PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESCUELA DE POSGRADO

DOMOLAB: SISTEMA DE MONITOREO Y CONTROL REMOTO DE VIVIENDAS

Tesis para optar el grado de Magíster en Ingeniería de Telecomunicaciones que presenta

JUAN CARLOS CULQUICHICÓN VALENTÍN

Dirigido por

CARLOS SILVA CARDENAS

San Miguel, 2015

Resumen

Actualmente, la inseguridad ciudadana se ha convertido en uno de los problemas que más afecta y preocupa a los ciudadanos de Lima y Callao. Por ello, este proyecto de tesis plantea la implementación de un sistema de seguridad, basado en tecnologías de la información y comunicaciones, para el monitoreo y control remoto de las viviendas en Lima Metropolitana. Este sistema se caracterizará por su capacidad de respuesta en tiempo real y por intercambiar mensajes a través de Internet. La tesis ha sido desarrollada en seis capítulos. En primer lugar, en el Capítulo 1, se presentará información estadística que permite describir la problemática de inseguridad ciudadana que se vive en Lima Metropolitana. Además, se plantearán la hipótesis y los objetivos generales del proyecto. En segundo lugar, en el Capítulo 2, se desarrollarán los conceptos teóricos relacionados al proyecto y se presentará información sobre el estado del arte y la industria. Además, se incluirá una sección en donde se explican los criterios utilizados para seleccionar la tecnología con la que se desarrollará la solución. En tercer lugar, en el Capítulo 3, se explicarán los criterios de diseño y se presentarán los aspectos relacionados con la implementación del proyecto. En cuarto lugar, en el Capítulo 4, se describirá el escenario de pruebas que fue ejecutado para verificar el funcionamiento del sistema implementado. Además, se realizó un análisis de riesgo informático para detectar vulnerabilidades del sistema y plantear algunos controles correctivos. En quinto lugar, en el Capítulo 5, se presenta un plan de negocios que permite demostrar la factibilidad comercial de la solución. Finalmente, en el último capítulo, se presentarán las conclusiones respectivas que permiten demostrar la hipótesis planteada.

ÍNDICE

CAPÍTULO I

INTRODUCCIÓN

El propósito del presente capítulo es proporcionar al lector información estadística sobre el contexto actual de la seguridad ciudadana en el país y la preocupación que esto representa en la vida de las personas. Además, se expondrá el problema que se desprende de este contexto, se enunciará la hipótesis y se plantearán los objetivos generales del presente proyecto de tesis.

1. Presentación del problema

En la actualidad, el clima de inseguridad ciudadana se ha convertido en uno de los problemas que más afecta a los ciudadanos de Lima y Callao en su vida cotidiana. De acuerdo con el documento "*Seguridad Ciudadana - Informe Anual 2013 – Crisis Política, temores y acciones de esperanza*" [1], el 62.5% de los entrevistados manifiesta que la delincuencia es el problema más importante para el Perú hoy en día. En la Tabla 1, se muestran todas las respuestas de los encuestados en el ámbito de Lima y Callao.

De acuerdo con la lista, ¿Cuál es el problema que más afecta al Perú hoy en día?

Problema	Total
Delincuencia	62.50%
Educación	31.90%
Pobreza	25.40%
Salud	24.10%
Economía	16.30%
Terrorismo	6.10%
Medio Ambiente	6.00%
Migración	0.90%

Tabla 1 - Percepción sobre la problemática que más afecta al país [1]

Por otra parte, según el "*Informe Técnico – Estadísticas de Seguridad Ciudadana – Marzo 2015*" [2], el 87.1% de las personas encuestadas[1] percibe que en los próximos doce meses podría ser víctima de algún hecho delictivo. Además, se consultó a este grupo de personas sobre su percepción de inseguridad respecto a un tipo delito específico. Las respuestas se muestran en el siguiente gráfico (Figura 1).

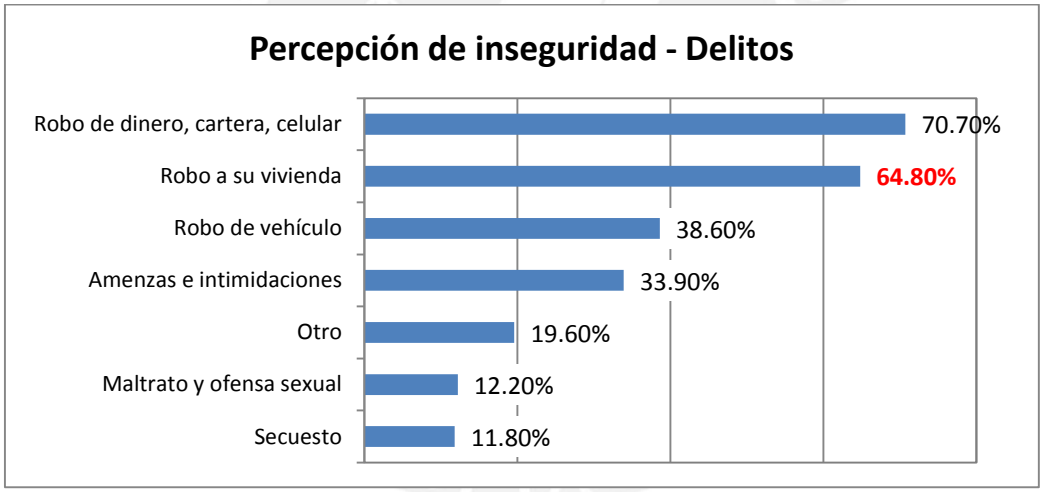


Figura 1 - Percepción de inseguridad por tipo de delito [2]

De la figura anterior, se concluye que el robo a las viviendas es percibido por los encuestados como el segundo delito con mayor probabilidad de ocurrencia en los próximos doce meses.

Por otra parte, en el mismo estudio [2], se menciona que el 12.3% de los encuestados fueron víctimas de robo o de intento de robo. Además, el 61% de las personas manifestaron que su zona de residencia cuenta con vigilancia por parte de la Policía Nacional del Perú, Serenazgo o patrullaje integrado. Sin embargo, si se compara la tasa de robos o intentos de robo entre lugares

[1] Personas de 15 años o más que viven en ciudades con más de veinte mil habitantes (Provincia de Lima – 43 distritos, Arequipa, Trujillo, Ayacucho, Cajamarca, Chiclayo, Chimbote, Cusco, Huancayo, Huánuco, Ica, entre otras).

con vigilancia y lugares sin vigilancia (Figura 2) se observa que la cantidad de actos delictivos es similar en ambos casos.

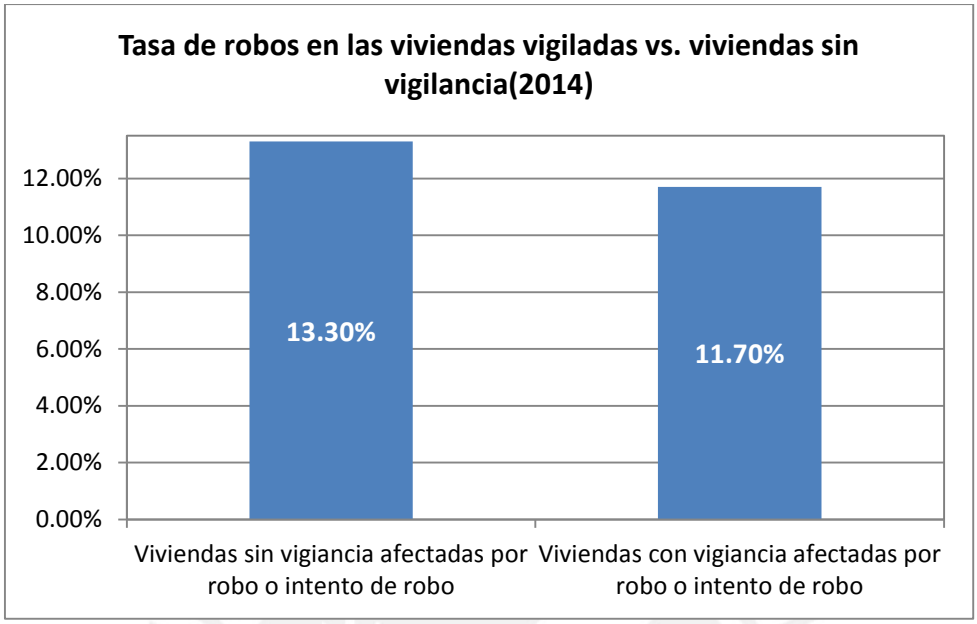
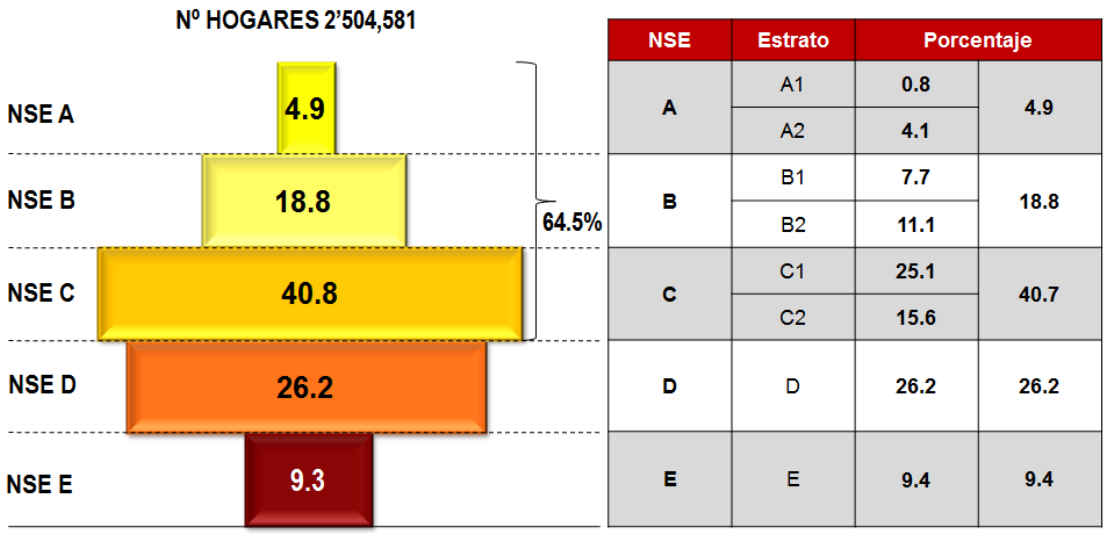


Figura 2–Tasa de robos en las viviendas vigiladas vs. Viviendas sin vigilancia [2]

De lo expuesto anteriormente, se concluye que los métodos de vigilancia brindados por la Policía Nacional o el Serenazgo no son del todo efectivos. Además, existe la necesidad de implementar mecanismos complementarios que refuercen la seguridad y permitan disminuir la cantidad de robos o intentos de robo en la vivienda.

Con el fin de complementar el análisis de la problemática de inseguridad ciudadana, se presentará información sobre la situación socioeconómica de las personas que habitan Lima Metropolitana. Para esto se tomará como referencia un estudio realizado por la *Asociación Peruana de Empresas de Investigación de Mercado* [3].

De acuerdo con el reporte del 2014 [3], existen aproximadamente dos millones y medio de hogares en Lima Metropolitana, de los cuáles, el 64.5% de ellos están distribuidos entre los sectores A, B y C. A continuación, se muestra un gráfico con la proporción de hogares por nivel socioeconómico (NSE).



NSE	Estrato	Porcentaje	
A	A1	0.8	4.9
	A2	4.1	
B	B1	7.7	18.8
	B2	11.1	
C	C1	25.1	40.7
	C2	15.6	
D	D	26.2	26.2
E	E	9.4	9.4

Figura 3 - Niveles Socioeconómicos - Lima Metropolitana 2014 [3]

En la Figura 3, se observa que más de la mitad de hogares de Lima Metropolitana pertenecen a los sectores socioeconómicos de mayor poder adquisitivo. Con el fin de entender mejor esta realidad, se presentará un cuadro estadístico donde se detallan los bienes materiales que poseen las personas que pertenecen a los diferentes sectores socioeconómicos de Lima.

Elementos del Hogar	NSE A	NSE B	NSE C1	NSE C2	NSE D	NSE E
TV	99.40%	99.20%	98.60%	97.70%	92.60%	83.10%
Refrigeradora	99.40%	98.50%	95.00%	87.80%	61.40%	31.60%
Celular	98.50%	94.90%	89.30%	89.90%	84.30%	82.10%
Plancha	98.30%	97.00%	95.10%	86.80%	73.40%	52.40%
Lavadora	97.50%	88.80%	71.60%	41.60%	18.20%	6.20%
Computadora	97.20%	87.20%	68.20%	46.00%	18.80%	6.40%
Licuadora	96.80%	96.80%	94.50%	89.30%	74.20%	53.00%
Horno Microondas	96.60%	84.20%	60.20%	30.50%	12.50%	3.40%
Teléfono Fijo	93.60%	85.60%	69.90%	48.00%	30.80%	9.70%
Cocina	90.40%	97.90%	97.90%	96.70%	92.40%	84.80%
DVD	87.70%	79.90%	78.10%	74.60%	61.40%	53.40%
Equipo de Sonido	81.20%	73.60%	62.10%	52.20%	38.40%	29.50%

Tabla 2 - Distribución de los elementos del hogar por sector socioeconómico [3]

En la Tabla 2, se observa que los sectores A y B son los que poseen mayor cantidad de bienes materiales y/o activos. Es por ello, que las personas que pertenecen a estos niveles socioeconómicos tienen la necesidad de resguardar o proteger dichos objetos.

Por otra parte, el estudio [3] muestra que el 90% de las personas del sector A accedieron a Internet durante el último mes. Así mismo, el 77% usaron este servicio en el sector B y el 61%, en el

sector C1. En el siguiente gráfico (Figura 4), se muestra la distribución del uso de Internet por nivel socioeconómico.

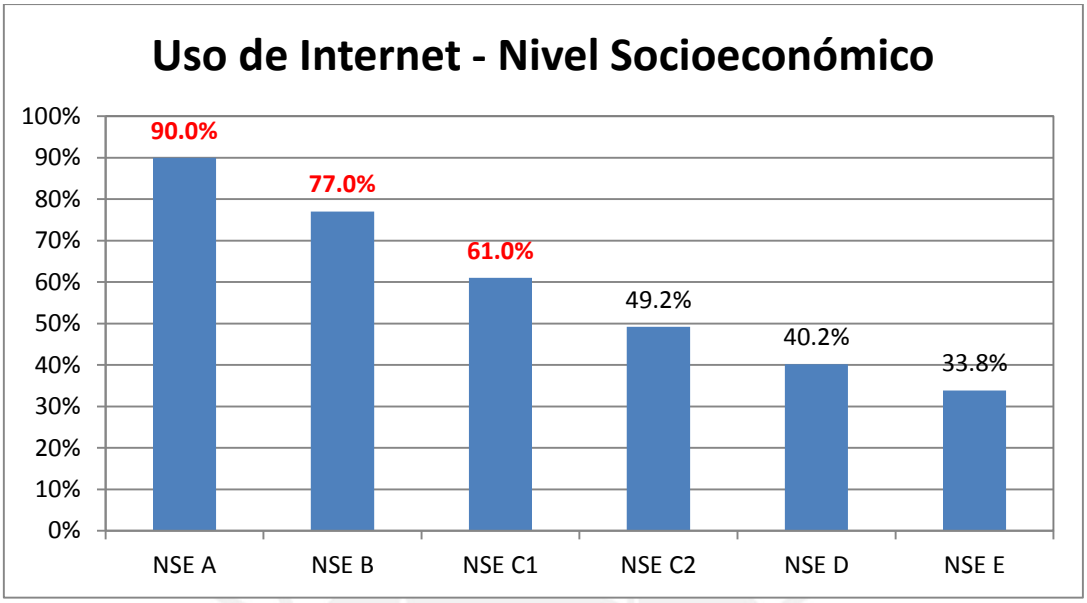


Figura 4 - Distribución del uso de Internet por nivel socioeconómico [3]

Además, en la siguiente tabla (Tabla 3), se tiene información respecto al lugar desde donde se accede a Internet, según el nivel socioeconómico.

Acceso a Internet	NSE A	NSE B	NSE C1	NSE C2	NSE D	NSE E
Hogar	63.1%	66.0%	56.3%	42.4%	22.1%	6.9%
Trabajo	22.9%	17.2%	12.3%	7.1%	6.1%	4.3%
Establecimiento Educativo	0.2%	0.9%	2.1%	2.5%	4.6%	2.8%
Cabina Pública	1.8%	4.3%	17.6%	34.6%	54.0%	73.5%
Otro	12.0%	11.5%	11.6%	13.3%	13.2%	12.6%

Tabla 3 - Lugar de acceso a Internet [3]

De lo presentado anteriormente, se observa que más de la mitad de las personas que pertenecen a los sectores A, B y C1 acceden a Internet desde su hogar. Cabe mencionar que en el caso de los sectores D y E, las cabinas públicas son las que predominan.

El presente proyecto de tesis busca desarrollar una solución que pueda complementar los mecanismos de vigilancia o protección tradicionales[2], y a la vez, permita combatir el problema de la inseguridad ciudadana de Lima metropolitana, específicamente el robo en los domicilios. Cabe mencionar que este proyecto estará basado en tecnologías de la información, por lo que contar con acceso a Internet desde el hogar es indispensable. Teniendo en cuenta esto, se puede inferir que el proyecto está orientado a los sectores A, B y C1, ya que poseen los recursos

[2] Vigilancia de la Policía Nacional del Perú, Serenazgo del distrito y patrullas vecinales.

tecnológicos necesarios y además, existe la necesidad de proteger los bienes materiales o activos de su domicilio.

2. Hipótesis

Después de analizar la problemática, se plantea la siguiente hipótesis:

Se implementará un sistema de seguridad, comercialmente viable, basado en tecnologías de la información y comunicaciones (redes celulares, redes de comunicación inalámbrica e Internet). Este sistema permitirá el monitoreo y control remoto de las viviendas de Lima Metropolitana, a través de un Smartphone o Tablet. Además, se caracterizará por su respuesta en tiempo real, vía el intercambio de mensajes, para la toma de acciones oportunas ante situaciones de emergencia.

3. Objetivos

Para desarrollar el presente proyecto de investigación se ha considerado establecer los siguientes objetivos generales:

- Diseñar e implementar un sistema que permita la interacción entre dispositivos electrónicos instalados en una vivienda para monitorear y controlar diferentes parámetros de ésta.
- Desarrollar un protocolo de comunicación que permita la interacción de los diferentes elementos de la vivienda a través de redes Wi-Fi y móviles.
- Desarrollar un plan de negocios que demuestre la viabilidad comercial del proyecto en la ciudad de Lima (Sectores A, B y C1).

Finalmente, se concluye que existe la necesidad de mejorar la seguridad de las viviendas de Lima metropolitana. Por ello, el proyecto propuesto hará uso de la tecnología disponible para crear una solución que permita satisfacer las necesidades de protección y confiabilidad de los usuarios potenciales. Cabe resaltar, que el acceso a Internet es un requisito indispensable para el uso de esta solución, por lo que, el público al que va dirigido pertenece a los sectores socioeconómicos A, B y C1.

CAPÍTULO II

ASPECTOS TEORICOS

El objetivo del presente capítulo es describir los fundamentos teóricos necesarios para el desarrollo del proyecto de tesis. Además, se mostrará información sobre el estado del arte y se explicará la selección de las tecnologías que conforman el diseño de la solución.

1. Fundamentos teóricos

Hogar Digital

De acuerdo el estudio *Vivienda Conectada – Las TIC en el hogar*, el concepto de Hogar Digital se define como la infraestructura en donde concurren servicios de entretenimiento, comunicación y gestión de los diferentes elementos (artefactos, puertas, luminarias, etc.) que la componen. Esto se realiza a través de la instalación de un conjunto de componentes de hardware y software. El objetivo es mejorar la calidad de vida de los residentes de la vivienda [4].

Domótica

Según la *Asociación Española de Domótica e Inmótica*, el término hace referencia al conjunto de soluciones basadas en tecnología que permiten optimizar algunos aspectos de la vivienda (confort, seguridad, ahorro de consumo de energía, comunicaciones, entretenimiento, etc.). En otras palabras, estas soluciones permitirán automatizar y controlar los diferentes elementos que componen la vivienda a través de la instalación de equipos tecnológicos en ella. Estos dispositivos serán capaces de comunicarse entre sí y operarán bajo un programa (algoritmo) configurado previamente por el usuario [5].

El uso de este tipo de soluciones conlleva los siguientes beneficios:

- Mejorar la calidad de vida de las personas que habitan la vivienda.
- Reducción del trabajo doméstico.
- Aumentar el bienestar y la seguridad.
- Racionalización de los consumos de energía, agua potable, etc.

Elementos del sistema:

Un sistema domótico está compuesto por los elementos mostrados en la Figura 5, mostrada a continuación:

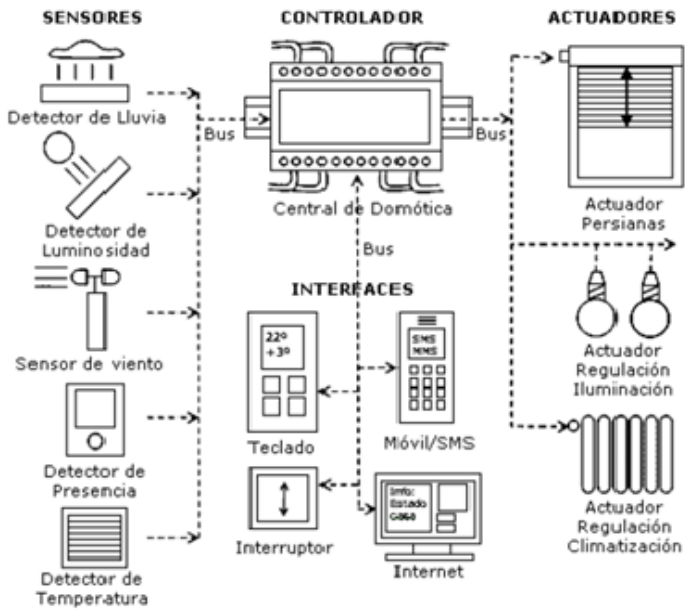


Figura 5 - Elementos de un sistema domótico [4]

Sensores

Son los elementos que se encargan de detectar y registrar los cambios en el entorno de la vivienda [4]. Por ejemplo, las variaciones de temperatura, la apertura de una puerta o ventana, si se produce alguna fuga de gas, entre otros.

Controlador

Es la entidad responsable de controlar y gestionar el sistema. Se encarga de procesar la información adquirida por los sensores, tomar decisiones y enviar instrucciones específicas a los actuadores. Toda la inteligencia del sistema se encuentra implementada en este elemento [4].

Actuadores

Responsables de ejecutar las instrucciones enviadas por la unidad de control. Por ejemplo, encender las luminarias, abrir una puerta, encender la calefacción, entre otros [4].

Interfaces

Componentes encargados de interactuar con el usuario final. Recibirán las instrucciones del usuario y las enviarán a la unidad de control para su ejecución. Un ejemplo de estos dispositivos son los teclados, pantallas táctiles, aplicaciones móviles, página web, etc. [4].

Arquitecturas

Los sistemas domóticos se clasifican según su arquitectura en centralizados, descentralizados y distribuidos [6]. A continuación, se desarrollará cada uno de estos conceptos.

Centralizado

El sistema está equipado con un elemento central único que se encarga del control y administración de todos los elementos que componen la red. La inteligencia del sistema radica en dicha unidad [5].En la Figura 6, mostrada a continuación, se puede observar un ejemplo de esta arquitectura.

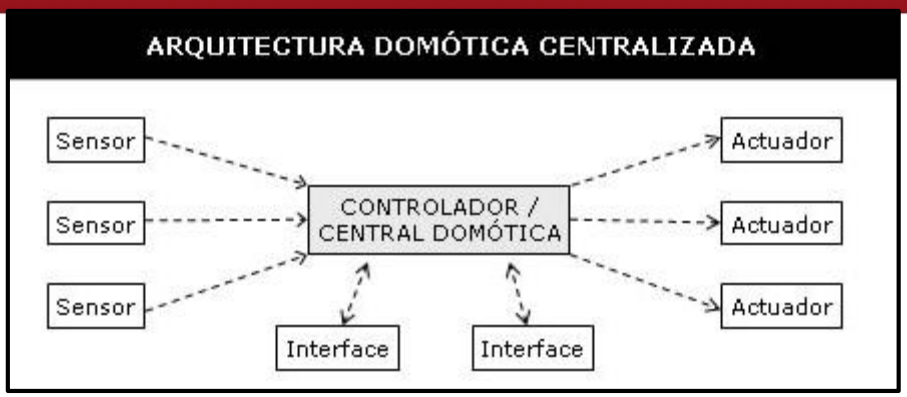


Figura 6 -Arquitectura Centralizada [6]

Descentralizado

A diferencia de la centralizada, en esta arquitectura no se depende de una sola unidad central. Existen múltiples unidades que se encargarán de las tareas de administración y control. En la Figura 7, se presenta un ejemplo de este tipo de arquitectura.

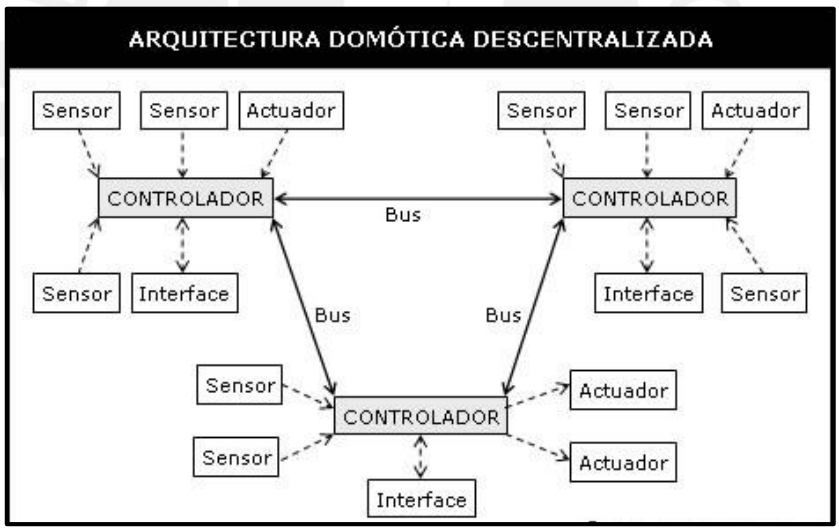


Figura 7 - Arquitectura Descentralizada [6]

Distribuida

Esta arquitectura se caracteriza porque la inteligencia del sistema se encuentra distribuida por todos los elementos que lo componen [5]. En la Figura 8, se muestra un diagrama de esta arquitectura en donde se observa que cada elemento está conectado directamente a la red puesto que tiene su propio controlador incluido.

