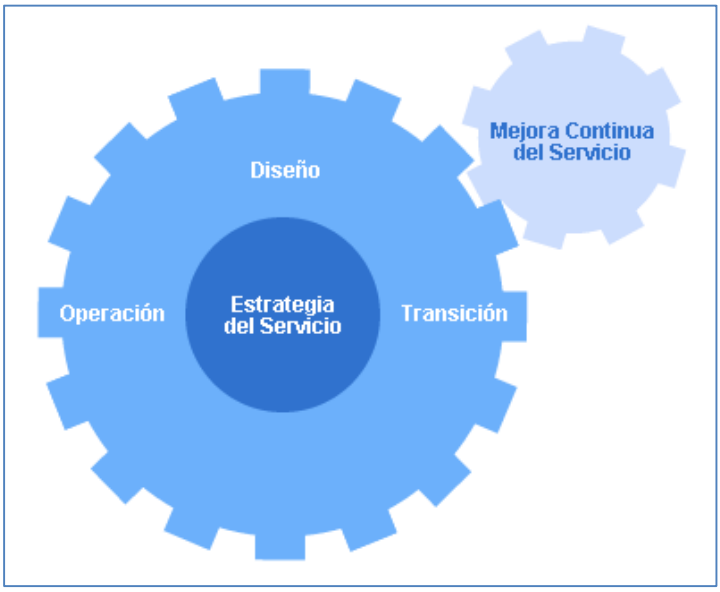


Figura 4.1: Ciclo de vida de los Servicios [41]

Los antiguos conceptos de Provisión y Soporte al Servicio han sido transformados en las cinco fases siguientes:

- **Estrategia del Servicio**: en donde se define qué servicios se proporcionarán, a qué clientes y en qué mercados.
- **Diseño del Servicio**: en esta fase se desarrollan nuevos servicios o se modifican los existentes, adecuándose a la estrategia predefinida.
- **Transición del Servicio**: es la encargada de la puesta en operación de los servicios diseñados.
- **Operación del Servicio**: fase ocupada de las tareas operativas y de mantenimiento de los servicios, incluyendo la atención al cliente.
- **Mejora Continua del Servicio**: tomando en cuenta los datos y la experiencia acumulada propone variantes para la mejora del servicio.

En cambio, ITIL v3 propone una visión más detallada de todos los aspectos involucrados en la Gestión de los Servicios y sus procesos.

ITIL v3 está orientada a procesos, y la relación de éstos con las fases del Ciclo de Vida no es tan rigurosa como lo era con la visión de Provisión y Soporte al Servicio de ITIL v2.

En la figura 4.2 se muestran las fases del Ciclo de Vida con sus procesos más destacados:

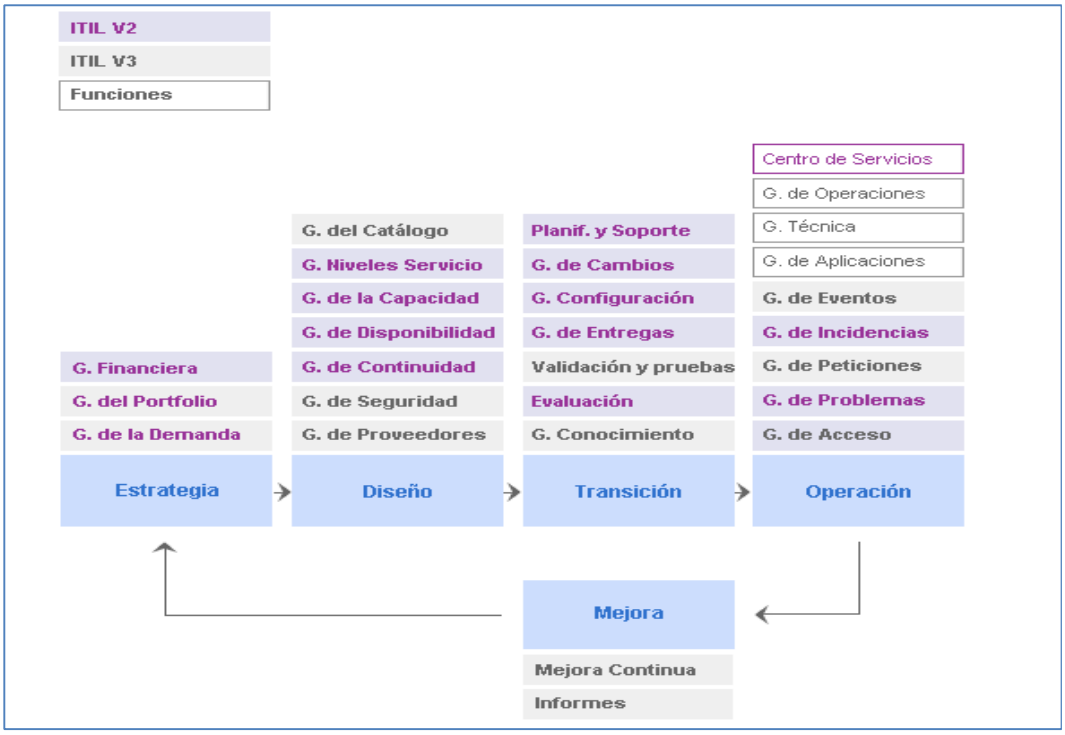


Figura 4.2: Procesos y funciones ITIL[35]

4.4 IMPLEMENTACIÓN ITIL

En este caso el manual a seguirse es una empresa que brinda servicio de seguridad para cual se ha desarrollado una serie de procesos teniendo como fin el concepto de Ciclo de vida del servicio, que tiene como objetivo convertir la Gestión del Servicio en un modo de trabajo mejorado.

Para conseguir este objetivo es necesario determinar qué servicios deben ser prestados y por qué han de ser prestados desde un punto de vista del cliente y el mercado.

[35] Imagen obtenida de http://itilv3.osiatis.es/ a Febrero 2013

4.4.1 DESCRIPCIÓN DEL SERVICIO

El servicio que se prestará es: instalación y soporte a los equipos de seguridad domiciliaria, tomando en cuenta los siguientes aspectos:

Instalación

Ubicar adecuadamente cada uno de los elementos constituyentes del Sistema de Seguridad en la casa que se requiere el servicio.

- Configurar e instalar la aplicación, encargada de la obtención de los datos de las cámaras y sensores.
- Comprobar el funcionamiento de los diferentes elementos del Sistema.
- Crear cuentas de usuario, de las personas interesadas y responsables del domicilio.
- Indicar a los diferentes responsables del domicilio el funcionamiento del Sistema.

Soporte

- Ir al domicilio cuando se reporte un daño en la infraestructura de la red.
- Verificar en los dispositivos de red, cual puede ser el problema de conectividad.
- Mirar si es problema de configuración o si es problema de lectura.
- Si alguno de los dispositivos presenta daño remplazarlo, y configurarlo.
- Finalmente verificar el correcto funcionamiento de todo el Sistema previo a la entrega al usuario del domicilio.

Ciclo de Vida

Este servicio se presta y se entrega funcionando correctamente. Toda la infraestructura instalada estará vigente hasta que se decida implementar una nueva tecnología.

4.4.2 FACTORES INTERNOS PARA EL LANZAMIENTO DEL SERVICIO

Empresa

- Creación, procesamiento y encaminado de la red de información y elementos varios, dependiendo del uso que se le va a dar.
- Procesamiento de las varias etapas y financiación ofrecida por los bancos.
- Respecto a los problemas que puede traer la producción, se tomó en cuenta las diferentes leyes económicas, precios y recursos disponibles.

