UNIVERSIDAD TECNOLOGICA ECOTEC

FACULTAD DE INGENIERÍAS

TÍTULO A OBTENER EN:

INGENIERÍA EN SISTEMAS INTELIGENTES CON ÉNFASIS EN ADMINISTRACIÓN DE REDES

TEMA:

“DESARROLLO DE UN SISTEMA IoT PARA EL CONTROL DE ACCESO Y SEGURIDAD EN LA ETAPA COSMOS DE VILLA CLUB, USANDO LOS SERVICIOS EN LA NUBE”

AUTOR:

OSCAR ANDRÉ LLAMUCA BRITO

TUTOR:

MGTR. MANUEL RAMÍREZ

2022

AGRADECIMIENTO

Dedico este trabajo a mi familia, quienes siempre me acompañan en cada victoria y animarme a dar el siguiente paso, los mismos que me brindaron su apoyo emocional y orientación profesional, a mis padres por sus enseñanzas, valores y ética como siempre lo han hecho durante el transcurso de mi vida, para que en el futuro poder continuar a niveles más altos de aprendizaje.

ANEXO N° 14

CERTIFICADO DE APROBACIÓN DEL TUTOR PARA LA PRESENTACIÓN A REVISIÓN DEL TRABAJO DE TITULACIÓN

Samborondón, 7 de noviembre de 2022

Magíster
Erika Ascencio
Decano(a) de la Facultad
Ingenierías
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: Desarrollo de un sistema IoT para el control de acceso y seguridad en la etapa Cosmos Villa Club, usando servicios en la nube según su modalidad PROPUESTA TECNOLÓGICA; fue revisado, siendo su contenido original en su totalidad, así como el cumplimiento de los requerimientos establecidos en la guía para la elaboración del trabajo de titulación, Por lo que se autoriza a: LLAMUCA BRITO OSCAR ANDRE**,** para que proceda a su presentación para la revisión de los miembros del tribunal de sustentación.

ATENTAMENTE,

Firmado electrónicamente por:
MANUEL OSMANY
RAMIREZ PIREZ

Mgtr/ PhD. Manuel Ramírez Pirez

Tutor(a)

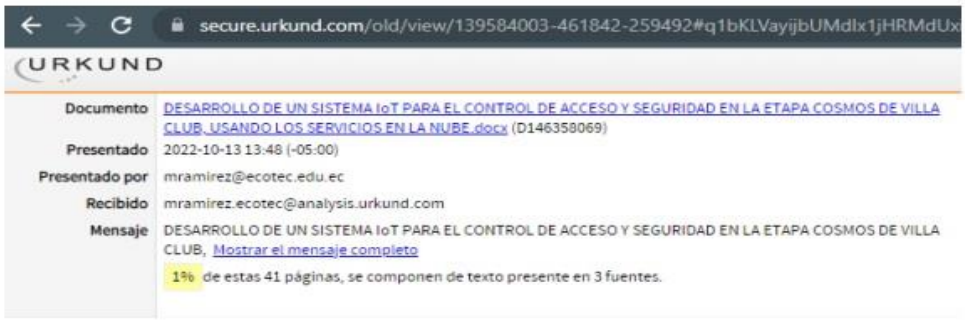
ANEXO N°15

CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

Habiendo sido nombrado MANUEL OSMANY RAMÍREZ PIREZ, tutor del trabajo de titulación “Desarrollo de un sistema IoT para el control de acceso y seguridad en la etapa Cosmos Villa Club, usando servicios en la nube” elaborado por OSCAR ANDRÉ LLAMUCA BRITO**,** con mi respectiva supervisión como requerimiento parcial para la obtención del título de INGENIERIA EN SISTEMAS CON ENFASIS EN ADMINISTRACIÓN DE REDES.

Se informa que el mismo ha resultado tener un porcentaje de coincidencias 1% mismo que se puede verificar en el siguiente link https://secure.urkund.com/old/view/139584003-461842-259492#q1bKLVayijbUMdIx1jHRMdUxi9VRKs5Mz8tMy0xOzEtOVbIy0DMwMDExtjAzNbAwMDO1MDYwMjSpBQA

Adicional se adjunta print de pantalla de dicho resultado.



Firmado electrónicamente por:
MANUEL OSMANY RAMIREZ PIREZ

FIRMA DEL TUTOR
MGTR. MANUEL RAMÍREZ PIREZ

ANEXO N°16

CERTIFICADO DE APROBACIÓN DEL TUTOR PARA LA PRESENTACIÓN DEL TRABAJO DE TITULACIÓN CON INCORPORACIÓN DE LAS OBSERVACIONES DE LOS MIEMBROS DEL TRIBUNAL

Samborondón, 7 de noviembre de 2022

Magíster
Erika Ascencio
Decano(a) de la Facultad
Ingenierías
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: Desarrollo de un sistema IoT para el control de acceso y seguridad en la etapa Cosmos Villa Club, usando servicios en la nube según su modalidad PROYECTO DE INVESTIGACIÓN, PROPUESTA TECNOLÓGICA O EXAMEN COMPLEXIVO (ESTUDIO DE CASO) **(PROPUESTA TECNÓLOGICA)**; fue revisado y se deja constancia que el estudiante acogió e incorporó todas las observaciones realizadas por los miembros del tribunal de sustentación por lo que se autoriza a: LLAMUCA BRITO OSCAR ANDRÉ**,** para que proceda a la presentación del trabajo de titulación para la revisión de los miembros del tribunal de sustentación y posterior sustentación.

ATENTAMENTE,

Firmado electrónicamente por:
MANUEL OSMANY
RAMIREZ PIREZ

Mgtr/ PhD. Manuel Ramírez Pirez

Tutor(a)

RESUMEN

Este proyecto de titulación abarca como objetivo principal mejorar el control de acceso y seguridad a través de un sistema de Internet de las Cosas (IoT), usando servicios en la nube en la urbanización Villa Club etapa Cosmos. Debido a que las entradas y salidas no disponen de una adecuada implementación tecnológica que permita gestionar el control de acceso y seguridad en la ciudadela.

El objetivo principal de la investigación fue describir la falta de control y la seguridad que existe en la urbanización para ello, se prevé implementar un sistema de Internet de las Cosas (IoT). Se planteo una metodología con enfoque cualitativo y de alcance descriptivo. El desarrollo de la perspectiva teórica se basará en la revisión de documentación académica.

Por otra parte, se describen los requerimientos para el dispositivo IoT y que permite el correcto funcionamiento del sistema para el control de acceso y seguridad. Por último, se especifica el modelo de referencia del IoT aplicado al dispositivo y la arquitectura seleccionada para la implementación del mismo.

De acuerdo con el análisis realizado se concluye que con un control automatizado que mejora el control de acceso y seguridad en la ciudadela Villa Club etapa Cosmos se pudo contar con un registro de entradas y salidas de las personas, y los datos obtenidos facilitarán la seguridad de los ciudadanos que residen en la urbanización.

Palabras clave: Tecnología, sistema IoT, servicios en la nube, AWS, seguridad.

ABSTRACT

The main objective of this titling project is to improve access control and security through an Internet of Things (IoT) system, using cloud services in the Villa Club urbanization, Cosmos stage. Because the entrances and exits do not have an adequate technological implementation that allows managing access control and security in the citadel.

The main objective of the research was to describe the lack of control and security that exists in the urbanization, for this, it is planned to implement an Internet of Things (IoT) system. A methodology with a qualitative approach and descriptive scope was proposed. The development of the theoretical perspective will be based on the review of academic documentation.

On the other hand, the requirements for the IoT device are described and that allows the correct operation of the system for access control and security. Finally, the IoT reference model applied to the device and the architecture selected for its implementation are specified.

According to the analysis carried out, it is concluded that with an automated control that improves access control and security in the citadel Villa Club Cosmos stage, it was possible to have a record of people's entrances and exits, and the data obtained will facilitate the security of citizens residing in the urbanization.

Keywords: Technology, IoT system, cloud services, AWS, security.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

En la actualidad, de manera general el concepto de Internet de las Cosas hace referencias a un mundo conectado donde objetos físicos interactúan en entornos virtuales en el mismo espacio y tiempo, con el fin poder monitorear y controlar un entorno completo, que facilita la vida de las personas que automatiza muchas de las tareas que realizan actualmente.

Por otro lado, para el presente proyecto el uso de tecnología de computación en la nube con la capacidad de almacenar datos en la nube generados por Internet, es indispensable y necesario para el desarrollo de sistemas de seguridad integrando IoT.

La importancia de la integración de IoT y la computación en la nube siempre ha tenido ventajas como la reducción de costos, la toma de decisiones oportunas y la confiabilidad. La utilización e implementación de esta tecnología se está expandiendo en organizaciones y empresas públicas o privadas; por lo tanto, existe la visión de fomentar esta tecnología en el mundo, considerando los beneficios de aporte en el IoT integrado y la computación en la nube, su implementación representa un desafío importante que requiere una toma de decisiones inteligente.

La novedad que aporta el estudio se referencia con la expansión de la tecnología de Internet de las cosas y el modelo integrado de computación en la nube. A partir de ello, para cumplir con este objetivo se utilizó la placa Arduino Uno, el microcontrolador NodeMCU-32 y una pantalla SPI ILI 9341, que gracias a la versatilidad que tienen permitió todo el desarrollo del dispositivo, permitiendo controlar el sistema de control de acceso y seguridad y al mismo tiempo permite alojar la aplicación web que monitorea las entradas y salidas cuando dicho usuario pase por el dispositivo.

La comunicación entre el microcontrolador NodeMCU-32 ya mencionado con anterioridad y la aplicación web se realizó mediante el servicio en la nube y de forma simultánea se administra los datos mediante un sensor de forma precisa; para el almacenamiento de la información

existente en la base de datos MYSQL que se utilizó para hacer las consultas.

Las tecnologías de la información y la inteligencia artificial en el campo de la interacción máquina a máquina han evolucionado a una velocidad sin precedentes. Este aspecto debe ser aprovechado en todo tipo de servicios, especialmente en el fortalecimiento de la seguridad considerando el entorno situacional local.

Internet de las Cosas (IoT), es un sistema que consta de dispositivos informáticos relacionados, máquinas mecánicas y digitales y cosas con una identificación específica y única que tiene la capacidad de transmitir datos a través de un objeto o una red, sin necesidad de interacción entre persona – persona y persona – cosas. En general, la integración de IoT y computación en la nube, prevé proporcionar un modelo sintético de estas dos tecnologías que representa el elemento central para la consecución de esta investigación.

Las aplicaciones desarrolladas en base a la estructura organizada que se establece del desarrollo e implementación del sistema IoT en el control y la seguridad, como elementos tecnológicos para el fortalecimiento de los sistemas digitalizados, representan una oportunidad para minimizar los desafíos de comunicación y maximizar elementos de seguridad y control, como el escenario previsto en el desarrollo de este documento.

Esto se realiza considerando los desafíos de procesamiento y almacenamiento asociados con esta tecnología y la provisión de soluciones computacionales que pueden mejorar el poder de procesamiento y la respuesta oportuna al utilizar la tecnología del internet de las cosas con los servicios en la nube.

Además, al especificar diferentes componentes y tareas de IoT y computación en la nube de acuerdo con los estándares existentes en el modelo propuesto, se pueden disminuir los desafíos de procesamiento en el entorno actual. Hoy, con la capacidad fundamental de Internet de las cosas, que siempre viene con muchos beneficios, está mejorando muy

rápidamente, sobre lo que, la falta de un modelo de procesamiento óptimo representa un desafío para las organizaciones e incluso un obstáculo para la rápida expansión de esta tecnología.