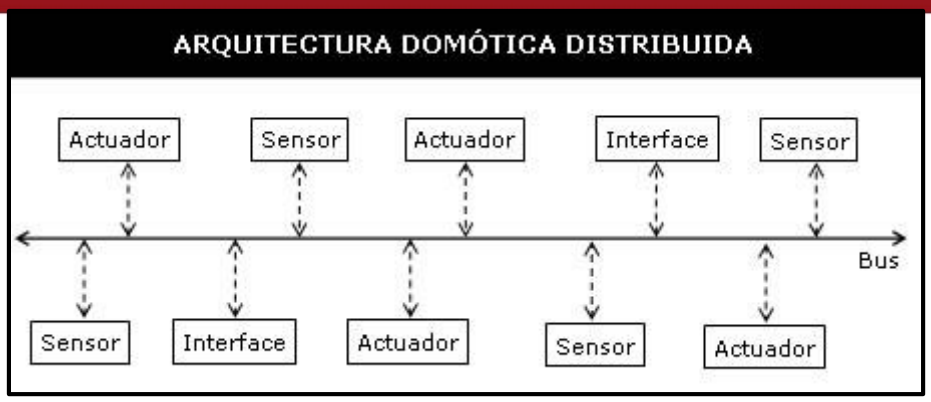


Figura 8 - Arquitectura Distribuida [6]

Internet of Things, IoT

Este concepto hace referencia a la idea de tener "objetos", dispositivos electrónicos dotados de inteligencia, conectados a Internet recopilando datos del mundo real. Esta información será analizada, servirá para la toma de decisiones y el control remoto de otros objetos [7]. De esta manera, se crearán nuevas formas de interacción entre las personas, los objetos, Internet y el mundo real.

Existen diversos tipos de aplicaciones comerciales que están basadas en este concepto. Por ejemplo, el monitoreo del transporte de carga pesada. Gracias a IoT, se puede recopilar información en tiempo real sobre la geolocalización de los camiones de la flota, los niveles de combustible, la presión de las llantas, etc. Luego de ello, estos datos serán analizados y se podrán determinar la ruta más óptima para un determinado recorrido, diagnosticar fallas en el motor o en los sistemas de freno de forma anticipada, optimizar el consumo de la gasolina, etc. En la Figura 9, se ilustra el ejemplo enunciado anteriormente.

Figura 9 - Monitoreo de unidades de transporte de carga pesada [8]

Como se observa en la figura anterior, la información se recopila a través de los sensores ("objetos") instalados en los camiones. Luego, se transmite a través de Internet y se almacena en

los data centers de la empresa. Finalmente, esta información se analiza y las estadísticas e indicadores son mostrados a través de una página web.

El concepto de IoT contempla el desarrollo de aplicaciones para los campos de la domótica, salud, telemedicina, agricultura, construcción, energía, entre otros.

Clasificación de las redes

Según el área de cobertura, las redes de datos reclasifican de la siguiente forma:

PAN (Personal area network)

Es una red de datos que tiene un rango de cobertura de aproximadamente 10 metros. Un ejemplo de este tipo de red es el *Bluetooth* que permite conectar Smartphones, Tablets, computadoras, sistemas de audio, etc., para intercambiar información o compartir archivos multimedia [9].

LAN (Local area network)

Es una red de datos que cubre un área geográfica reducida. En general, este tipo de redes operan en espacios como el de una vivienda, oficina o un edificio. Se caracterizan por tener altas velocidades de transmisión de datos debido al área de operación [9]. Un ejemplo son las redes del hogar o la oficina conectadas a través de un cable RJ-45.

WLAN (Wireless local area network)

Es una red LAN inalámbrica que no necesita de un cable o medio físico para establecer la conexión entre los dispositivos que se conectan a ella. Se basa en técnicas de modulación de radio frecuencia. Un ejemplo es el Wi-Fi, tecnología que se encuentra en el estándar IEEE 802.11 y se caracteriza por operar en bandas de frecuencia libres (no licenciadas), con velocidades de transmisión de hasta 300 Mbits/s[3] y un radio de cobertura de hasta 100 metros [9].

MAN (Metropolitan area network)

Son redes que cubren espacios geográficos más amplios que las redes LAN [9].

WAN (Wide area network)

Es una red de datos que cubre un área geográfica amplia y se enlazan entre sí para interconectar a usuarios que se encuentran en diferentes ubicaciones [9].

[3] IEEE 802.11n

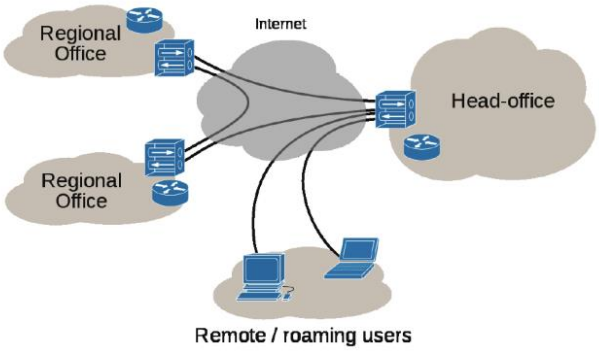
En la Figura 10, se muestra la clasificación de las redes según el área geográfica de cobertura.

Figura 10- Tipos de red, según su cobertura geográfica [10]

VPN – Red Privada Virtual

Es la tecnología que permite el acceso a redes LAN privadas desde cualquier tipo de red pública mediante una conexión virtual denominada túnel. Generalmente, está conexión se realiza a través de Internet donde toda la información intercambiada en el canal es encriptada para garantizar la seguridad y la confiabilidad de la misma. Además, para poder establecer el túnel VPN entre ambas redes, es necesario que los usuarios se autentiquen [11].

Un ejemplo práctico del uso de esta tecnología es el concepto de "*Home Office*", ya que algunos empleados tienen la posibilidad de trabajar desde su hogar y para conectarse a la red del trabajo utilizan una conexión VPN. De esta forma, los trabajadores podrán acceder a los recursos, servicios y sistemas de la empresa desde cualquier lugar y sin comprometer la seguridad de la red corporativa. En la Figura 11, mostrada a continuación, se ilustra el ejemplo previamente enunciado



.

Figura 11 - Conexión a la red corporativa a través de VPN [11]

Como se observa en la figura anterior, los usuarios "Remote / Roaming" se pueden conectar a la red de la empresa gracias a la tecnología VPN. No es necesario que se encuentren en la misma ubicación geográfica que la oficina principal "Head Office", solo necesitan conexión a Internet y estar autenticados en el sistema.

Comunicación Cliente - Servidor

Es un tipo de arquitectura de red que está compuesto por dos entidades [12]:

Servidores

Son computadoras de alta capacidad de procesamiento y almacenamiento, encargados de la gestión de recursos o servicios de red (almacenamiento, impresoras, tráfico de red, datos, aplicaciones).

Clientes

Son las computadoras que hacen uso de los recursos que ofrecen los servidores.

Se caracterizan porque la comunicación se establece a través de un esquema de solicitud (cliente) y respuesta (servidor). Un ejemplo práctico de este tipo de comunicación es un servicio de biblioteca multimedia compuesto por varios servidores. Este sistema debe ser capaz de manejar gran variedad de peticiones, ya que los clientes (usuarios del servicio) pueden solicitar información sobre las películas o fotos a través una página web (Servidor web). Además, los usuarios pueden acceder a la transmisión de video (Servidor de video) o a un álbum de fotografías digitalizadas (Servidor de fotos). [13]

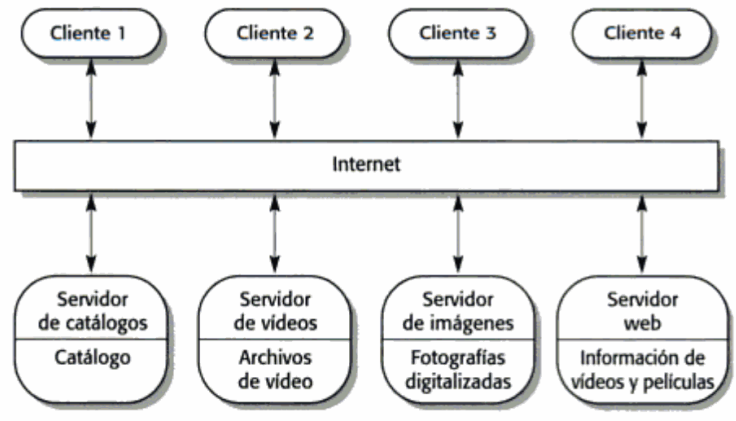


Figura 12 - Arquitectura de un sistema de biblioteca multimedia [13]

En la Figura 12, se observa que el sistema de biblioteca multimedia está compuesto por diferentes servidores que se encargan de manejar un servicio específico. Cabe resaltar que las peticiones

realizadas por los clientes son distribuidas entre cada uno de los servidores según corresponda para ser atendidas.

Cloud Computing

Es un esquema de comercialización de recursos de cómputo configurables (almacenamiento, servidores, aplicaciones y servicios) a los que se pueden acceder de forma remota a través de una red de comunicaciones. Cabe resaltar, que estos recursos estarán disponibles según las necesidades y la demanda de los clientes [14].

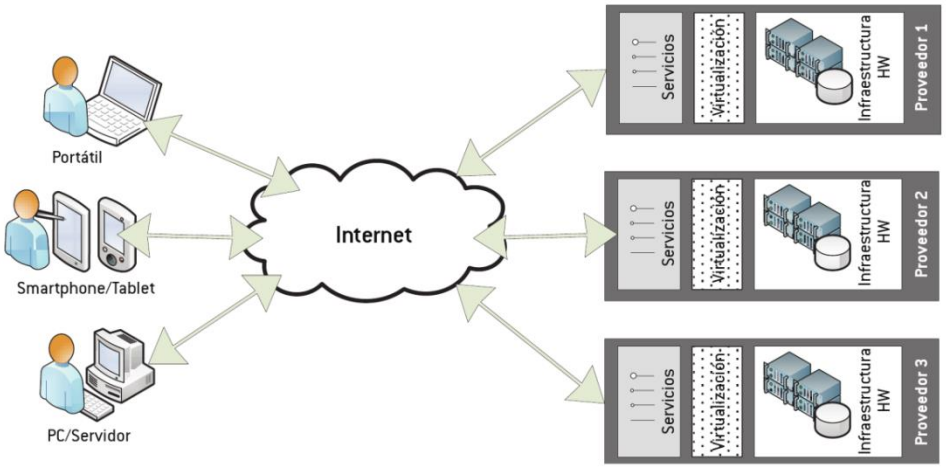


Figura 13 - Concepto de Cloud Computing [14]

En la Figura 13, se ilustra el concepto de Cloud Computing. Se observa que los proveedores ofrecen, a través de Internet, servicios de cómputo configurables tanto en software (virtualización) como en hardware (infraestructura). Además, se puede emplear cualquier dispositivo (PC, Servidor, Smartphone, Tablet, Laptop, etc.) para consumir estos servicios.

Los esquemas de comercialización del Cloud Computing se clasifican en tres tipos, según la naturaleza del servicio:

Infrastructure as a Service (IaaS)

Hace referencia a la modalidad de ofrecer infraestructura de computación (usualmente máquinas virtuales) como un servicio. El proveedor alquila la infraestructura a los clientes y se paga solo por los recursos consumidos (tiempo de uso del procesador, tráfico de red, etc.). Cabe mencionar que los clientes finales se encargan de administrar y configurar los servicios instalados en la infraestructura alquilada [15].

Platform as a Service (PaaS)

Es el concepto de ofrecer tanto el software como el hardware bajo el esquema de servicio al cliente final. Esto significa que el cliente solo debe preocuparse por la funcionalidad de la aplicación que desea instalar. La administración o modificación de la configuración del hardware o software alquilados será responsabilidad total del proveedor de servicio [15].

Software as a Service (SaaS)

Es un esquema de servicio bajo la que se ofrece una solución de software (aplicación) a la que el usuario podrá acceder desde cualquier computador a través de un cliente (en la mayoría de casos un navegador web). Cabe resaltar que esta aplicación se encuentra instalada en el *Cloud* y el usuario final no necesitará instalar software adicional para acceder al servicio [15].

2. Estado del arte

Protocolos

A continuación, se describirán los protocolos más importantes usados por los sistemas domóticos que se comercializan actualmente:

X10

Es un estándar de comunicación para dispositivos electrónicos aplicado en la domótica. Usa como medio de comunicación el cableado eléctrico para enviar y recibir las señales de control. Esta tecnología está limitada por su baja tasa para transmisión de datos, confiabilidad y escalabilidad [16].

KNX

Es un estándar propietario (ISO/IEC 14543) usado en la automatización de hogares y edificios, el cuál es gestionado por la Asociación KNX. Es compatible con diferentes medios de transmisión como el cable de par trenzado, red eléctrica, radio frecuencia, infrarrojo y Ethernet [16].

Lonworks

Este protocolo propietario[4] fue creado por la compañía *Echelon Corporation* y es compatible con diferentes medios como el cable de par trenzado, fibra óptica, radio frecuencia y la red eléctrica. Es usado para aplicaciones de control de luminarias, temperatura y edificios inteligentes. Existen algunas limitantes respecto a la flexibilidad y escalabilidad del protocolo [16].

ZigBee

Es un estándar (IEEE 802.15.4) de comunicación inalámbrica que se caracteriza por el bajo consumo de energía, bajo costo y bajas velocidades de transmisión, el cuál es gestionado por el *Zigbee Alliance.* Emplea la radio frecuencia como medio de comunicación entre los elementos de red, específicamente la banda de 2.4 GHz. Además, es comúnmente usado en aplicaciones de administración de energía, automatización del hogar, control de luminarias. Las principales ventajas son la topología de red, que permite la comunicación entre miles de componentes, y el bajo consumo de energía [10].

Z-Wave

Es un protocolo de comunicación inalámbrica que se caracteriza por su baja capacidad de transmisión de datos y bajo costo. Tiene por objetivo transmitir pequeñas cantidades de información con baja latencia. Sin embargo, tiene menor desempeño si es comparado con ZigBee (velocidad de intercambio de datos, robustez) [17].

Wi-Fi

Estándar (IEEE 802.11) de comunicación inalámbrica basado en IP[5] que emplea la radio frecuencia (2.4 GHz y/o 5 GHz) para el envío y recepción de datos. Gracias a la masificación de Smartphones, Tablets y laptops es posible encontrar una conexión Wi-Fi en cualquier lugar (hogares, trabajo, universidad, aeropuertos, restaurantes, etc.). En la actualidad, esta tecnología se está integrando con elementos comunes de una vivienda, por ejemplo los televisores (*Smart TV*) y algunos electrodomésticos. Esto supone que el Wi-Fi es el estándar ideal para la automatización de los hogares [10].

El protocolo IP se caracteriza por su implementación extensa y compleja. En el caso de los Smartphones y laptops, esto no significa un problema, ya que están equipados con potentes procesadores, memoria y batería. Hasta hace poco, era complicado crear

[4] Estándar cerrado desde la Capa 3 a la Capa 7 del modelo OSI.
[5] IP: Internet Protocol

dispositivos para la automatización del hogar basados en Wi-Fi por las limitaciones de procesamiento, memoria y batería. Sin embargo, gracias al avance de la tecnología, se han desarrollado módulos con Wi-Fi incorporado que superan las limitaciones mencionadas anteriormente [10]. El uso de esta tecnología en la automatización del hogar podría ayudar a mitigar las barreras de entrada, ya que se puede aprovechar la masificación del Wi-Fi y la infraestructura instalada que existe en la mayoría de hogares.

6LoWPAN (IPv6 over Low power personal area networks)

Es un estándar creado bajo el grupo de trabajo de la IETF[6] y formalizado en el RFC 6282. Tiene como objetivo crear dispositivos basados en IP que se caractericen por el bajo consumo de energía y capacidades limitadas para el procesamiento de información. Es el primer estándar creado específicamente para IoT, sin embargo, aún no existe alguna organización responsable de la gestión del protocolo, de los procesos de certificación y control [10].

En la siguiente tabla (Tabla 4), se muestra un cuadro comparativo de los protocolos inalámbricos usados en domótica.

	ZIgBee	Z-Wave	WI-FI	6LoWPAN
Network Type	Wireless mesh	Wireless mesh	Wireless	Wireless mesh
Frequency Band	868MHz, 915MHz, 2.4GHz	900MHz ISM	2.4GHz	900MHz, 2.4GHz
Peak Data Rate	20-900 Kbps	9.6-40 Kbps	54 Mbps(802.11g)	20-250 Kbps
Cost	Low cost	Low cost	Higher cost	Low cost
Power Consumption	Low power	Low power	Higher power	Very low power
Standard	Open	Proprietary	Open	Open

Tabla 4-Cuadro comparativo, protocolos inalámbricos de domótica [18]

[6] IETF: Internet Engineering Task Force

3. Industria

En la industria tecnológica se tienen las siguientes iniciativas en el campo de la domótica:

Google

Esta empresa ha creado la plataforma domótica denominada *@Home Framework*- 2011, integrada de forma nativa con sus servicios más populares (Correo electrónico, calendario, tienda de aplicaciones, etc.). La compañía busca aprovechar el ecosistema de dispositivos móviles (*Smartphones* y *Tablets*) basados en el sistema operativo *Android* de gran popularidad en el mercado. El objetivo es promover el uso de *Android* como una plataforma estándar de domótica. Por el momento, no existen noticias sobre el estado del proyecto [19].

Microsoft

Son los autores del proyecto *Home OS* (2010), que consiste en la creación de un sistema operativo (plataforma) dedicado para la automatización del hogar. Además, es compatible con los protocolos Z-Wave, ZigBee, X10, DLNA y Wi-Fi que son los más comunes en el campo de la domótica [20].

Samsung

En la última versión de la feria tecnológica CES (*Consumer Electronics Show* – Las Vegas 2014), presentaron el proyecto *Smart Home*. Samsung busca aprovechar la nueva generación de artefactos (lavadoras, refrigeradoras, aire acondicionado, televisores, equipos de sonido, etc.) que se caracterizan por tener la capacidad de conectarse a Internet a través de Wi-Fi. Además, su nueva plataforma *Smart Home Software* está basada en la nube y esto permite el monitoreo y control de los elementos de la vivienda [21].

AT&T

Ofrece una solución comercial denominada *Digital Life* que tiene la capacidad de controlar los accesos, la administración energética, detección de fugas de agua y el monitoreo de la propiedad a través de cámaras IP. Este servicio se caracteriza por el soporte al usuario, instalación por técnicos capacitados y por contar con centros de monitoreo certificados. Además, la facturación se integra a la mensualidad regular de los abonados [22].

Comcast

Esta empresa de TV por cable y servicios de banda ancha (Estados Unidos) ofrece el servicio de automatización y monitoreo usando sensores (humo, movimiento y temperatura, contacto para las puertas) y controladores (luminarias y termostatos). Emplean la tecnología Wi-Fi para la comunicación entre dispositivos [23].

Estas empresas, líderes en el sector tecnológico, se encuentran promoviendo sus propios servicios, productos y proyectos de forma aislada. Bajo este escenario, fabricar o comercializar soluciones domóticas genera que los diferentes dispositivos desarrollados por las compañías no sean compatibles entre sí. Esto ocasiona que los usuarios estén limitados a los distintos proveedores del producto y no puedan personalizar la solución en base a sus necesidades. Por el momento, no existe alguna asociación o grupo de empresas que tenga una iniciativa concreta para estandarizar esta industria. Por otro lado, existe una oportunidad de negocio importante, ya que los analistas especializados pronostican que para el 2016 el mercado crecerá en 12% (valor monetario) [24].

4. Selección de tecnologías

Para esta sección, se tomó como referencia un estudio elaborado por la empresa *Casadomo*, una de las más importantes del mercado de domótica español [25]. En esta publicación, se recopila información sobre los sistemas de seguridad y domóticos instalados en los hogares españoles. A continuación, se realizará un análisis de la arquitectura, tecnologías de conectividad y los protocolos o estándares utilizados.

En primer lugar, se presenta un cuadro (Figura 14) con la información de la arquitectura utilizada en los sistemas domóticos que fueron instalados en los hogares españoles.

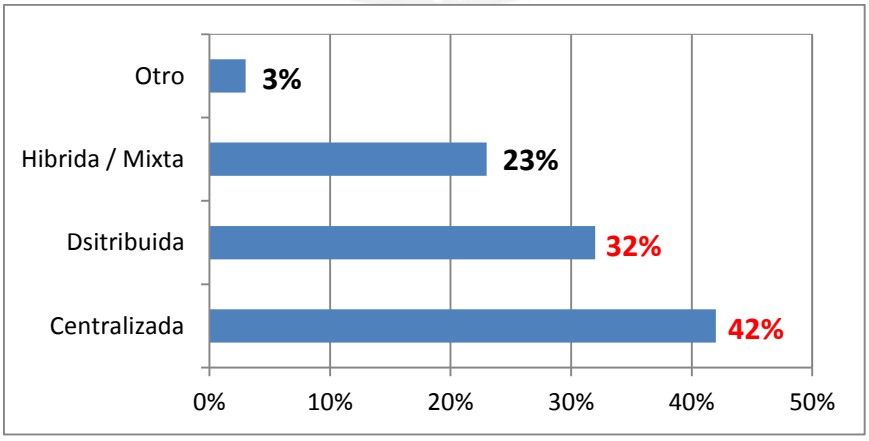


Figura 14 - Arquitectura de los sistemas domóticos [25]

En el gráfico anterior, se observa que las arquitecturas que predominan son la centralizada con 42% de participación, y la distribuida con 32%. La distribuida se caracteriza por qué el sistema no depende de un elemento de control único y cada dispositivo que lo compone tiene la capacidad de controlar y gestionar el sistema de forma independiente. En el caso de la centralizada, se tiene un elemento de control único y si este presenta algún problema, el sistema quedará fuera de servicio hasta que esto se solucione. Al comparar ambas arquitecturas, se concluye que la distribuida es más robusta y confiable, ya que continúa operando a pesar de que algún elemento en la red quede fuera de servicio.

En segundo lugar, se presenta un cuadro (Figura 15) con la participación de las tecnologías de conectividad empleadas en la instalación de sistemas de seguridad en España.

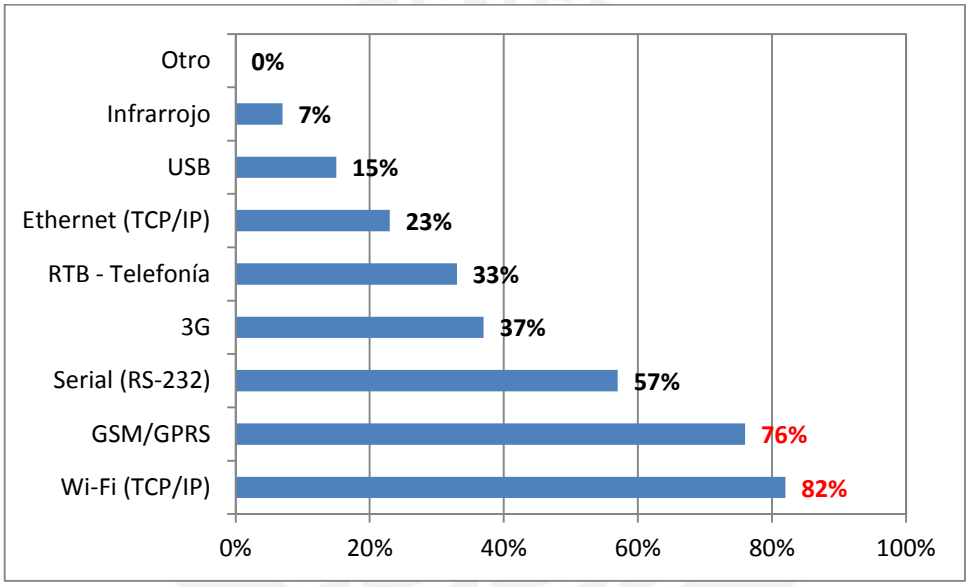


Figura 15 -Tecnologías de conectividad empleados en sistemas de seguridad [25]

En el gráfico anterior, se observa que el uso de redes Wi-Fi (TCP/IP) y Móviles (GSM/GPRS) predominan en la instalación de sistemas de seguridad. Emplear tecnologías de conectividad inalámbrica evita el uso de cables o conexiones físicas, por lo que el proceso de instalación se simplificará y evitará alterar la estética de la vivienda.

En tercer lugar, se presenta un cuadro (Figura 16) con la participación de los estándares empleados en la instalación de sistemas domóticos en España.

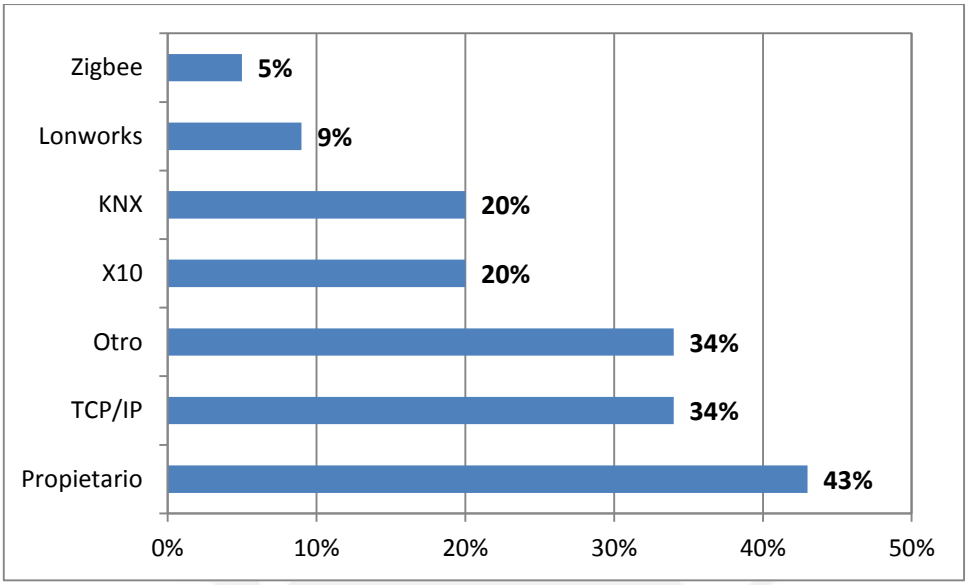


Figura 16 -Estándares empleados en sistemas domóticos [25]

En el gráfico anterior, se observa que predomina el uso de los protocolos propietarios. Cabe resaltar, que esta es una de las desventajas que más afecta a la industria, ya que dificulta la interoperabilidad o compatibilidad entre las soluciones de los distintos fabricantes. Además, si el usuario necesita dispositivos para alguna función específica, dependerá del portafolio de productos del fabricante de la solución propietaria. Por otra parte, el protocolo TCP/IP, de alta difusión en redes LAN y WLAN, cuenta con un 34% de participación. La gran mayoría de dispositivos móviles y electrónica de consumo (laptops, computadoras, televisores, blue-rays, etc.) son compatibles con TCP/IP a través de Wi-Fi o Ethernet. Esto representa una oportunidad importante, ya que se puede aprovechar la gran difusión de este protocolo para aplicarlo en la automatización del hogar.