Clientes

- El valor percibido por el producto sería bajo.
- Gran fidelidad y velocidad de la información transportada.

Competencia

- La competencia del producto es variada, dependiendo del nivel de seguridad a implementarse.
- Se producirá la mayor cantidad de bienes reduciendo lo más posible los precios.
- Alta duración del producto, debido a la evolución y estructura del mercado.

Intermediarios

- La empresa maneja la distribución del producto sin intermediarios ya que tiende a servir principalmente a domicilios.

- En lo que se refiere a encontrar clientes utilizaría anuncios publicitarios en radio y televisión.

Proveedores

- Compañías en cargadas de la venta de sensores, cámaras y equipos de interconectividad.
- Programadores de micro-controladores necesarios para la configuración de cada uno de los sensores requeridos.
- Bancos que faciliten dinero que permitan mantener a la empresa en sus requerimientos tecnológicos y de mercado.

Públicos

- Manejo de opiniones tanto en periódicos, revistas, radios y televisión.
- Trabajadores de la misma empresa.

4.4.3 FACTORES EXTERNOS PARA EL LANZAMIENTO DEL SERVICIO

Demográficos

- Dirigida a la población entre 30 y 60 años.
- No habrá problema con la expansión del servicio por incremento poblacional.

Económico

- Usuarios con capacidad adquisitiva media-alta.

Natural

- No presentaría impacto medio-ambiental por utilizar medios de transmisión inalámbricos.

Tecnológico

- La invención del producto es una innovación al manejo usual de los materiales que lo conforman.

Político

- Se necesitan permisos por el servicio que se quiere ofertar.
- Cumplimiento de los estándares establecidos para el uso e instalación de cada uno de los servicios ofrecidos.

Cultural

- Origina cambios culturales por el aprendizaje, manejo de tecnología antes no conocida y por la información a la cual tendría acceso el interesado en el producto.

4.4.4 COMPORTAMIENTO DE COMPRA

4.4.4.1 Necesidades de los Consumidores o Usuarios que cubre este Servicio

Debido a que la empresa ofrece el servicio de instalación y soporte con el fin de permitir la vigilancia automática del domicilio, se cubren varias necesidades en diferentes campos, a través de:

- Seguridad y Orden: Instantaneidad a la hora de obtener datos y estadísticas verídicos y sin temor de manipulación indebida.
- Estatus y Prestigio: El uso de elementos tecnológicos avanzados afianzada con la seriedad de la empresa proveedora del servicio incrementa el nivel de credibilidad e imagen del usuario.

4.4.4.2 Segmentación para el Marketing de Consumidores del Producto

Segmentación geográfica

Es la variable que utilizaremos para segmentar nuestro producto, debido al uso que le daremos al mismo, y lo dividiremos empezando por provincia, luego por ciudad, a continuación sector y por último por barrio.

Provincia

De la investigación realizada se conoce con seguridad y certeza que este tipo de control se da en la Provincia de Pichincha, que va a ser la primera donde se ofrecerá el producto y se procederá a su instalación, para luego promocionar a las distintas provincias del país que requieran el servicio.

Ciudad

Como se sabe este tipo de control ya se observa en los diferentes hogares en la ciudad de Quito que será donde se iniciará la comercialización del producto, ya que, se tiene un número de clientes probables suficientes en toda la ciudad lo que justifica la segmentación en este nivel.

Sector

La ciudad de Quito está dividida en tres sectores bien definidos como son: Norte, Centro y Sur aquí, se procede a identificar la cantidad de dispositivos necesarios.

Barrio

Por último identificamos cada uno de los barrios de cada sector de manera que se pueda establecer los domicilios con más necesidad, para así, obtener la información requerida de cada una de ellas luego proceder a programar los dispositivos y localizar el lugar donde se llevará a cabo su instalación.

4.5 PROCESOS ITIL A IMPLEMENTARSE

A continuación una descripción de los procesos presentados en dos bloques, el *Service Support* y el *Service Delivery*.

4.5.1 PROCESOS DEL SERVICE SUPPORT

4.5.1.1 Service Desk

Para implementar un *Service Desk* es necesario una planificación minuciosa. A continuación se presentan los pasos a seguir:

- Especificar las funciones que va a realizar
- Estudiar las necesidades a contratar a terceros. Ejemplo: el soporte técnico
- Estructura de *Service Desk*: ya sean: distribuido, central o virtual
- Nombrar a responsables.
- Herramientas tecnológicas que se necesitarán.
- Métricas para medir el rendimiento del *Service Desk*.

Además, la zona de soporte principal deberá estar apartado del área de *Service Desk;* en un entorno de bajo nivel de ruido y privacidad. También se debe instalar una biblioteca con la documentación de *hardware, software* y material de que puedan necesitar los clientes. Es imprescindible tener siempre presente que el Catálogo de Servicio debe estar actualizado y disponible a todas horas. Respecto a la parte técnica se debe tener en cuenta disponer de:

- Equipos para conferencias telefónicas, manos libres.
- Espacios destinados para reuniones.
- Base de Clientes pública.

Con respecto al "factor humano" se debe tener en cuenta las siguientes consideraciones y consejos imprescindibles para el éxito del *Service Desk*:

- Comunicar a los clientes de los favores del nuevo servicio de atención y soporte.
- Disponer de reglas de comunicación con el cliente.
- Tener el apoyo y compromiso de la dirección.
- Investigar las necesidades de los clientes.

La dirección de la Empresa deberá implantar un *Service Desk* centralizado para clientes internos, externos y el resto de la organización TI. Para ello se deberá:

- Nombrar a la persona encargada del *Service Desk*.
- Definir las necesidades de la organización y los usuarios, identificando las funciones del mismo:
  - ✓ Gestionar la primera línea de soporte de la Gestión de incidencias.
  - ✓ Ofrecer información sobre los servicios ofrecidos.
  - ✓ Supervisar la calidad del servicio brindado respecto a los SLAs.
  - ✓ Encuestar y elaborar reportes periódicamente sobre el grado de satisfacción del cliente.
- Anunciar los servicios nuevos a los clientes potenciales y existentes.
- Creación de páginas Web para la comunicación con los usuarios, de manera que puedan realizarse consultas remotas, del estado de los incidentes activos, históricos y cumplimiento de los SLAs, además de las FAQs[36] actualizadas que permitan a los clientes consultar sobre los servicios prestados, errores conocidos, entre otros.
- Hacer uso de los procedimientos de comunicación con los usuarios dependiendo de la situación en presentada.

[36] Sección que ofrece una recopilación de las preguntas y respuestas más solicitadas por los visitantes o usuarios de un sitio *web*.

4.5.1.2 Gestión de Incidencias

Para la implementación de la Gestíon de Incidencias se ha establecido las siguientes acciones:

- Nombrar a la persona responsable del proceso de gestión de incidencias.
- Definición de las actividades que el proceso conlleva:
  - ✓ Gestionar la primera línea de soporte de la Gestión de incidencias.
  - ✓ Clasificar los incidentes de acuerdo al entorno de la Empresa.
  - ✓ Supervisión el proceso de gestión de incidencias respecto a los SLAs.
  - ✓ Realización de informes periódicos con la información adquirida.
- Una vez analizada la infraestructura, se debe implantar una infraestructura que facilite la ejecución de los procesos mediante:
  - ✓ Un sistema automatizado de registro de incidentes y relación con los clientes.
  - ✓ Una Base de datos actualizada para guardar y comparar nuevos incidentes con los anteriores ya sea resueltos o en curso.
  - ✓ Poner a disposición del cliente parte de estos datos (en forma de FAQs) en una *WEB*. Lo que permitirá que el usuario no necesite notificar la incidencia.
  - ✓ Una CMDB (*Configuration Management Database),* que contenga configuraciones y el impacto que pueden tener en la resolución del incidente.
- Anunciar los servicios nuevos a los clientes potenciales y existentes.
- Poner a disposición de los usuarios un espacio *Web* que sirva de medio para la resolución de las incidencias.
- Capacitar al personal perteneciente al área del proceso de gestión de incidencias.