Por ello, al utilizar la tecnología IoT en tareas de alta prioridad como la seguridad y el control continuo de entornos, en las que siempre una respuesta inmediata y rápida juega un papel importante, la falta de un modelo de procesamiento eficiente agrega tiempo de procesamiento y, como resultado, falta de capacidad de respuesta cuando se trata de usar la tecnología IoT. Por tanto, el desarrollo de un sistema IoT usando los servicios en la nube constituye un aporte al crecimiento tecnológico en la localidad y el país.

Siendo así, se espera que un nuevo escenario de tecnologías de información en el que la nube y el IoT sean dos tecnologías complementarias fusionadas, aporten al desarrollo de nuevos modelos de innovación en la seguridad y la utilización de tecnologías para la comunicación y el mejoramiento continuo de datos en la nube. Razón por lo cual, se estima adecuado implementar procesos de actualización e innovación en el entorno local de seguridad, aplicando IoT en integración con los servicios en la nube como un nuevo modelo de desarrollo operativo en áreas sensibles de empresas públicas y/o privadas.

Sobre ello, cabe mencionar que, en la actualidad, existen alrededor de 13 mil millones de dispositivos IoT, que aportan al desarrollo tecnológico e interacción entre las personas y las cosas para una comunicación continua y previsión de elementos de seguridad operativa constante (Banco Mundial, 2021). Estos elementos de desarrollo integrado, entre IoT y computación en la nube, están basados en tecnología de comunicación inalámbrica, con capacidades limitadas y amplias en términos de computación y almacenamiento de datos.

A medida que a los sistemas IoT se les confía cada vez más la detección y gestión de ecosistemas altamente complejos, las preguntas sobre la seguridad y la confiabilidad de los datos que se transmiten hacia y

desde los dispositivos IoT se están convirtiendo rápidamente en una preocupación importante (Marcet & Martínez, 2019). Sobre ello, las redes de IoT enfrentan varios desafíos de seguridad que incluyen autenticación, autorización, fuga de información, privacidad, verificación, manipulación, interferencia, espionaje, etc.

Por lo cual, IoT proporciona una infraestructura de red con protocolos de comunicación y *software* interoperables, con herramientas para habilitar la conectividad a Internet para dispositivos portátiles inteligentes. Tales dispositivos, se pueden estructurar sobre teléfonos inteligentes, asistentes digitales personales (PDA), aparatos domésticos inteligentes (televisores inteligentes, aire acondicionado, sistemas de iluminación inteligente, nevera inteligente, etc.), automóviles y adquisición sensorial de sistemas (Cisneros & Altamirano, 2021).

La introducción de dispositivos IoT restringidos y tecnologías IoT en aplicaciones tan sensibles genera nuevos desafíos de seguridad; sobre ello, en los últimos años, IoT se ha convertido en una de las tecnologías más importantes del siglo XXI, por lo cual, actualmente se puede conectar con objetos cotidianos como electrodomésticos, automóviles, termostatos, monitores de bebes a internet a través de dispositivos integrados (Fernández & Noguera, 2017). Considerando aquello, más allá de la propia tecnología, hay que tener en cuenta las ventajas y desventajas del internet de las cosas; es decir, se trata de una tecnología con grandes posibilidades, pero que también planean algunas interrogantes de aplicación.

La principal ventaja que ofrece IoT es la capacidad de conectarse a internet y tener el acceso total a ello; otra de las ventajas IoT es que el intercambio de información se realiza de forma rápida y en tiempo real (Piedra, Sari, & Cedillo, 2018). Aunque los dispositivos IoT pueden parecer demasiados pequeños o demasiado especializados como para ser peligrosos, existe un riesgo en los computadores de uso general conectados a una red que pueden piratear atacantes y dar lugar a problemas más allá de la seguridad de IoT (Calva, Rojas, Román, & Radicelli, 2020).

En función de todo lo anterior, el presente proyecto tecnológico aborda la combinación de IoT y servicios en la nube, considerando la importancia de actualizarse a un sistema de modelado avanzado, capaz de manejar la complejidad y los cambios automáticos, proporcionando un sistema confiable, fuerte, flexible y actualizable, con plantillas integradas orientadas a objetos para facilitar las interfaces y reutilizar el sistema. Con ello, se prevé desarrollar un sistema IoT, maximizando la seguridad y control en los puntos de acceso de la urbanización objeto de estudio, como un modelo tecnológico para la localidad y el país.

Planteamiento del problema

La situación actual del problema se estable para la urbanización Villa Club, en la etapa Cosmos, donde, de manera específica, la administración ha presentado inconsistencias en el control de acceso y seguridad del lugar, escenario que requiere de una revisión exhaustiva para los procesos de seguridad interna y externa. Los procesos que se han ejecutado en el control de acceso de la etapa, no han realizado las revisiones correspondientes en el manejo y control de la información, toma de datos y referencia de entradas y salidas de personas.

Por ello, estos procesos se ejecutan con el control de una bitácora de control para las entradas y salidas, lo cual no se ha escrito correctamente, dejando ingresar y salir personas de la etapa Cosmos, sin que estas hayan sido revisadas, ni ingresadas en la bitácora de control y sistema de acceso. Por ello, el problema de seguridad se define sobre la inexistencia de un modelo de arquitectura integrada de control de accesos que bride información adecuada y clara, en monitoreo diario y periódico, generando errores de control e inseguridad para la etapa habitacional.

Este problema se ha revisado en esta investigación para el período enero 2021 – enero 2022, donde los problemas de control de acceso en la etapa Cosmos de Villa Club, presentaron inadecuados procedimientos en el registro de ingresos y salidas, entre residentes, visitantes y personal de ayuda doméstica, laboral e interna institucional. La problemática se

fundamenta en la seguridad que actualmente necesitan las urbanizaciones privadas, específicamente para este estudio en la etapa Cosmos, en Villa Club, del cantón Daule, considerando que carece de un sistema integrado de control que requiere mantener una constante vigilancia en el acceso de personal y residentes.

Siendo así, el desarrollo de elementos tecnológicos representa una gran oportunidad de innovación para la urbanización y fortalecimiento de su seguridad en control de acceso. Consecuentemente, la combinación de IoT y servicios en la nube representa un elemento de gran importancia en el desarrollo tecnológico de hoy en día, ya que proporciona innumerables aplicaciones posibles en los sistemas de monitorización de la seguridad en tiempo real de los entornos que se desean revisar de manera constante y continua, evitando la continuidad de procesos inadecuados como el manejo de bitácora, que ha dado lugar a un control deficiente en el registro y seguridad de la ciudadela.

Basados en ello, se han planteado los problemas de seguridad y control, lo cual ha generado problemas en la etapa Cosmos, la cual está constantemente expuesta a inseguridad e incidencia del no registro de acceso de las personas que frecuentan el lugar. A continuación, se presentan los datos estadísticos de incidencias de seguridad en el control de acceso.

La descripción de los problemas que se suscitan en el control de acceso de la etapa Cosmos, presenta elementos de identificación y control, que inciden en la seguridad interna y externa de todo el conjunto residencial.

Por ello, los datos referidos (2020 – 2021), sobre las falencias en control, se han presentado sobre una población de 12,726 personas que han ingresado a la etapa según datos de la Corporación Samborondón Cía. Ltda. CORSAM (2022), empresa que maneja la seguridad de la etapa Cosmos en Villa Club.

Consecuentemente, debido a la falta de un sistema integrado de comunicación y control a través de las nuevas tecnologías e internet de las cosas, no se ha podido llevar de manera adecuada y profesional el control constante y continuo que se requiere en el acceso y seguridad.

Los datos de los problemas en el control de acceso a la etapa Cosmos de Villa Club, se presentan sobre la Unidad de Identificación, donde no se requirió identificación a 3,411 personas de un total de 12,726 en el periodo enero 2021 a enero 2022; de la misma forma, las falencias en el control de acceso se pueden revisar en la Unidad de Entrada, sobre lo cual ingresaron 5,627 sin ninguna revisión de la garita, Unidad de Contacto de Puerta, con 2,916 personas que pasaron sin ningún tipo de requerimiento documental o anuncio al residente y asimismo, salieron 4,928 personas sin ningún tipo de registro de salida.

Estos datos se presentan sobre 2021 – 2022 (enero – enero), sobre una población de 12,726 personas, debido a que anterior a ello, el flujo de personas se redujo considerablemente a causa de la pandemia de Covid-19, que resultó en el distanciamiento social, por lo que, los datos se han tomado sobre el último año para poder revisar el problema actual y sobre ello proponer una solución que integre al sistema IoT usando los servicios en la nube, como un modelo de tecnología integrada para la comunicación y control continuo en la garita y administración de la etapa Cosmos.

Sobre este antecedente del problema, se considera que, el potencial de conocimiento que entregan las aplicaciones IoT solo pueden explotarse si se ha realizado una correcta implementación, especialmente orientadas al ámbito de la seguridad y control, que es fundamental en la actualidad en las ciudadelas privadas de la localidad.

Cabe resaltar que, las aplicaciones en IoT pueden resultar desafiantes entre otras cosas, por la necesidad de coordinar diferentes equipos operativos y unidades de negocio para una implementación efectiva, la eficiencia, la satisfacción del cliente y la productividad a largo plazo resulta crucial.

Por lo tanto, descubrir los indicadores claves de rendimiento para medir e introducir mejoras resulta complejo en el ámbito operativo de desarrollo y ejecución de sistemas de seguridad. Teniendo en cuenta lo antes expuesto surge la siguiente pregunta problémica.

Formulación del problema

¿Cómo mejorar el control y seguridad de acceso integral en la etapa Cosmos de la ciudadela Villa Club?

Objetivos

Objetivo general

Desarrollar un sistema de Internet de las cosas (IoT), para el control de acceso y seguridad, a través de los servicios en la nube, en la etapa Cosmos de la urbanización Villa Club.

Objetivos específicos

- Determinar la teoría relacionada con la implementación de sistemas IoT, como soluciones de seguridad, usando los servicios de la nube.
- Conocer el escenario situacional, referente al control de acceso y seguridad en la etapa Cosmos para el desarrollo de un sistema IoT a través de los servicios en la nube.
- Diseñar un sistema IoT, usando los servicios de la nube para el control de acceso y seguridad.
- Validar los resultados a partir de la implementación propuesta.

Justificación de la investigación

La justificación del presente estudio se define sobre la importancia actual de las nuevas tecnologías en beneficio de los escenarios sociales y operativos que benefician para su implementación e integración, especialmente en el internet de las cosas y los servicios en la nube, que representan un elemento de innovación tecnológica que debe ser revisado en el crecimiento nacional y local.

Por ello, el desarrollo e implementación de procesos operativos que integran a IoT y servicios en la nube, especialmente en el ámbito de la seguridad, promueven mejoramiento del uso de las tecnologías y procesos de información activa entre los interesados del control y la seguridad, estimando que es fundamental para el desarrollo tecnológico y su ejecución.

Por esa razón, se plantea la implementación de un sistema IoT para la seguridad y servicios en la nube, sobre lo que, el propósito es poder dar a conocer a las personas los posibles problemas que pueden ocasionar en los dispositivos IoT de manera incorrecta y mediante una simulación se pueda estimar los beneficios del uso de la tecnología IoT en aplicación actual y directa.

Con ello, se pretende desarrollar una solución de seguridad para la transferencia de datos por el medio. En este caso, se trata de una implementación de cifrado y descifrado para un sistema de internet de las cosas, y promover su aplicación en la generalidad de procesos, sistemas de seguridad y desarrollo de infraestructura en la localidad y el país.

Desde el punto metodológico, sobre tal escenario, se seleccionará el protocolo MQTT basado en el principio de comunicación que es máquina a máquina, acompañado de los servicios en la nube ofrecidos por *Amazon Web Services*. Consecuentemente, es de gran importancia la aplicación de IoT y los servicios en la nube en los diferentes entornos como la ubicación, la confiabilidad, alto rendimiento, eficiencia y escalabilidad.