Por otro lado, existe una nueva tendencia que busca ofrecer soluciones de automatización del hogar a través de aplicaciones alojadas en la nube [15]. De acuerdo con este concepto, el usuario solo debe preocuparse por instalar los dispositivos (sensores / actuadores) y registrarlos en la aplicación. La nube se encargará de la administración y control de todos los elementos que componen el sistema. El objetivo es crear una plataforma que emplee Internet como medio de comunicación con los dispositivos de control.

Para la implementación de este tipo de soluciones, se debe tener en cuenta lo siguiente:

- Almacenamiento y procesamiento de la información en la nube.
- Monitoreo y control de los dispositivos a través de Internet.
- Control automático basado en las reglas definidas por el usuario en la aplicación de la nube.

En conclusión, después de analizar el estado del arte y las tecnologías que se emplean actualmente, se determinó que la solución propuesta en esta tesis debe contar con las siguientes características:

- Se utilizará una arquitectura distribuida, debido a que es la solución más robusta y confiable ante fallas de los controladores del sistema.
- Estará basado en tecnologías de comunicación inalámbricas para evitar complejidad en la instalación.
- Utilizará en el protocolo TCP/IP y la tecnología Wi-Fi para aprovechar la infraestructura común (Routers instalados) de los hogares con conexión a Internet.
- La solución estará basada en la nube para aprovechar la capacidad de almacenamiento y de procesamiento de la misma. Por lo que, los dispositivos de control (sensores / actuadores) no requieren de un hardware complejo.

CAPÍTULO III

DISEÑO DEL SISTEMA

Este capítulo tiene como objetivo presentar los aspectos relacionados al diseño del sistema propuesto. Para ello, se describirán los criterios de diseño, la arquitectura del sistema, la implementación y el escenario final.

1. Criterios de diseño

De acuerdo con IBM, los elementos que componen un hogar inteligente (domótico) deben contar con las siguientes características:

Instrumentación

Los elementos que componen el sistema deben tener la capacidad de monitorear los cambios en las variables del ambiente de la vivienda (temperatura, detección de humo, niveles de humedad, etc.). [26]

Interconexión

Los dispositivos deben ser capaces de comunicarse e interactuar con las personas, sistemas y otros equipos. La capacidad de interconexión hace posible acceder a la información remota sobre el estado del dispositivo y permite el control remoto del mismo. [26]

Inteligencia

Habilidad de tomar decisiones a través del procesamiento de la información recopilada. La inteligencia permite optimizar el uso de los recursos de la vivienda. [26]

En la Figura 17, se muestra una vivienda equipada con un sistema domótico desarrollado bajo la visión de IBM:

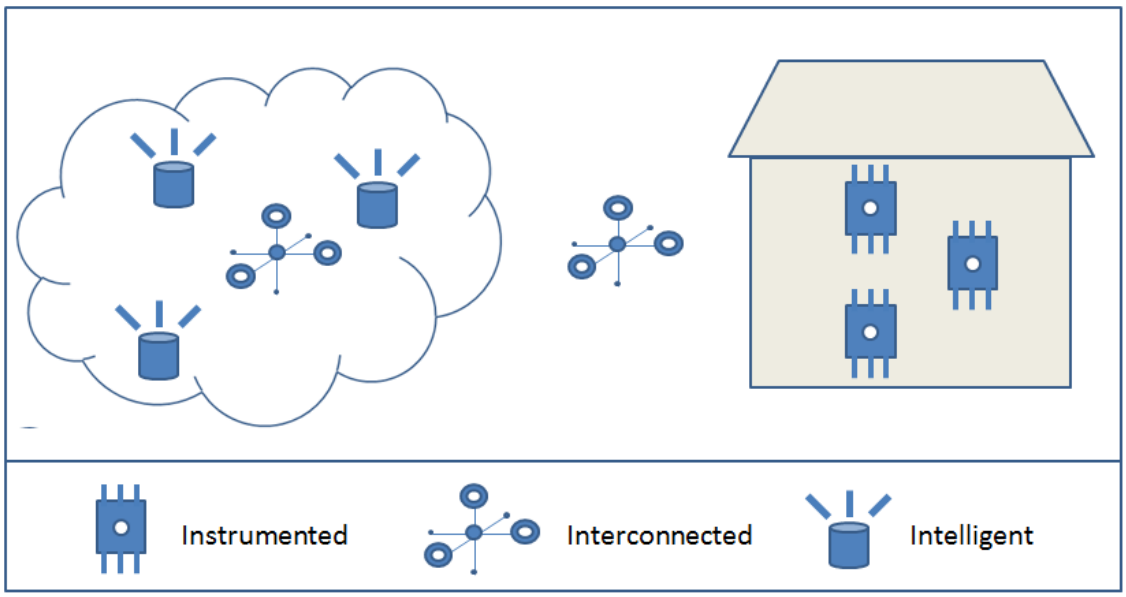


Figura 17 - Vivienda equipada con un sistema domótico (Visión de IBM) [26]

En la figura anterior, se observa que los dispositivos de instrumentación están interconectados con la nube y permiten recopilar información. La inteligencia del sistema radica en la capacidad de procesamiento de los datos de la nube para la toma de decisiones y la ejecución de acciones.

Considerando lo expuesto anteriormente, para el presente proyecto de tesis, se propone una solución basada en la nube tomando como base el modelo *Software as a Service (Cloud Computing)*. Se busca ofrecer una solución bajo el concepto *Domotics as a Service* [27], donde el usuario solo instalará los dispositivos y los conectará a Internet. Por otro lado, la aplicación alojada en la nube se encargará de recopilar, almacenar y analizar la información, y le dará al usuario las sugerencias y herramientas necesarias para el control remoto de los elementos de la vivienda.

En la Figura 18, se muestra un diagrama que permitirá explicar el concepto de *Domotics as a Service*.

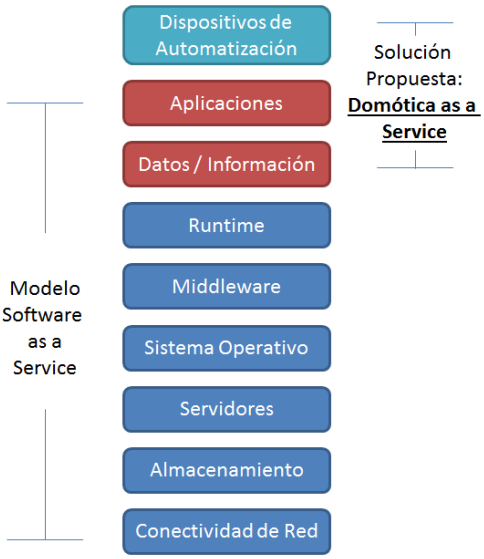


Figura 18 - Domótica as a Service [27]

En la figura anterior, se observa que a partir del modelo *Software as a Service* se propone una modificación que tiene como resultado el modelo *Domotics as a Service*. Las primeras seis capas del modelo se mantienen (desde conectividad de red hasta runtime) y las capas de aplicación y datos se modificarán para el desarrollo del presente proyecto de tesis. Además, se agregó un nivel adicional que hace referencia a los Dispositivos de Automatización que se instalarán en la vivienda del usuario.

2. Arquitectura del sistema

En la Figura 19, se muestra el diagrama general de la solución propuesta en el presente proyecto de tesis.

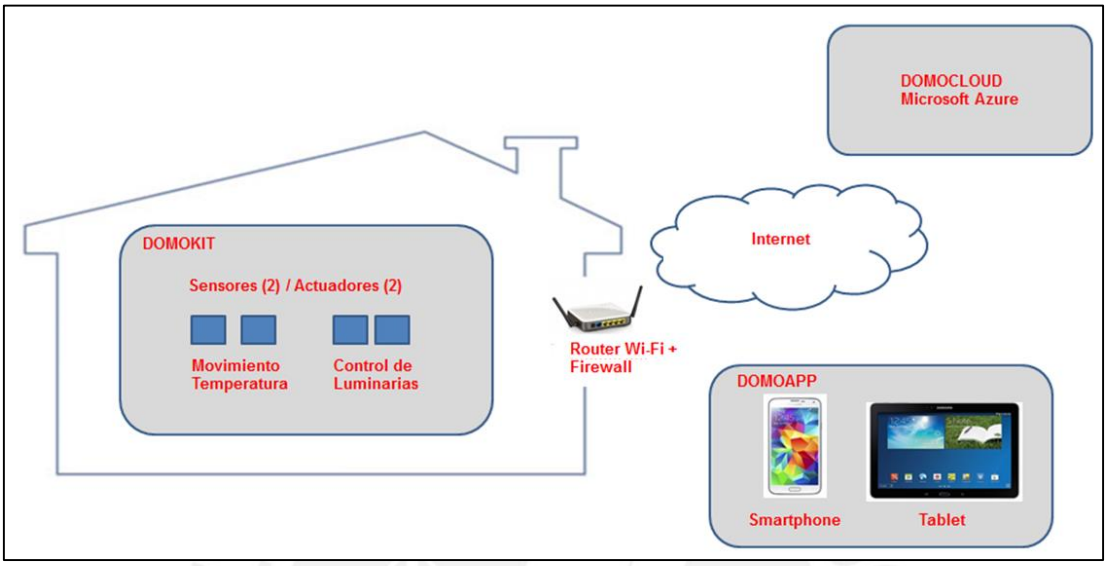


Figura 19 - Arquitectura del Sistema [Elaboración propia] [28] [29] [30]

A continuación, se describirán cada uno de los bloques que componen el sistema mostrado en la figura anterior.

DomoKit

Conjunto de dispositivos electrónicos instalados en la vivienda que tienen por objetivo el monitoreo de algunos parámetros del ambiente (temperatura, humedad, humo, etc.) y el control de los elementos de uso común (luminarias, puertas, aire acondicionado, etc.). Estos equipos cuentan con la tecnología Wi-Fi que permite el envío de la información recopilada a la aplicación de la nube *DomoCloud*. Así mismo, pueden recibir instrucciones para controlar (encender o apagar) las luminarias o algunos artefactos conectados.

Por otra parte, para la construcción de estos dispositivos, se utilizó la tarjeta electrónica *Spark Core* (Figura 20). A continuación, se detallan las características técnicas:

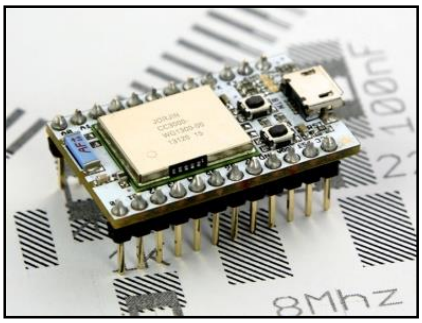


Figura 20 - Tarjeta de desarrollo Spark Core [31]

Especificaciones:

- Basado en las tarjetas de desarrollo Arduino
- Conexión Wi-Fi 802.11 b/g (TCP, HTTP)
- Microprocesador ARM Cortex M3
- Memoria Flash de 128KB
- 10 Pines de Entradas/Salidas digitales
- Lenguaje de programación basado en C

Se optó por utilizar este equipo, ya que cuenta con las siguientes ventajas [32]:

- Precio económico
- Conectividad basada en las tecnologías Wi-Fi, HTTP[7], TCP
- Lenguaje de programación estándar y de alta difusión

DomoApp

Es una aplicación para dispositivos móviles (Smartphones y Tablets) que permite acceder, en tiempo real, a la información del estado de los sensores del *DomoKit*. Además, permite enviar instrucciones de control remoto a los actuadores del *DomoKit*. Está desarrollada con el lenguaje de programación *Java* y es compatible con el sistema operativo *Android* de *Google*.

Para garantizar el funcionamiento de la aplicación, es necesario que los dispositivos móviles en donde se instalará la aplicación cumplan con los requerimientos mostrados a continuación:

- Versión del sistema operativo: Android 4.2 (Jelly Bean) o superior
- Tamaño de pantalla:

[7] HTTP: Hyper Text Transfer Protocol

  - Smartphones: Entre cuatro a seis pulgadas
  - Tablets: Mayor a siete pulgadas
- Procesador: Quad Core 1.2 GHz o superior
- Memoria RAM: 1 GB o superior
- Conectividad: Wi-Fi / 3G / 4G LTE

La arquitectura de la aplicación está compuesta por cuatro módulos, tal como se muestra en la siguiente figura (Figura 21).

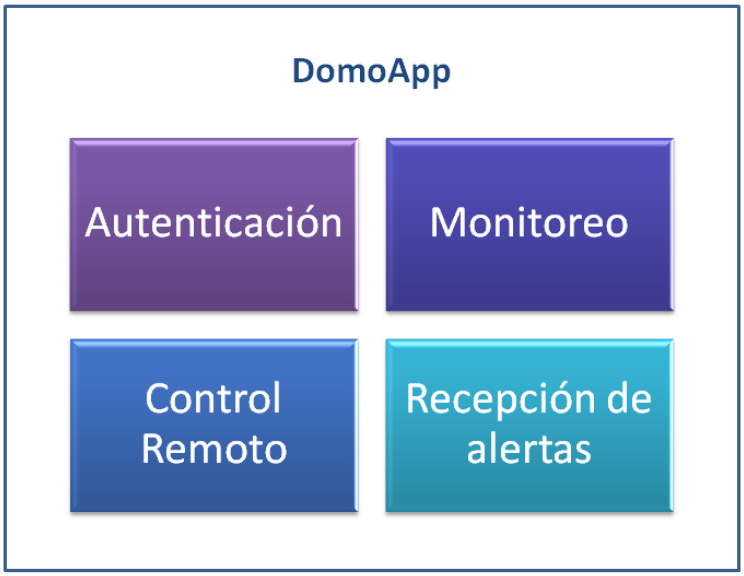


Figura 21 - Arquitectura DomoApp [Elaboración Propia]

A continuación, se describirá cada uno de los elementos mostrados en la figura anterior.

Autenticación

Este bloque contiene la lógica que permite validar la identidad del usuario. Para ello, se comparan los datos ingresados por el usuario (nombre y contraseña) y la información almacenada en la nube - *DomoCloud*. Si este proceso se realiza satisfactoriamente, el usuario podrá acceder e interactuar con los otros módulos de la aplicación.

Monitoreo

Este módulo muestra el estado de los sensores del *DomoKit* en tiempo real. Además, permite visualizar reportes con información sobre algunos parámetros del funcionamiento del sistema (temperatura, humedad, etc.).

Control Remoto

Este bloque se encarga de enviar las instrucciones de control a los actuadores del *DomoKit* a través de la nube *DomoCloud*. Este proceso de comunicación se realiza a través de Internet. Por ejemplo, desde la aplicación *DomoApp* se pueden encender o apagar las luminarias de la vivienda, activar alguna alarma o encender el equipo de aire acondicionado.

Recepción de alertas

Este módulo es responsable de la recepción de las notificaciones de alerta enviadas por el *DomoKit* a través de la nube *DomoCloud*. Esta comunicación se realiza por Internet en tiempo real. Por ejemplo, se pueden recibir alertas sobre la presencia de intrusos en el domicilio, una fuga de gas, un incremento acelerado en los niveles de temperatura, entre otros.

DomoCloud

Es una aplicación alojada en la nube que está implementada en la plataforma *Microsoft Azure*. Es la unidad de control, administración y monitoreo de todos los elementos que componen la solución (*DomoKit* y *DomoApp*). En el siguiente gráfico (Figura 22), se muestran los elementos que componen esta aplicación.

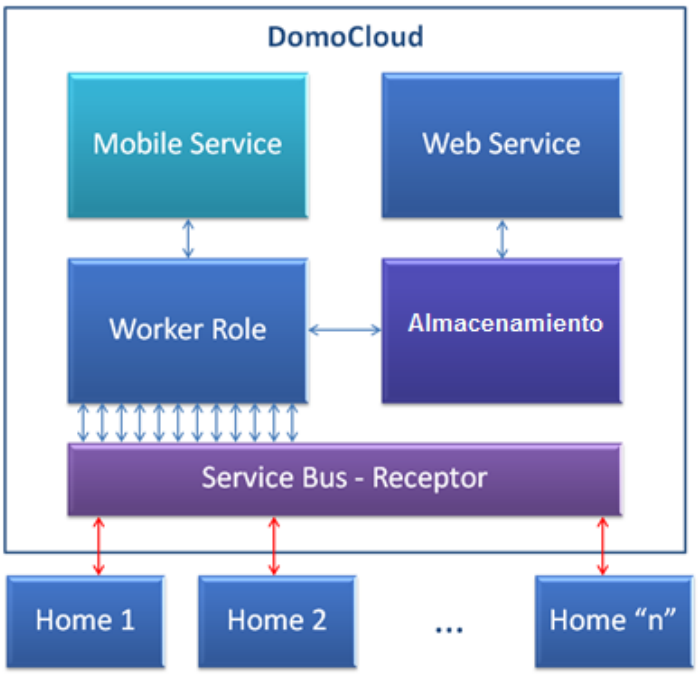


Figura 22 - Arquitectura DomoCloud [Elaboración Propia]

A continuación, se describirá cada uno de los elementos mostrados en el gráfico anterior.

Service Bus – Receptor

Es una aplicación desarrollada para la plataforma .NET (C#) y alojada en el *DomoCloud*. Actúa como una pasarela de recepción de mensajes, estos son enviados desde el *Domokit* o la aplicación móvil *DomoApp*. Además, la comunicación se establece a través de Internet bajo el protocolo HTTP. En la Figura 23, se muestra el diagrama bloques de este componente.

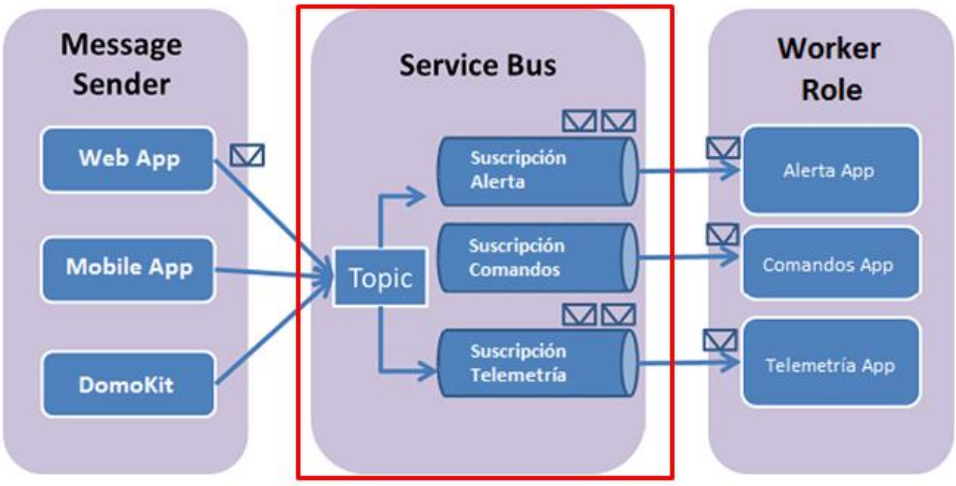


Figura 23 - Receptor de mensajes - Service Bus [33]

El receptor de mensajes permite la interacción entre los siguientes elementos:

Topic

Es un servicio web (URL) encargado de la recepción de los mensajes que provienen del *DomoKit*, la aplicación móvil *DomoApp* o el portal web de administración. Para enviar la información al *Topic*, es necesario establecer una conexión por Internet usando el protocolo HTTP. Además, este elemento es el responsable de clasificar estos mensajes según su propósito (alertas, comandos, ping y telemetría) y re-direccionarlos a las *Suscripciones* (buffers dedicados) para el procesamiento de la información.

Suscripción

Es un conjunto de *buffers* que se encargan de almacenar los mensajes enviados por el *Topic*. Cada *buffer* está asociado a un tipo de mensaje, en el caso del presente proyecto de tesis, se tendrán cuatro tipos: Alertas, Comandos, Ping y Telemetría. Estos mensajes se almacenarán hasta que la aplicación encargada del procesamiento de esta información los solicite.

Worker Role

Es un conjunto de aplicaciones desarrolladas para la plataforma .NET (C#) que se encargan del procesamiento de los mensajes almacenados en la *Suscripción*. Cada aplicación está asociada a un determinado tipo de mensaje, por lo que se tendrán programas específicos para los mensajes de alerta, uno para los comandos y otro asociado a telemetría. En la Figura 24, se muestra el diagrama de bloques de este componente. Se observa que cada *Suscripción* está conectada a un *Worker Role* según el tipo de mensaje.

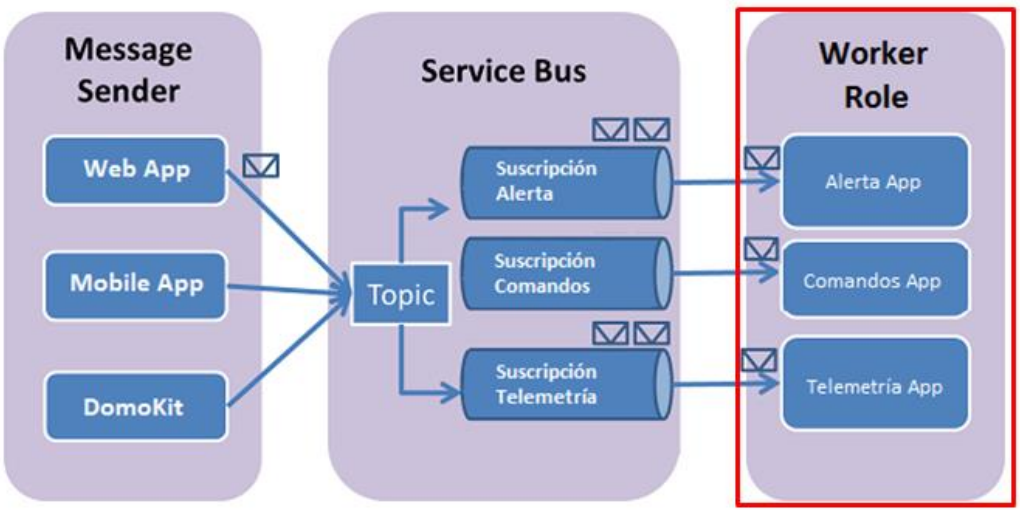


Figura 24 - Worker Role [33]

A continuación, se describirán dos casos prácticos sobre el funcionamiento del *Service Bus* y el *Worker Role*:

- El *Domokit* está equipado con un sensor de movimiento que es el responsable de monitorear el acceso al hogar. Si este sensor detecta la presencia de un intruso, el *Domokit* generará un mensaje del tipo *alerta* que será enviado al *Topic* a través de la conexión a Internet. El *Topic* se encargará de re-direccionar esta información a la *Suscripción Alerta* y la aplicación asociada se encargará de procesarla. El objetivo es comprobar el origen del mensaje, almacenar la información y determinar a qué usuarios se notificará. Con esta información, el sistema *DomoCloud* enviará una notificación a los dispositivos móviles asociados.

- El *DomoKit* posee un sensor de temperatura que se encarga de medir las condiciones del ambiente y reportarlas al sistema cada treinta minutos. Para ello, el *DomoKit* generará un mensaje del tipo *telemetría* que se enviará al *Topic* a través de la conexión a Internet. El *Topic* se encargará de re-direccionar esta información a la *Suscripción Telemetría* y la

aplicación asociada se encargará de procesarla. El objetivo es crear un registro histórico de estas mediciones que será mostrado a través de un reporte en la página web o en la aplicación móvil. Además, con esta información, el sistema puede determinar en qué circunstancias se debería encender o apagar el equipo de aire acondicionado para mejorar la eficiencia de consumo de energía.

Unidad de almacenamiento

Es la base de datos en donde se almacenará la información de los usuarios y los dispositivos *DomoKit*. De esta forma, se podrá mantener un registro histórico de los datos para su posterior análisis o para la elaboración de reportes.

Mobile Service

Es una aplicación desarrollada en lenguaje *Javascript* que se encarga de enviar mensajes de tipo *Push*. Estas notificaciones son generadas por el *DomoCloud* y serán enviadas, a través de Internet, a los dispositivos *DomoKit* o a la aplicación móvil *DomoApp*. En la Figura 25, se muestra el mecanismo de funcionamiento.

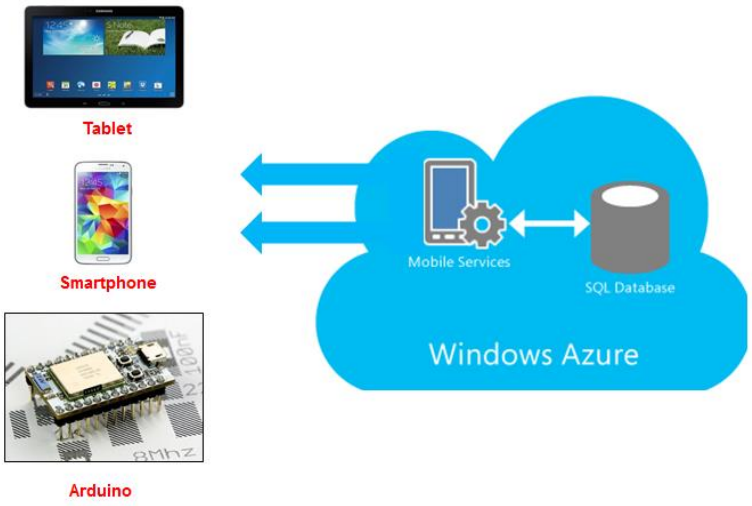


Figura 25 - Mobile Service [29] [30] [31] [34]

En la figura mostrada anteriormente, se observa que el *Mobile Service* recibe un mensaje proveniente del *Worker Role* que contiene los datos del destinatario y la información. Luego, el *Mobile Service* verifica la plataforma del destino y emplea un servicio específico asociado. Por ejemplo, para dispositivos con sistema operativo Android, se emplea *Google Cloud Messaging*, para el caso de iOS, se utilizará *Apple Push Notifications* y, para las tarjetas de desarrollo, se utilizará un servicio basado en *Javascript*.