- Definición del plan de implantación progresiva del proceso de gestión de incidencias.

Ya implantada la gestión de incidencias, el proceso se verá de la siguiente manera. Suponiendo el ejemplo en que el *Service Desk* recibe una llamada de un cliente pidiendo un servicio de soporte urgente, en donde informa que el responsable asignado todavía no ha llegado a solucionarlo.

El responsable de contestar del *Service Desk* realiza una búsqueda del pedido y confirma que si se realizó.

Siguiendo los procedimientos, el responsable realiza las siguientes acciones:

- Analiza la prioridad del caso.
- Procede al registro de los datos del incidente.
- Se realiza una consulta a la Base de Datos para verificar si el incidente es un error conocido y cuáles son las posibles soluciones temporales.
- Propone una solución temporal al cliente.
- Contacta con el área de sistemas ya que este incidente puede volver a repetirse.

En cambio por el lado del área de sistemas:

- Realiza pruebas y comprueba que el Sistema funciona correctamente.
- No logra identificar la causa del incidente.
- Llama al *Service Desk* y plantea que se eleve el problema a la Gestión de problemas.

El *Service Desk* recibe la propuesta y determina que:

- Registra la solución temporal al incidente junto a la información proporcionada por el área de sistemas.
- Cierra el incidente.

4.5.1.3 Gestión de Problemas

El funcionamiento del proceso de gestión de problemas ya implementado será.

Siguiendo el ejemplo el *Service Desk* de la Empresa eleva el incidente a la Gestión de Problemas ya que no se ha podido encontrar un error conocido y una solución. En ese momento la Gestión de Problemas comineza el proceso de análisis del incidente según los procedimientos definidos.

Se realiza el proceso de identificación y clasificación del problema.

A lo que se refiere a la clasificación, se debe en tener en cuenta el origen, la frecuencia y el impacto del problema.

Luego se realiza un análisis de las posibles causas del problema, que pueden ser:

- Errores de la programación en la aplicación de cliente.
- Errores en los módulos de registro.
- Errores de configuración de la base de datos.

Se trata de identificar la causa más probable, luego del análisis de la información registrada por la Gestión de incidencias e intentando reproducir el problema.

Una vez ubicada la raíz del problema se procede a recrear un entorno de pruebas y se realizan las modificaciones pertinentes en la programación para solucionar el problema.

Finalmente se comprueba que ya no se vuelve a presentar el problema.

A partir de la solución al problema, éste se convierte en un error conocido, y se traslada a Control de Errores quién se encargará de crear un documento con la solución propuesta.

4.5.1.4 Gestión del Cambio

La gestión del cambio es de los procesos más críticos en la implantación de ITIL. Para implementación pertinente se ha determinado realizar las siguientes acciones:

- Elegir al responsable de la gestión de cambios.
- Definir las necesidades de la Empresa.
- Crear un plan de gestión del cambio y gestión de configuración, estableciendo métricas, informes de gestión y auditorias.

El proceso de gestión de cambios comienza su labor en el momento en el que la dirección de la compañía, solicita documentación a la Gestión de Cambios con los siguientes objetivos:

- Incremento de la capacidad de los servidores de Internet para optimizar la conectividad y capacidad de respuesta.
- Creación de nuevos servicios *Web*.

Por tanto se realizarán las siguientes actividades:

- Evaluación preliminar del proyecto.
- Informe de evaluación realizado por el Gestor del Cambio con ayuda de la Gestión de la Capacidad, Gestión de la Disponibilidad, Gestión Financiera, Niveles de Servicio y Gestión de Proyectos de:
  - ✓ Impacto de cambios en la infraestructura TI.
  - ✓ Costes y recursos necesarios.
  - ✓ Cronograma preliminar de cambio.

Es necesario que la Gestión de Configuraciones debe estar bien informada sobre todos los CIs[37] afectados y documentar la información para la Gestión de Versiones para que esta pueda implementar todas las pruebas y cambios.

Ya implementado el cambio se confirma que ha sido bien implementado verificando que el nuevo sistema dispone de la capacidad suficiente para proporcionar los niveles de servicio y disponibilidad previstos.

[37] Elementos de configuración

Por último se da por cerrado el cambio.

4.5.1.5 Gestión de Configuración

La gestión de configuración consume gran cantidad de recursos, lo que podría perjudicar la implantación de ITIL. Por lo tanto es preferible estandarizar las configuraciones aplicables a los CIs.

Para estandarizar se ha decidido que la documentación aprobada sea de:

- Configuraciones de *software*.
- Configuraciones de *hardware.*
- SLAs.

El alcance es el punto central del proceso de Gestión de la configuración, pero para su implementación se debe definir los objetivos, propósito, alcance, prioridades y planteamiento de la misma, de tal forma que se alineen con los objetivos de negocio, añadiendo:

- Nombrar al Gestor de la configuración.
- Analizar las necesidades para la gestión de la documentación.
- Estudio de los sistemas actuales y de datos.
- Capacitación al personal sobre de los cambios que implica la inclusión de este nuevo proceso.

4.5.1.6 Gestión de Software

El proceso de gestión del *software* funciona de la siguiente forma en relación a un documento escrito.

La Gestión de *Software* se encarga de la compra, prueba, distribución y desarrollo de las nuevas versiones de *hardware* y *software* mediante las siguientes acciones:

- Evaluación de necesidades del nuevo *hardware,* encargándose también de su compra y configuración con la ayuda de Gestión de la Capacidad y la Disponibilidad.
- Elaboración de documentos de la nueva versión. Manual de usuario y FAQs en la Web.
- Informar a los usuarios sobre la nueva versión y aviso delas formas de mantenimiento
- Instalación de la nueva versión.

4.5.2 PROCESOS DEL SERVICE DELIVERY

4.5.2.1 Gestión de Niveles de Servicio

El proceso de Gestión de Niveles de Servicio se realiza mediante:

- El nombramiento del gestor del proceso de gestión de niveles de servicio.
- La elaboración de un catálogo de servicios.
- El desarrollo de un Plan Integral de Calidad del Servicio y la creación SLAs asociados a sus principales servicios.

El gestor de niveles de servicio tendrá la responsabilidad de la negociación y la forma en que se provee los de servicios a los clientes representando a la Empresa, así como:

- Definición de los SLAs.
- Negociación de los SLAs con clientes y proveedores.
- Supervisión del cumplimiento de los SLAs.
- Creación y mantenimiento del catálogo de los servicios.
- Elaboración de reportes sobre el rendimiento del proceso.
- Reporte de información a otros procesos.

Elaborar un Catálogo de Servicios en el que se clasifiquen los servicios donde se especifiquen las diferencias y opciones de tipos de servicio.