Además, se prevé dar la oportunidad de debatir sobre la seguridad, ya que al momento de transferir los datos a un sistema de nube se debe tener la preocupación y el cuidado adecuado antes de su implementación. Actualmente, muchos dispositivos están conectados en la red que facilitan las tareas diarias mejorando actividades de la vida de las personas, por eso es oportuno considerar qué pasaría si estos dispositivos se comunican entre sí, ya que pueden llegar a mejorar los procesos e interacción en el entorno.

De acuerdo a lo revisado en el párrafo anterior, se prevé mejorar los tiempos de revisión de control y seguridad, con procedimientos tecnológicos enfocados en IoT, con el cual se reducirán costos de producción y a su vez ahorro de tiempo; por consiguiente, muchos beneficios que son cruciales para un funcionamiento eficaz y efectivo para el medio de seguridad y operatividad en tiempo real, adecuado a las necesidades que demandan en los objetivos de estudio.

Este proyecto se documenta en tres capítulos. En el capítulo I se da a conocer la teoría relacionada al Internet de las Cosas: antecedentes, conceptos fundamentales, aplicación de campo y normalización.

En el capítulo II se describe los diferentes actuadores que participan para el prototipo automatizado para el control de acceso. Se presenta información detallada y la elección del hardware y software que se necesita para la construcción del entorno de desarrollo del Internet de las Cosas (IoT), el diseño de los procesos que se llevaron a cabo en la placa Arduino Uno tanto para el microcontrolador NodeMcu-32, como la pantalla SPI ILI9341, para poder cumplir con los requerimientos mencionados y permitir el correcto funcionamiento tanto en hardware como software. Además, se especifica el modelo de referencia de IoT aplicado al control de acceso y la arquitectura realizable elegida.

En el capítulo III se detalla la implementación IoT para el control de acceso, describiendo las etapas de instalación del dispositivo y sus actuadores, configuración del servidor web, configuración del servicio en Amazon Web

Services (AWS), configuración del servidor de base de datos, la programación que se desarrolló en el dispositivo y la de la aplicación web que se adapta al dispositivo mediante una cuenta de usuario. Se da a conocer las pruebas de funcionamiento realizadas entre el dispositivo, aplicación web, el servidor, la base de datos que estará bajo condiciones establecidas. Adicionalmente, se muestra un resultado adecuado para responder a la integración de procesos de control de acceso, mejorando la seguridad y fomentado la utilización del IoT en las prácticas de revisión continua, en tiempo real para la etapa Cosmos que servirá para validar las entradas y salidas en la urbanización.

CAPÍTULO 1

MARCO TEÓRICO

MARCO TEÓRICO

En este capítulo se abordarán los aspectos teóricos relacionados con la implementación de sistemas IoT, como soluciones de seguridad, usando los servicios de la nube. Para ello, se describirán cada una de las variables que intervienen en el estudio.

El Internet de las cosas (IoT) permite conectar personas y dispositivos de una manera completamente nueva, ya que permite conexiones entre dispositivos físicos y aplicaciones virtuales, lo que facilita la transferencia de datos del mundo real al mundo virtual. Su mayor fortaleza es que tiene el potencial de afectar a las vidas de las personas en una gran variedad de formas.

Tiene usos interesantes tanto para usuarios privados como comerciales, que van desde la seguridad electrónica y el aprendizaje mejorado hasta la fabricación industrial y la logística. La importancia de IoT incluso fue reconocida por la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (2021), ya que forma parte de su lista de tecnologías civiles disruptivas.

Sobre ello, la Conferencia mencionada estimó que la combinación de los avances tecnológicos y la demanda impulsaría el desarrollo, y que para el año 2025, los artículos comunes podrían haberse conectado a Internet. Esto conducirá a una gran cantidad de dispositivos conectados, estimando que para 2022 habrá alrededor de 18 mil millones de dispositivos conectados relacionados con IoT.

Otra área interesante que ha crecido es la computación en la nube, que permite a los usuarios llegar a las aplicaciones a través de la nube como servicio, en lugar de ejecutar las aplicaciones en sus propias máquinas (Marcet & Martínez, 2019). La implementación del Internet de las Cosas (IoT) incentiva a la innovación y mejoramiento de procesos para los

desarrolladores que anteriormente no podían pagar la infraestructura y los gastos para operarla desarrollar sus sistemas, ya que no necesitan pagar por adelantado.

También tenemos que conocer los tipos de nube, que pueden ser públicas, privadas o híbridas: las públicas son las que están a disposición de forma libre al público, y que son dadas por un proveedor industrial de los servicios en la nube. En las nubes privadas existen dentro de una organización y son administradas por el mismo personal capacitado de la empresa por eso, la empresa crea y administra sus servicios en la nube. Finalmente, las nubes híbridas usan lo mejor de ambas tanto de públicas y privadas, por lo tanto, la empresa y el proveedor comparten la responsabilidad en la administración de la nube, al momento de usar una nube híbrida las organizaciones determinan sus necesidades en función a sus objetivos y requisitos.

A través del IoT, se fomenta la capacidad de escalar los sistemas según la demanda, lo que significa que no es necesario asignar los recursos cuando no se están utilizando (Tejada, 2020). Dado que la computación en la nube es adecuada para IoT, los proveedores de la nube han comenzado a ofrecer características específicas de IoT; actualmente ejemplos de proveedores que brindan tales funciones son Amazon, Microsoft y Google.

Poder aprovechar estos servicios para crear soluciones mejores y más económicas podría ser muy beneficioso, pero también requiere conocimiento sobre los servicios, basados en interrogantes fundamentales como: ¿Qué ofrecen? ¿Qué se requiere del desarrollador? ¿Cuáles son los inconvenientes, los riesgos y los costos?

Como existe una gran cantidad de proveedores disponibles, elegir cuál usar tampoco es trivial, por lo que, de repente, se vuelve importante no solo tener conocimiento sobre el IoT en sí mismo, sino también sobre los servicios que se pueden usar para ejecutarlo (Norero & Salazar, 2019). Este estudio profundizará en estos servicios en la nube para generar

conocimiento y recopilar experiencia en torno a ellos en integración de la tecnología IoT.

Internet de las Cosas (IoT)

El concepto de Internet de las Cosas (IoT) fue introducido por primera vez por Kevin Ashton, un miembro de la comunidad de desarrollo de identificación por radiofrecuencia en 1999 (Rose, Eldridge, & Chapin, 2018). A partir de ello, se ha vuelto más relevante para el mundo debido al rápido crecimiento de los dispositivos móviles, la comunicación, la computación en la nube y el análisis de datos.

IoT se define no solo como una red de computadoras, sino que ha desarrollado una red de todo tipo de dispositivos como cámaras digitales, vehículos, teléfonos inteligentes, electrodomésticos, instrumentos médicos y sistemas industriales, personas, edificios, todos estos dispositivos conectados pueden comunicarse y compartir para lograr reorganizaciones inteligentes, posicionamiento, actualización en línea, control de procesos y administración (Martínez-Santander & Cruz, 2021). Es decir, se define como una infraestructura de objetos conectados que permite su gestión, minería de datos y el acceso a los datos que generan.

La definición más completa y recomendada de IoT es propuesta por la Unión Internacional de Telecomunicaciones (2012), en la Oficina de Normalización de las Telecomunicaciones (UIT), que lo define como una infraestructura global para la sociedad de la información, que permite servicios avanzados mediante la interconexión de cosas (físicas y virtuales) basadas en tecnologías de información y comunicación interoperables existentes y en evolución (Alcázar, 2018).

La interconexión del mundo físico con el mundo virtual abre nuevas posibilidades que permiten acceder a cualquier cosa desde cualquier lugar; esta interconexión también puede aumentar las posibilidades de nuevas amenazas, riesgos de seguridad y vulnerabilidades. El IoT se puede definir

de diferentes maneras como se menciona en las definiciones anteriores y todas estas definiciones son de alguna manera relevantes entre sí.

Por tanto, se puede definir como una infraestructura de dispositivos conectados geográficamente como teléfonos inteligentes, sistemas industriales, vehículos, etc. que se conectan mediante tecnologías de comunicación para generar y acceder a los datos para proporcionar un posicionamiento preciso, seguridad y administración (Laguna, Rosales, Balbuena, Zamora, & Frías, 2020).

Hoy en día, IoT representa un elemento de tecnología útil para alrededor de 7,000 millones de personas, según datos de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (2021), sobre lo cual, Internet se constituyó como una herramienta útil para realizar diferentes tipos de tareas, como enviar y recibir correos electrónicos, compartir información en las redes sociales, leer libros, jugar juegos, navegar y comprar en línea. Según datos del Banco Mundial (2021), la proyección del número de dispositivos conectados al IoT en todo el mundo a 2021 y con proyección a 2030, son los siguientes:

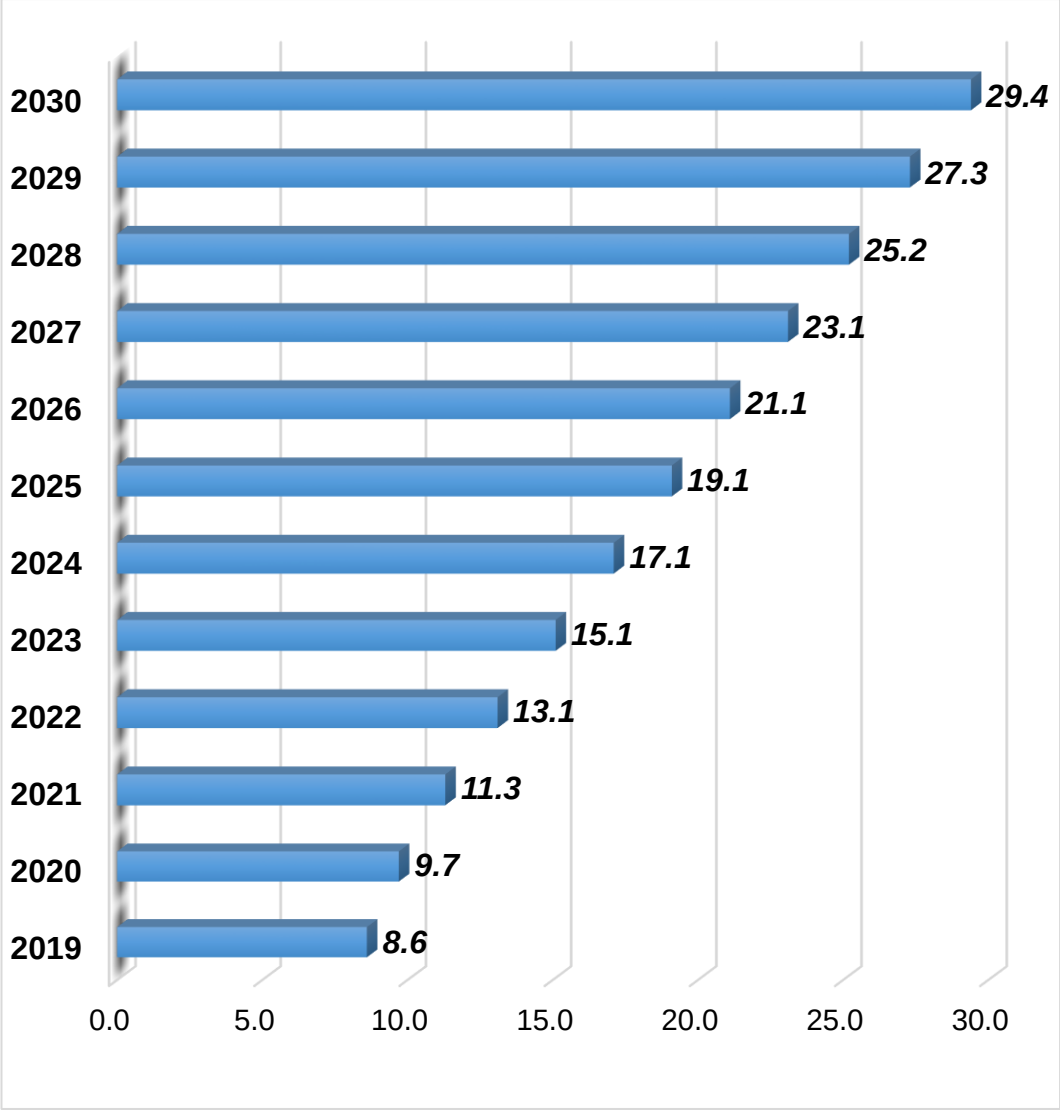


Figura 1. Número de dispositivos contactados al IoT, proyecciones 2022 – 2030

Fuente: (Banco Mundial, 2021)

Este uso a gran escala de Internet que permite introducir nuevas tendencias, esta infraestructura de comunicación global que permite que las máquinas se comuniquen entre sí y tomen decisiones, es la que ha dado lugar a la integración de todas las cosas en internet, como resultado del internet de las cosas.