Módulo de reportes – Servicio Web

Es un módulo alojado en el *DomoCloud* y está diseñado para mostrar información sobre el funcionamiento general del sistema en tiempo real. Los reportes se generan utilizando los registros almacenados en la base de datos. Adicionalmente, el usuario puede controlar remotamente los actuadores del *DomoKit* a través de la interfaz gráfica de la página web. Por ejemplo, es posible encender las luminarias de una habitación específica o activar el aire acondicionado. En la Figura 26, se muestra un panel prototipo que será implementado en el sistema.

Figura 26 - Ejemplo de la interfaz gráfica - Módulo de reportes [35]

Por otra parte, este módulo está conformado por 3 elementos: la base de datos, el servicio web y la página web. La distribución de estos elementos se muestra a continuación en la siguiente figura (Figura 27).

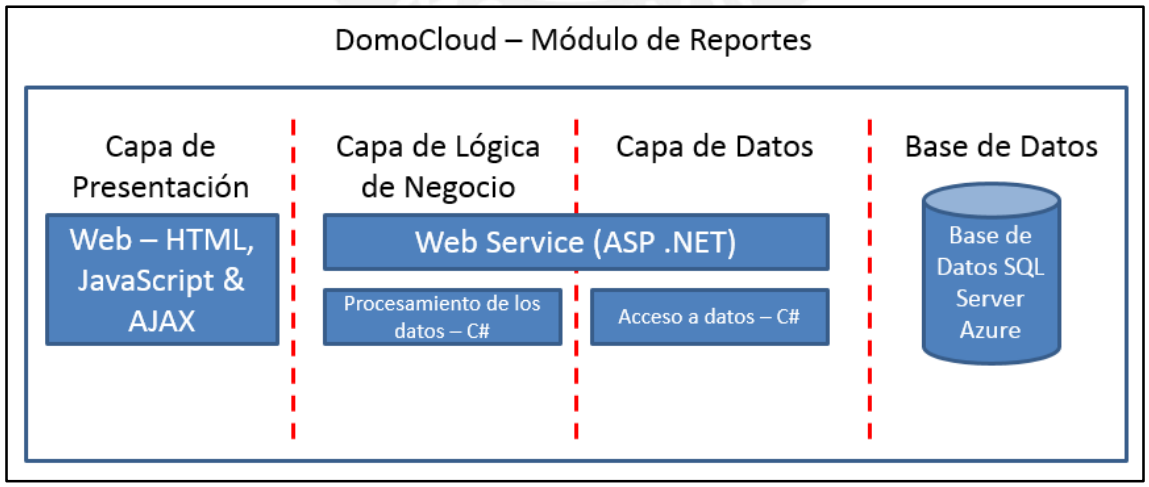


Figura 27 - Arquitectura del módulo de reportes (Elaboración propia)

En la figura mostrada anteriormente, se observa que la información es almacenada en una base de datos SQL Server que está alojada en la nube de Microsoft Azure. Además, el *Web Service* está desarrollado en el lenguaje de programación C# (Microsoft .NET) y se encargará de 2 tareas. En primer lugar, es el responsable de acceder a la información alojada en la base de datos a través de consultas (capa de datos). En segundo lugar, una vez que la consulta a la base de datos es ejecutada, este elemento se encargará de procesar los datos que son el resultado de esa petición (capa de lógica de negocio). Por otra parte, el módulo de reportes tendrá una interfaz gráfica (página web) que ha sido desarrollada en los lenguajes HTML y JavaScript. Este bloque se encarga de presentar la información procesada previamente por el *Web Service* (capa de presentación),

3. Implementación

En esta sección del capítulo se describirá la implementación de cada uno de los bloques del sistema.

Servicio de comunicación asistida

Los métodos tradicionales para conectar dispositivos o aplicaciones a Internet son las redes VPN o el modelo Cliente-Servidor con NAT (*Network Address Translation*). Este último se caracteriza por exponer los elementos de una red privada a Internet a través de la combinación entre una IP Pública y un puerto. Para el caso de soluciones domóticas, ambos modelos tienen como limitante las características de hardware con las que están equipadas los dispositivos que se instalarán en la vivienda.

Estos dispositivos tienen que manejar la autenticación, las conexiones entrantes, el procesamiento e interpretación de las peticiones, etc. Debido a la baja capacidad de procesamiento, memoria y energía, el manejo de estos procesos puede hacer que el dispositivo colapse y en consecuencia el servicio no estará disponible. [36]

Para establecer la comunicación entre el *DomoKit* y el *DomoCloud* se empleará una técnica propuesta por Microsoft denominada Servicio de Comunicación Asistida. En la Figura 28, se muestra un gráfico que permitirá explicar este concepto.

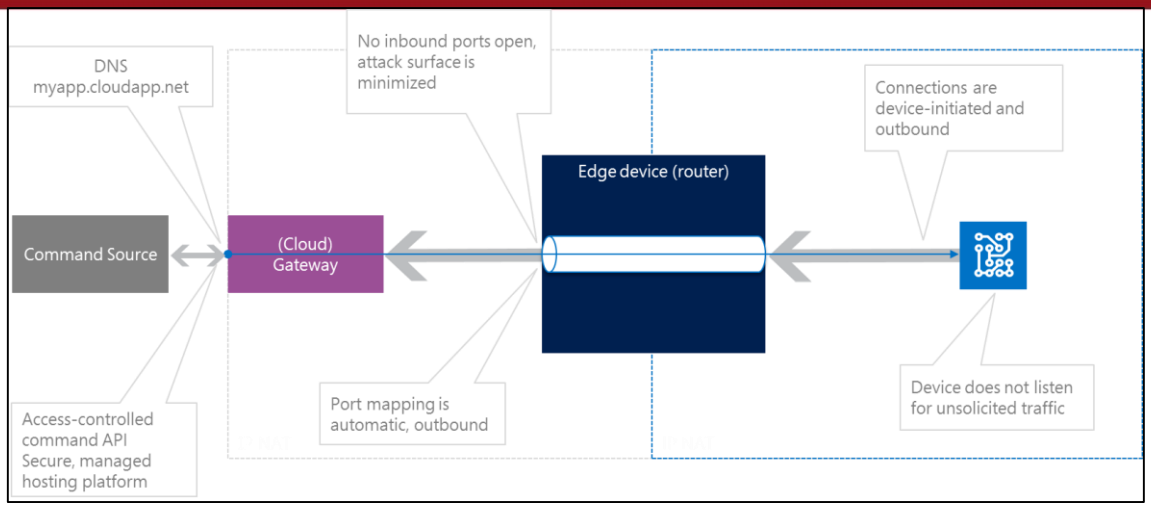


Figura 28 - Modelo de comunicación asistida [36]

En la figura anterior, se observa que el tráfico es manejado por una entidad intermedia denominada *Service Gateway (Cloud).* Este elemento se encargará de manejar el tráfico entrante: autenticación, conexiones entrantes, procesamiento de la información, etc. El dispositivo solo se conectará al *Service Gateway* y solicitará la información entrante. Esto permite contrarrestar el efecto de la baja capacidad de procesamiento y memoria de los dispositivos que instalarán en el hogar. [36]

Cloud

Recepción de mensajes

En la Figura 29 se muestra el diagrama de flujo del funcionamiento del bloque de recepción de los mensajes. Se observa que el *Topic* (Servicio Web) recibe el mensaje, a través del protocolo HTTP, y lo clasifica según su tipo (alerta, comando, telemetría, ping). A continuación, este mensaje es reenviado a la *Suscripción* a la que pertenece y es procesado por el *Worker Role* en donde se ejecutarán las acciones que correspondan. Finalmente, el mensaje es almacenado en la base de datos asociada al *Worker Role* con el fin de llevar un registro histórico de la actividad de cada aplicación.

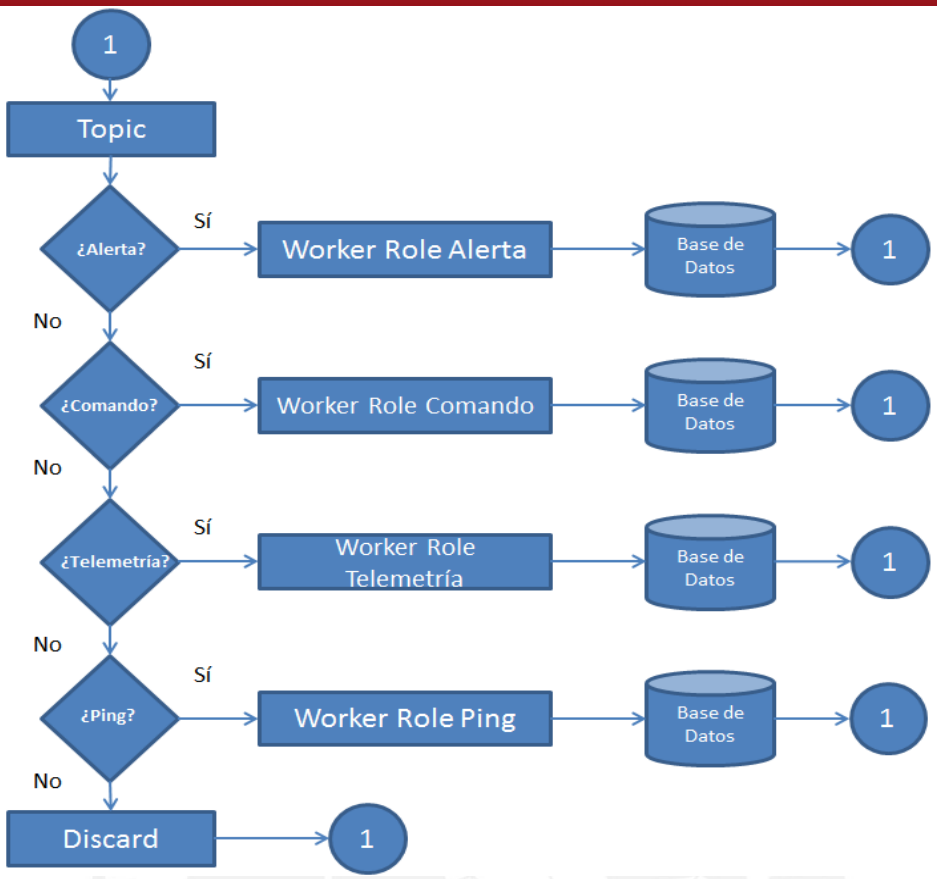


Figura 29 - Recepción de Mensajes (Diagrama de Flujo) [Elaboración Propia]

Worker Roles

Alerta

El mensaje *Alerta* está compuesto por cuatro parámetros, tal como se muestra en la siguiente tabla (Tabla 5).

Campos	Valor	Tipo
Message Type	0	2 bits
Device Token	ABCDEFGHIJK	String
User Token	ABCDEFGHIJK	String
Message Content	ABCDEFGHIJK	String

Tabla 5 - Parámetros del mensaje *Alerta* [Elaboración Propia]

Parámetros:

- *Message Type*, indica el tipo de mensaje y el valor es "0" para indicar que es una *Alerta*.
- *Device Token*, es el identificador del dispositivo *Domokit*.
- *User Token*, es el identificador del usuario.

- *Message Content*, es el contenido del mensaje que se reenviará a los dispositivos móviles asociados al identificador de usuario.

En la Figura 30, se muestra un diagrama de flujo que permite explicar la lógica de funcionamiento de la aplicación *Worker Role Alerta*.

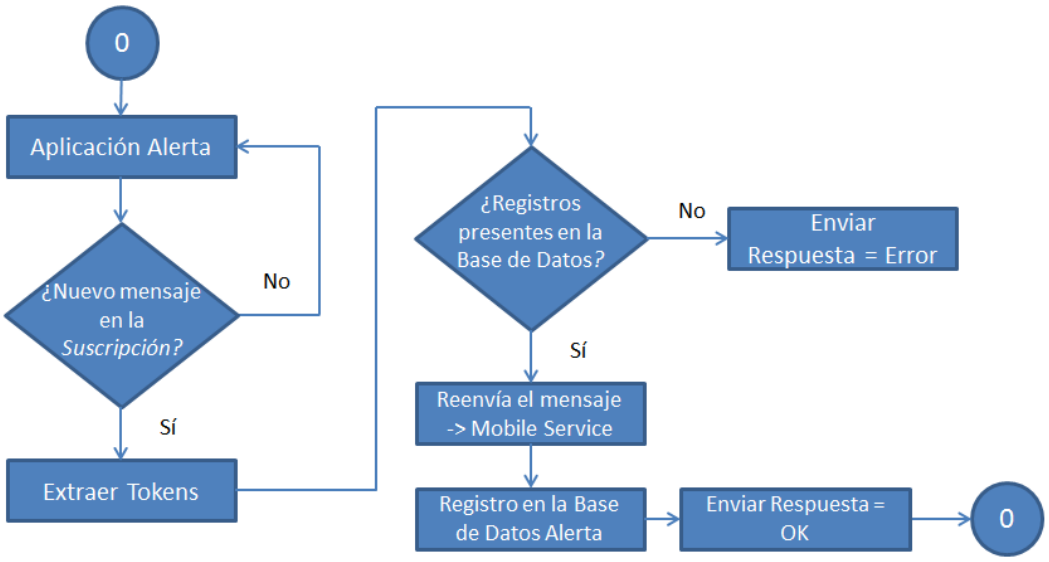


Figura 30 - Funcionamiento del *Worker Role Alerta* (Diagrama de Flujo) [Elaboración Propia]

En la figura anterior, se observa que la aplicación monitorea permanentemente la llegada de un nuevo mensaje en la *Suscripción Alerta*. En caso se detecte un mensaje nuevo, la aplicación extraerá el *Device Token* y el *User Token*. Ambos parámetros serán comparados con la información almacenada en la base de datos (identificador de usuario y dispositivo). De esta forma, se valida la identidad del emisor del mensaje.

Si la validación culmina de forma satisfactoria, el mensaje se reenviará a otro módulo denominado *Mobile Service* que se encarga de alertar a los dispositivos móviles asociados al identificador de usuario. En caso no se pueda verificar la identidad del emisor o se produzca un error durante la extracción de los parámetros, la aplicación responderá con un mensaje de error.

Telemetría

El mensaje *Telemetría* está compuesto por cinco parámetros, tal como se muestra en la siguiente tabla (Tabla 6).

Campos	Valor	Tipo
Message Type	1	2 bits
Device Token	ABCDEFGHIJK	String
User Token	ABCDEFGHIJK	String
Units	ABC	String
Value	0.0	Float

Tabla 6 - Parámetros del mensaje Telemetría [Elaboración Propia]

Parámetros:

- *Message Type*, indica el tipo de mensaje y el valor es "1" para indicar que es del tipo *Telemetría*.
- *Device Token*, es el identificador del dispositivo *Domokit.*
- *User Token*, es el identificador del usuario.
- *Units*, es la unidad de medición. Por ejemplo, para la temperatura este valor será centígrados.
- *Value*, es el valor de la medición y está en formato decimal.

En la Figura 31, se muestra un diagrama de flujo que permite explicar la lógica de funcionamiento de la aplicación *Worker Role Telemetría.*

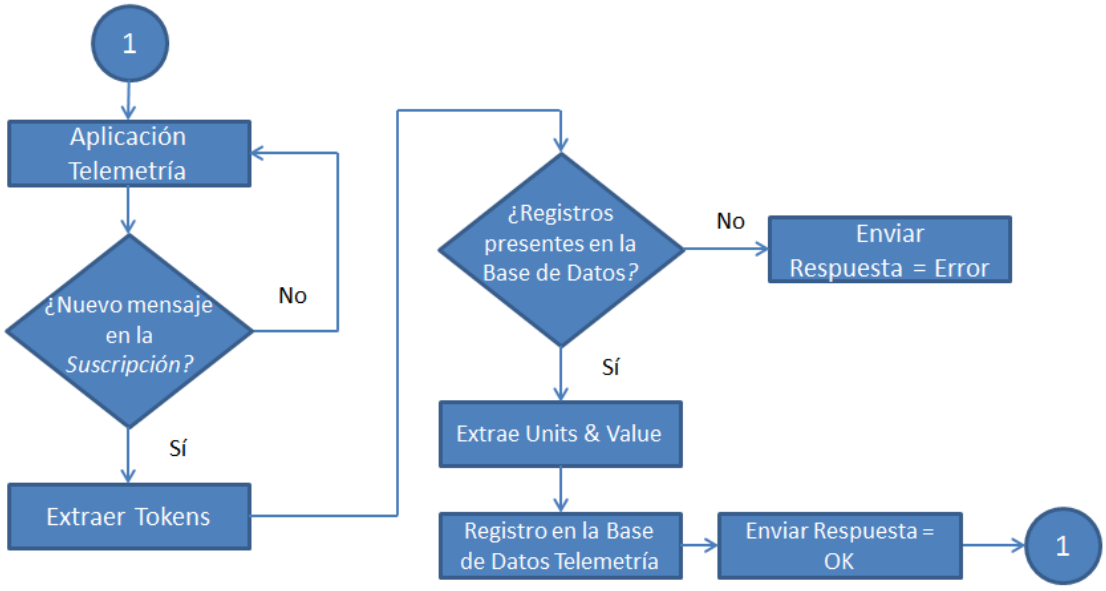


Figura 31- Funcionamiento del *Worker Role Telemetría* (Diagrama de Flujo) [Elaboración Propia]

En la figura anterior, se observa que la aplicación monitorea permanentemente la llegada de un nuevo mensaje en el *Suscripción Telemetría.* En caso se detecte un mensaje nuevo, la aplicación extraerá el *Device Token* y el *User Token* para validar e identificar el origen del mensaje como el caso anterior.

Si la validación culmina de forma satisfactoria, se extraerán el valor de la medición y la unidad de medida para almacenarlos en la base de datos. De esta forma, se podrá llevar un registro histórico de la información. En caso no se pueda verificar la identidad del emisor o se produzca un error durante la extracción de los parámetros, la aplicación responderá con un mensaje de error.

Comando

El mensaje *Comando* está compuesto por seis parámetros, tal como se muestra en la siguiente tabla (Tabla 7).

Campos	Valor	Tipo
Message Type	2	2 bits
Device Token - Originated	ABCDEFGHIJK	String
Device Token - Destination	ABCDEFGHIJK	String
User Token	ABCDEFGHIJK	String
Command	1 / 0	1 bit
Time to Live (TTL)	00	0 < Integer < 120 segundos

Tabla 7- Parámetros del mensaje Comando [Elaboración Propia]

Parámetros:

- *Message Type*, indica el tipo de mensaje y el valor es "2" para indicar que es un *Comando.*
- *Device Token Originated*, es el identificador del dispositivo móvil desde donde se genera el comando.
- *Device Token Destination,* es el identificador del dispositivo *Domokit* que recibirá el comando para su ejecución.
- *User Token*, es el identificador del usuario.
- *Command,* es la instrucción para habilitar (valor "1") o deshabilitar (valor "0") algún equipo / artefacto asociado al *Domokit.*
- *Time to Live*, es el periodo de tiempo en la que el comando tendrá validez.

En la Figura 32, se muestra un diagrama de flujo que permite explicar la lógica de funcionamiento de la aplicación *Worker Role Comando.*

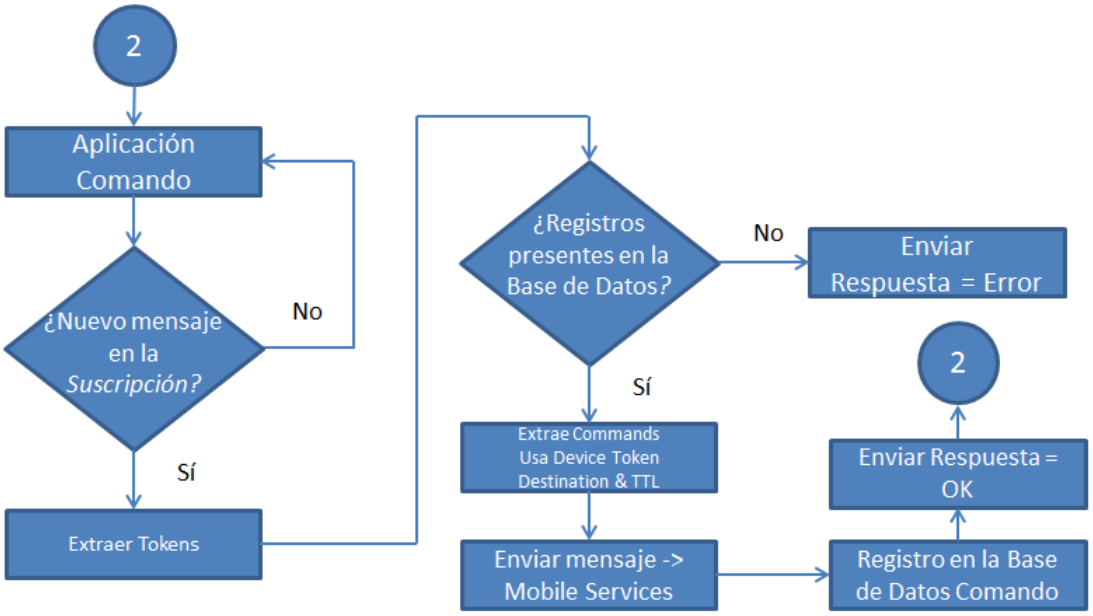


Figura 32 - Funcionamiento del *Worker Role Comando* (Diagrama de Flujo) [Elaboración Propia]

En la figura anterior, se observa que la aplicación monitorea permanentemente la llegada de un nuevo mensaje en el *Suscripción Comando.* En caso se detecte un mensaje nuevo, la aplicación extraerá el *Device Token Originated* y el *User Token* para validar e identificar el origen del mensaje como en el primer caso (*Alerta*).

Si la validación culmina de forma satisfactoria, se extraerán los parámetros *Device Token Destination*, *Command* y TTL. Con esta información se generará un nuevo mensaje que se reenviará al *Domokit* asociado al *Device Token Destination,* a través del módulo *Mobile Services.* En caso no se pueda verificar la identidad del emisor o se produzca un error durante la extracción de los parámetros, la aplicación responderá con un mensaje de error.

Ping

El mensaje *Ping* está compuesto por cuatro parámetros, tal como se muestra en la siguiente tabla (Tabla 8).

Campos	Valor	Tipo
Message Type	3	2 bits
Device Token	ABCDEFGHIJK	String
User Token	ABCDEFGHIJK	String
Stay Alive	1	1 bit

Tabla 8 - Parámetros del mensaje Ping [Elaboración Propia]

Parámetros:

- *Message Type*, indica el tipo de mensaje y el valor es "3" para indicar que es del tipo *Ping*.
- *Device Token*, es el identificador del dispositivo *Domokit*.
- *User Token*, es el identificador del usuario.
- *Stay Alive*, es el indicador de actividad del dispositivo.

En la Figura 33, se muestra un diagrama de flujo que permite explicar la lógica de funcionamiento de la aplicación *Worker Role Ping*.

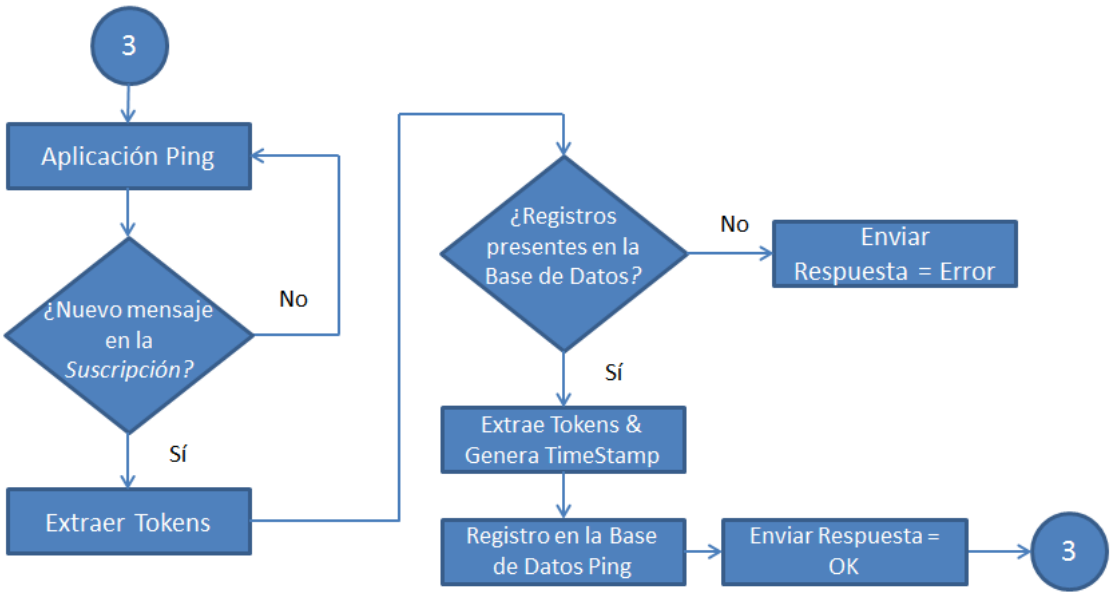


Figura 33 - Funcionamiento del Worker Role Ping (Diagrama de Flujo) [Elaboración Propia]

En la figura anterior, se observa que la aplicación monitorea permanentemente la llegada de un nuevo mensaje en el *Suscripción Ping*. En caso se detecte un mensaje nuevo, la aplicación extraerá el *Device Token* y el *User Token* para validar e identificar el origen del mensaje como en el primer caso (*Alerta*).

Si la validación culmina de forma satisfactoria, se extraerá el parámetro *Stay Alive* y se almacenará en la base de datos. De esta forma, se podrá llevar un registro histórico de la última conexión de los dispositivos *DomoKit*. En caso no se pueda verificar la identidad del emisor o se produzca un error durante la extracción de los parámetros, la aplicación responderá con un mensaje de error.