El Catálogo de Servicios tendrá información de:

- Disponibilidad del servicio
- Marco legal
- Plazos de entrega
- Servicios opcionales
- Programas
- Soporte

La elaboración de los SLA tiene un proceso previo en el que se fabrican las plantillas para los servicios y clientes En cada plantilla de SLA contiene:

- Responsables del acuerdo (cliente y proveedor)
- La descripción general (no técnica) de los servicios.
- Plazos para la entrega del servicio.
- Duración del acuerdo y condiciones para de renovación y/o cancelación.
- Soporte.
- Condiciones de disponibilidad del servicio.
- Tiempos de respuesta.
- Tiempos de recuperación en casos de incidentes.
- Tiempos de entrega de las mercancías.
- Planes de contingencia.
- Métodos de facturación.
- Criterios de evaluación de la calidad del servicio

4.5.2.2 Gestión de la Disponibilidad

El objetivo empresarial es tener una disponibilidad 24x7 sobre los servicios ofrecidos.

El proceso de Gestión de la Disponibilidad, es la responsable de la definición y creación de planes de disponibilidad cumplimiento del objetivo.

Los planes de disponibilidad se encargan de revisar los actuales y nuevos SLAs con los proveedores de servicios, el diseño de la disponibilidad 24x7 de los servicios TI ofrecidos, la definición de niveles de disponibilidad para los nuevos servicios, y los nuevos planes de gestión del mantenimiento.

La gestión de la disponibilidad de servicio reporta periódicamente información de:

- Tiempos de respuesta para cada incidente.
- Tiempos entre incidentes y de parada del servicio.
- Tiempos de entrega del servicio.

Esta información permite incremetar la confianza de los clientes y alertar a la organización de TI sobre posibles bajones en los niveles de calidad del servicio.

4.5.2.3 Gestión de la Capacidad

Este proceso es usado con el fin de minimizar el número de futuros incidentes que bajen la calidad del servicio, asegurar el cumplimiento del objetivo de disponibilidad, racionalizar el uso de la capacidad de la infraestructura TI y aumentar la productividad y satisfacción del cliente.

Primerio es necesario designar un Gestor de la Capacidad cuyas responsabilidades son:

- El estudio del impacto de los diferentes CIs en la capacidad del sistema.
- La monitorización del rendimiento de la infraestructura y de la eficiencia de los servicios ofrecidos.

- La valoración de los parámetros de rendimiento, almacenamiento y ancho de banda que suponen los SLAs vigentes y planificados.
- La elaboración de informes periódicos del estado de la tecnología afín con los servicios ofrecidos.
- La evaluación de los costes reales de cada servicio.

El proceso tiene como objetivo obtener un Plan de Capacidad anual con el que se estudian los datos reales con lo previsto para la Empresa.

4.5.2.4 Gestión de la Continuidad

El proceso de gestión de la continuidad se encarga de garantizar la continuidad de los servicios en un plazo nunca supere las 8 horas, mientras se restablecen los servicios en caso de desastre.

Se deberá nombrar un gestor de la gestión de la continuidad quien se encargará de la coordinación de las actividades de la Continuidad del Negocio. También deberá llegar a acuerdos con empresas de suministros de emergencia que cubran a los clientes más importantes de los servicios.

El gestor de continuidad define períodos de pruebas anuales de los planes de recuperación. Conjuntamente con las medidas a tomarse para atenuar el impacto de una interrupción del servicio, también se encargará de elaborar planes de prevención. Estos planes incluyen la contratación de servicios externos de *hosting* con un proveedor que ofrece disponibilidad con una garantía del 100% respecto a la conectividad a su *backbone*; la replicación de los sistemas críticos en diferentes localizaciones geográficas; el control y verificación de la política de *backup* de los servidores de datos.

4.5.2.5 Gestión Financiera

El proceso de Gestión Financiera permite conocer el impacto de los servicios TI en los costes de cada uno de los servicios prestados. Por lo tanto, para implementar la gestión financiera, se requiere una política de precios de los

servicios TI que permita trasladar los costes al usuario final del Sistema de Seguridad Domiciliario.

La implementación del proceso requiere las siguientes actividades:

- Evaluación y prorrateado entre los diferentes costes de los servicios.
- Valoración de los costes de personal y los costes operativos.
- Elaboración de un listado de todos los CIs que intervienen en la prestación de servicios a los clientes.
- Estimación de los costes directos asociados a los servicios TI.
- Evaluación de los costes indirectos: costes administrativos, instalaciones, entre otros.
- Implementación de criterios contables para la administración de los costes TI.

Mediante estas definiciones se establecerán correctamente los costes asociados a los servicios TI prestados y se podrán precisar las tarifas adecuadas en un futuro inmediato donde se trasladarán los costes de los servicios a los clientes.

Con la gestión del proceso se garantiza la planificación de gastos e inversiones futuras, que con la ayuda de la Gestión de la Disponibilidad, Gestión de Niveles de Servicio y Gestión de la Capacidad se realizarán un análisis de los requisitos de los clientes y las tendencias de mercado; el impacto en los costes de las necesidades futuras y proyecciones de la capacidad TI. Luego con estos datos se elaboran los "presupuestos anuales TI"

4.5.3 MEJORA CONTINUA DEL SERVICIO (CSI)

4.5.3.1 Service Desk

4.5.3.1.1 Equilibrio

Tiempo vs atención: Para establecer un equilibrio entre lo que se puede demorar con el cliente, y el número de clientes que puede atender un asesor, se procurara

por resolver todas las dudas que tiene el cliente, pero en ningún momento se le debe inducir a generar nuevas dudas.

4.5.3.1.2 Comunicación

- Toda la comunicación asesor- cliente será grabada.
- El asesor deberá tomar nota de toda duda y sugerencias del servicio y este la debe enviar al área correspondiente.

4.5.3.1.3 Procesos de operación

- El asesor debe seguir el guion respecto a cómo debe hablar con el cliente.
- El asesor debe responder a todas las inquietudes de los clientes.
- El asesor deberá evitar hacer la pregunta “¿Le puedo colaborar en algo más?
- Los Asesores en la *Service Desk*, trabajaran en 2 turnos, 6 a 18 y de 18 a 6.

4.5.3.1.4 Controladores internos y externos

- Internos:
  - ✓ En la empresa hay un buzón de sugerencias donde los asesores pueden anotar todas las inquietudes.
  - ✓ También se puede acercar al jefe inmediato para sugerir posibles mejoras.
- Externos:
  - ✓ Siempre se le da la opción al cliente, que una vez finalizada la asesoría por teléfono, el podrá calificar de 1 a 5 como le pareció el servicio prestado.

- ✓ El cliente también tiene la opción de sugerir a través del asesor que se hagan mejoras, que se denuncie algún error o irregularidad. Todo esto deberá ser anotado y enviado al área correspondiente, ya sea su superior, u a otras personas relacionada con el servicio.

4.5.3.1.5 CSI

Toda falla deberá ser analizada por la persona afectada en un tiempo máximo de 3 días en lo cual se decide si aplica ejecutarlo o no.

Si aplica ejecutarlo, deberá generar los pasos para implementarlos, y luego publicarlos, en el *Intranet*, para que todos queden enterados acerca de que cambios ha habido, y como se aplicara de ahora en adelante.

1. Áreas a medir.

   Tiempo de respuesta ante inquietudes del cliente, seguimiento del guion sobre el trato al cliente.

2. Que se puede medir.

   El tiempo que transcurre entre llamada y llamada, cuánto tiempo se demora con cada cliente.