El IoT es un mundo donde miles de millones de objetos pueden comunicarse y compartir información, todos estos objetos están conectados a través del protocolo de Internet (IP) (Kezherashvili, 2017). Estos objetos conectados generan una gran cantidad de datos

regularmente que se recopilan, analizan y utilizan para realizar acciones, proporcionar inteligencia para la toma de decisiones.

La incidencia del IoT prevé su implementación en casi todos los dominios del mundo como transporte, agricultura, salud, producción y distribución de energía, lo cual está transformando la forma en que se vive y desarrollan actividades, hoy al crear dispositivos inteligentes alrededor de todos los escenarios para realizar tareas diarias, hogares inteligentes, ciudades inteligentes, transporte inteligente, etc.

Consecuentemente, el número de dispositivos conectados con el entorno IoT aumenta cada día, como se pudo revisar en la figura 2, que estima que la razón de este rápido aumento es que los dispositivos conectados brindan comodidad y producen buenos resultados en comparación con los humanos (Salazar & Silvestre, 2018).

Las aplicaciones de IoT reducen los esfuerzos humanos porque realizan tareas de forma automática; además de los beneficios de estos dispositivos, también tienen que enfrentar desafíos, uno de los mayores desafíos es la seguridad y la privacidad (González, García, Gallego, & Sastoque, 2016).

La comunicación es la parte más importante del IoT porque todos los dispositivos conectados deben poder comunicarse entre sí. Los componentes principales de IoT para la comunicación se muestran en la figura 3, donde se presenta:

a. Hardware, que consta de componentes físicos, sensores, actuadores, etc.;
b. Software intermedio, se utiliza para el almacenamiento de datos y contiene herramientas informáticas que se utilizan para el análisis de datos y,
c. Presentación, herramientas de visualización e interpretación a las que se puede acceder ampliamente en diferentes plataformas

Sobre ello, los componentes de las telecomunicaciones IoT, se establecen sobre los componentes y datos de almacenamiento, que representan las herramientas para visualización e interpretación de la siguiente manera:

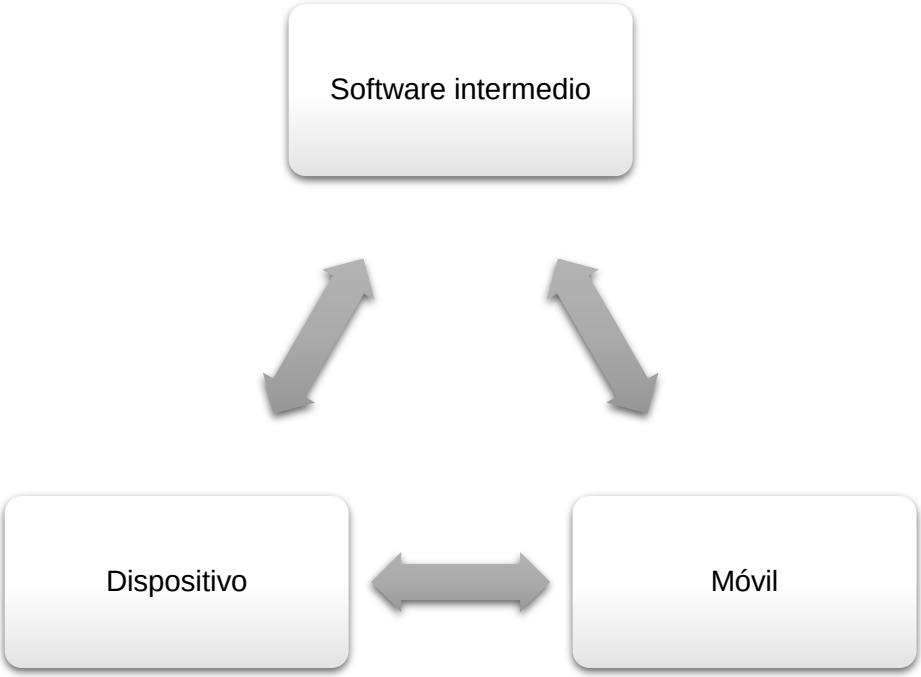


Figura 2. Componentes de comunicación IoT

Fuente: (Martínez-Santander & Cruz, 2021)

Sobre ello, s+e estima que IoT ha establecido una conexión universal de personas, objetos, sensores y servicios (Tejada, 2020). El objetivo principal del IoT es proporcionar una infraestructura de red que permita protocolos de comunicación, *software* e incorporación de sensores físicos/virtuales, computadoras personales, dispositivos inteligentes, automóviles y diferentes objetos de la vida real para conectarse entre sí en cualquier momento y en cualquier red.

Las crecientes capacidades de diferentes tecnologías como la identificación por radiofrecuencia, la red de sensores inalámbricos y la mayor capacidad de almacenamiento de estas tecnologías aumentarán los dispositivos interconectados (Laguna, Rosales, Balbuena, Zamora, & Frías, 2020).

Los diferentes objetos de la vida cotidiana como personas, vehículos, computadores, libros, televisores, teléfonos móviles, ropa, alimentos, medicinas, pasaportes, equipaje, etc. tendrán al menos una identificación única que les permita comunicarse entre sí.

Internet de todo (IoE) es la combinación de personas, procesos, datos y cosas para hacer que las conexiones de red sean más valiosas que nunca (Alcázar, 2018). Es útil convertir la información en acciones que crean nuevas capacidades y aumentan las oportunidades económicas para las empresas, las personas y los países. Sobre ello, se prevé el desarrollo de componentes principales de IoE, tales como:

a. Las personas estarán conectadas de maneras más relevantes y valiosas
b. Los datos serán más inteligentes para tomar mejores decisiones
c. El proceso entregará la información correcta a la persona correcta en el momento correcto y
d. Las cosas son dispositivos físicos y objetos conectados a internet.

Consecuentemente, IoE es una variación de IoT y es útil para mejorar los resultados de la industria al aumentar el poder de Internet, también es útil para aumentar el progreso del internet de las cosas en la aplicación de la vida diaria.

Características de Internet de las Cosas (IoT)

El Internet de las Cosas es la mezcla de diferentes tecnologías de *hardware* y *software*; por lo que, las soluciones de IoT basadas en la integración de tecnología de la información, se basan en *hardware* y *software* utilizados para almacenar, recuperar y procesar datos (Estévez & Castro, 2016).

Internet es la principal fuente de comunicación para la conectividad entre diferentes dispositivos que utilizan tecnologías inalámbricas como Identificación por radiofrecuencia (RFID), Red de sensores inalámbricos (WSN), y Lectores de huellas digitales.

Estas tecnologías utilizan sensores para detectar y monitorear el entorno, estos dispositivos tienen bajos recursos en términos de capacidad de cómputo, memoria, almacenamiento y energía. A continuación, se presenta la figura 4 donde se exponen las características de IoT.

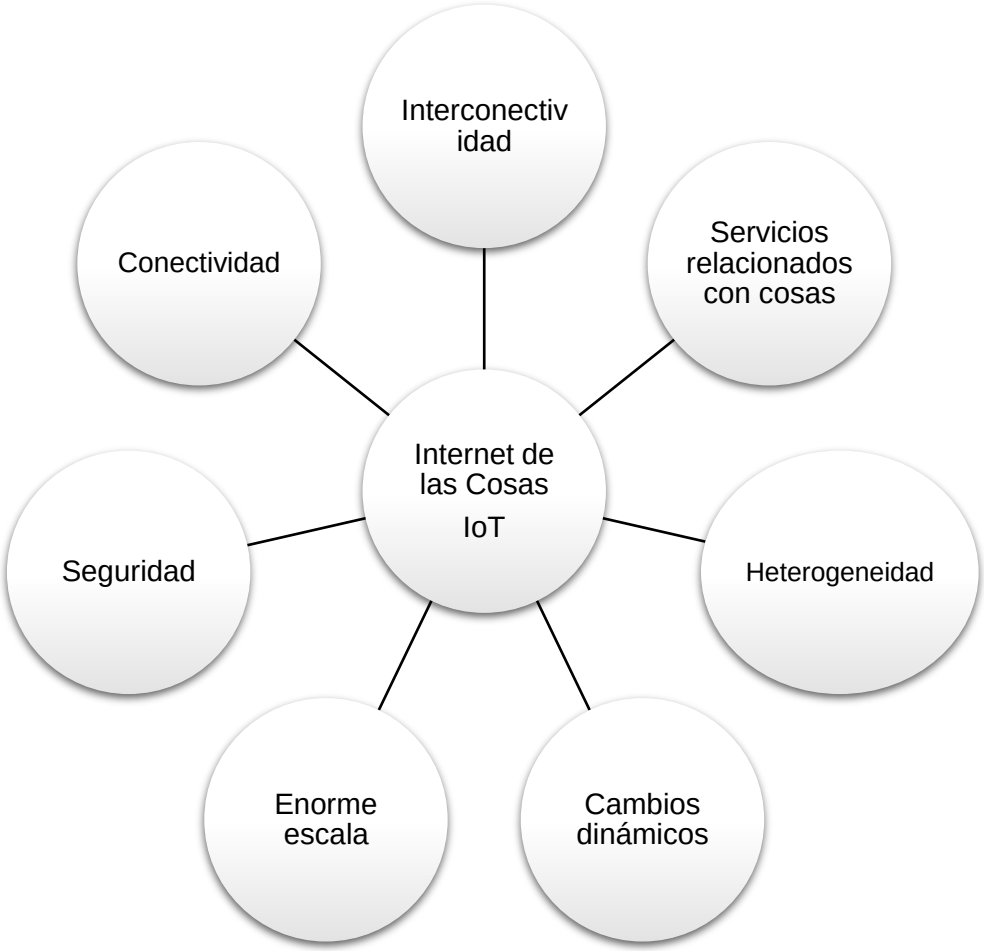


Figura 3. Características de Internet de las Cosas

Fuente: (Alcázar, 2018)

Las características fundamentales del IoT se muestran en la figura 4, presentando a las características como elementos centrales de desarrollo, los cuales son la interconectividad, los servicios relacionados

con las cosas, la heterogeneidad, los cambios dinámicos, la enorme escala, la seguridad y la conectividad.

Interconectividad

El IoT es la conexión de diferentes dispositivos, estos dispositivos se pueden interconectar entre sí utilizando cualquier red; por tanto, los dispositivos conectados se pueden ubicar en ubicaciones distribuidas geográficamente (Bonilla-Fabela, Tavizon, Escobar, Muñoz, & Laines, 2016).