Además, se tiene otra aplicación que se ejecuta en paralelo y se encarga de analizar la información almacenada en la base de datos para determinar si los dispositivos DomoKit tienen algún problema en la conexión al *DomoCloud*. A continuación, se muestra un diagrama de flujo (Figura 34) que permite explicar la lógica de funcionamiento:

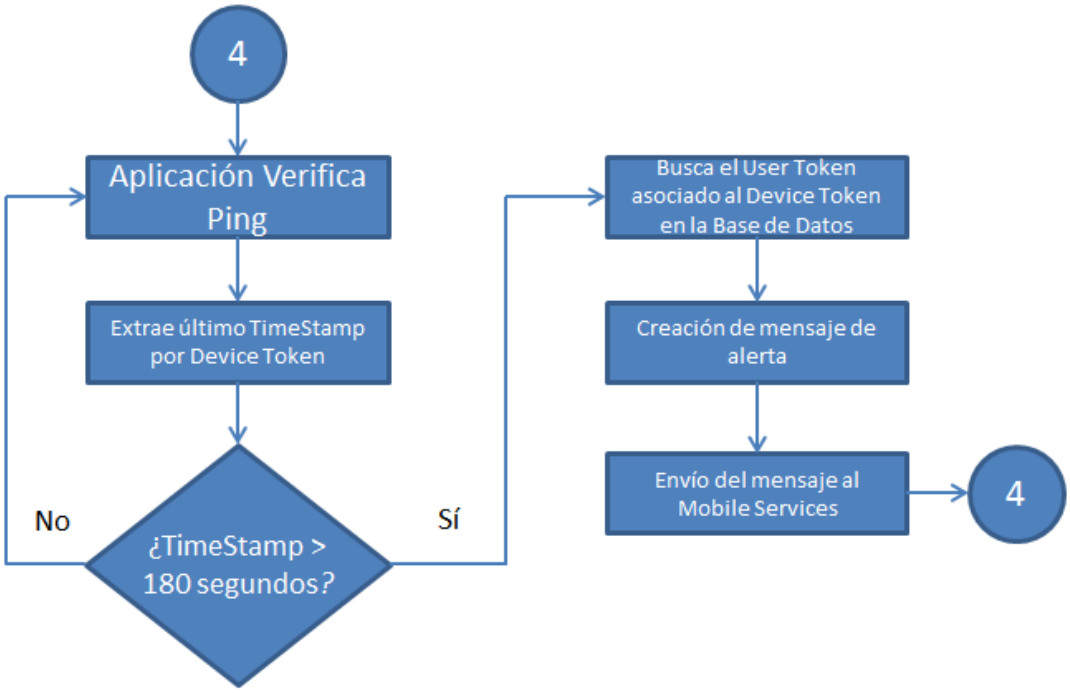


Figura 34 - Funcionamiento de la aplicación Verificación de Ping (Diagrama de Flujo) [Elaboración Propia]

En la figura anterior se observa que la aplicación se conecta con la base de datos *Ping* y extrae la información de la última conexión (*timestamp* = fecha y hora) de cada uno de los dispositivos *DomoKit* registrados. A continuación, se compara esa información con la

fecha y hora actual, si hay una diferencia mayor a tres minutos se enviará un mensaje de alerta al dispositivo móvil asociado al *DomoKit.*

Mobile Services

En la Figura 35, se muestra el diagrama de flujo del funcionamiento del módulo Mobile Services.

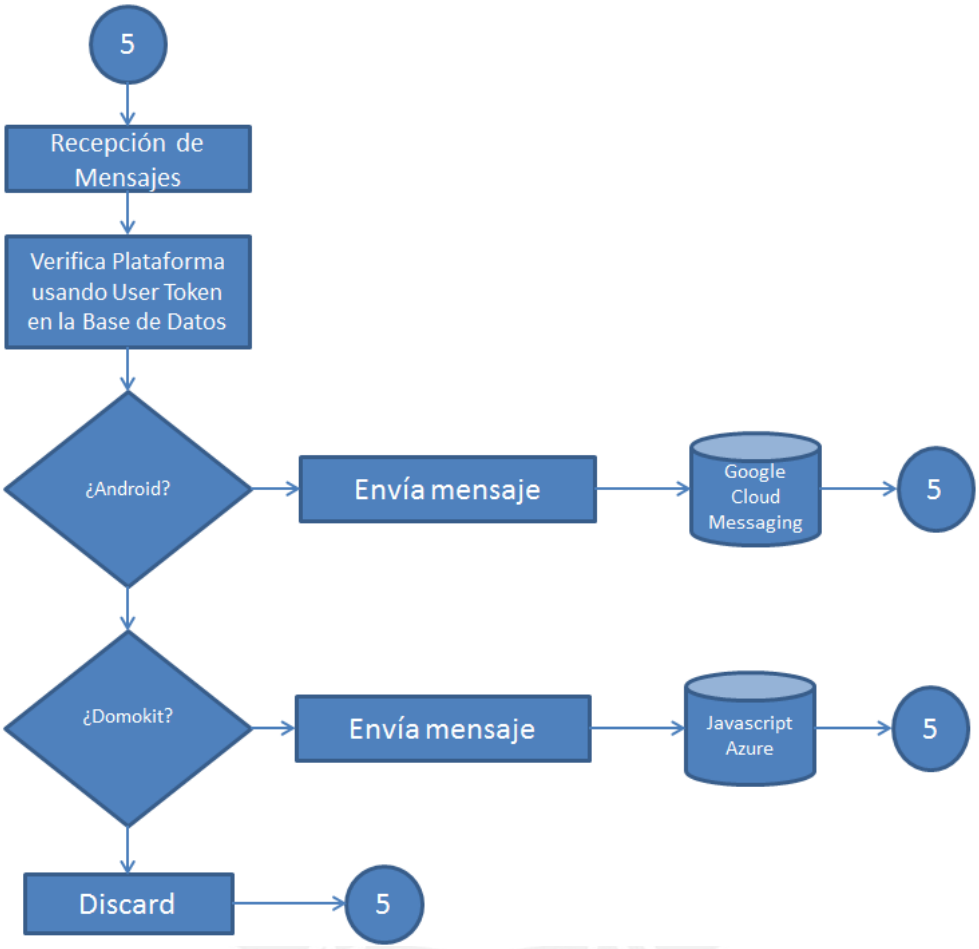


Figura 35 – Mobile Services (Diagrama de Flujo) [Elaboración Propia]

Como se observa en la figura anterior, este módulo recibe los mensajes enviados por las aplicaciones *Worker Rol* y a través de una consulta a la base de datos, usando el *User Token* como referencia, se determina la plataforma de destino: Dispositivos Android o *DomoKit*. Para los dispositivos Android, el *Mobile Services* realiza una petición HTTP al servicio *Google Cloud Messaging* (GCM) que se encargará de entregar el mensaje a los dispositivos asociados al usuario *User Token.* En el caso del *DomoKit,* este módulo enviará el mensaje a través de un servicio *Javascript* alojado en el *DomoCloud.*

4. Escenario final

En la Figura 36, se muestra el diagrama de la implementación final. El sistema está compuesto por tres bloques: *DomoKit*, *DomoCloud* y *DomoApp*.

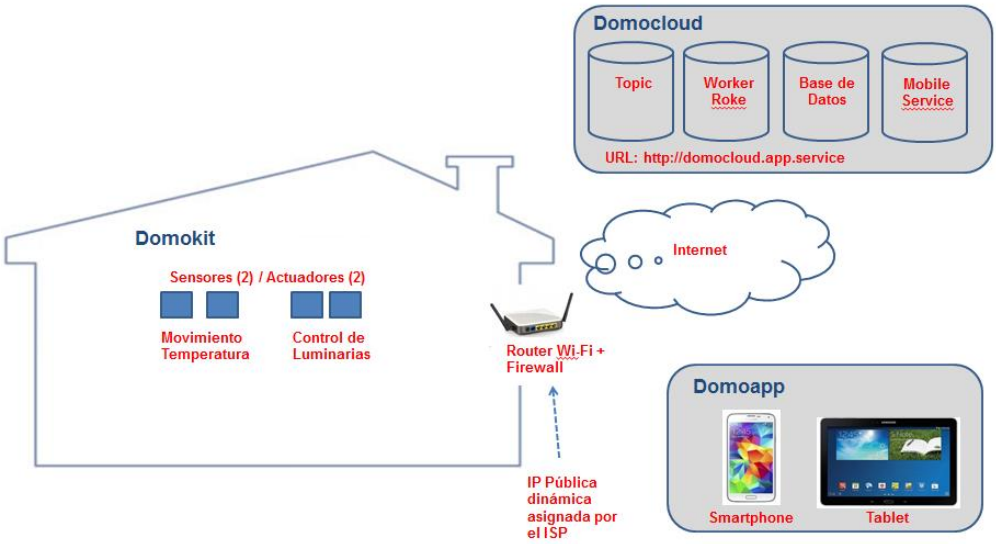


Figura 36 - Escenario Final [Elaboración propia] [28] [29] [30]

En primer lugar, el *DomoKit* es un dispositivo electrónico que está equipado con sensores y actuadores. Está instalado en la vivienda del usuario y permite monitorear algunos parámetros del ambiente (temperatura, humedad, humo, etc.) y el control de los elementos de uso común (luminarias, puertas, aire acondicionado, etc.). Esta información se intercambia con la aplicación alojada en la nube, denominada *DomoCloud*, a través de Internet usando una conexión Wi-Fi.

En segundo lugar, el servicio *DomoCloud* está alojado en la nube específicamente en la plataforma *Microsoft Azure.* Este servicio está compuesto por un conjunto de aplicaciones que se encargan de cuatro tareas fundamentales: recepción de los mensajes enviados por el *DomoKit*, el procesamiento de la información que contienen estos mensajes, el almacenamiento de la información en la base de datos para llevar un registro histórico, y el envío de instrucciones de control al *DomoKit* para la ejecución de acciones. El intercambio de información se realiza a través de Internet usando el protocolo HTTP.

Finalmente, DomoApp es una aplicación desarrollada para Smartphones y Tablets de la plataforma *Android*. Actúa como la interfaz para que los usuarios puedan acceder, en tiempo real, a la información del estado de los sensores del *DomoKit.* Además, permite el control remoto de los actuadores y recibir notificaciones de alerta en caso se tenga alguna incidencia en la vivienda del usuario.

En conclusión se propone un diseño basado en la nube bajo el concepto de *Domotics as a Service*. La solución considera tres criterios: instrumentación, ya que los dispositivos que lo componen tiene la capacidad de monitorear las variables del ambiente de la vivienda; interconexión, ya que los elementos del sistema son capaces de intercomunicarse con la nube y se puede acceder a la información de su estado en tiempo real; e inteligencia, ya que la nube tiene la capacidad de procesar grandes cantidades de información lo que permite sugerir al usuario algunas acciones para optimizar los recursos de la vivienda.

CAPÍTULO IV

PRUEBAS Y RESULTADOS

El propósito del presente capítulo es describir las pruebas que se realizaron para verificar la propuesta y se presentarán los resultados obtenidos que permiten validar el funcionamiento de la solución. Además, se elaboró un análisis de riesgo informático que permitió identificar algunas amenazas y vulnerabilidades del sistema implementado. Por ello, se plantearán algunos mecanismos de control que permiten mitigar el riesgo.

1. Verificación del protocolo de comunicación

Para verificar que la estructura de los mensajes, intercambiados por los diferentes elementos del sistema, está acorde con el planteamiento del CAPÍTULO III, se consideró el monitoreo de los registros de actividad de cada una de las aplicaciones (*Worker Rol*) dedicadas al procesamiento de la información. En la Figura 37, se presenta un gráfico con el escenario de pruebas.

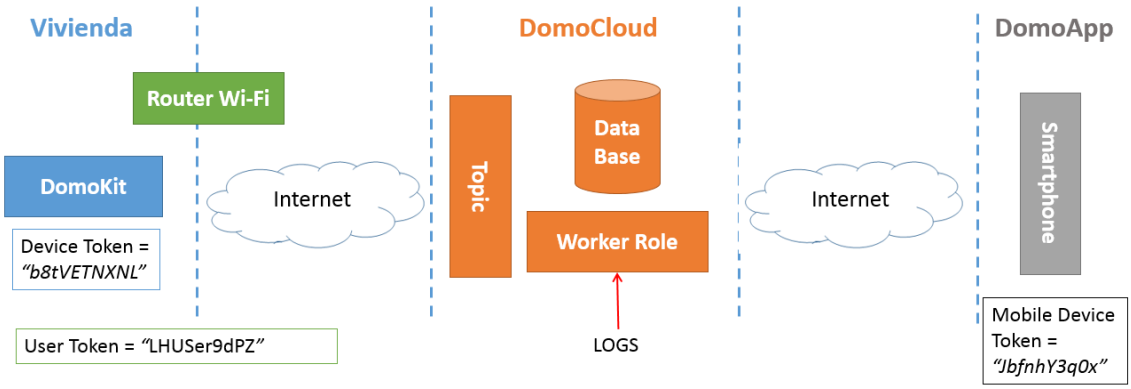


Figura 37 - Escenario de pruebas para verificar el protocolo de mensajería [Elaboración Propia]

En la figura anterior, se observa que el *DomoKit* y el *DomoApp* tendrán asignado un *token* único que permite identificarlos. Por otra parte, las aplicaciones dedicadas al procesamiento de mensajes y alojadas en el *DomoCloud* cuentan con una implementación (código y lógica) adicional que permite capturar el tráfico de los mensajes que se intercambian en el sistema.

El objetivo de esta prueba es verificar que la estructura de los mensajes de la implementación final está acorde con el planteamiento teórico del protocolo de mensajería, presentado en el capítulo anterior. Para ello, se comparará cada tipo de mensaje: alerta, telemetría, comando y ping.

Alerta

A continuación, se presenta la Tabla 9 que permite comparar el diseño del protocolo de comunicación (expuesto en el Capítulo III) con la implementación real para los mensajes del tipo Alerta.

Estructura del Mensaje – Planteamiento Teórico	Log capturado – Implementación real

Campos	Valor	Tipo
Message Type	0	2 bits
Device Token	ABCDEFGHIJK	String
User Token	ABCDEFGHIJK	String
Message Content	ABCDEFGHIJK	String

```
LOG EVENT: New Incoming Message 10/05/2015 09:32:15 a.m.
=========================================================
Message Type = 0                    !!  Type = Alerta
User Token = LHUSer9dPZ             !!  User Id
Device Token = b8tVETNXNL           !!  Device Id
Message = Intruso detectado en el PRIMER NIVEL
```

Tabla 9 - Mensaje del tipo Alerta [Elaboración Propia]

En la tabla mostrada anteriormente, se observa que los campos que conforman la estructura del mensaje Alerta, recibido por la aplicación (*Worker Role*), son iguales a los del planteamiento teórico expuesto en la sección de "Implementación" del Capítulo III. Además, se puede comprobar que los *tokens* (*DomoKit* y usuario) están asignados de acuerdo con el escenario de pruebas (Figura 37).

Telemetría

En el caso de los mensajes de Telemetría, se tiene la siguiente comparación:

Estructura del Mensaje – Planteamiento Teórico	Log capturado – Implementación real

Campos	Valor	Tipo
Message Type	1	2 bits
Device Token	ABCDEFGHIJK	String
User Token	ABCDEFGHIJK	String
Units	ABC	String
Value	0.0	Float

```
LOG EVENT: New Incoming Message 10/05/2015 10:19:32 a.m.
=========================================================
Message Type = 1                 ||  Type = Telemetría
User Token = LHUSer9dPZ          ||  User Id
Device Token = b8tVETNXNL        ||  Device Id
Units = ºC
Value= 19.3
```

Tabla 10 - Mensaje del tipo Telemetría [Elaboración Propia]

En la Tabla 10, se observa que la composición del mensaje es igual en ambos casos, tanto en el planteamiento teórico del Capítulo III como en la implementación real. Además, los *tokens* (usuario y *DomoKit*) están asignados de acuerdo al escenario de pruebas planteado (Figura 37).

Comando

En el caso de los mensajes del tipo Comando, se tiene la siguiente comparación:

Estructura del Mensaje – Planteamiento Teórico	Log capturado – Implementación real

Campos	Valor	Tipo
Message Type	2	2 bits
Device Token - Originated	ABCDEFGHIJK	String
Device Token - Destination	ABCDEFGHIJK	String
User Token	ABCDEFGHIJK	String
Command	1 / 0	1 bit
Time to Live (TTL)	00	0 < Integer < 120 segundos

```
LOG EVENT: New Incoming Message 10/05/2015 09:42:19 a.m.
=========================================================
Message Type = 2                          ||  Type = Comando
User Token = LHUSer9dPZ                   ||  User Id
Device Token Source = JbfnbY3qOx          ||  Mobile Device Id
Device Token Destination = b8tVETNXNL     ||  Device Id
Command = 1                               ||  Command = Enable
TTL = 30                                  ||  TTL < 120 segundos
```

Tabla 11 - Mensaje del tipo Comando [Elaboración Propia]

En la tabla mostrada anteriormente, se observa que los campos que conforman la estructura del mensaje Comando, recibido por la aplicación (*Worker Role*), son iguales a los del planteamiento teórico expuesto en la sección de "Implementación" del Capítulo III. Además, se puede comprobar que los *tokens* (usuario, *DomoKit* origen y destino) están asignados de acuerdo con el escenario de pruebas (Figura 37).

Ping

En el caso de los mensajes del tipo Ping, se tiene la siguiente comparación:

Estructura del Mensaje – Planteamiento Teórico	Log capturado – Implementación real

Campos	Valor	Tipo
Message Type	3	2 bits
Device Token	ABCDEFGHIJK	String
User Token	ABCDEFGHIJK	String
Stay Alive	1	1 bit

```
LOG EVENT: New Incoming Message 10/05/2015 09:45:30 a.m.
=========================================================
Message Type = 3                 ||  Type = Ping
User Token = LHUSer9dPZ          ||  User Id
Device Token = b8tVETNXNL        ||  Device Id
Stay Alive = 1                   ||  Value = True
```

Tabla 12 - Mensaje del tipo Ping [Elaboración Propia]

En la Tabla 12, se observa que la composición del mensaje es igual en ambos casos, tanto en el planteamiento teórico del Capítulo III como en la implementación real. Además, los *tokens* (usuario y *DomoKit*) están asignados de acuerdo al escenario de pruebas planteado (Figura 37).

2. Verificación del tiempo de envío de los mensajes

Telemetría / Ping

Para verificar el tiempo total que se toma el envío de un mensaje (extremo a extremo) se consideró el monitoreo de los registros de actividad de las aplicaciones (*Worker Rol*) de Telemetría y Ping dedicadas al procesamiento de la información. En la Figura 38, se presenta un gráfico con el escenario de pruebas.

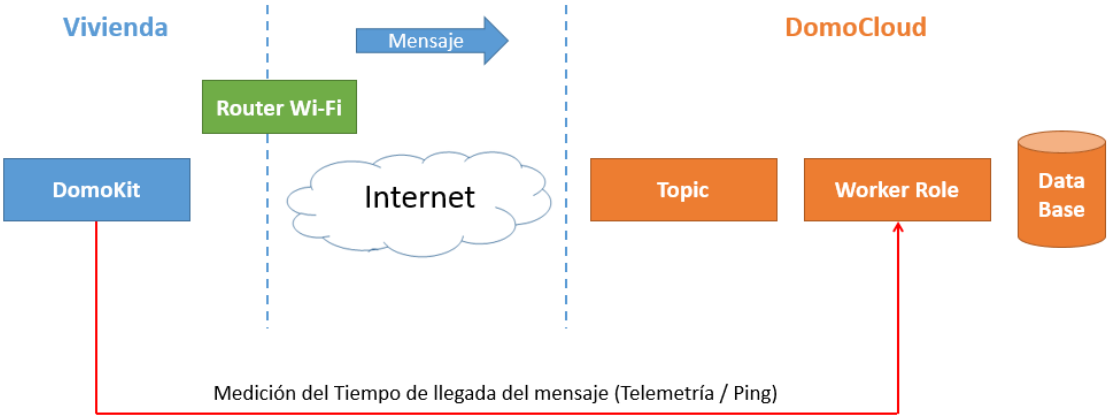


Figura 38 - Escenario de pruebas para verificar el tiempo de envío de los mensajes de Telemetría / Ping [Elaboración Propia]

En la figura anterior, se observa que el *DomoKit* envía un mensaje del tipo Telemetría o Ping a la aplicación, a través de Internet. Para calcular el valor se añadió un campo adicional en el protocolo de mensajería, que incluye la información del tiempo (*timestamp*) al momento de generar el mensaje (*DomoKit)* y al recibirlo (*Worker Rol).* La diferencia de los valores en el origen y el destino permitirán determinar el tiempo total que toma enviar el mensaje. A continuación, se muestran los resultados obtenidos.

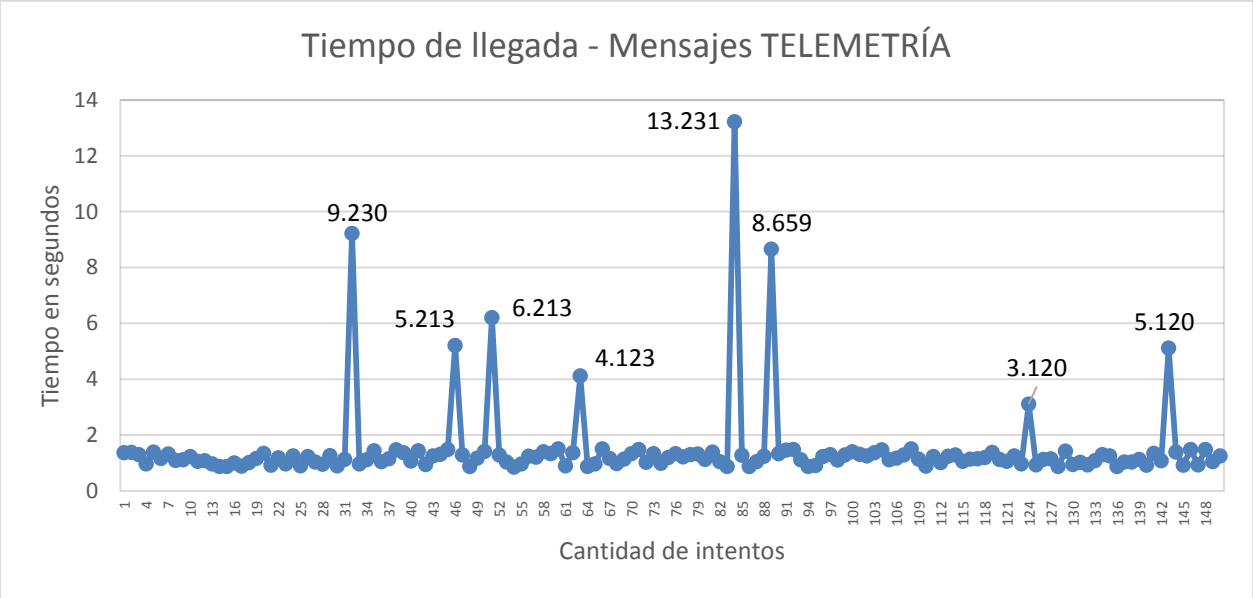


Figura 39 - Mensajes del tipo Telemetría [Elaboración Propia]

En la Figura 39, mostrada anteriormente, se observa que se ejecutaron 150 pruebas y en cada uno de los intentos se registró el tiempo total que toma el envío del mensaje del tipo telemetría. En la Tabla 13, se muestran el valor promedio, máximo y mínimo de los resultados obtenidos.

Promedio (s)	1.475
Valor Max (s)	13.231
Valor Min (s)	1.355

Tabla 13 - Resumen de resultados – Telemetría [Elaboración Propia]

De la tabla anterior, se observa que el tiempo promedio que toma el envío de un mensaje del tipo telemetría (extremo a extremo) es de 1.48 segundos.

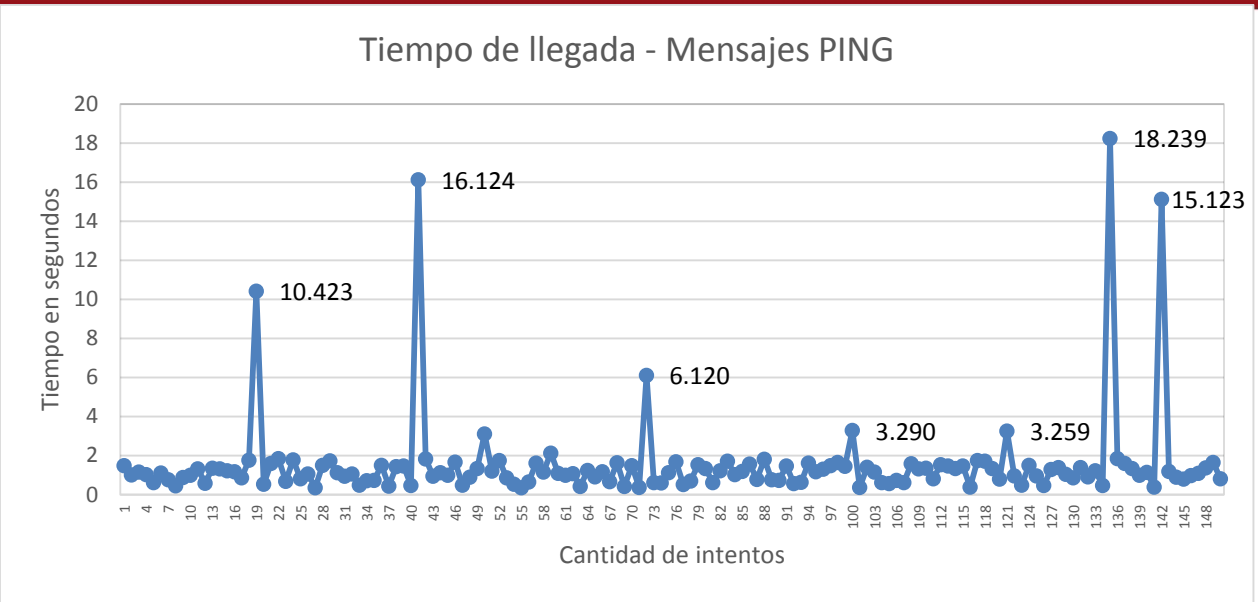


Figura 40 - Mensajes del tipo Ping [Elaboración Propia]

En la Figura 40, mostrada anteriormente, se observa que se ejecutaron 150 pruebas y en cada uno de los intentos se registró el tiempo total que toma el envío del mensaje del tipo Ping. En la Tabla 14, se muestran el valor promedio, máximo y mínimo de los resultados obtenidos.

Promedio (s)	1.544
Valor Max (s)	18.239
Valor Min (s)	0.364

Tabla 14 - Resumen de resultados – Ping [Elaboración Propia]

De la tabla anterior, se observa que el tiempo promedio que toma el envío de un mensaje del tipo ping (extremo a extremo) es de 1.54 segundos.