3. Hacer mediciones de los datos.

   Todos los datos serán registrados a través de un software, que generará los informes

4. Procesos.

   Se genera una medía que muestre las mediciones para el día y luego a la semana, y de aquí se establece patrones, como las horas picos, tipos de cliente, entre otros. Y se genera informe que será analizada por el área de calidad.

5. Analizar datos

Se suelen presentar problemas al tratar un cliente “muy preguntón”, o empieza contar historias.

También hay problemas con usuario intolerantes, que quieren todo al mismo tiempo.

6. Presentar información.

   Se generará un documento en el que se plantee el problema y los pasos sobre como deberá ser solucionado, esto será realizado por el área de gestión de incidentes o problemas según sea el caso.

7. Que se puede corregir.

   La solución a las inquietudes de los clientes, será enviada por correo en los 3 días de presentada la queja.

4.5.3.2 Mantenimiento de Hardware:

4.5.3.2.1 Equilibrio

Proactivo – Reactivo: Hay que buscar un equilibrio, entre el mantenimiento preventivo y la capacidad de respuesta ante un daño. Es decir que entre menos fallas se presenten, se lograra una respuesta más rápida ante un problema, por eso es que se presta especial atención para que los equipos queden funcionando de la mejor forma.

4.5.3.2.2 Comunicación

Se debe informar la causa de las fallas al líder del grupo y cuál es el procedimiento que siguió para su solución.

4.5.3.2.3 Procesos de operación

- Se deberá tener un inventario al día de todos los insumos que hay en bodega, esto deberá estar siempre actualizado en el sistema.

- Asignar tareas: Todos los técnicos deberán estar listados y programados, para saber en qué espacio pueden ser asignados.
- Los técnicos solo trabajan en horario de oficina, y deberán responder al tiempo asignado en la *Service Desk*.
- Los técnicos se desplazaran en un taxi, junto con todo el material que necesiten, para la reparación del computador.
- Los técnicos deben reportar los gastos generados.
- Los técnicos deberán registran los materiales que le hagan falta.

4.5.3.2.4 Controladores Internos y Externos

- Internos

  Las fallas que puedan ver los asesores respecto a la forma en que se presta el servicio, y también toda nueva tecnología que se pueda implementar para mejorar la calidad del servicio, debe hacerlos a través de la plataforma dedicada para ello, en el cual indicara el motivo de queja de los clientes, como debe mejorarse el servicio y cosas por el estilo.

- Externos.

  Dentro de la prestación del servicio, siempre se le da al cliente un registro donde se especifique que fue lo que se hizo, y además un teléfono de contacto donde puede comunicar sus inquietudes.

4.5.3.2.5 CSI

Las fallas que presenten deberán ser documentadas y publicadas en una plataforma para tal objetivo, en donde se detallara problema y la solución implementada, luego esto deberá ser estudiado por el área.

1. Áreas que interesa medir.

Como es el trato que recibe el cliente por parte del técnico, cuánto tiempo se lleva cada proceso en los que repara.

2. Áreas que se pueden medir.

   Cuánto tiempo se demora el técnico reparando un equipo, cuanto tiempo pasa para que un nuevo cliente pida una reparación.

3. Hacer mediciones de los datos.

   Los datos se medirán a través del control que ejerce el líder del grupo, que es el que se encarga de recopilar y controlar todo.

4. Procesos

   De los datos que se recopilen se establecerán unos parámetros para así poder evitar fallas al futuro, como sacar un promedio de fallas al año, las fallas por cada cliente, cuáles son las fallas más comunes.

5. Analizar datos.

   Identificar donde están las fallas, cuales son los procesos que están demorando mayor tiempo en repararse, cuales son los clientes que más fallas reportan, cuales son los repuestos que más fallan, cual es el técnico que más se demora.

6. Presentar información

   Todos los datos serán anotados por el líder del grupo y se prepara un informe que se envía al área de calidad.

7. Que se puede corregir.

   Sobre estos datos se puede concluir, si es necesario cambiar de proveedor, si es el técnico el que está presentando falla entonces hay que remplazarlo por otro, si hay algo que en la metodología que pueda estar fallando.

4.5.3.3 Administración de Servidores

4.5.3.3.1 Equilibrio

Regularmente los usuarios recurren a llamar a los administradores de servidores por fallas que son muy obvias de solución. Por eso es importante que el usuario esté presente en el momento de la solución para que en un próximo incidente él pueda solventarlo.

4.5.3.3.2 Comunicación

Todas las fallas serán reportadas al líder de grupo.

4.5.3.3.3 Procesos de operación

- Los técnicos deberán tener programadas todas sus tareas y responder a lo asignado en la *Service Desk*.
- Los técnicos deberán estar actualizados y continuamente probando en máquinas virtuales actualizaciones y configuraciones, en momentos que no tengan asignados tareas.
- Los técnicos deberán asistir inmediatamente reportado el daño, si y solo si en la *Service Desk* no lo pudieron solucionar.
- Los técnicos deberán hacer un manual donde detallen cual era el problema y cuáles son los pasos exactos para darle solución. Este manual pasara a formar parte de la *Service Desk*.

4.5.3.3.4 Propiedad

Como persona responsable del área se elegirá a uno de los asesores del área con más experiencia y actitud de líder.

4.5.3.3.5 Controladores Internos y Externos

- Internos

Los administradores de redes deberán comentar sus sugerencias a su superior y también anotarlas por escrito dentro de la plataforma. También se realizara un foro donde anoten sus dudas para que otros usuarios las respondan.

- Externos

  Todas las sugerencias de los usuarios siempre las podrán enviar al administrador@gmail.com

4.5.3.3.6 CSI

Las fallas que presenten deberán ser documentadas y publicadas en una plataforma para tal objetivo, en donde se detallara problema y la solución implementada, luego esto deberá ser estudiado por el área.

1. Áreas que interesan medir.

   Atención hacia los usuarios, como solucionan los problemas en el servidor, cuanto se demoran en cada proceso, cuanto tiempo tardan en llegar al lugar, que es lo que le hace generar fallas al servidor del cliente.

2. Áreas que se puede medir.

   Cuantas fallas se presentan por usuario, cuánto tiempo se demora un administrador de redes en darle solución a una falla, cuantas fallas se presentan en el mes.

3. Hacer mediciones de los datos.

   El encargado del área llevará un registro de todos los pormenores en el sistema.

4. Procesos.

   El administrador de redes asignado a la solución del problema con el servidor, anotara en una libreta, cual fue el problema encontrado y como fue la solución, luego esto lo ingresará a la plataforma, e informará a su

líder, el cual enviará el informe al área de calidad, el cual se encarga de la publicación.

5. Analizar datos.

   Con los datos se podrá evidenciar cual es el personal que más está fallando en el área, cuales son los problemas más comunes, cuales son los clientes que suelen reportar más fallas, porque pueden estar sucediendo los problemas.

6. Presentar informes.

   Los datos son anotados por el líder de grupo, el cual lo envía al área de calidad, el cual se encarga de generar informes generales, mensuales al área administrativa, para así enterarse de cómo marcha el funcionamiento de determinada área.

7. Que se puede corregir.

   En base a los datos recopilados se puede decir si hay que cambiar a alguno del personal, si hay un cliente al que se le debería dar una inducción quizás gratuita, debido a su continuo reporte de fallos.

4.5.3.4 Entrenamiento de TI

4.5.3.4.1 Equilibrio

Se deberá buscar un equilibrio entre lo que se le enseña y el material de apoyo que se publique. No se puede demorar mucho tiempo en la capacitación, ya que este personal es normalmente requerido para otras labores. Primeramente se publicará un material en vídeos, y seles enseñara como funciona, y luego en la capacitación, se les enseñaran cosas más avanzadas.