Los dispositivos conectados pueden producir y compartir una gran cantidad de datos que se almacenan y procesan en una ubicación centralizada como la nube.

Servicios relacionados con las cosas

Estos servicios se brindan dentro de los límites de cosas como la privacidad y la coherencia entre las cosas físicas y sus cosas virtuales asociadas (Estévez & Castro, 2016).

Por ello, los servicios relacionados con las cosas están integrados dentro de los sistemas de internet de las cosas para brindar acceso y continuidad en tiempo real a cada persona que requiere su observancia dentro del proceso de revisión de datos e información real.

Heterogeneidad

El sistema IoT consta de diferentes tipos de dispositivos conectados, cada uno de estos dispositivos tiene su propio *hardware* y *software* y sigue un protocolo diferente (Piedra, Sari, & Cedillo, 2018).

Estos dispositivos pueden interactuar entre sí a través de diferentes redes.

Cambios dinámicos

El entorno de IoT es muy dinámico y adopta continuamente los cambios; por ello, los dispositivos conectados a través del sistema IoT se pueden distribuir en ubicaciones geográficas. El estado de los dispositivos cambia dinámicamente, tal como la conexión y desconexión de la red (Molano, Lovelle, & Montenegro, 2017).

Además, la cantidad o número de dispositivos conectados y desconectados puede cambiar dinámicamente según la variación del requerimiento. Lo cual se adapta y adecua a las necesidades cambiantes de los sistemas integrados que requiere los elementos de coordinación y comunicación constante en el control y manejo integrado realizado a través de las nuevas tecnologías, específicamente de IoT, como un elemento que aporta a cambios dinámicos constantes.

Enorme escala

La enorme cantidad de datos es producida por los dispositivos interconectados (Ramírez, Hernández, & Duarte, 2019). Los datos e información producidos por estos dispositivos deben gestionarse de forma sistemática.

Conectividad

Permite una red de accesibilidad y compatibilidad; razón por lo que, la accesibilidad se está introduciendo en una red, mientras que la compatibilidad proporciona la capacidad de consumir y producir datos. Siendo así, la conectividad permite la coordinación y comunicación constante de la información necesaria para mantener el control de los procesos integrados a través de IoT.

Sistema de Seguridad

La seguridad de la información es un aspecto importante de la vida de las organizaciones y las personas que utilizan el sistema de información (Tello & Velásquez, 2017). Estos sistemas almacenan y comparten información importante que requiere protección contra una variedad de amenazas que requieren una variedad de controles de seguridad y estos sistemas e información deben protegerse contra el acceso no autorizado, la divulgación, la interrupción o la modificación.

Sin embargo, para sacar el máximo potencial a este mundo del Internet de las Cosas (IoT), es crucial tener la confianza de que los objetos conectados y los datos que se generan sean solo accesibles para personas y las máquinas autorizadas. Implementar soluciones del IoT de una manera efectiva y eficacia significa desplegarlas de manera segura.

Hay muchas maneras en que un atacante puede acceder a las funciones del dispositivo o los datos que generamos. Los puntos principales de ataque se muestran a continuación en las capas del IoT: los dispositivos, la red y la conectividad y la infraestructura de la nube:

a. Ataques a los dispositivos: un pirata informático puede extraer, eliminar o cambiar información dentro de los dispositivos de Internet de las cosas porque estos dispositivos a menudo se dejan en el entorno.
b. Ataques a la red: un atacante puede obtener información antes de que llegue al destinatario. Hay muchos problemas de seguridad diferentes en esta área y es un gran desafío.
c. Infraestructura de la nube: la seguridad en la nube en gran medida está en manos de los proveedores. Por esta razón, los protocolos, y las buenas prácticas son fundamentales para la seguridad en los entornos de la computación en la nube.

La privacidad significa que el proveedor de información (con un usuario) solo puede identificarse observando el uso del sistema (y al menos su detección debe ser muy difícil). La minería de datos se realiza en los

sistemas de Internet de las cosas, y la razón de esto es la existencia de diferentes formas en los sistemas IoT, como (sistema de control de recursos domésticos),

Por lo que, para garantizar la privacidad de la información personal, hay tres cuestiones principales que se deben tener en cuenta:

a. ¿Quién recopila información personal?
b. ¿Cómo se recopila esta información?
c. ¿Cuánto dura el proceso de recolección?

Además, se debe garantizar que la información recopilada por las personas autorizadas se utilice y almacene en los servicios autorizados. Asimismo, todos deben saber qué información sobre su privacidad se proporciona a las personas autorizadas y todo este proceso debe realizarse con el conocimiento de su permiso y consentimiento.

Por tanto, el uso de IoT está aumentando rápidamente, lo que lo convierte en más vulnerabilidades y problemas de seguridad. A partir de ello, se estima que la comunicación y la seguridad de IoT las proporciona una enorme infraestructura inalámbrica y por cable que proporciona conectividad entre los dispositivos (Bernal, 2020).

Consecuentemente, Internet es la base subyacente de IoT, ambas tecnologías, por tanto, enfrentan el mismo tipo de problemas de seguridad, el cual es abordado desde una perspectiva de innovación y mejoramiento de los procesos operativos, funcionales, comunicacionales y de coordinación, especialmente en el control y seguridad de los sistemas integrados. Asimismo, se referencia que internet de las cosas se compone de tres capas principales:

a. Capa de percepción,
b. Capa de transporte,
c. Capa de aplicación.

Cada una de estas capas tiene sus propios problemas de seguridad; la seguridad de la información se compone de tres objetivos, que son: confidencialidad, integridad y disponibilidad (Barrio & Leroux, 2018). La explicación de los objetivos de seguridad de la información se presenta en la tabla 3:

Tabla 1.

Objetivos de la seguridad de la información

Objetivos	***Descripción***
Confidencialidad	Confidencialidad significa que la información no debe estar disponible o divulgarse a personas no autorizadas.
Integridad	Integridad significa garantía de exactitud y confiabilidad de que nadie puede hacer cambios sin autorización.
Disponibilidad	Disponibilidad significa que los datos o la información deben estar disponibles cuando se necesiten.

Fuente: (Vecchio, Martínez, & Cosentino, 2018)

Los principales objetivos de la seguridad de la información se analizan en la tabla 3, los cuales son los más comúnmente disponibles en toda la literatura de seguridad de la información, pero existen algunas propiedades más que son igualmente importantes para la seguridad de la información (Pisano & Hoffman, 2018). Esas propiedades se explican sobre lo siguiente:

a. Autenticidad: Significa que los datos/información son genuinos y pueden ser verificados y confiables.
b. Responsabilidad: Presenta los medios de responsabilidad, no repudio, disuasión, aislamiento de fallas, detección y prevención de intrusiones y acción legal.
c. No repudio: Tanto el remitente como el receptor proporcionan la prueba del envío y recepción de los datos.

d. Confiabilidad: Significa que los resultados son consistentes y tal como están previstos.

Un sistema de control de acceso hace referencia al funcionamiento de la identificación ya autenticada que permite acceder a datos o recursos. Actualmente, podemos encontrar múltiples formas y para diversas aplicaciones para sistemas de control de acceso.

Un caso común de un sistema de control de acceso es por software cuando digitamos nuestra contraseña para ingresar al correo, o cuando debemos colocar nuestra huella en un lector biométrico para ingresar a un edificio o establecimiento.

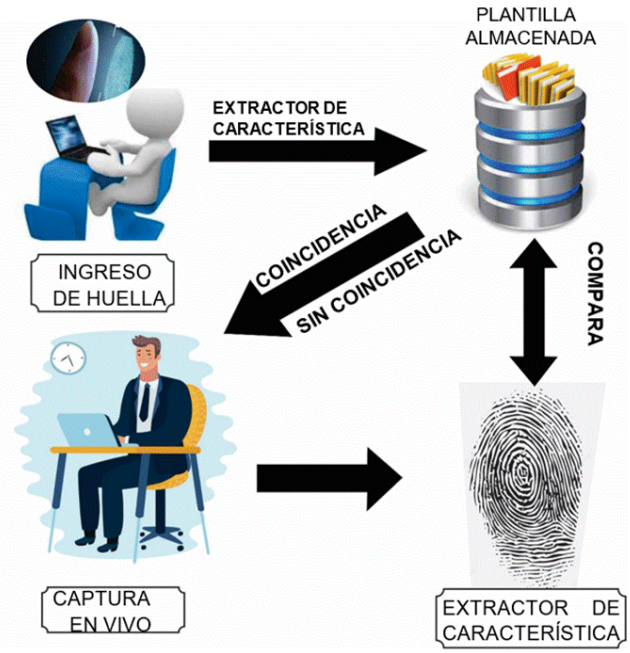


Figura 4. Arquitectura de un sistema biométrico.

Sin embargo, nuestro enfoque se ve relacionada en la seguridad electrónica que está vinculada al acceso de los recursos. Un sistema de control de acceso que restringe o permite el acceso de un usuario en un área específica que es validada la identificación por medio de diferentes tipos de lectura como: claves por teclado, tags de proximidad o biometría y que a su vez está controlando una puerta o torniquete mediante un

dispositivo que tiene sensores y actuadores que le ayudan a realizar dicha tarea.

Los sistemas de control de acceso tienen 2 clasificaciones:

1) Sistemas de Control de Acceso Autónomos.
2) Sistemas de Control de Acceso en Red.

Los sistemas autónomos son los que permiten controlar una o más puertas, sin tener una conexión a una PC o un sistema central, por consiguiente, no guardan registro de los eventos o sucesos.

La principal limitante, debido a algunos controles de acceso autónomos no pueden limitar el acceso por horarios o por grupos de puertas, esto va depender de la instalación de los dispositivos en el área que se emplean. Uno de los métodos más sencillos es la de identificación ya sea por clave, proximidad, lector RFID como una “tarjeta” electrónica.

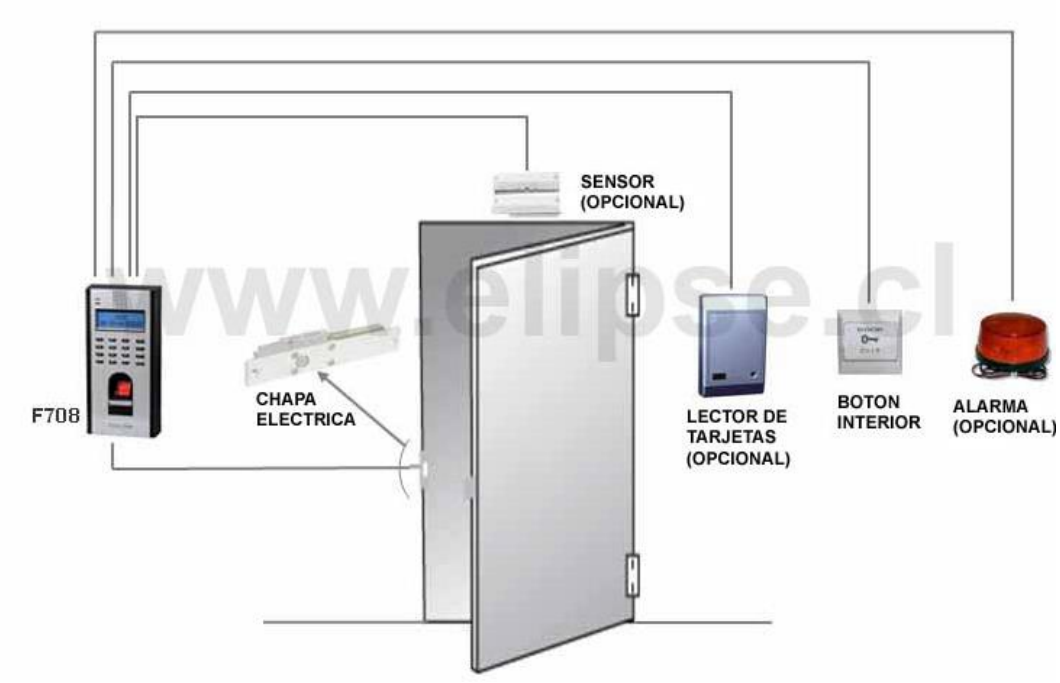


Figura 5. Sistema de Control de Acceso Autónomo.