Alerta

Para verificar el tiempo total que se toma el envío de un mensaje (desde el *DomoKit* hasta el *DomoApp*) se consideró el monitoreo de los registros de actividad de la aplicación *DomoApp*. En la Figura 41, se presenta un gráfico con el escenario de pruebas.

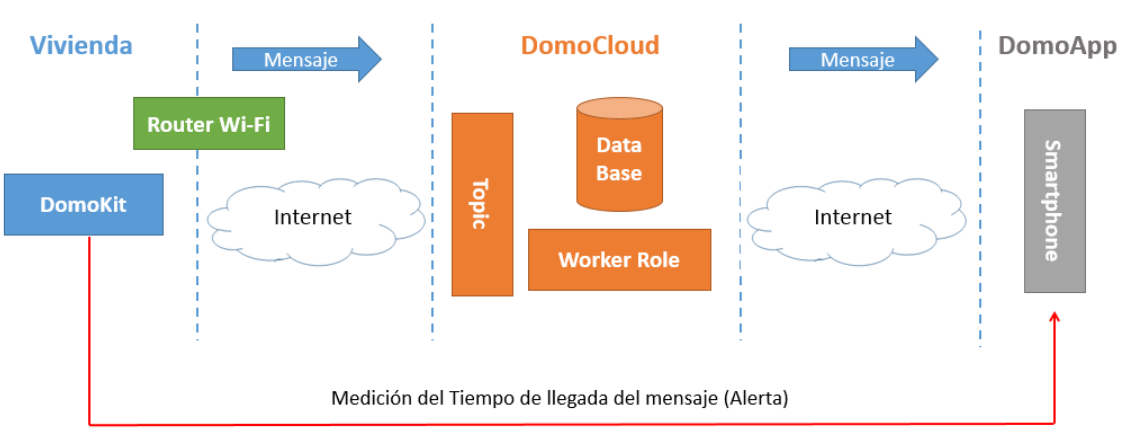


Figura 41 - Escenario de pruebas para verificar el tiempo de envío de los mensajes de Alerta [Elaboración Propia]

En la figura anterior, se observa que el *DomoKit* envía un mensaje del tipo Alerta al *DomoApp*, a través de Internet. Para calcular el valor se añadió un campo adicional en el protocolo de mensajería, que incluye la información del tiempo (*timestamp*) al momento de generar el mensaje (*DomoKit)* y al recibirlo (*DomoApp*).La diferencia entre los valores en el origen y el destino permitirán determinar el tiempo total que toma enviar el mensaje. A continuación, se muestran los resultados obtenidos.

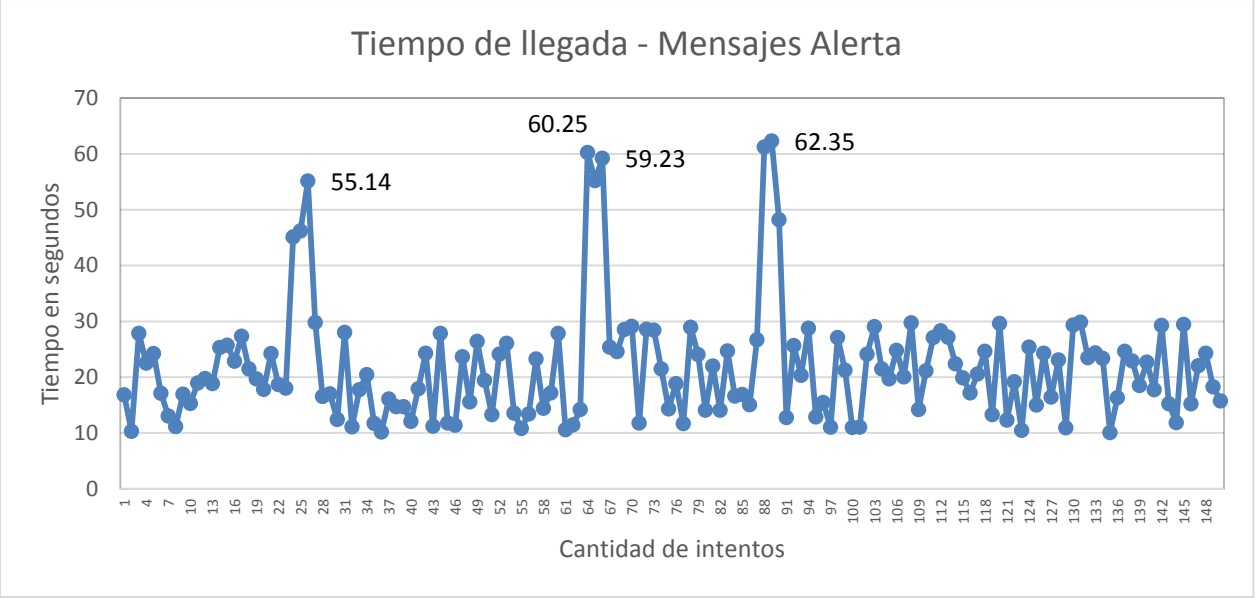


Figura 42 - Mensajes del tipo Alerta [Elaboración Propia]

En la Figura 42, mostrada anteriormente, se observa que se ejecutaron 150 pruebas y en cada uno de los intentos se registró el tiempo total que toma el envío del mensaje del tipo Alerta. En la Tabla 15, se muestran el valor promedio, máximo y mínimo de los resultados obtenidos.

Promedio (s)	21.80
Valor Max (s)	62.35
Valor Min (s)	10.10

Tabla 15 - Resumen de resultados – Alerta [Elaboración Propia]

De la tabla anterior, se observa que el tiempo promedio que toma el envío de un mensaje del tipo alerta (extremo a extremo) es de 21.8 segundos.

Comando

Para verificar el tiempo total que se toma el envío de un mensaje (desde el *DomoApp* hasta el *DomoKit*) se consideró el monitoreo de los registros de actividad de la aplicación *DomoKit*. En la Figura 43, se presenta un gráfico con el escenario de pruebas.

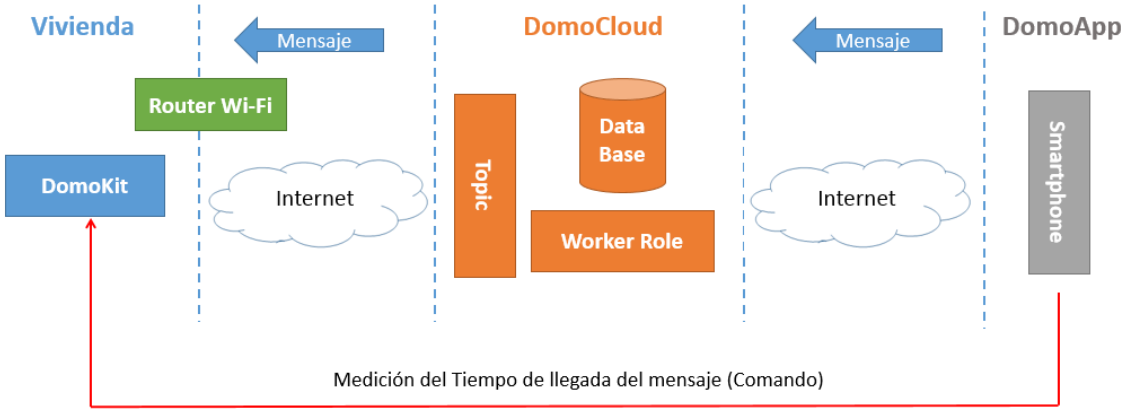


Figura 43 - Escenario de pruebas para verificar el tiempo de envío de los mensajes de Comando [Elaboración Propia]

En la figura anterior, se observa que el *DomoApp* envía un mensaje del tipo Comando al *DomoKit*, a través de Internet. Para calcular el valor se añadió un campo adicional en el protocolo de mensajería, que incluye la información del tiempo (*timestamp*) al momento de generar el mensaje (*DomoApp)* y al recibirlo (*DomoKit*).La diferencia entre los valores en el origen y el destino permitirán determinar el tiempo total que toma enviar el mensaje. A continuación, se muestran los resultados obtenidos.

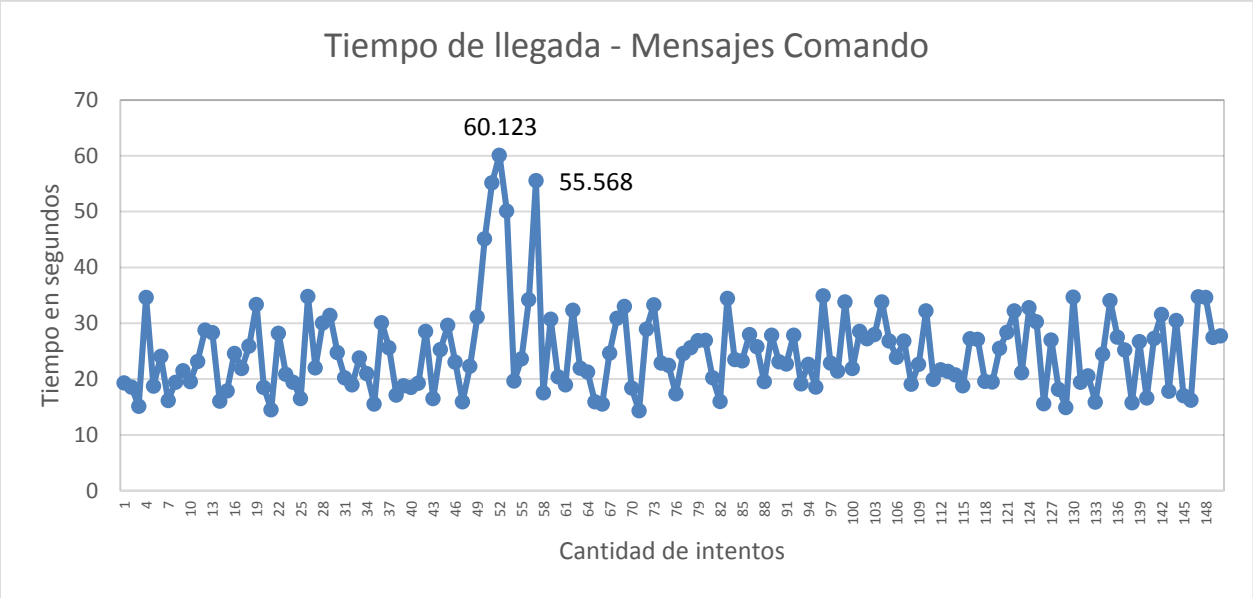


Figura 44 - Mensajes del tipo Comando [Elaboración Propia]

En la Figura 44, mostrada anteriormente, se observa que se ejecutaron 150 pruebas y en cada uno de los intentos se registró el tiempo total que toma el envío del mensaje del tipo Alerta. En la Tabla 16, se muestran el valor promedio, máximo y mínimo de los resultados obtenidos.

Promedio (s)	24.835
Valor Max (s)	60.123
Valor Min (s)	14.331

Tabla 16 - Resumen de resultados – Comando [Elaboración Propia]

De la tabla anterior, se observa que el tiempo promedio que toma el envío de un mensaje del tipo comando (extremo a extremo) es de 24.8 segundos.

De lo expuesto anteriormente, se concluye que el sistema funciona de acuerdo a lo esperado. En primer lugar, se verificó la implementación del protocolo de comunicación a través del monitoreo del tráfico que reciben las aplicaciones (*Worker Role*). En segundo lugar, se realizaron las mediciones del tiempo de viaje del mensaje (desde el origen hasta el destino) a través de pruebas experimentales. Para mensajes del tipo Ping se obtuvo un tiempo promedio de 1.54 segundos, para Telemetría 1.47 segundos, para mensajes del tipo Alerta 21.8 segundos y para mensajes del tipo Comando 24.8 segundos.

3. Análisis de riesgo informático

Esta sección tiene por objetivo identificar y evaluar los riesgos de la implementación del proyecto de tesis. Además, se presentarán propuestas de control para mitigar cada uno de los riesgos detectados. Para llevar a cabo esta tarea, se tomó como base la metodología planteada por el

National Institute of Standards and Technology Special Publication (NIST SP 800-30 Guide for Conducting Risk Assessments) [37] que comprende los procesos que se muestran en la siguiente figura.

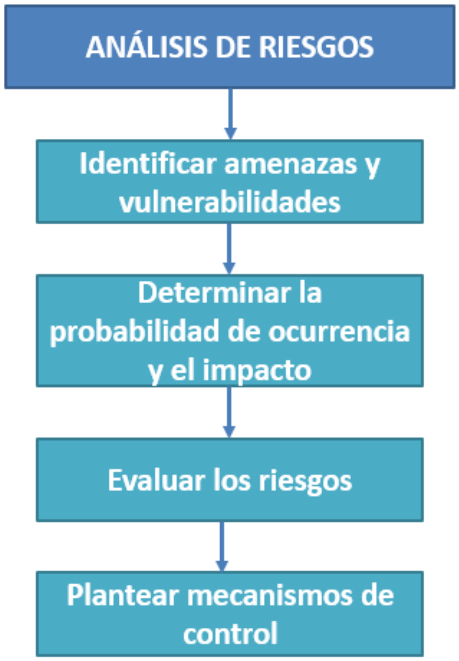


Figura 45 - Metodología análisis de riesgos (Adaptación de [37])

En la Figura 45, mostrada anteriormente, se presenta la metodología para realizar el análisis de riesgos del sistema DomoLab. Este método considera 4 etapas: identificar amenazar y vulnerabilidades, cuantificar el impacto y la probabilidad, evaluar los riesgos y plantear mecanismos para controlar los riesgos detectados.

A continuación, se desarrollarán cada uno de los procesos de la metodología.

Identificación de riesgos potenciales

En primer lugar, se identificarán los activos y las categorías de riesgo del sistema implementado. A continuación, se presenta la información detallada en las tablas (Tabla 17 y Tabla 18).

Categorías de activos		
Identificador	**Categoría**	**Ejemplo**
DK	Sensores, Actuadores conectados a internet	DomoKit
DC	Servidor en la nube (Cloud)	DomoCloud
TSA	APIs del DomoCloud	Topic, Suscripción, Autenticación
ST	Dispositivos móviles	Smartphones, Tablets
DA	Aplicación instalada en los dispositivos móviles	DomoApp
U	Usuarios	Usuarios del servicio

Tabla 17 - Categorías de activos del sistema DomoLab (Elaboración propia)

Categorías de riesgo	
Identificador	**Descripción**
H	Hardware
S	Software
I	Información
RC	Red / Conectividad
FU	Factor Humano

Tabla 18 - Categorías de riesgo (Elaboración propia)

En segundo lugar, se muestran las amenazas y vulnerabilidades asociadas a los activos del sistema y clasificadas por categoría de riesgo.

Hardware

Activos	Id	Amenaza	Vulnerabilidad
DomoKit	DK-1	Corte del suministro eléctrico	1. Falta de implementación de mecanismos de emergencia. Por ejemplo: UPS
	DK-2	Condiciones inadecuadas de temperatura o humedad	1. Uso de componentes electrónicos inadecuados para trabajar en ambientes con condiciones de temperatura o humedad irregular.
	DK-3	Fallo en el servicio de comunicaciones	1. Falta de implementación de redundancia de comunicaciones. Por ejemplo: Internet Fijo, Móvil

Tabla 19 - Amenazas y vulnerabilidades asociadas a la categoría Hardware (Elaboración Propia)

Software

Activos	Id	Amenaza	Vulnerabilidad
DomoKit	DK-4	Acceso no autorizado	1. Políticas de acceso y control inadecuadas 2. Bugs en los mecanismos de autenticación
DomoCloud	DC-1	Acceso no autorizado	1. Políticas de acceso y control inadecuadas 2. Bugs en los mecanismos de autenticación
	DC-2	Eventos del sistema no registrados en la base de datos	1. Bugs en el proceso encargado de registrar los eventos (logs) en la base de datos.
	DC-3	Denegación de Servicio	1. Configuración inadecuada del Firewall 2. Falta de implementación de redundancia
DomApp	DA-1	Acceso al sistema sin autorización	1. Incorrecta implementación de las políticas de autenticación (HTTP, SSL) 2. Bugs en los mecanismos de autenticación
	DA-2	Modificación de los parámetros del sistema sin autorización	1. Políticas de control y configuración inadecuadas
API DomoCloud	TSA-1	Acceso al sistema sin autorización	1. Políticas de acceso y control inadecuadas 2. Bugs en los mecanismos de autenticación

Tabla 20 - Amenazas y vulnerabilidades asociadas a la categoría Software (Elaboración Propia)

Información

Categorías	Id	Amenaza	Vulnerabilidad
DomoCloud	DC-4	Acceso al sistema sin autorización	1. Políticas de acceso y control inadecuadas 2. Bugs en los mecanismos de autenticación
	DC-5	Manipulación, alteración o divulgación de la información del sistema	1. Políticas de control y configuración inadecuadas
	DC-6	Pérdida de la información del sistema	1. Políticas de back-up inadecuadas 2. Falta de implementación de redundancia
Dispositivos Móviles	ST-1	Acceso al sistema sin autorización	1. Incorrecta implementación de las políticas de autenticación (HTTP, SSL) 2. Bugs en los mecanismos de autenticación
	ST-2	Manipulación, alteración o divulgación de la información del sistema	1. Políticas de control y configuración inadecuadas

Tabla 21 - Amenazas y vulnerabilidades asociadas a la categoría Información (Elaboración Propia)

Red/Conectividad

Activos	Id	Amenaza	Vulnerabilidad
DomoKit	DK-5	Manipulación, alteración o interceptación de la información durante la transmisión / recepción	1. Políticas de control y autenticación inadecuadas 2. Uso de protocolos inseguros para transportar la información
	DK-6	Caída del sistema por sobrecarga	1. Cálculo inadecuado del tráfico de información 2. Uso de equipamiento de conectividad de red inadecuado para el volumen de información.
DomoCloud	DC-7	Manipulación, alteración o interceptación de la información durante la transmisión / recepción	1. Políticas de control y autenticación inadecuadas 2. Uso de protocolos inseguros para transportar la información
	DC-8	Caída del sistema por sobrecarga	1. Cálculo inadecuado del tráfico de información 2. Uso de equipamiento de conectividad de red inadecuado para el volumen de información.

Tabla 22 - Amenazas y vulnerabilidades asociadas a la categoría Red / Conectividad (Elaboración Propia)

Factor Humano

Activos	Id	Amenaza	Vulnerabilidad
Usuario	U-1	Distribución o divulgación de información confidencial del sistema	1. Personal de mantenimiento descontento 2. Mal uso de las cuentas de acceso con privilegios de administrador
	U-2	Vulnerar los mecanismos de autenticación	1. Configuración o uso de contraseñas poco seguras por parte del usuario final
	U-3	Ingeniería social	1. Ingenuidad del usuario
Dispositivo Móvil	ST-1	Manipulación, alteración o interceptación de la información durante la transmisión	1. Instalación de aplicaciones maliciosas en el Smartphone o Tablet por parte del usuario final

Tabla 23 - Amenazas y vulnerabilidades asociadas a la categoría Factor humano (Elaboración Propia)

En las tablas mostradas anteriormente, se presentaron las amenazas y vulnerabilidades asociadas a los activos del sistema DomoLab. En la siguiente etapa, se procederá a cuantificar la probabilidad de ocurrencia y el impacto de cada una.

Cálculo de la probabilidad de ocurrencia y el impacto

En primer lugar, para cuantificar los riesgos identificados en la etapa previa, es necesario determinar los niveles de impacto y probabilidad. A continuación, se especificarán dichos criterios.

Escala de impacto		
Valor	**Nivel**	**Consecuencias**
1	Insignificante	No afecta el funcionamiento del sistema
2	Marginal	Afecta de forma leve al sistema pero es tolerable
5	Grave	Afecta de forma parcial al sistema pero no pone en peligro su funcionamiento
10	Crítico	Afectan parcialmente el funcionamiento del sistema
20	Desastroso	Afectan totalmente el funcionamiento del sistema
50	Catastrófico	Afectan totalmente el funcionamiento del sistema y no es posible restablecer el funcionamiento

Tabla 24 - Escala de impacto del riesgo [38]

Escala de probabilidad		
Valor	**Grado**	**Significado**
1	Improbable	Riesgo no ha sucedido hasta ahora Difícil que ocurra
2	Remoto	Riesgo ha sucedido excepcionalmente Probabilidad de ocurrencia muy baja
3	Ocasional	Riesgo ha sucedido pocas veces Baja posibilidad de ocurrencia
4	Moderado	Riesgo ha sucedido de forma esporádica Limitada posibilidad de ocurrencia
5	Frecuente	Riesgo sucede algunas veces Significativa posibilidad de ocurrencia
6	Constante	Riesgo sucede reiteradas veces Alta posibilidad de ocurrencia

Tabla 25 - Escala de probabilidad del riesgo [38]

En segundo lugar, se definirá la fórmula con la que se podrá calcular el valor del riesgo identificado tal como se muestra a continuación, en la Ecuación 1.

$$\boldsymbol{Riesgo = Impacto\ x\ Probabilidad}$$

Ecuación 1 - Cálculo del riesgo [38]

Adicionalmente, se presenta la fórmula para escalar estos valores y convertirlos a un porcentaje.

$$\% = \frac{\boldsymbol{Riesgo}}{\boldsymbol{Máx.Impacto\ x\ Máx.Probabilidad}}$$

Ecuación 2 - Conversión del riesgo a porcentaje (Elaboración propia)

Finalmente, se muestra el cálculo del riesgo de cada una de las amenazas y vulnerabilidades identificadas en la etapa previa.

Categoría	Id	Amenaza	Impacto	Probabilidad	Riesgo	%
Hardware	DK-1	Corte del suministro eléctrico	20	4	80	27%
	DK-2	Condiciones inadecuadas de temperatura o humedad	5	3	15	5%
	DK-3	Fallo en el servicio de comunicaciones	20	4	80	27%
Software	DK-4	Acceso no autorizado	10	2	20	7%
	DC-1	Acceso no autorizado	10	1	10	3%
	DC-2	Eventos del sistema no registrados en la base de datos	2	2	4	1%
	DC-3	Denegación de Servicio	20	1	20	7%
	DA-1	Acceso al sistema sin autorización	10	2	20	7%
	DA-2	Modificación de los parámetros del sistema sin autorización	10	2	20	7%
	TSA-1	Acceso al sistema sin autorización	10	1	10	3%
Información	DC-4	Acceso al sistema sin autorización	10	1	10	3%
	DC-5	Manipulación, alteración o divulgación de la información del sistema	10	1	10	3%
	DC-6	Pérdida de la información del sistema	20	1	20	7%
	ST-1	Acceso al sistema sin autorización	10	2	20	7%
	ST-2	Manipulación, alteración o divulgación de la información del sistema	10	2	20	7%
Red / Conectividad	DK-5	Manipulación, alteración o interceptación de la información durante la transmisión / recepción	10	2	20	7%
	DC-7	Manipulación, alteración o interceptación de la información durante la transmisión / recepción	10	1	10	3%
Factor Humano	U-1	Distribución o divulgación de información confidencial del sistema	10	2	20	7%
	U-2	Vulnerar los mecanismos de autenticación	10	5	50	17%
	U-3	Ingeniería social	10	5	50	17%
	ST-3	Manipulación, alteración o interceptación de la información durante la transmisión	10	4	40	13%

Tabla 26 - Cálculo del riesgo (Elaboración propia)

Evaluación de los riesgos

En primer lugar, para evaluar los riesgos identificados en la etapa previa, es necesario determinar el nivel de tolerancia. A continuación, se especificará dicho criterio tomando como referencia lo expuesto en [38].

Niveles de tolerancia		
Zona	**% Vulnerabilidad**	**Significado**
Aceptable	Hasta 3%	No requiere acciones adicionales
Tolerable	Desde 3.1% hasta 5%	Acciones de control con prioridad de segundo nivel
Inaceptable	Desde 5% hasta 25%	Acciones de control prioritarias a corto plazo
Inadmisible	Más de 25%	Acciones de control con alta prioridad, ejecutadas inmediatamente

Tabla 27 - Niveles de tolerancia del riesgo [38]

En segundo lugar, se clasificarán los riesgos identificados tomando en cuenta el valor cuantitativo calculado previamente. A continuación, se muestra la Figura 46 que será denominada perfil de riesgos del sistema.

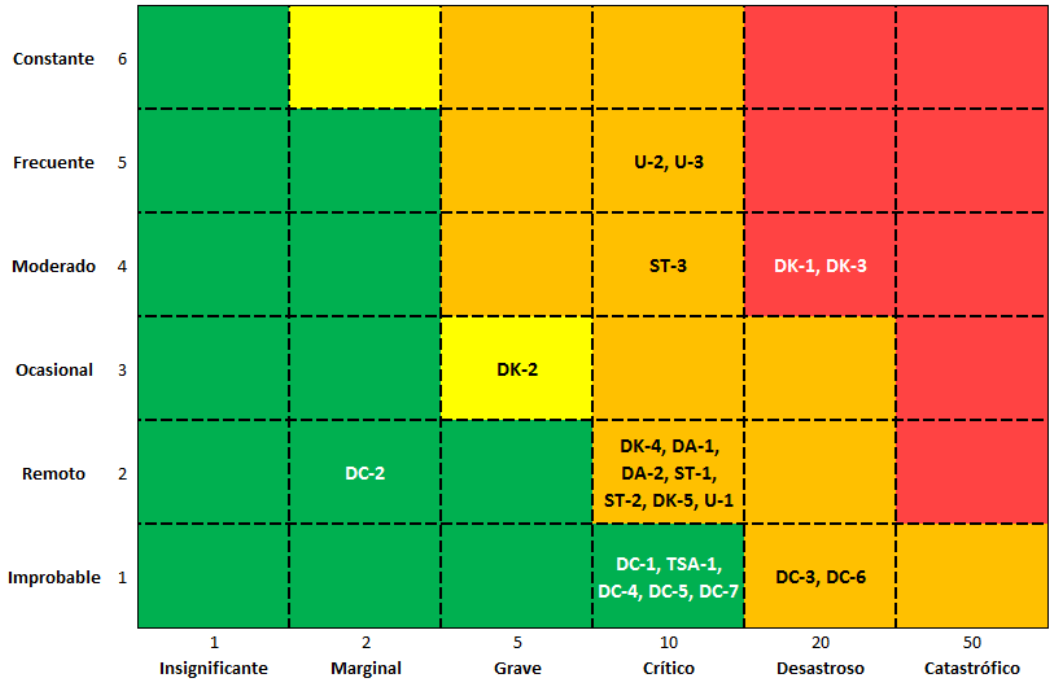


Figura 46 - Perfil de riesgos del sistema (Elaboración propia)

Tomando como referencia la figura mostrada anteriormente, en la siguiente etapa, se plantearán los mecanismos de control para los riesgos que se encuentran clasificados en los niveles inaceptable e inadmisible.