4.5.3.4.2 Comunicación

Todos los pormenores que se presenten en las capacitaciones serán reportadas al líder del grupo.

4.5.3.4.3 Procesos de Operación

- Los entrenadores deberán estar completamente actualizados en los temas, y mensualmente seles hará evaluaciones respecto al conocimiento de nuevos temas.
- En un documento deberán estar registrados todos los temas que forman parte del entrenamiento, y los entrenadores se apegaran a él. Dicho documento deberá contener una lista de preguntas y respuestas comunes.
- Todo conocimiento nuevo deberá ser compartido, y luego puesto en discusión, y si este es aprobado como parte del entrenamiento, entonces se hará una documentación.
- Semestralmente se hará una revisión al documento para ver que artículos van quedando obsoletos y que nuevos temas se le pueden añadir.

4.5.3.4.4 Controladores Internos y Externos

- Internos

  Todas las sugerencias por parte de los capacitadores, serán entregadas al líder.

- Externos

  Todas las sugerencias por parte de los asistentes a las capacitaciones, pueden hacerse directamente al instructor, o por medio de la plataforma donde se subirán los vídeos de capacitación.

4.5.3.4.5 CSI

Se medirán todos los posibles factores que produzcan deficiencias en la capacitación. Todo esto será documentado y formará parte de próximas capacitaciones.

1. Áreas que interesa medir

Como se desenvuelve en la capacitación, cuales son los temas que no se entienden con facilidad, con qué frecuencia y quienes entran a la plataforma donde se encuentran los vídeos, la capacidad para resolver inquietudes de los clientes, si los clientes entienden el tema que se les explica.

2. Áreas que se pueden medir

   Quienes asisten a la capacitación, cuales presentan más dudas, cuales son los de mejor desempeño.

3. Hacer mediciones de los datos

   El capacitador tomará nota de los pormenores de la capacitación, y comentara a su líder, los pormenores más destacados. El líder llevará por su parte las mediciones que haga a sus capacitadores, anotándolas en un informe que deberá presentar a sus superiores.

4. Procesos

   El capacitador en una hoja que lleve en el computador deberá anotar los detalles que surjan con los capacitados, esto deberá compartirlo con su superior, y a partir de ahí explicar lo más destacado.

5. Analizar datos

   Con base a los datos recopilados, se analizará cuáles son los capacitadores con más fallas, quienes asisten menos a las capacitaciones, cuales requieren refuerzos, también nos podemos dar de cuenta si los vídeo tutoriales necesitan ser renovados.

6. Presentación de informes

   Con todos los datos recopilados el líder del área presentara un informe legible, de cómo marcha su sección, que problemas ha encontrado y que soluciones propone, para que tomen medidas futuras.

7. Que se puede corregir

En esta parte se decide si hay alguna información que deba ser incluida en las capacitaciones, o si hay que cambiar de metodología.

4.5.3.5 Soporte a una Infraestructura de Red

El soporte a una infraestructura de red, es algo que suele frenar mucho los procesos de una empresa, pero además es algo que requiere atención inmediata. Por eso hay que encontrar un equilibrio entre estos aspectos. Para ello hay que hacer esfuerzos en ambas partes. De parte de la empresa se madrugara a solucionar los servicios que requieran el frenado de las operaciones, y departe del cliente deberá sacrificar algo de sus servicios cuando deban ser detenidos. En lo posible, si un servicio no está afectando mucho al usuario, entonces para evitar el frenado de las operaciones se hará los domingos.

4.5.3.5.1 Comunicación

Los técnicos deberán hacer un reporte de cuál fue la falla que encontraron, y como la solucionaron, y todo esto deberá ser informado a su líder de grupo, y este último preparara informes que puedan ser analizados por instancias superiores.

4.5.3.5.2 Procesos de Operación de Servicio

- En la *Service Desk* se atiende el reporte de los daños, y se le da indicaciones previas al cliente.
- El personal asiste en el horario que se organizó con el cliente.
- El personal asignado presenta todo funcionando al cliente.
- El personal asignado se reporta ante su jefe inmediato.

4.5.3.5.3 Controladores Internos y Externos

- Internos

  Todas las posibles mejoras deben ser sugeridas al jefe inmediato, y también es indispensable, que todo el personal este continuamente

estudiando y actualizándose en nuevas tecnologías, para que puedan sugerir ideas nuevas e innovadoras.

- Externos

  Los clientes podrán sugerir mejoras al personal que asista a la empresa o podrá llamar a una línea la cual lo conecta con el *Service Desk*, y allí podrá dejar su inquietud.

4.5.3.5.4 CSI

Se deberá medir una cantidad de factores en las que se pueda ver que es lo que produce los fallos, y todas las fallas detectadas deberán ser registradas en una base de datos para que se estudiada, por el personal asignado a esta área.

1. Las áreas que interesa medir

   Cuanto se demora el técnico en solucionar la falla, cuales son los pormenores de la falla, medir si la causa del error es por mal manejo del cliente, o por problemas dejados por aquellos que implementaron el sistema.

2. Lo que se puede medir

   Medir cuales son las fallas que más se presentan, cuales son los responsables de las fallas, que elementos dentro de la red son los que más fallan, medir cuales son los problemas de configuración que más se presentan.

3. La medición

   Los técnicos asignados a la labor deberán anotar cuales son las fallas que se presentaron y cuál fue la solución que implemento, también deberá indagar con el personal afectado, que fue lo que produjo la falla y que sectores no funcionan.

4. Procesos

Los técnicos deben anotar todo, luego depositarlo en una base de datos, donde especifican todos los apuntes, estos apunten deberán ser clasificados del tal manera que todo el resto de personal los pueda consultar con facilidad. También el personal de calidad deberá verificar, que todo esto esté bien realizado.

5. Analizar datos

Con base a todas las mediciones que se hagan se puede mirar que tipo de fallas son más continuas, mirar si el responsable de estas fallas es alguien del personal del almacén el que las está produciendo, también mirar si las fallas son producto de una mala implementación, mirar si es problema de calidad con alguno de los productos.

6. Presentar informes

   El líder de grupo deberá revisar todos estos informes y realizar estadísticas para mensualmente presentar informes al área superior y así estos estén enterados de cuáles son las fallas, y en que se puede mejorar o que se ha decidido implementar.

7. Que se puede corregir

   - Con base al análisis de los datos, se puede establecer si es necesario una capacitación especial al personal que manipule el Sistema.

   - Si son los equipos los que están presentando los fallos, entonces se deberá conseguir una nueva marca.

4.5.3.6 Documentación Requerida para el Control de Gestión de Empresa

- Un documento donde detalle los activos, los proveedores

- Un documento donde se describe que deben seguir la persona de *Service Desk*.

- Documentos para cada área donde están registradas las sugerencias internas y externas.
- Un documento donde describe los tipos de servicio que va a ofrecer.
- Documentos donde describe todos los insumos que necesita la empresa en cada área.
- Documento donde describe las políticas de transición de la empresa.
- Documento donde describe las funciones de cada de los empleados en cada área.
- Un documento donde describe los procesos de operación del servicio.
- Documento donde se describe los insumos que faltan en determinada área.
- Un documento donde se muestran las fallas y soluciones en el área requerida.