Los sistemas de Control de Acceso en Red son sistemas que se integran a través de una PC de forma remota o local, en donde tenemos disposición un software de control de acceso que permite llevar a cabo los

registros de todas las operaciones realizadas sobre el sistema con fecha, horario, autorización, etc. Por lo tanto, va desde aplicaciones sencillas hasta sistemas muy complejos y sofisticados para industrias según el requerimiento.

Figura 6. Sistema de Control de Acceso en Red.

Normas ISO

ISO conjuntamente con IEC fueron los primeros que decidieron reunir las mejores prácticas para crear estándares de IoT, el cual fue establecido en 2018, a través de un grupo de trabajo especial de estandarización del Comité Técnico Conjunto ISO/IEC, que desarrolla y facilita el mejoramiento de estándares para IoT (Norma ISO/IEC 30141 , 2018).

Desarrollada conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), la serie de normas ISO/IEC (30141) es una colección de normas publicadas, relacionados con la tecnología de la información, las técnicas de seguridad, la privacidad, la respuesta ante incidentes y la gestión de riesgos que se

pueden utilizar en una amplia gama de tipos y tamaños de organizaciones empresariales.

La serie de normas ISO/IEC tiene un alcance amplio y cubre una variedad de áreas que incluyen privacidad, confidencialidad, integridad, disponibilidad, tecnología de la información técnica y otras áreas de ciberseguridad (Berreño, Herrera, & Alarcón, 2020). Sin embargo, un buen número de estándares también cubren tecnología de la información y técnicas de seguridad, con lo que, el diferenciador de estas normas se centra en la seguridad para el usuario.

Todos estándares de la serie ISO/IEC se aplican a organizaciones de todos los tamaños, especialmente en la evaluación y mitigación de los riesgos de información y seguridad cibernética (Bonilla-Fabela, Tavizon, Escobar, Muñoz, & Laines, 2016). También es importante tener en cuenta en este punto que la serie de estándares se actualiza continuamente para estar en línea con la naturaleza dinámica de la ciberseguridad, así como las amenazas de seguridad, vulnerabilidades y otros impactos en constante cambio de los incidentes de ciberseguridad.

ISO/IEC han desarrollado estándares en esta área (IoT) y reúnen todos los requisitos de seguridad en una sola forma universal. Los estándares brindan a las personas y organizaciones una base para una comprensión mutua del IoT. Esto abarca desde estándares para la calibración de medidores de flujo, pasando por estándares para el cumplimiento de la comunicación inalámbrica, hasta estándares para implementaciones y consideraciones de IoT, lo cual se hace para:

a. Alinear la comprensión de temas técnicos profundamente especializados en todo el mundo.
b. Ayuda a crear un vocabulario común conciso para las tecnologías emergentes
c. Está al tanto de los estándares emergentes que son relevantes para que la industria prospere.

d. Es capaz de asegurar que el contenido de los estándares esté alineado con sus intereses desde una perspectiva local y empresarial.

En concordancia con lo anterior, ISO/IEC 30141 (IoT), proporciona una arquitectura de referencia de IoT estandarizada internacionalmente, que según la organización ayudará a garantizar que los sistemas conectados sean perfectos, más seguros y mucho más resistentes.

Su propósito es lograr esto proporcionando un marco común para los diseñadores y desarrolladores de aplicaciones de IoT y facilitando el desarrollo de sistemas confiables, lo que significa que son confiables, seguros, amigables con la privacidad y pueden soportar interrupciones como desastres naturales y ataques.

Destaca los requisitos funcionales, como la gestión de datos, la gestión de dispositivos, la seguridad, la confidencialidad y la privacidad, y también destaca los requisitos no funcionales, como la mantenibilidad, la fiabilidad, la facilidad de uso, la alta disponibilidad y la escalabilidad de su sistema.

Por lo tanto, al usar la arquitectura de referencia, es posible que personas externas entiendan su sistema y fomenten una mayor interoperabilidad, lo que permite que otros usen sus datos. La arquitectura de referencia de IoT destaca seis dominios y entidades relacionadas que se comunican e intercambian datos por medio de la red, lo que genera mejores resultados en seguridad y operatividad.

Amenazas y vulnerabilidades de seguridad de IoT

La seguridad y la privacidad son desafíos inherentes a muchos dominios de aplicaciones de IoT. La piratería de dispositivos IoT está causando serios desafíos de seguridad y privacidad que tienen el potencial de arrastrarse hacia el futuro imprevisible de IoT.

Con nuevos dispositivos IoT que se fabrican diariamente y se agregan a las redes existentes, su conectividad a Internet proporciona a los actores maliciosos un punto de entrada a entornos inteligentes donde pueden llevar a cabo sus actividades maliciosas, especialmente porque muchos de los dispositivos IoT sufren lagunas de seguridad conocidas. Dentro de estas perspectivas de amenazas y vulnerabilidades se prevé lo siguiente:

a. Desafíos técnicos
b. Cambios legales
c. Cambios éticos de la innovación
d. Cambios operativos
e. Cambios adaptativos
f. Desafíos de registro de información

Por ello, la conectividad con nuevos dispositivos IoT que ingresan al mercado, también se están convirtiendo en un desafío (Condori, 2019). Por lo que, es necesario desarrollar nuevos modelos, protocolos y tecnologías de comunicación para admitir las decenas, cientos y miles de nuevos dispositivos que se conectan diariamente a Internet.

Otros desafíos y vulnerabilidades de seguridad, incluyen compatibilidad, interoperabilidad, escalabilidad, análisis y acciones inteligentes, confiabilidad, gestión de la red de IoT y sus recursos, confidencialidad y visualización de datos (Carrillo & Marroquín, 2016). Estos elementos se constituyen los referentes de los cambios y desafíos que requieren ser observados para minimizar las vulnerabilidades y amenazas del uso del sistema de manera integral.

Implementación de seguridad IoT

Como se discutió en la sección anterior, cada una de las capas tiene diferentes tipos de ataques de seguridad (Cruz, Ortega, Demera, &

Zambrano, 2018). Las diferentes medidas de seguridad se implementan para proteger los datos, tales como:

a. Cifrado;
b. Autenticación,
c. Confidencialidad y
d. Control de acceso.

En consecuencia, la implementación de medidas de seguridad en el sistema de IoT, es fundamental para el desarrollo y ejecución de los sistemas en cualquiera de los escenarios de la vida diaria donde se desee posicionar y operar de manera integrada (Joyanes, 2021).

Protocolos para Internet de las Cosas (IoT)

Para implementar un sistema de Internet de las Cosas (IoT) vamos a necesitar conectividad, algunos protocolos y ciertos estándares. Entonces veamos a que le llamamos conectividad.

Podemos decir que la conectividad son todos los recursos, elementos técnicos desplegados en una zona que vamos a utilizar para transportar la información entre dispositivos o desde dispositivo hacia humano y a su vez entre humanos. Cuando hablamos de conectividad para implementar un sistema IoT podemos utilizar diferentes formas de conectarnos:

- LAN
- Wifi
- GSM, LTE, 5G
- Bluetooh

IPV6 para el Internet de las Cosas (IoT)

El agotamiento de la IPV4 tiene un limitante que en el Internet de las Cosas (IoT) no va poder conectar tantos dispositivos debido a la falta de direcciones IP, ya que solo cuenta con 4 mil millones de direcciones por lo

que con el crecimiento de los “Servicios en la Nube” no va ser suficiente para satisfacer la demanda global. Por esa razón las organizaciones están optando por el IPV6 ya que permite el crecimiento de la red ya que puede contar con infinitas direcciones IP.

El IPV6 mejora el protocolo de comunicación y básicamente permite asignar un número mayor de direccionamiento. Las direcciones pasaron a ser de 128 bits en cambio el protocolo IPV4 son un número de 32 bits.

A nivel global la migración de IPV4 a IPV6 al principio iba a un ritmo muy lento y en América Latina el agotamiento de direcciones ha crecido exponencialmente. La organización LACNIC (Registro de direcciones de Internet de América Latina) hace el llamado a migrar a esta tecnología lo más pronto posible.

Es fundamental entender a IPV6 como una herramienta clave que nos beneficia para lograr un mayor desempeño de las aplicaciones de Internet. Para esto, LACNIC (Registro de direcciones de Internet de América Latina) como será posible el crecimiento continuo a través de la red con una correcta transición al protocolo de internet IPV6, de manera segura y estable para toda América Latina.

El protocolo de Internet es una necesidad y un requisito para llevar a cabo una conexión a Internet. Por ese motivo se ha llevado a cabo una transición a IPV6 como se puede ver en la Figura 8 usuarios que acceden a Internet a través del protocolo IPV6. Por lo tanto, será elegido para interconectar con casi todos los dispositivos IoT inteligentes.

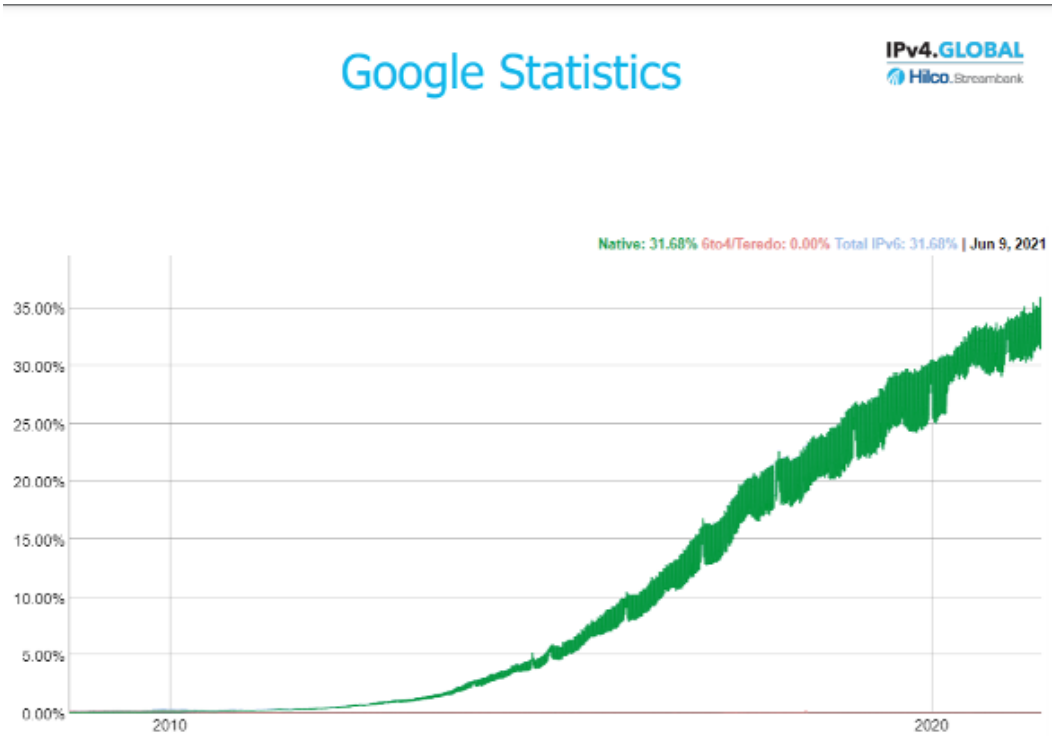


Figura 7. Estadísticas de usuario que acceden a Internet a través de IPV6.