Control

A continuación, se plantearán los mecanismos de control para cada uno de los riesgos identificados.

Categoría	Id	Amenaza	Vulnerabilidad	Control
Hardware	DK-1	Corte del suministro eléctrico	1. Falta de implementación de mecanismos de emergencia. Por ejemplo: UPS	- Establecer mecanismos de notificación (alerta alta prioridad) al Smartphone del usuario, en caso se pierda la comunicación con el DomoKit. - El uso de un UPS implica un costo adicional elevado. Este riesgo se puede mitigar si el usuario obtiene la información en tiempo real y puede ejecutar sus propios mecanismos de protección.
	DK-2	Condiciones inadecuadas de temperatura o humedad	1. Uso de componentes electrónicos inadecuados para trabajar en ambientes con condiciones de temperatura o humedad irregular.	- Verificar el nivel de tolerancia y operación de los componentes electrónicos que componen el DomoKit.
	DK-3	Fallo en el servicio de comunicaciones	1. Falta de implementación de redundancia de comunicaciones. Por ejemplo: Internet Fijo, Móvil	- Establecer mecanismos de notificación (alerta alta prioridad) al Smartphone del usuario, en caso se pierda la comunicación con el DomoKit. - El mantenimiento de una conexión adicional es costoso. Este riesgo se puede mitigar si el usuario obtiene la información en tiempo real y puede ejecutar sus propios mecanismos de protección.
Software	DK-4	Acceso no autorizado	1. Políticas de acceso y control inadecuadas 2. Bugs en los mecanismos de autenticación	- Realizar pruebas en la aplicación DomoKit para verificar y garantizar el funcionamiento del mecanismo de autenticación.
	DC-3	Denegación de Servicio	1. Configuración inadecuada del Firewall 2. Falta de implementación de redundancia	- Configuración del firewall, monitoreo de las políticas de conectividad, redundancia física de los servidores DomoCloud.
	DA-1	Acceso al sistema sin autorización	1. Incorrecta implementación de las políticas de autenticación (HTTP, SSL) 2. Bugs en los mecanismos de autenticación	- Realizar pruebas en la aplicación DomoApp para verificar y garantizar el funcionamiento del mecanismo de autenticación.
	DA-2	Modificación de los parámetros del sistema sin autorización	1. Políticas de control y configuración inadecuadas	- Revisar el plan de asignación de privilegios a las cuentas de usuario. Restringir los permisos de las cuentas de usuario.
Información	DC-6	Pérdida de la información del sistema	1. Políticas de back-up inadecuadas 2. Falta de implementación de redundancia	- Implementar políticas de back-up en los servidores de Microsoft Azure.
	ST-1	Acceso al sistema sin autorización	1. Incorrecta implementación de las políticas de autenticación (HTTP, SSL) 2. Bugs en los mecanismos de autenticación	- Realizar pruebas en la aplicación DomoApp para verificar y garantizar el funcionamiento del mecanismo de autenticación.
	ST-2	Manipulación, alteración o divulgación de la información del sistema	1. Políticas de control y configuración inadecuadas	- Revisar el plan de asignación de privilegios a las cuentas de usuario. Restringir los permisos de las cuentas de usuario.

Tabla 28 -Mecanismos de control - Categoría de riesgos: Hardware, Software e Información (Elaboración propia)

Categoría	Id	Amenaza	Vulnerabilidad	Control
Red / Conectividad	DK-5	Manipulación, alteración o interceptación de la información durante la transmisión / recepción	1. Políticas de control y autenticación inadecuadas 2. Uso de protocolos inseguros para transportar la información	- Establecer mecanismos de encriptación y cifrado de la información que se intercambiará a través de Internet.
Factor Humano	U-1	Distribución o divulgación de información confidencial del sistema	1. Personal de mantenimiento descontento 2. Mal uso de las cuentas de acceso con privilegios de administrador	- Políticas de recursos humanos especiales para mantener buena relación con el personal de mantenimiento. - Firma de acuerdos de confidencialidad con el personal.
	U-2	Vulnerar los mecanismos de autenticación	1. Configuración o uso de contraseñas poco seguras por parte del usuario final	- Forzar el uso de contraseñas complejas en las cuentas de usuario (Política general)
	U-3	Ingeniería social	1. Ingenuidad del usuario	- Ejecutar planes de capacitación / educación para el usuario final.
	ST-3	Manipulación, alteración o interceptación de la información durante la transmisión	1. Instalación de aplicaciones maliciosas en el Smartphone o Tablet por parte del usuario final	

Tabla 29 - Mecanismos de control - Categoría de riesgos: Red / Conectividad y Factor Humano (Elaboración propia)

De lo expuesto anteriormente, se puede concluir que la metodología planteada por el NIST (SP 800-30) [37], ayudó a detectar amenazas y vulnerabilidades en el sistema implementado. Estos riesgos se pueden mitigar a través de la ejecución de los mecanismos de control planteados anteriormente.

CAPÍTULO V

PLAN DE NEGOCIOS

El presente capítulo tiene como objetivo presentar el desarrollo de un plan de negocios para demostrar la viabilidad comercial de la solución descrita en el CAPÍTULO III. Por ello, se considerará el análisis del mercado, el desarrollo de los planes de marketing y finanzas.

1. Análisis del mercado

El mercado a analizar es Lima Metropolitana, ya que concentra la mayor cantidad de hogares que poseen conexión a Internet, recurso vital para la instalación y uso del producto. En la siguiente Tabla 30, se calculará el mercado potencial tomando como referencia un estudio de IPSOS Apoyo (2013) [39] sobre la cantidad de hogares y conexión a Internet en Lima Metropolitana.

Segmento	Cantidad de Hogares	Conexión a Internet	Mercado Potencial
A	123,994	96%	119,034
B	441,132	80%	352,906
C	915,646	65%	595,170
D	722,502	27%	195,076
E	181,222	13%	23,559
Total	**2,384,496**	**-**	**1,285,744**

Tabla 30- Cantidad de hogares y conexiones a Internet por nivel socioeconómico [39]

En la tabla mostrada anteriormente (Tabla 30), se observa que el mercado potencial es de 1, 067, 110 hogares que pertenecen a los sectores A, B y C. Actualmente, el mercado de Lima metropolitana es atendido por cuatro compañías:

- Prosegur
- Clave 3
- Boxer
- BTicinno

2. Análisis del cliente

Respecto al perfil del cliente, de acuerdo con la información de un especialista en análisis de mercados [40], el consumidor de este tipo de productos tiene las siguientes características:

- Estabilidad económica
- Cuentan con objetos de valor y tienen la necesidad de protegerlos
- Sienten inseguridad en su distrito

En lo referente a la composición del mercado, el especialista [40] señala que en el sector A la penetración es de 4%, y en el B es de 1% en Lima Metropolitana. Si se emplea la información del estudio de IPSOS Apoyo, se puede estimar la cantidad de hogares que poseen un servicio o producto domótico. En la Tabla 31, se muestran los resultados.

Segmento	Cantidad de Hogares	% Penetración	Mercado Atendido
A	123,994	5%	6,200
B	441,132	1%	4,411
C	915,646	0%	-
D	722,502	0%	-
E	181,222	0%	-
Total	2,384,496	-	10,611
% Penetración Total			**0.45%**

Tabla 31 - Estimación del mercado actual de productos domóticos - Lima Metropolitana [Elaboración Propia]

De la tabla anterior, se puede calcular que el mercado atendido (hogares que cuentan con un servicio de monitoreo y/o seguridad) es de 10,611 viviendas. Este valor representa menos del 1% del total de viviendas de Lima Metropolitana.

Además, se puede realizar una estimación adicional sobre el mercado potencial combinando la información expuesta en las tablas mostradas anteriormente (Tabla 30 y Tabla 31). A continuación, se presentarán los resultados.

Segmento	Cantidad de Hogares	% Conexión a Internet	Mercado Total	Mercado Atendido	Mercado Potencial
A	123,994	96%	119,034	6,200	112,835
B	441,132	80%	352,906	4,411	348,494
C	915,646	65%	595,170	-	595,170
D	722,502	27%	195,076	-	-
E	181,222	13%	23,559	-	-
Total	2,384,496	-	1,285,744	10,611	1,275,133

Tabla 32 - Estimación del mercado potencial de productos domóticos - Lima Metropolitana [Elaboración Propia]

De acuerdo con lo expuesto en la Tabla 32, el mercado potencial es de 1, 275,133 hogares de Lima Metropolitana los cuales pertenecen a los sectores socioeconómicos A, B y C.

3. Análisis de los competidores

Como se mencionó anteriormente, existen cuatro compañías consideradas como los principales competidores en el mercado de Lima Metropolitana. Estas compañías son Prosegur, Clave 3, Boxer y BTicinno. A continuación, se presenta una tabla comparativa (Tabla 33) que considera algunos atributos del producto como el precio, los canales de distribución y la ubicación geográfica.

Competidores	Producto	Precio	Distribución	Ubicación
Bóxer	Alarma Monitoreo	Sistema: S/. 1,500 Monitoreo Mensual: S/.70	Venta Directa Consultoría por cliente	Análisis en Lima Metropolitana
Clave 3	Alarma Monitoreo Aplicación Móvil	Sistema: S/. 1,800 Monitoreo Mensual: S/.100	Venta Directa Consultoría por cliente	
Prosegur	Alarma Monitoreo Aplicación Móvil	Sistema: S/. 2,300 Monitoreo Mensual: S/.100	Venta Directa Consultoría por cliente	
Bticinno	Alarma Aplicación Móvil	Sistema: S/. 3,800	Venta Directa Consultoría por cliente	

Tabla 33 - Mercado Actual – Competidores [Elaboración Propia]

4. Plan de marketing

Estrategia de producto

Empaque

Estará diseñado para contener cada uno de los elementos que componen el *DomoKit*, distribuidos de forma ordenada. Se ha considerado el uso de una maleta con divisiones, tal como se muestra en la Figura 47. Además, se incluirá documentación impresa como el certificado de garantía, el manual de configuración, una guía rápida de uso e información sobre los datos de contacto para solicitar asistencia técnica.

Figura 47 - Empaque de *Domokit* [41]

Proceso de venta

Para determinar el canal de comercialización del producto, se realizó una encuesta [42] (Resultados adjuntos en el ANEXO I – ENCUESTA) a un grupo de 150 personas y en los resultados se observó que más del 90% de entrevistados prefería adquirir este tipo de productos a través de tiendas por departamento (Saga Falabella, Ripley, etc.). Por ello, para comercializar el producto se aprovechará la infraestructura de las principales cadenas de tiendas por departamento. El *DomoKit* estará distribuido en un total de 16 tiendas seleccionadas de acuerdo al segmento socioeconómico objetivo. A continuación, se mostrará la lista de tiendas.

Saga Falabella	Ripley
Angamos → Av. Angamos Este 1803 (Angamos Open Plaza), Surquillo	Primavera → Av. Aviación y Angamos Oeste, San Borja
Atocongo→Av. Circunvalación (Open Plaza), San Juan de Miraflores	Chorrillos → Av. Paseo de la República S/N – Chorrillos
Jockey Plaza → Av. Javier Prado Este 4200 (Jockey Plaza), Santiago de Surco	Jockey Plaza → Av. Javier Prado Este 4200 (Jockey Plaza), Santiago de Surco
Miraflores → Av. Arequipa 5280, Miraflores	Miraflores → Av. Shell Nro. 202 – Miraflores.
San Isidro → Av. Paseo de la República 3220, San Isidro	San Isidro → Calle Begonias Nro. 577 – San Isidro
San Miguel → Av. La Marina 2100 (Plaza San Miguel), San Miguel	San Miguel → Av. Universitaria S/N Urb. Pando, San Miguel
Mega Plaza → Av. Industrial 3515 (MegaPlaza), Independencia	Plaza Norte → Av. Alfredo Mendiola Nro. 1400 – Independencia.
Lima →Jr. de la Unión 517, Lima Cercado	Nuevo San Juan → Canto Grande – Flores – SJL

Tabla 34 - Lista de tiendas seleccionadas para comercializar el producto [Elaboración Propia]

Adicionalmente, se implementarán módulos de experiencia para que el usuario pueda interactuar con el producto. En cada uno de estos puntos, se contará con dos asesores de venta, encargados de explicar las características, beneficios y ventajas del sistema *DomoKit*.

Estrategia de producto

Para establecer la estrategia de precios, se consideró tres criterios. En primer lugar, se analizaron los resultados de una encuesta de elaboración propia. En segundo lugar, se examinaron los costos de producción, distribución y el margen de ganancia. Finalmente, se desarrolló un comparativo de precios con los productos de la competencia que se comercializan actualmente.

Se realizó una encuesta [42] (Resultados adjuntos en el ANEXO I – ENCUESTA) a un grupo de 150 personas y una de las preguntas fue: *¿Cuál es el precio que está dispuesto a pagar por un producto que permita el control remoto de algunos elementos del hogar a través de su Smartphone? Además, dicho producto permitirá recibir notificaciones de alerta en caso de alguna incidencia en la vivienda.*

A continuación, se muestran los resultados en la Figura 48.

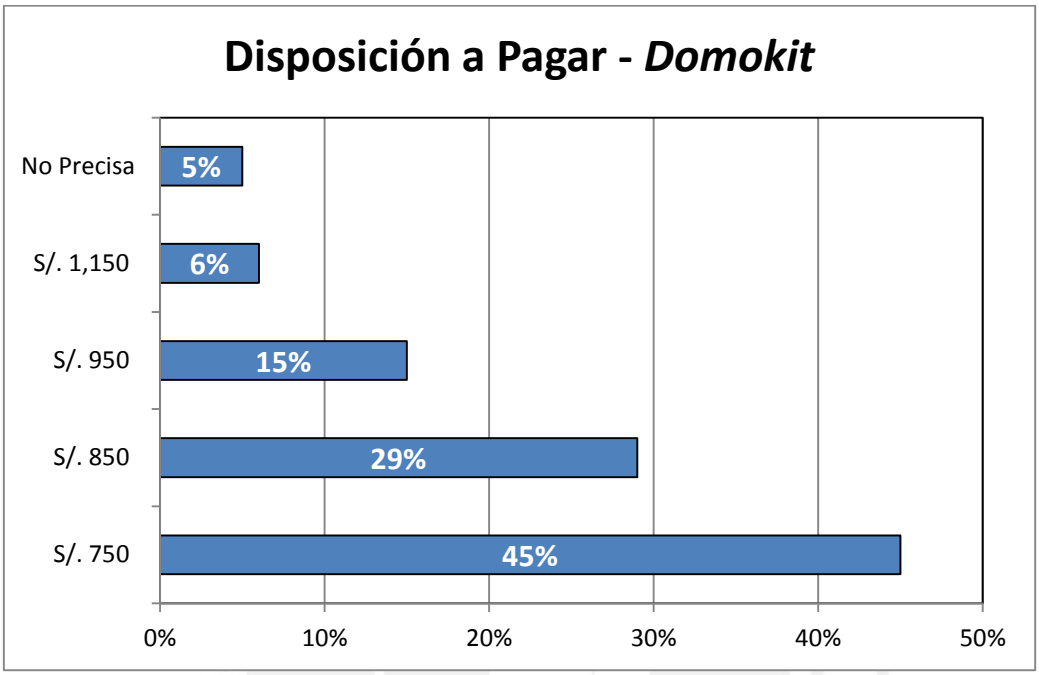


Figura 48 - Resultados de la encuesta - Disposición a pagar por el producto [Elaboración Propia]

Del gráfico anterior, se observa que el 45% de los entrevistados está dispuesto a pagar S/. 750 Nuevos Soles y que el 29% pagaría S/. 850 Nuevos Soles.

Por otra parte, en la Tabla 35, se puede observar la composición del precio considerando los costos de producción, margen, publicidad y distribución del producto.

Concepto	Monto
Costo Neto	S/. 400
Margen (30%)	S/.120
Publicidad (10%)	S/.40
Distribución (2%)	S/.8
Precio de Venta al Canal	**S/.568**
Margen del canal (12%)	S/.68
IGV (18%)	S/.115
Precio de Venta - Usuario Final	**S/.751**

Tabla 35 - Precio de Venta - Usuario Final [Elaboración Propia]

Respecto a la comparación de los precios con los principales competidores, se muestra la siguiente figura (Figura 49) que permitirá explicar el escenario actual de manera gráfica.

Figura 49 - Escala de Precios – Competidores [43] [44] [45]

Finalmente, luego de analizar las preferencias del usuario final, la estructura de costos y el posicionamiento versus los principales competidores, se llegó a la conclusión que el precio de venta sugerido al público será de S/. 751 Nuevos Soles. Cabe mencionar que el precio de venta a los distribuidores es de S/. 568 Nuevos Soles y para calcular el precio de venta al público se debe considerar un margen de canal de 12% y un recargo del 18% por concepto de impuesto general de ventas.

Estrategia de distribución

Como se mencionó anteriormente el producto se comercializará a través de las cadenas de tiendas por departamento. Por ello, se firmará un contrato de distribución y comercialización con Saga Falabella y Ripley. De acuerdo con el especialista, si se comercializan productos de electrónica de consumo a través del canal *retail*, se tiene que considerar un margen de 12% sobre el precio de venta en el contrato [46]. Por otra parte, se seleccionó un total de dieciséis tiendas, tal como se mostró anteriormente en la Tabla 34.

A continuación, se presentan las ventajas y desventajas del uso de este modelo de distribución.

Ventajas

- Se aprovechará la infraestructura con la que cuentan las cadenas de tiendas por departamento.

- El posicionamiento de las cadenas por departamento permitirá que el producto llegue al público objetivo.
- Las tiendas seleccionadas se encuentran ubicadas en Lima Metropolitana y garantizan gran afluencia de público.

Desventajas

- El distribuidor cuenta con un gran poder de negociación y puede establecer condiciones de *revenue share* elevadas.

Estrategia de publicidad y promoción

Respecto a las actividades de publicidad, se consideraron los siguientes aspectos:

Campaña de publicidad On-Line

Se utilizarán las redes sociales para la difusión de videos, gráficas que muestren en el concepto, funcionamiento y beneficios del producto. Para ello, se utilizarán banners y anuncios de Facebook.

Figura 50 - Medios de publicidad On-Line [47]

A continuación, se muestra una tabla (Tabla 36) que incluye el costo y la cobertura de la publicidad en dicha red social (Tipo de cambio referencial [48]).

Periodo	4 semanas
Coberura	
Visitas	50,000
Impresiones - Visibilidad Publicaciones	300,000
Click	20,000
Costo Mensual Dolares	$2,500
Tipo de Cambio	S/. 3.10
Costo mensual Soles	S/. 7,750

Tabla 36 - Costo mensual de publicidad On-Line [Elaboración Propia]

Tomando como referencia la información presentada anteriormente, se asignará un presupuesto de S/. 7, 750 Nuevos Soles mensuales para anunciar en medios on-line.

Catálogos

Se incluirá información del producto *DomoKit* en los catálogos de las tiendas por departamento donde se comercializará el producto.

Figura 51 – Catálogos [49] [50] [51]

En la siguiente Tabla 37, se muestra el costo de las publicaciones en los catálogos de Saga Falabella y Ripley. Se promocionará el producto en ambos catálogos que se publican trimestralmente (Tipo de cambio referencial [48]).

Catálogo media página Dólares		$3,300
Tipo de Cambio	S/.	3.10
Costo Publicación Soles	S/.	10,230
Publicaciones por trimestre		2
Costo por trimestre Soles	S/.	20,460

Tabla 37 - Costo trimestral de la publicidad en catálogos [Elaboración Propia]

Tomando como referencia la información mostrada anteriormente, se asignará un presupuesto de S/. 20,460 Nuevos Soles trimestrales para anunciar en este medio.

Periódicos y Revistas

Se publicarán anuncios en los principales medios de comunicación escrita como El Comercio, y la Revista Somos.

Figura 52 - Periódicos y Revistas [52] [53]

Para publicar un anuncio de media página en El Comercio y la revista Somos, se necesita un presupuesto de USD 5,500 Dólares Americanos por publicación. Se considera que durante un trimestre se anunciará dos veces en El Comercio y una vez en la revista Somos. A continuación, se presenta una tabla (Tabla 38) que incluye el costo total de las publicaciones (Tipo de cambio referencial [48]).

Costo Publicación media página Dólares		$5,500
Tipo de Cambio	S/.	3.10
Costo Publicación Soles	S/.	17,050
Publicaciones por trimestre		3
Costo por trimestre Soles	S/.	51,150

Tabla 38 – Costo trimestral de las publicaciones en periódicos y revistas [Elaboración Propia]

Se asignará un presupuesto trimestral de S/. 51, 150 Nuevos Soles para anunciar en medios escritos (periódicos y revistas).

Estrategia de ventas

Como se mencionó anteriormente, el producto se venderá a través de las cadenas de tiendas por departamento (Saga Falabella y Ripley). Se seleccionaron dieciséis tiendas y, en cada una de ellas, se colocará un módulo de experiencia para que los usuarios puedan experimentar los beneficios y ventajas del producto. Cabe resaltar que en cada uno de los puntos habrá dos consultores responsables de explicar los beneficios del *DomoKit*.

Proyección de ventas

La empresa tiene como objetivo conseguir el 10% de participación de mercado durante los primeros cinco años de operación.

Mercado Potencial	1,275,133
Mercado Objetivo (10%)	127,513

Tabla 39 -Mercado objetivo al final de los 5 primeros años de operación [Elaboración Propia]

Se estima que gracias a la inversión en publicidad (on-line, periódicos, revistas y catálogos) y a la preparación del punto de venta (implementación de módulos de experiencia, material impreso, consultores de venta) se podrá lograr el objetivo planteado. A continuación, en la Figura 53, se presenta la proyección de ventas en los primeros cinco años de operación.

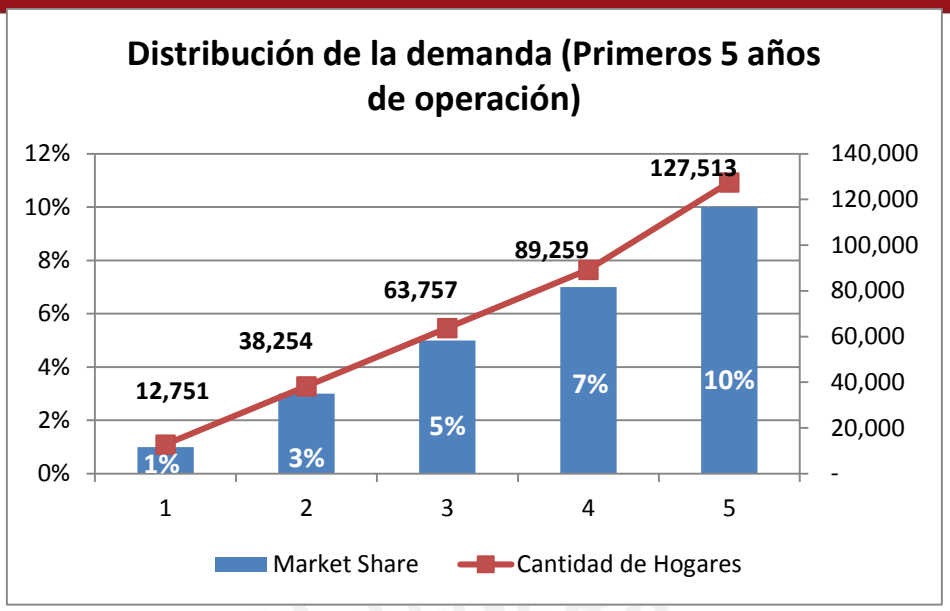


Figura 53 - Distribución de la demanda – Primeros 5 años de operación [Elaboración Propia]

5. Plan de finanzas

A continuación, se presentará el cálculo del flujo de caja. Para ello, se consideró los siguientes criterios:

Ingresos

Para calcular los ingresos en los primeros cinco años de operación, se considerará la proyección de ventas en ese periodo de tiempo. Se multiplicará la demanda por el precio de venta al canal.

En la Tabla 40, se muestra el cálculo de los primeros cinco años de operación.

Mercado Potencial	1,275,133
Precio Venta Canal	568

Años	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Market Share		1%	3%	5%	7%	10%
Mercado	-	12,751	38,254	63,757	89,259	127,513
Demanda		12,751	25,503	38,254	51,005	76,508
Ingresos	-	**S/. 7,242,755**	**S/. 14,485,511**	**S/. 21,728,266**	**S/. 28,971,022**	**S/. 43,456,533**

Tabla 40 - Cálculo de los Ingresos [Elaboración Propia]

Costos Operativos

Los costos operativos están compuestos por el Alquiler de almacén y oficinas, pago de los salarios del personal, costo del producto, gastos de marketing, hosting y servicios básicos. A continuación, se mostrará el detalle de cada concepto. Cabe resaltar que para realizar los cálculos, se tomó como referencia un tipo de cambio de S/. 3.10 Nuevos Soles equivalente a 1.00 USD Dólares Americanos [48].

Alquiler de almacén y oficinas

El almacén y las oficinas estarán ubicados en la provincia constitucional del Callao. El espacio es de 700 m^2 y el costo del alquiler mensual es de USD 6, 000 Dólares Americanos. Para el cálculo del costo de alquiler anual, se consideró el tipo de cambio (Dólares Americanos a Nuevos Soles) y un periodo de doce meses. A continuación, se presenta una tabla (Tabla 41) que incluye los detalles.

Alquiler Almacen y Oficinas		$6,000
Tipo de Cambio	S/.	3.10
Alquiler Soles Mensual	S/.	18,600
Alquiler Soles Anual	**S/.**	**223,200**

Tabla 41 - Cálculo del costo de alquiler de almacén y oficinas [Elaboración Propia]

De la tabla anterior, se observa que el monto de alquiler anual del almacén y las oficinas es de S/. 223, 200 Nuevos Soles.

Pago de los salarios del personal

Para las contrataciones del personal de la empresa, se considerarán dos modalidades: planilla (personal administrativo y de operaciones) y *out-sourcing* (fuerza de ventas y técnicos del punto de venta). Para el cálculo de la remuneración anual, se considerará 14 sueldos, que incluyen las gratificaciones de los meses de Julio y Diciembre. A continuación, se muestra la Tabla 42, que contiene los cálculos del salario del personal considerando ambas modalidades.