4.6 SOFTWARE PARA IMPLEMENTACIÓN DE ITIL

4.6.1 SYSAID SOFTWARE HELP DESK Y GESTIÓN DE ACTIVO

SysAid es un dominio web basado en herramientas de *software* IT. Se encarga de la configuración del hardware, la supervisión de activos, automatizar los procesos de ayuda de escritorio, las licencias de *software* y demás proyectos. Mediante un escaneo y testeo automático en la red local proveyendo detalles para cada máquina y permitiendo un control de forma remota. La ayuda de escritorio centraliza mediante una interfaz intuitiva y cómoda los datos de usuario, el historial de peticiones de servicio y el inventario, tanto de *hardware* como de *software* de ayuda de escritorio.

Puede ser descargado en ***http://www.ilient.es/***

4.6.2 SERVICE DESK PLUS - HELP DESK THE WORLD LOVES

ServiceDesk Plus es una solución de *Service Desk* y Gestión de Inventario. Brinda un paquete integrado con la gestión de incidencias, gestión de activos, compras, gestión de contratos, inventario automático, gestión de conocimientos y portal de autoservicio para usuarios finales. *ServiceDesk Plus* incluye lo necesario para gestionar procesos de informática interna, lo cual ayuda a tener una mayor productividad y mejor servicio para usuarios finales.

Puede ser descargado en ***http://www.manageengine.com/products/service-desk/spanish/index.html***

4.6.3 NUMARA SOFTWARE

El sistema brinda administración de servicios de IT, con prácticas y sencillas soluciones pueden estar activas y funcionando en pocos días; proporcionando un rápido retorno de la inversión y un bajo costo total de propiedad con un mínimo de interrupción del negocio.

Puede ser descargado en ***http://www.numarasoftware.com/spanish/***

4.6.4 SOFTWARE DE CÓDIGO ABIERTO DE ITIL

El *software* de código abierto de ITIL, utilizado por las organizaciones como factor clave para sus procesos de ITIL. Hay cinco principales disciplinas en ITIL que tiene *software* de código abierto de ITIL fuente para apoyar los procesos de la disciplina.

Puede ser descargado en ***http://www.wareprise.com/2007/04/14/open-source-itil-software/es/***

4.6.5 PROCESSWORX

ProcessWorx es una herramienta que ha sido autorizada por miles de profesionales de TI y las organizaciones, incluyendo una extensa lista de compañías Fortune 500. ProcessWorx ITIL basada en herramientas de *software* y las plantillas son aprovechadas por los directores técnicos de todo el mundo para

implementar más rápidamente las mejores prácticas de ITSM y establecer una base para la mejora de los servicios de TI y medir las reducciones de costes.

Puede ser descargado en ***http://www.processworx.com/***

4.6.6 ARANDA

Soluciones para la gestión de sus recursos IT

- IT *Infrastructure Management*

Productos que aseguran la estructura informática sólida para un negocio exitoso.

- *TAsset Management*

Esta suite fue desarrollada para permitir a las empresas determinar y monitorear los recursos corporativos, sean o no informáticos.

- IT *Security Management*

Este grupo de aplicaciones garantiza la protección efectiva y proactiva de los recursos informáticos de las organizaciones.

- *IT Support*

Productos que optimizan, aumentan y facilitan los servicios IT alineados directamente con las necesidades del negocio

- IT *Output Management*

  Conjunto de soluciones que intervienen en la administración y control de tareas propias de impresión y manejo de documentación.

Puede ser descargado en ***http://www.arandasoft.com/***

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Con el actual nivel de inseguridad en el país este proyecto permite proteger a los domicilios de robos, alertando a los usuarios en tiempo real del ingreso de personas no autorizadas al hogar, gracias al uso de tecnología de SMS y mail.

- La implementación del Sistema de Seguridad Domiciliario permite integrar: un sistema de video vigilancia, sensores de movimiento y gas y aletas vía SMS y mail en un aplicativo *web* al cual tienen acceso los integrantes del hogar.

- La seguridad no solamente se refiere a evitar la entrada de intrusos, sino también, que el hogar sea un ambiente libre de accidentes, y esto se logra en base a una buena arquitectura, usando materiales de calidad y tomando medidas preventivas de seguridad que permitan evitar accidentes. En este caso la tecnología inalámbrica resulta altamente versátil, ya que permite la implementación del sistema de manera más rápida por no requerir el uso de cables representando ahorro de dinero.

- El Sistema de Seguridad Domiciliario permite aprovechar el acceso a Internet, controlando el encendido y apagado de luces desde cualquier lugar del mundo y de esta forma simular presencia ayudando a los integrantes del hogar a salir de viaje sin preocupaciones.

- Uno de los aspectos importantes es la salud en las personas y con el uso de sensores de gas se tiene un mecanismo de prevención de

accidentes en el hogar ocasionados por inhalación de gas de cocina, CO2 como también prevención de incendios, lo que representa un beneficio a los usuarios del hogar evitando acudir al hospital y perdida de bienes materiales.

- Las habilidades y conocimientos de los usuarios, para operar el sistema de seguridad domiciliario, son básicos, lo que permite una fácil manipulación de las herramientas y ayuda a visualizar la distribución de los equipos en el hogar.

- Hacer uso de ITIL ayudará a hacer más eficientes los procesos empresariales, ya que propone la realización de procesos puedan hacerse de una forma más eficaz, que se adopten ciertas métricas y procedimientos que han sido probados por proveedores de Tecnología.

5.2 RECOMENDACIONES

- Implementar un respaldo eléctrico al sistema de Seguridad Domiciliario, para el caso de falla en el sistema eléctrico principal, ya que en caso de apagado de los equipos el sistema quedará inoperante.

- Evitar la manipulación de los equipos que conforman el Sistema de Seguridad Domiciliario, a través de elementos de protección u ocultándolos de la vista de los usuarios, para prevenir daños en el funcionamiento del sistema.

- Para el uso del sensor de detección de movimiento se recomienda activarlo cuando el ingreso al domicilio sea restringido, de tal forma que se pueda evitar falsas alarmas y prolongar la vida de las baterías. Mientras que el sensor de gas nocivo se recomienda tenerlo activado durante las 24 horas del día, para alertar a los usuario en caso de concentración de algún gas nocivo para la salud.

- Para las alertas mediante el envío de mensajes SMS, es necesario contratar un paquete de mensajes con alguna operadora celular, que permitan tener activo el Sistema de Seguridad Domiciliario el mayor tiempo posible.

- Se debe solicitar al proveedor de Internet la asignación de una IP pública estática para tener un sitio fijo de acceso desde Internet, o en su defecto registrar la IP pública en un dominio de Internet.

- Para el acceso al Sistema de Seguridad Domiciliario desde Internet, de preferencia no hacerlo desde los Cyber Cafés, Centros de Cómputo o dispositivos a los cuales el acceso sea de todo el público.

- El Sistema de Seguridad Domiciliario puede ser mejorable en aspectos de inclusión de mayor número de sensores, que permitan aprovechar de mejor manera la tecnología ZigBee. También podría incluir cámaras de mayor capacidad de detección de imágenes que permitirá evaluar con mayor detalle los videos capturados.
- Es necesario que las instituciones educativas brinden referencias para adoptar mejores prácticas ITIL ya que implica que todos lleguen a un nivel de eficiencia que se traduzca en una buena prestación de servicios en el mediano y largo plazo. Y es que este conjunto de estrategias con un foco claro permitirán alinear la tecnología con los objetivos que los negocios piensan alcanzar.

REFERENCIAS BIBLIOGRÁFICAS

[1] Estadísticas de Seguridad Nacional.