Consecuentemente, se presentan algunos de los protocolos estándar definidos para los ecosistemas de IoT; asimismo, existen una serie de protocolos de comunicación utilizados en Internet de las cosas (IoT).

Protocolo de aplicación restringida (CoAP)

Este es un protocolo de utilidad de Internet diseñado para dispositivos con recursos limitados. Fue creado para permitir que dispositivos simples y de recursos limitados se conecten a sistemas IoT a través de redes restringidas con ancho de banda limitado (Norero & Salazar, 2019).

Este protocolo se utiliza para la comunicación de máquina a máquina (M2M) y se creó específicamente para los sistemas de Internet de las cosas (IoT) que utilizan protocolos HTTP.

El protocolo de aplicación restringida utiliza el protocolo UDP para la implementación normal. También utiliza una arquitectura tranquila que es similar al protocolo HTTP; utiliza DTLS para el cambio de estadísticas sin problemas dentro de la capa deslizante. Los dispositivos IoT se están convirtiendo en componentes importantes en la implementación de diferentes tipos de servicios en entornos inteligentes.

Para superar los diferentes desafíos que pueden suscitarse de su implementación, la literatura actual prevé soluciones potenciales que pueden ayudar a proteger entornos inteligentes basados en IoT y garantizar la continuidad y estabilidad de los servicios en implementaciones futuras (Bonilla-Fabela, Tavizon, Escobar, Muñoz, & Laines, 2016).

Protocolo de transporte de telemetría de cola de mensajes (MQTT)

Es un protocolo de mensajería desarrollado conjuntamente por Andy Stanford Clark de IBM y Arlen Nipper de Arcom en 1999 (Cosin & Manzoni, 2021). Se creó principalmente para la comunicación M2M (máquina a máquina) y el seguimiento remoto en entornos de IoT; su objetivo principal es recopilar datos de diferentes dispositivos, objetos y dispositivos.

Este protocolo vincula dispositivos y redes a paquetes de software y software intermedio; por lo que, los protocolos MQTT ayudan a TCP a facilitar fuentes de información seguras y confiables. Hay tres componentes principales de este protocolo, que son: suscriptor, editor y distribuidor.

El escritor genera los datos y transmite los datos a los suscriptores a través del distribuidor, luego, el distribuidor garantiza la seguridad al verificar la autorización de los editores y suscriptores.

Protocolo Avanzado de Cola de Mensajes (AMQP)

Es un protocolo de capa de *software* de infraestructura de software medio, orientado a mensajes. Utiliza primitivas de garantía de transporte de mensajes para garantizar un intercambio verbal fluido y seguro (Castillo & Navarro, 2019).

Estos protocolos de Internet de las cosas están formados por componentes duros y rápidos que enrutan y guardan mensajes dentro de un operador intermediario, así como un conjunto de políticas para conectar los componentes.

A través de ello, hacen posible que los servicios de los clientes interactúen con los distribuidores y el modelo AMQP. Los tres componentes de este protocolo son los siguientes:

a. Intercambio: que recibe mensajes de los editores y los enruta a las colas de mensajes.
b. Cola de mensajes: que almacena mensajes hasta que se procesan completamente a través del *software* del cliente.
c. Vinculación: que describe la conexión entre la cola de mensajes y el cambio.

Servicio de distribución de datos (DDS)

A través de la técnica de envío y suscripción, el servicio de distribución de datos proporciona un cambio de estadísticas escalable, en tiempo real, preciso, mejor en general e interoperable (Augé, 2018). La multidifusión se utiliza para ofrecer QoS de alta calidad a las aplicaciones de IoT.

Por tanto, DDS está disponible en una variedad de plataformas, que van desde dispositivos de bajo consumo hasta la nube, y es compatible con el consumo de ancho de banda verde, así como con la orquestación ágil de componentes del marco.

El protocolo DDS, para IoT tiene las siguientes capas: envío – suscripción centrada en hechos (DCPS) y capa de reconstrucción local de estadísticas (DLRL).

a. La capa DCPS realiza la tarea de entregar los hechos a los suscriptores.
b. La capa DLRL proporciona una interfaz para las funcionalidades de DCPS, lo que permite compartir datos distribuidos entre dispositivos habilitados para IoT.

Estos protocolos mencionados anteriormente son los más importantes para comprender el aspecto técnico del entorno IoT. A partir de ello, se promueve el uso de las nuevas tecnologías como un elemento de innovación y desarrollo en cualquier escenario donde se prevé implementar.

Servicios en la nube

En lugar de una computadora personal o un servidor local, se puede usar un servidor remoto de red almacenado en Internet para alojar, administrar y procesar datos, lo que se denomina computación en la nube o servicios en la nube, en el cual se puede brindar acceso a la red por solicitud, adecuado y escalable que facilite aportar recursos de cómputo (Hernández & Fuentes, 2018).

Con éxito, la combinación de datos dinámicos de una variedad de fuentes de datos está autorizada y habilitada; y a través de ello, se brindan servicios que hacen posible que los recursos informáticos se distribuyan a través de Internet.

La computación en la nube se compone de un conjunto de servicios de cómputo por solicitud que están listos y presentes en Internet. En dichos servicios, se proporcionan disposiciones fundamentales como el cómputo y el almacenamiento de datos; además, se puede definir como un modelo

reciente relacionado con la informática en el que se entrega un nuevo paradigma empresarial para que las empresas y/u organizaciones adquieran TI (Gutiérrez, 2018).

De modo que proporcione una nueva visión de los sistemas informáticos dispensados de alto rendimiento y basados en Internet en los que los recursos relacionados con la informática se proporcionan en forma de servicio.

Amazon Web Services (AWS)

Los AWS (*Amazon Web Services*) es una etapa de computación en la nube y un servicio de almacenamiento en la nube que permite a las empresas, gobiernos e individuos almacenar sus datos y ofrece API (Interfaz de programación artificial).

API es una subsidiaria de Amazon, con sus centros de datos físicos ubicados en todo el mundo, la cual es preferida por la mayoría de los clientes debido a su eficiencia para brindar servicios. Según lo informado por Amazon, aproximadamente el 50% del mercado de marcos de nube pública, se fortalece con un valor de alrededor de US$ 32 mil millones de dólares estadounidenses, atendiendo a miles de clientes en más de 190 países (Amazon.com, Inc., 2022).

Otro factor importante que convierte a AWS en la opción principal es que sus servicios son muy baratos en comparación con otros proveedores (Brañes & Osoria, 2019). Dada la amplia presencia en el mercado y la prominencia de la empresa, evaluar el área temática en el contexto de AWS puede permitir el desarrollo de hallazgos fácilmente generalizables.

Esto permite a los usuarios hacer que sus aplicaciones sean mejores y más fáciles de usar con su interfaz fluida, proporciona una estructura fluida para todas las industrias (Carrillo & Marroquín, 2016). Administrar una

infraestructura propia puede ser muy difícil y requiere una gran inversión, por ello, bajo la reflexión de AWS elimina este problema para los usuarios.

A partir de ello, se ofrece una plataforma para que cada usuario perteneciente a diversas industrias, que haga su trabajo escalable y atractivo. Sus usuarios involucran entrega de contenido, comercio electrónico, alojamiento de medios, motores de búsqueda, alojamiento web y muchos más. Consecuentemente, podría denominarse como una colección de servicios que están disponibles en conjunto. Estos servicios pueden ser los siguientes:

a. Amazon EC2
b. Amazon S3
c. Amazon Simple Queue Service

Amazon EC2 (*Elastic Compute Cloud*) se considera un servicio web que ofrece capacidad de cómputo a la nube que podría redimensionarse. Amazon Simple Storage Services (Amazon S3) es una de las divisiones que se utiliza para acceder a una gran cantidad de datos desde cualquier lugar y en cualquier momento.

Los desarrolladores cuentan con un acceso sólido, un sistema de almacenamiento de datos rápido y confiable; el sistema es utilizado por Amazon y opera utilizando sus servicios (Toledo, Nogales, & Zaragoza, 2017). La disponibilidad del contenido durante la extracción de los detalles debe ser constante y la fuente no debe interrumpirse. Con ello, se reduce el riesgo de pérdida de datos durante el proceso de transmisión.

Amazon SQS (*Amazon Simple Queue Service*) gestiona la transmisión de maquinaria, la complejidad de los datos junto con las estadísticas biomédicas que se está llevando a la nube.

En consecuencia, *Amazon Web Services* ayuda a proporcionar a los operadores del sistema CUP, memorias, redes y sistema operativo. Sin embargo, a pesar de los avances realizados, quedan algunos problemas fundamentales de escalabilidad y seguridad considerando los *petabytes* de

mensajes de información para mantener los datos intactos mientras el mensaje se transmite de un sistema informático a otro.

La computación en la nube ha facilitado la realización de negocios y la prestación de servicios, también ha impulsado el crecimiento de las pequeñas y medianas empresas (pyme), microempresas, y todo el segmento de desarrollo y productividad en Ecuador y el mundo, en grandes proporciones, las cuales han sido motivadas a la implementación de herramientas tecnológicas como elemento de modernización. AWS demuestra ser el mejor en ofrecer servicios de computación en la nube para individuos, organizaciones y muchas entidades comerciales.

Por esta razón, la provisión de estos servicios de desarrollo tecnológico que integran elementos de IoT, de manera asequible hace que Amazon Web Services (AWS), sea más popular y lidere el servicio a nivel mundial, considerando todos los aportes que realiza en la industria, la empresa y la comunidad en general para el crecimiento y modernización de los recursos de todo tipo. La prestación de servicios de computación en la nube no se limita únicamente al sector empresarial.

Consecuentemente, la seguridad es una preocupación importante para todos los clientes, especialmente debido a la vulnerabilidad de los datos, por lo que, los clientes son especialmente sensibles a que se acceda a sus datos sin su consentimiento. Es así, que las estimaciones de seguridad en las integraciones de protocolos en el desarrollo tecnológico, se constituye como una importante herramienta que puede y debe ser utilizada por todos los entornos de crecimiento, sean públicos y/o privados, para fomentar el desarrollo, control y seguridad en tiempo real.

Sin embargo, las pequeñas y medianas empresas observan una mayor sensación de seguridad con Amazon Web Services, además de su asequibilidad. Como resultado, AWS es una opción preferible para todas las empresas nuevas y futuras que han proyectado sus elementos de desarrollo a través de la utilización de herramientas tecnológicas como parte de la modernización e integración a un mundo globalizado.

Comparativa: Amazon Web Services (AWS) VS. Microsoft Azure VS. Google Cloud Platform

En la actualidad son 3 las empresas, entre otras; que ostentan la gran mayoría del mercado del Cloud Computing como son Amazon Web Services, Microsoft Azure y Google Cloud Platform, cada uno ofrece los servicios que cumplen funciones diferentes y dependiendo en que se lo vaya a utilizar (Bernal, 2020). Sobre ello, la demanda de servicios en la nube ha aumentado rápidamente en los últimos años, lo que ha dado como resultado un gran auge en la escalabilidad de los usuarios de la plataforma en la nube.

La comparativa de estas plataformas, se estima en el mundo actual, donde la computación en la nube se ha convertido en una de las principales tecnologías líderes. Los beneficios de la nube tienen un impacto directo en los proveedores de servicios y los clientes. Las compañías como Microsoft, Google y Amazon, cambian regularmente el esquema de precios para brindar un servicio más amigable al cliente.

Las plataformas de servicios en la nube prueban una variedad de servicios que incluyen almacenamiento, carga y descarga. La computación en la nube ha cambiado la forma de almacenar y administrar datos del enfoque tradicional al nuevo enfoque en la nube (Calva, Rojas, Román, & Radicelli, 2020). La computación en la nube brinda administración de datos a un precio eficiente y a un costo razonable.