Planilla

Personal	Salario	Cantidad	Total
Gerente General	S/. 10,000	1	S/. 10,000
Asistente de Gerencia	S/. 800	1	S/. 800
Gerente de Operaciones	S/. 5,000	1	S/. 5,000
Jefe de Logistica	S/. 2,500	1	S/. 2,500
Operario Logistico	S/. 1,000	1	S/. 1,000
Gerente de Finanzas	S/. 5,000	1	S/. 5,000
Contador	S/. 2,500	1	S/. 2,500
Gerente de Producto	S/. 5,000	1	S/. 5,000
Jefe de Ingeneria	S/. 2,500	1	S/. 2,500
Ingenieros I+D	S/. 1,800	3	S/. 5,400
Jefe Marketing	S/. 2,500	1	S/. 2,500
Diseñador	S/. 800	1	S/. 800
Gerente de RR.HH	S/. 5,000	1	S/. 5,000
Gerente de Ventas	S/. 5,000	2	S/. 10,000
		Total Mensual	**S/. 58,000**
		Total Anual	**S/. 812,000**

Outsourcing

Personal	Salario	Cantidad	Total
Consultores de Ventas	S/. 700	32	S/. 22,400
Técnicos	S/. 1,000	16	S/. 16,000
		Total Mensual	**S/. 38,400**
		Total Anual	**S/. 537,600**

Total	S/. 1,349,600

Tabla 42 - Salarios del personal de la empresa [Elaboración Propia]

En la tabla anterior, se observa que el monto total anual es de S/. 1, 349, 600 Nuevos Soles.

Costo del producto

Para el cálculo del costo del producto, se multiplicará el costo neto por la proyección de la demanda en cada año de operación. En la siguiente tabla (Tabla 43), se muestra el costo en los primeros cinco años de operación.

Mercado Potencial	1,275,133
Costo Neto	400

Años	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Market Share		1%	3%	5%	7%	10%
Mercado	-	12,751	38,254	63,757	89,259	127,513
Demanda		12,751	25,503	38,254	51,005	76,508
Costo del Producto	-	**S/. 5,100,532**	**S/. 10,201,064**	**S/. 15,301,596**	**S/. 20,402,128**	**S/. 30,603,192**

Tabla 43 - Cálculo del costo del producto [Elaboración Propia]

Gastos de marketing

El presupuesto de marketing estará distribuido tal como se muestra a continuación.

Concepto	Periodo	Presupuesto	Total Anual
On-line	Mensual	S/. 7,750	S/. 93,000
Periodicos - Revistas	Trimestral	S/. 51,150	S/. 204,600
Catalogos	Trimestral	S/. 20,460	S/. 81,840
		Total	S/. 379,440

Tabla 44 - Presupuesto de marketing [Elaboración Propia]

En la Tabla 44, se observa que la publicidad en medios on-line tiene asignado un presupuesto mensual de S/. 7, 750 Nuevos Soles, las publicaciones en periódicos tienen asignados un monto de S/. 51, 150 Nuevos Soles para cada trimestre del año. Además, los anuncios en catálogos tienen un presupuesto de S/.20, 460 Nuevos Soles. El costo total anual de los gastos de marketing es de S/ 379, 440 Nuevos Soles.

Otros

Además, se consideró conceptos adicionales como el alquiler del espacio de cada una de las tiendas seleccionadas, los servicios básicos (luz, agua, teléfono, etc.) y el alquiler de los servidores para ofrecer el servicio. A continuación, se presentan las tablas (Tabla 45 y Tabla 46) que contienen los costos anuales de cada uno de los conceptos.

Alquiler Espacio Tienda	$2,000
Cantidad de Tiendas	16
Tipo de Cambio	S/. 3.10
Alquiler Mensual	S/. 99,200
Total Anual	**S/. 1,190,400**

Tabla 45 - Alquiler del espacio en las tiendas por departamento [Elaboración Propia]

Concepto	Periodo	Presupuesto	Total Anual
Hosting	Mensual	S/. 500	S/. 6,000
Servicios Basicos	Mensual	S/. 1,800	S/. 21,600

Tabla 46 - Alquiler de los servidores (hosting) y presupuesto de servicios básicos [Elaboración Propia]

Después de calcular el total de los costos operativos, se tiene la siguiente tabla que incluye el consolidado de los gastos en los primeros cinco años de operación.

Años	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Alquiler Almacen y Oficinas	S/. 223,200	S/. 223,200	S/. 223,200	S/. 223,200	S/. 223,200	S/. 223,200
Salarios	S/. 1,349,600	S/. 1,349,600	S/. 1,349,600	S/. 1,349,600	S/. 1,349,600	S/. 1,349,600
Costo del Producto	S/. 0	S/. 5,100,532	S/. 10,201,064	S/. 15,301,596	S/. 20,402,128	S/. 30,603,192
Marketing		S/. 379,440	S/. 379,440	S/. 379,440	S/. 379,440	S/. 379,440
Alquier de Espacio en Tienda		S/. 1,190,400	S/. 1,190,400	S/. 1,190,400	S/. 1,190,400	S/. 1,190,400
Hosting		S/. 6,000	S/. 6,000	S/. 6,000	S/. 6,000	S/. 6,000
Serivicios Básicos		S/. 21,600	S/. 21,600	S/. 21,600	S/. 21,600	S/. 21,600
Costos Operativos	**S/. 1,572,800**	**S/. 8,270,772**	**S/. 13,371,304**	**S/. 18,471,836**	**S/. 23,572,368**	**S/. 33,773,432**

Tabla 47 - Costos Operativos - Cuadro de gastos consolidado [Elaboración Propia]

Inversión

Para iniciar las operaciones de la empresa, se ha considerado la adquisición de equipos de cómputo, muebles, central telefónica y la fabricación de los módulos de experiencia que se instalarán en cada una de las tiendas seleccionadas previamente. En la Tabla 48, se muestra un cuadro con el detalle de la compra.

Concepto	Cantidad	Precio	Total
Computadoras del Personal	17	S/. 2,500	S/. 42,500
Computadoras Tiendas	16	S/. 2,500	S/. 40,000
Computadoras Call Center	5	S/. 2,500	S/. 12,500
Muebles	10	S/. 500	S/. 5,000
Gastos varios - Oficina	1	S/. 6,000	S/. 6,000
Central Telefónica	1	S/. 6,000	S/. 6,000
Modulos de Experiencia	16	S/. 5,000	S/. 80,000
		Total	S/. 192,000

Tabla 48 - Inversión [Elaboración Propia]

Además, se considerará la depreciación de estos activos. En la Tabla 49, se presentarán los detalles.

Concepto	Vida útil	Costo	Depreciación Anual
Equipos de Computo	5	S/. 95,000	S/. 19,000
Muebles	10	S/. 5,000	S/. 500
Central	5	S/. 6,000	S/. 1,200
Módulos	10	S/. 80,000	S/. 8,000
		Total	S/. 28,700

Tabla 49 - Depreciación de los bienes [Elaboración Propia]

Flujo de Caja

Considerando los cálculos realizados anteriormente, se elaboró un flujo de caja que será mostrado a continuación.

Mercado Potencial	1,275,133
Precio Venta Canal	568
Costo Neto	400

Años	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Market Share		1%	3%	5%	7%	10%
Mercado	-	12,751	38,254	63,757	89,259	127,513
Demanda		12,751	25,503	38,254	51,005	76,508
Ingresos	-	**S/. 7,242,755**	**S/. 14,485,511**	**S/. 21,728,266**	**S/. 28,971,022**	**S/. 43,456,533**
Costos Operativos	S/. 1,572,800	S/. 8,270,772	S/. 13,371,304	S/. 18,471,836	S/. 23,572,368	S/. 33,773,432
Depreciación		S/. 28,700	S/. 28,700	S/. 28,700	S/. 28,700	S/. 28,700
UTILIDAD ANTES DE IMPUESTOS	S/. -1,572,800	S/. -1,056,717	S/. 1,085,507	S/. 3,227,730	S/. 5,369,954	S/. 9,654,401
IMPUESTOS			S/. 325,652.06	S/. 968,319.10	S/. 1,610,986.13	S/. 2,896,320.19
UTILIDAD	**S/. -1,572,800**	**S/. -1,056,717**	**S/. 759,855**	**S/. 2,259,411**	**S/. 3,758,968**	**S/. 6,758,080**
Amortización		S/. 10,000	S/. 10,000	S/. 10,000	S/. 10,000	S/. 10,000
Depreciación	S/. -	S/. 28,700	S/. 28,700	S/. 28,700	S/. 28,700	S/. 28,700
Inversión	S/. 192,000					
Préstamo	S/. 50,000					
FFN	**S/. -1,714,800**	**S/. -1,038,017**	**S/. 778,555**	**S/. 2,278,111**	**S/. 3,777,668**	**S/. 6,776,780**
FFNA	**S/. -1,714,800**	**S/. -2,752,817**	**S/. -1,974,262**	**S/. 303,849**	**S/. 4,081,517**	**S/. 10,858,298**

VNA	S/. 2,887,403
TIR	54%

Tabla 50 - Flujo de caja [Elaboración Propias]

En la Tabla 50, se calculó el VAN (Valor actual neto) usando los flujos de cada año de operación. Este resultado es mayor a cero, por lo que se puede concluir que el proyecto es factible. Además, se obtuvo un TIR (Tasa Interna de Retorno) de 54%. Este valor es mayor al del interés de inversión que ofrecen las entidades financieras, por lo que invertir en el proyecto es una opción atractiva. Finalmente, las utilidades se generan a partir del tercer año de operaciones.

Punto de equilibrio

Para complementar el análisis presentado anteriormente, se calculará el punto de equilibrio. Es el escenario en donde se calcula la cantidad mínima de unidades que se debería comercializar para que el resultado del flujo de caja sea igual a cero, es decir no habrá ganancia ni pérdida. Para ello, se utilizará la siguiente ecuación como punto de partida:

$$(Precio\ del\ Producto - Costo\ Neto\ del\ Producto) \times Cantidad - Costo\ Fijo = 0$$

Ecuación 3 - Cálculo del punto de equilibrio

Al despejar la variable *Cantidad* se obtiene la siguiente expresión:

$$Cantidad = \frac{Costo\ Fijo}{(Precio\ del\ Producto - Costo\ Neto\ del\ Producto)}$$

Ecuación 4 - Punto de equilibrio en base a la cantidad (Resultado al despejar la Ecuación 3)

Para continuar con el análisis se considerarán los costos operativos del flujo de caja que se plantearon anteriormente y se calculará el *Costo Fijo* de la siguiente forma:

Años	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Alquiler Almacen y Oficinas	S/. 223,200	S/. 223,200	S/. 223,200	S/. 223,200	S/. 223,200	S/. 223,200
Salarios	S/. 1,349,600	S/. 1,349,600	S/. 1,349,600	S/. 1,349,600	S/. 1,349,600	S/. 1,349,600
Costo del Producto	S/. 0	S/. 5,100,532	S/. 10,201,064	S/. 15,301,596	S/. 20,402,128	S/. 30,603,192
Marketing		S/. 379,440	S/. 379,440	S/. 379,440	S/. 379,440	S/. 379,440
Alquier de Espacio en Tienda		S/. 1,190,400	S/. 1,190,400	S/. 1,190,400	S/. 1,190,400	S/. 1,190,400
Hosting		S/. 6,000	S/. 6,000	S/. 6,000	S/. 6,000	S/. 6,000
Serivicios Básicos		S/. 21,600	S/. 21,600	S/. 21,600	S/. 21,600	S/. 21,600
Costos Operativos	**S/. 1,572,800**	**S/. 8,270,772**	**S/. 13,371,304**	**S/. 18,471,836**	**S/. 23,572,368**	**S/. 33,773,432**

Tabla 51 - Costos Operativos (Flujo de Caja)

$$Costo\ Fijo = Costo\ Operativo - Costo\ del\ Producto$$

Ecuación 5 - Cálculo del costo fijo

$$Costo\ Operativo = Alquileres + Salarios + Marketing + Hosting + Servicios\ Básicos$$

Ecuación 6 - Cálculo del costo operativo

Después de reemplazar los valores de la Tabla 51 en la Ecuación 5 y en la Ecuación 6, se obtiene:

$$Costo\ Fijo = S/.3,170,240\ (Nuevos\ Soles)$$

Luego, para calcular el punto de equilibrio se reemplaza el valor calculado anteriormente en la Ecuación 4. Se obtiene el siguiente resultado:

$$Cantidad = \frac{S/.\ 3,170,240}{(S/.568 - S/.400)}$$

$$Cantidad = 18,871\ unidades$$

Finalmente, después de realizar los cálculos se concluye que es necesario vender 18, 871 unidades por año para tener un flujo de caja en donde no se obtengan pérdidas ni ganancias, es decir obtener el punto de equilibrio.

En conclusión, los indicadores de VAN y TIR demuestran la factibilidad del proyecto de inversión bajo un escenario conservador. Para lograr estos resultados se tienen que ejecutar las siguientes acciones:

- Ofrecer productos con una propuesta de valor atractiva para el usuario final y diferente a la de los principales competidores (Prosegur, Clave 3 y Bóxer).
- Firmar un acuerdo comercial con las principales cadenas de tiendas por departamento. El producto se distribuirá y se comercializará a través de 18 tiendas que pertenecen a los sectores socioeconómicos A, B y C.
- El producto debe tener un precio de venta al usuario final de S/. 751 Nuevos Soles.
- Ejecutar acciones de publicidad y comunicación a través de redes sociales (on-line), periódicos, revistar y catálogos. Esto permitirá obtener el 10% de participación de mercado al final del quinto año de operación.

CONCLUSIONES

1. Después de analizar el contexto de inseguridad ciudadana en Lima Metropolitana, se puede concluir que existe la necesidad de mejorar la seguridad de las viviendas en la ciudad. Por ello, se puede aprovechar la tecnología disponible para crear un producto que permita satisfacer las necesidades de protección y seguridad de los usuarios.

2. Al revisar el estado del arte de la domótica y las tendencias tecnológicas actuales, se llegó a la conclusión que la arquitectura distribuida es la más adecuada, ya que es la más robusta y confiable ante fallas de los controladores del sistema. Además, se emplearán tecnologías de comunicación inalámbrica para evitar complejidad en la instalación del sistema.

3. Tomando en cuenta los modelos de Cloud computing existente, se llegó a la conclusión de que *Domotics as a Service* es la más adecuada, porque considera tres criterios importantes: instrumentación, ya que tiene la capacidad de monitorear las variables del ambiente de la vivienda; interconexión, debido a que es capaz de intercomunicarse con la nube y se puede acceder a la información de su estado en tiempo real; e inteligencia, ya que, por estar basado en la nube, tiene la capacidad de procesar grandes cantidades de información para optimizar los recursos de la vivienda.

4. Se realizaron pruebas para validar la funcionalidad del sistema. En primer lugar, se verificó la implementación del protocolo de comunicación a través del monitoreo del tráfico que reciben las aplicaciones (*Worker Role*). En segundo lugar, se realizaron las mediciones del tiempo de viaje del mensaje (desde el origen hasta el destino) a través de pruebas experimentales. Para mensajes del tipo Ping se obtuvo un tiempo promedio de 1.54 segundos, para Telemetría 1.47 segundos, para mensajes del tipo Alerta 21.8 segundos y para mensajes del tipo Comando 24.8 segundos.

5. Después de analizar el mercado y el perfil del consumidor, se estimó que hay un mercado potencial de 1, 275, 133 viviendas para adquirir servicios domóticos.

6. Respecto al análisis financiero, se elaboró el flujo de caja de los primeros 5 años de operación. Se obtuvo como resultado un VAN (Valor Actual Neto) mayor a cero, por lo que se puede concluir que el proyecto es factible. Además, se obtuvo un TIR (Tasa Interna de Retorno) de 54%. Este valor es mayor al del interés de inversión que ofrecen las entidades financieras, por lo que invertir en el proyecto es una opción atractiva. Además, se obtienen flujos de caja positivos a partir del tercer año de operación.

RECOMENDACIONES

1. Es necesario implementar mecanismos de seguridad más robustos para proteger la información de control y monitoreo que se transmite a través de Internet (Red Pública). Estos mecanismos deben garantizar que la información no sufrirá alteraciones durante la transmisión, el tráfico no se podrá desviar a otros servidores y que personas ajenas no accederán al contenido.

2. Se recomienda implementar mecanismos de redundancia (conectividad de red y suministro de energía) en el servidor DomoCloud. Esto permitirá incrementar la confiabilidad y la disponibilidad del sistema.

BIBLIOGRAFÍA

[1] C. Bazán Seminario, N. Mejía Huisa y J. Levaggi Tapia, «SEGURIDAD CIUDADANA INFORME ANUAL 2013 Crisis política, temores y acciones de esperanza,» IDL - Instituo de Defensa Legal, Lima, 2013.

[2] INEI - Instituto Nacional de Estadística e Informática, «Informe Técnico - Estadísticas de Seguridad Ciudadana (Julio - Diciembre 2014),» INEI - Instituto Nacional de Estadística e Informática, Lima, 2015.

[3] APEIM - Asociación Peruana de Empresas de Investigación de Mercados, «Niveles Socioeconómicos 2914,» APEIM, Lima, 2014.

[4] Consejería de Fomento, *Vivienda Conectada - Las TIC en el hogar,* Valladolid: Consejería de Fomento, 2008.

[5] Asociación Española de domótica e inmótica - CEDOM, *Cuaderno de divulgación domótica,* Madrid: Aenor, 2008.

[6] CASADOMO, «La domótica,» 19 Abril 2004. [En línea]. Available: https://www.casadomo.com/noticias/-2185. [Último acceso: 11 Abril 2015].

[7] Microsoft Coportation , *Creating the Internet of Your Things,* Redmond: Microsoft Coportation , 2014.

[8] T. McCourt, D. Toomey, S. Leopold y G. Kyriakopoulos, «Technology & Communications,» Raymond James & Associates, St. Petersburg, 2014.

[9] J. Edwards y R. Bramante, Networking Self-Teaching Guide: OSI, TCP/IP, LANs, MANs, WANs, Implementation, Management, and Maintenance, John Wiley & Sons, 2009.

[10] G. Reiter, *Wireless connectivity for the Internet of Things - White Paper,* Dallas: Texas Instruments, 2014.

[11] K. Roebuck, Virtual Private Networks: High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors, Australia: Tebbo, 2011.

[12] S. Luján Mora, Programación de aplicaciones web: historia, principios básicos y clientes web, Editorial Club Universitario, 2002.

[13] I. Sommerville, Ingeniería del software, Pearson Educación, 2005.

[14] M. BELTRÁN PARDO y F. SEVILLANO JAÉN, «Cloud Computing, tecnología y negocio,» Ediciones Paraninfo, S.A., 2013.

[15] C. Pühringer, «Cloud Computing for Home Automation,» Viena, 2012.

[16] S. Khan y J. Lloret Mauri, *Green Networking and Communications: ICT for Sustainability,* 2013: CRC Press.

[17] A. Thomas Lodamo, *M2M Protocols, Solutions and Platforms for Smart Home Environments,* Mid Sweden University, 2012.

[18] C. Wan y D. Low, *Capturing Next Generation Smart Home Users with Digital Home - White Paper,* Huawei Technology Co., Ltd., 2013.

[19] Google Inc., «Android Developers,» Android, 2010. [En línea]. Available: http://developer.android.com/index.html. [Último acceso: 21 Marzo 2014].

[20] C. Dixon, R. Mahajan, S. Agarwal, A. Brush, B. Lee, S. Saroiu y P. Bahl, *An Operating System for the Home,* Microsoft Research, 2012.

[21] Samsung Electronics Corporation, «Samsung Tomorrow,» Samsung, 2014. [En línea]. Available: http://global.samsungtomorrow.com/?p=32187. [Último acceso: 13 Junio 2014].

[22] CISCO, «Customer Case Study,» Cisco, 2013. [En línea]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/vni-service-adoption-forecast/Cisco_ATT_DigitalLife_CS.pdf. [Último acceso: 16 Junio 2014].

[23] Comcast Corporation, «XFINITY® Home,» 2014. [En línea]. Available: http://es.comcast.com/home-security.html. [Último acceso: 10 Agosto 2014].

[24] Z. Shahan, «[Infographic] Home Automation Benefits,» 5 Noviembre 2013. [En línea]. Available: http://cleantechnica.com/2013/11/06/home-automation-benefits-infographic/. [Último acceso: 24 Junio 2014].

[25] Casadomo Soluciones S.L., ESTUDIO MINT-CASADOMO 2008: Sistemas de Domótica y Seguridad en Viviendas de Nueva Promoción, Madrid: Casadomo Soluciones S.L., 2008.

[26] IBM Corporation, «The IBM vision of a smarter home - White Paper,» IBM Corporation, Nueva York, 2010.

[27] A. Maiti, «Home Automation as a Service,» *IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC),* vol. 2, nº 3, Junio 2012.

[28] «Router Inalámbrico - Imagen,» [En línea]. Available: http://www.zbyteinformatica.com/imagenes/productos/TP-LINK-TLWN841ND.jpg. [Último acceso: 04 Abril 2015].

[29] «Samsung Galaxy S5 - Imagen,» [En línea]. Available: http://trainitright.com/blog/wp-content/uploads/2014/04/GALAXY-S5_White.jpg. [Último acceso: 04 Abril 2015].

[30] «Samsung Galaxy Note 10.1 - Imagen,» [En línea]. Available: http://images.pcworld.com/images/article/2012/08/galaxy20note2010.120black20front-11397865.jpg. [Último acceso: 04 Abril 2015].

[31] «Spark Core - Imagen,» [En línea]. Available: http://www.seeedstudio.com/depot/images/product/The%20Spark%20Core.jpg. [Último acceso: 04 Abril 2015].

[32] Arduino, «Arduino - Home,» 2012. [En línea]. Available: http://arduino.cc/en/pmwiki.php?n=Guide/Introduction. [Último acceso: 13 Noviembre 2014].

[33] Microsoft Azure Service Bus - Imagen, [En línea]. Available: https://acomdpsstorage.blob.core.windows.net/dpsmedia-prod/azure.microsoft.com/en-us/documentation/articles/service-bus-dotnet-how-to-use-topics-subscriptions/20150508050839/includes/howto-service-bus-topics/sb-topics-01.png. [Último acceso: 03 Abril 2015].

[34] «Microsoft Azure Mobile Service - Imagen,» [En línea]. Available: https://mscblogs.blob.core.windows.net/media/scottgu/Media/mobile-services-diagram_thumb_6A266D81.png. [Último acceso: 04 Abril 2015].

[35] «Dashboard - Imagen,» [En línea]. Available: http://atlassian.wpengine.netdna-cdn.com/devtools/fisheye-source-crucible-code-review-dashboard.png. [Último acceso: 03 Abril 2015].

[36] M. Hoogendoorn y M. Kottke, «Building the Internet of Things - Early learnings from architecting solutions focused on predictive maintenance - White Paper,» Microsoft Corporation, Redmond, 2014.

[37] National Institute of Standards and Technology - NIST, Guide for Conducting, Gaithersburg: U.S Department of Commerce, 2012.

[38] A. R. Márquez Mejía, K. M. Cuadra Orellana y W. D. Chávez Amaya, Propuesta de un plan de valoración de riesgo para lograr la efectividad en los proyectos informáticos en las empresas desarrolladoras de software de la ciudad de San Miguel, San Miguel: Universidad de Oriente (UNIVO), 2009.

[39] IPSOS APOYO, «Perfiles Socioeconómicos Lima Metropolitana,» Lima, 2013.

[40] O. R. Troya, Interviewee, *Análisis del mercado de domótica en Perú.* [Entrevista]. 15 Marzo 2015.

[41] «ELECTROMISIONES - IMAGEN,» [En línea]. Available: http://www.electromisiones.com.ar/fotos/1403902551561_lg.jpg. [Último acceso: 11 Abril 2015].

[42] Elaboración propia, *Muestra: 150 casos, Jefes de Hogar/Amas de Casa, Nivel Socioeconómico A, B y C de Lima Metropolitana. Edad: 20 a 55 años. Estudio para determinar el nivel de aceptación del producto Domolab.,* Lima, 2014.

[43] «Prosegur - Logo,» [En línea]. Available: http://cf.juggle-images.com/matte/white/280x280/prosegur-logo-primary.jpg. [Último acceso: 03 Marzo 2015].

[44] «Clave 3 - Logo,» [En línea]. Available: http://www.issomedic.com/wp-content/uploads/2014/01/logo-clave-3.jpg. [Último acceso: 03 Marzo 2015].

[45] «Boxer - Logo,» [En línea]. Available: http://boxer.com.pe/images/placa-boxer.jpg. [Último acceso: 03 Marzo 2015].

[46] R. O. Troya, Interviewee, *Análisis de Mercados - Canal Retail.* [Entrevista]. 12 Mayo 2015.

[47] «Facebook - Logo,» [En línea]. Available: https://www.facebook.com/. [Último acceso: 03 Marzo 2015].

[48] Superintendencia de banca, seguros y AFP, «Cotización de oferta y demanda tipo de cambio promedio ponderado,» [En línea]. Available: http://www.sbs.gob.pe/app/stats/tc-cv.asp. [Último acceso: 08 Abril 2015].

[49] «Catálogo de Saga Falabella - Imagen,» [En línea]. Available: http://webadicto.net/image.axd?picture=catalogo-saga-falabella-televisores-bluray-camaras-marzo-2012-01_1.jpg. [Último acceso: 03 Marzo 2015].

[50] «Catálogo de Ripley - Imagen,» [En línea]. Available: http://webadicto.net/image.axd?picture=catalogo-ripley-diciembre-2012-navidad-electronica_1.jpg. [Último acceso: 03 Marzo 2015].

[51] «Catálogo de Saga Falabella - Imagen,» [En línea]. Available: http://webadicto.net/image.axd?picture=saga-falabella-catalogo-conexion-digital-enero-febrero-2012-08_1.jpg. [Último acceso: 03 Marzo 2015].

[52] «Diario El Comercio - Logo,» [En línea]. Available: http://upload.wikimedia.org/wikipedia/commons/thumb/9/98/El_Comercio_logo.jpg/240px-El_Comercio_logo.jpg. [Último acceso: 03 Marzo 2015].

[53] «Revista Somos - Logo,» [En línea]. Available: https://lamula.pe/media/uploads/ed458f35-85ef-4e18-b22e-d4035b71ca6a.jpg. [Último acceso: 03 Marzo 2015].

[54] S. Folea y D. Bordencea, «Smart Home Automation System Using Wi-Fi Low Power Devices,» Technical University of Cluj-Napoca, Cluj-Napoca, 2012.