20091026 encuesta_de_victimizacion.pdf

Actualización de datos provistos por La Policía Nacional del Ecuador a Diciembre de 2012 a través de un archivo en Excel en Febrero de 2013.

[2] Valverde Rebaza Jorge Carlos Universidad Nacional de Trujillo – Perú – 2007, El Estándar Inalámbrico ZigBee.

http://www.seccperu.org/files/ZigBee.pdf

[3] ZigBee Alliance, "Tutorial".

http://dspace.epn.edu.ec/bitstream/15000/8637/2/T10110CAP2.pdf

[4] J. Martín Moreno, D. Ruiz Fernández, Informe Técnico: Protocolo ZigBee (IEEE 802.15.4), Junio, 2007.

http://rua.ua.es/dspace/bitstream/10045/1109/7/Informe_ZigBee.pdf

[5] IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks. 802.15.4 TM.

http://www.zigbee.org

[6] Carlos Alberto Ortega Huembes, Deyanira del Socorro Roque, Leslie Eduardo Úbeda Sequeira; Universidad Nacional de Ingeniería Facultad de Electrotecnia y Computación ZigBee: El nuevo estándar global para la Domótica e Inmótica ZigBee.

http://www.monografias.com/trabajos-pdf/zigbee/zigbee.pdf

[7] ZigBee Specification Document 053474r17, January 17, 2008, Sponsored by: ZigBee Alliance

http://people.ece.cornell.edu/land/courses/ece4760/FinalProjects/s2011/kjb79_ajm232/pmeter/ZigBee%20Specification.pdf

[8] Shahin Farahani; ZigBee Wireless Networks and Transceivers, Copyright © 2008, Elsevier Ltd. All rights reserved.

[9] Robert Cragie Chair, ZigBee Alliance ZARC Security Task Group Principal Engineer, Jennic Ltd, ZigBee Security.

http://docs.zigbee.org/zigbee-docs/dcn/09-5231.PDF

[10] Sergio Lillo Moreno, Tesis: Desarrollo de un entorno para la configuración y monitorización de redes ZigBee/802.15.4; Málaga 2010.

http://webpersonal.uma.es/~ECASILARI/Docencia/Memorias_Presentaciones_PFC/54_MemoriaSergioLilloMoreno.pdf

[11] Jorge Pablo Dignani; Análisis del protocolo ZigBee, Facultad de Informática Universidad Nacional de La Plata 2011.

http://sedici.unlp.edu.ar/bitstream/handle/10915/18349/Documento_completo__.pdf?sequence=1

[12] FIPS Pub 197, Advanced Encryption Standard (AES) , Federal Information Processing Standards Publication 197, US Department of Commerce/NIST, Springfield, VA, 2001.

http://csrc.nist.gov

[13] ZigBee Alliance

http://www.zigbee.org/About/FAQ.aspx

[14] Software Tecnologies Group: Services for product developers

http://www.stg.com/wireless/ZigBee_comp.html

[15] Lorena Isabel Baraona López, TESIS Escuela Politécnica Nacional: Diseño de un sistema de vigilancia basado en tecnología IP para la protección de los condominios La Merced de la ciudad de Ambato año 2010.

[16] Sensores con tecnología CCD vs CMOS

http://www.xatakafoto.com/camaras/sensores-con-tecnologia-ccd-vs-cmos

[17] SECUEN; Sensores Inflarojos Pasivos para Iluminacion.

http://www.secuen.com/lineassensorestecnicopro.asp

[18] Sensor de movimiento PIR

http://chuperfantasticarduinos.wordpress.com/2009/09/16/sensor-de-movimiento-pir/

[19] Internet fijo CNT

www.andinadatos.com.ec

[20] Internet Netlife

http://www.netlife.ec/

[21] Internet Movistar

http://www.movistar.com.ec/site/internet-personas/

[22] Internet fijo Claro

http://www.claro.com.ec/wps/portal/ec/pc/personas/internet/

[23] Internet Home

Referencia:

http://www.punto.net.ec/home/index.php?option=com_content&view=frontpage&Itemid=1

[24] Servidor Apache – Tomcat

http://www.apache.org/

[25] OpenSSL Project

http://www.openssl.org

[26] Web Seguro

http://www.iec.csic.es/criptonomicon/ssl.html

[27] Crear Certificados Digitales SSL para apache

http://www.linuxtotal.com.mx/index.php?cont=info_seyre_001

[28] OpenSSL Command-Line HOWTO

http://www.madboa.com/geek/openssl/

[29] Manejo de certificados con keytool para la activación de SSL

http://www.adictosaltrabajo.com/tutoriales/tutoriales.php?pagina=securitySSLKeytool

[30] Instalar y Configurar Samba en Centos

http://inforysol.blogspot.com/2008/12/instalar-y-configurar-servidor-samba.html

[31] MySQL 5.0 Reference Manual

http://dev.mysql.com/doc/refman/5.0/es/index.html

[32] MySQL Documentation: MySQL Reference Manuals

http://dev.mysql.com/doc/

[33] Información NetBeans

http://netbeans.org/community/releases/61/index_es.html

[34] JACOBSON I., BOOCHG., RUMBAUGH J.; Proces Unificado de Desarrollo de Software

[35] José M. Drake; Proceso de desarrollo de aplicaciones software

http://www.ctr.unican.es/asignaturas/MC_OO/Doc/OO_08_I2_Proceso.pdf

[36] Guerrón Tacoamán, Karina Alexandra; Proaño Salazar, Jadira Alexandra; TESIS: Escuela Politécnica Nacional: Implementación de un prototipo de

prueba para la automatización del manejo de la información del estado clínico de pacientes y la medición de signos vitales a través de sensores, para la Clínica "Durán" de la ciudad de Ambato; año

http://bibdigital.epn.edu.ec/bitstream/15000/5104/1/T10390.pdf

[37] ALLSOFT S.A de C.V Monterrey N.L

http://www.slideshare.net/inventa2/modelos-de-desarrollo

[38] Carlos Alberto Fernández; El Proceso Unificado Rational para el Desarrollo de Software año 2000

http://nuyoo.utm.mx/~caff/doc/El%20Proceso%20Unificado%20Rational.pdf

[39] Luis A. Guerrero; Rational Unified Process

http://www.slideshare.net/juliopari/proceso-unificado-de-rational

[40] Introducción a Itil v3

http://itilv3.osiatis.es/

[41] ITIL® & IT Service Management (ITSM) Software

http://www.processworx.com/

[42] ManageEngine ServiceDesk Plus

http://www.manageengine.com/products/service-desk/spanish/index.html

ANEXOS

ANEXO A: DATASHEET CÁMARA IP D’Link DCS 2121

ANEXO B: DATASHEET SENSOR PIR 555 - 28027

ANEXO C: DATASHEET SENSOR DE GAS MQ5

ANEXO D: DATASHEET MÓDULOS ZIGBEE

ANEXO E: DATASHEET PIC 16F87XA

ANEXO F: ESQUEMA DE LA BASE DE DATOS

ANEXO G: PROGRAMACIÓN PIC 16F87XA

ANEXO H: PROGRAMACIÓN MÓDULOS XBEE

ANEXO I: COSTOS DE MATERIALES DE CONEXIÓN

ANEXO J: DIAGRAMAS DE IMPRESIÓN DE PLACAS

ANEXO K: PANTALLAS DE INGRESO DEL APLICATIVO WEB

ANEXO L: PANTALLAS CONFIGURACIÓN CÁMARAS Y SERVIDOR TOMCAT