Una de las diferencias fundamentales, es que la nube proporciona varios tipos de certificados SLA entre el cliente y el proveedor de servicios. Como nube, ofrece varios modos de precios y varios beneficios para sus clientes. El precio es un elemento importante para que la organización brinde un servicio basado en la nube porque afecta directamente los requisitos del cliente y las ganancias de la empresa.

La fijación de precios tiene un impacto directo en la economía, las acciones, las ganancias y las pérdidas. Las opciones de precios de la computación en la nube son muy flexibles y personalizadas según los requisitos del cliente y la experiencia de los proveedores de servicios (Castillo & Navarro, 2019). El proveedor de servicios se centra en la calidad de servicio (QoS) garantizada para los clientes.

Aunque el precio del servicio se basa en un marco comercial establecido en la industria de la tecnología, esta tendencia está cambiando ahora. Debido a los modelos de cadena de valor recientemente evolucionados adoptados por los servicios de TI tradicionales después del advenimiento de la computación en la nube, se han desarrollado nuevos modelos de precios en esta área de servicio.

Sobre ello, se describe a la cadena de valor como un sistema de actividades independientes, que están conectadas por vínculos. Existe un enlace si la forma en que se realiza una actividad afecta el costo o la eficacia de otras actividades (Norero & Salazar, 2019). Los enlaces explican cómo una actividad afecta a otras actividades y se convierte en fuente, ventaja y valor agregado.

Los productos y servicios pasan por todas las actividades en un orden secuencial y en cada nivel el servicio o producto gana valor, por lo tanto, esta cadena de actividades le da algún valor al producto. Sobre ello, a continuación, se procede a revisar la comparativa entre Amazon Web Services (AWS) VS. Microsoft Azure VS. Google Cloud Platform.

Tabla 2.

Comparativa de servicios en la nube

Proveedores de servicios en la nube	***Beneficios***	***Limitaciones***
Amazon Web Services (AWS)	Amplitud y profundidad de sus servicios Funcionalidad de desarrollador Beneficios económicos para los clientes.	Costo prohibitivo El uso no es fácil. administración del precio superación

	Estándar de oro para confiabilidad y seguridad Controlar la posición del mercado Importante, desarrollar ofertas completas Ayuda para grandes organizaciones Alcance mundial	Tarifa de soporte técnico
Microsoft Azure	Facturación ajustable Platform-as-Service (PaaS) es una demanda bien defendida de Microsoft Precisión y ampliable. Disponibilidad de alto nivel Precio efectivo diferenciarse de la competencia Después del primer proveedor más grande Combinación con dispositivos y software de Microsoft Nube pública y privada integrada Ayuda para código abierto	Consecuencias con la documentación Dispositivos de gestión imperfectos Comparativamente difícil de usar Caro Costo de transferencia de datos Requiere experiencia en la plataforma
Google Cloud Plattform	Tecnología de experiencia profunda Innovación actual, bien autorizada en computación en la nube Modelo de precios ajustable Costo anticipado que los competidores Migración en vivo de máquinas virtuales Delegación a Continuación	Seguridad y privacidad Control y flexibilidad limitados Identificación del proveedor Caracteres o servicios insuficientes Históricamente no como centrado en la empresa

Fuente: (Amazon.com, Inc., 2022)

Siendo así, existe determinado número de proveedores de servicios en el mercado y este documento comprende la comparación de los tres principales proveedores de servicios de plataforma en la nube. Estas plataformas permiten a los clientes centrarse en el negocio en lugar de los aspectos técnicos; la cuestión es que las tres plataformas tienen en común los servicios bajo demanda, la flexibilidad, el soporte y la seguridad.

AWS fue el primero en ingresar al mercado y los consumidores que buscan un producto confiable para abordar todas sus necesidades tecnológicas terminan eligiendo los servicios de nube empresarial.

Microsoft ha asegurado su propia reputación como el nombre más confiable en los negocios empresariales en términos de confianza del consumidor debido a su alta calidad de servicio.

Por otro lado, la nube de Google tiene mucho que ofrecer en términos de innovación y Google tiene sus manos en tantas innovaciones de proyectos pequeños, lo que significa opciones limitadas para empresas más grandes.

Detección como servicio en la nube

Los términos detección como servicio se presentan para describir el proceso de hacer que los datos del sensor y el evento de interés estén disponibles para los clientes y las aplicaciones, respectivamente, sobrevolando la nube en base a su infraestructura (Ávila, 2016).

Las aplicaciones de la red de sensores que utilizan computación en la nube se explican en aplicaciones de sensores, considerando que la nube de sensores es una infraestructura que permite una computación verdaderamente generalizada utilizando sensores como interfaz entre los mundos físico y cibernético, los clústeres de computación de datos como la columna vertebral cibernética e Internet como medio de comunicación.

La nube de sensores integra redes de sensores a gran escala con aplicaciones de detección e infraestructuras de computación en la nube. A partir de ello, recopila y procesa datos de varias redes de sensores, permitiendo compartir datos a gran escala y colaboraciones entre usuarios y aplicaciones en la nube (Cortés & Cabero, 2017).

Consecuentemente, ofrece o brinda de manera oportuna servicios en la nube a través de dispositivos móviles ricos en sensores, con lo que,

permite aplicaciones interdisciplinarias que abarcan los límites de la organización.

Características de sensores de la nube

Los sensores en la nube permiten a los usuarios recopilar, acceder, procesar, visualizar, archivar, compartir y buscar fácilmente grandes cantidades de datos de sensores de diferentes aplicaciones (Calva, Rojas, Román, & Radicelli, 2020). Admite el ciclo de vida completo de los datos del sensor, desde la recopilación de datos hasta el sistema de soporte de decisiones de *backend*.

A partir de ello, se puede procesar, analizar y almacenar una gran cantidad de datos de sensores utilizando recursos informáticos y de almacenamiento de la nube (Paternina & Henríquez, 2016). Permite que diferentes usuarios y aplicaciones compartan recursos de sensores en escenarios de uso flexibles, permitiendo así, que los dispositivos sensores manejen tareas de procesamiento especializadas.

Infraestructura de sensores en la nube

Es la computación en la nube extendida para administrar sensores, y con ello, proporciona dispositivos sensores como parte de los recursos de TI (por ejemplo, CPU, memoria y disco) para los usuarios finales. Así, permite provisionar instancias de servicio automáticamente, monitorear sensores y controlar sensores (Sapién, Diez, & Piñón, 2021). Estas funciones se pueden utilizar a través de la interfaz de usuario mediante del navegador web.

Los propietarios de sensores permiten que el servicio de computación en la nube use sus dispositivos sensores de manera similar a los propietarios de recursos de TI. Los sensores son dispositivos costosos y el mantenimiento del sensor alimentado por batería es bastante alto, con

este intercambio a través del sensor de la nube puede mantener efectivamente este costo con el alquiler generado con varias aplicaciones que comparten los dispositivos.

Estructura de Internet de las Cosas (IoT)

Los dispositivos IoT consisten en múltiples dispositivos como sensores, actuadores, procesadores y transceptores, constando de múltiples tecnologías que funcionan juntas. Los sensores y actuadores son dispositivos que se utilizan para interactuar con el entorno físico (Molano, Lovelle, & Montenegro, 2017). Los datos recopilados por los sensores deben almacenarse y procesarse de manera inteligente para poder derivar inferencias útiles a partir de ellos.

La comunicación entre los dispositivos IoT es inalámbrica porque estos dispositivos están ubicados en una ubicación geográfica preestablecida según los requerimientos de quien opera el sistema de servicios integrado en el internet de las cosas. Por tanto, la comunicación a través de conexión inalámbrica siempre tiene un alto índice de riesgo de falta de fiabilidad y distorsión.

Estructura de capas IoT

La arquitectura IoT consta de tres o cinco capas (Unión Internacional de Telecomunicaciones, 2012). La arquitectura de tres capas se considera la arquitectura más básica. A continuación, se establece los elementos centrales de la arquitectura de capas de IoT.

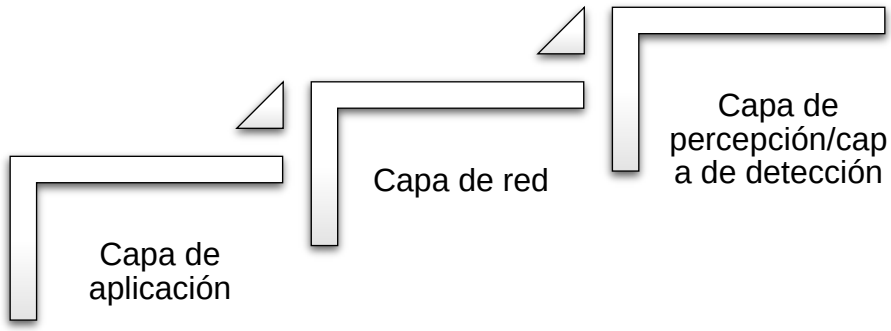


Figura 8. Arquitectura de tres capas de IoT

Fuente: (Barrio & Leroux, 2018)

La figura 5 muestra la arquitectura de tres capas de IoT; la arquitectura de capas mencionada anteriormente se describe de la siguiente manera:

Capa de percepción

Es la capa física, esta capa tiene sensores para detectar y recopilar información sobre el entorno (Bernal, 2020). Esta capa identifica todos los dispositivos que están conectados en el entorno físico.

Capa de red

Esta capa es responsable de conectarse a otras cosas inteligentes, dispositivos de red y servidores (Molano, Lovelle, & Montenegro, 2017). Esta capa también se utiliza para transmitir y procesar datos entre dispositivos conectados.

Capa de aplicación

Esta capa es responsable de entregar servicios específicos de la aplicación al usuario (Tello & Velásquez, 2017). Esta capa define varias aplicaciones en las que se puede implementar IoT en escenarios tales como hogares inteligentes, ciudades inteligentes y salud inteligente.

Estructura de cinco capas

La estructura de cinco capas es la descripción más detallada de la arquitectura IoT. La figura 6 muestra las cinco capas de IoT.

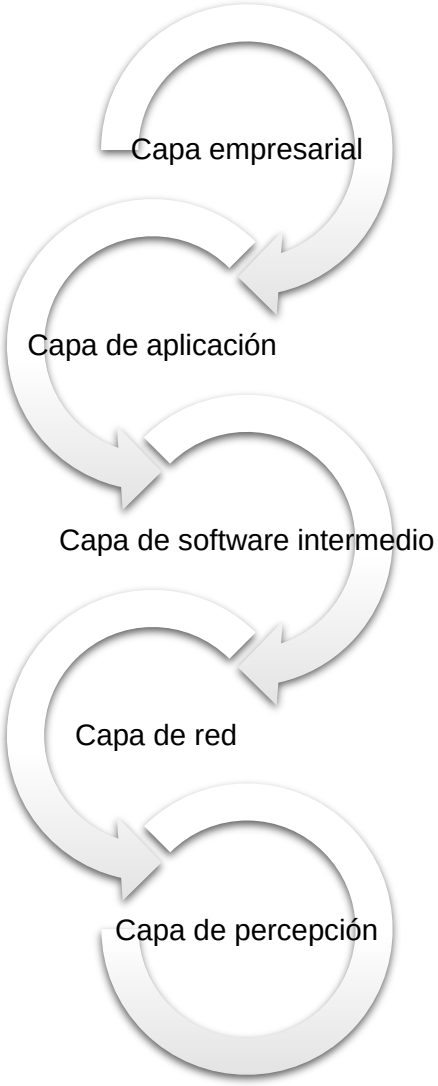


Figura 9. Estructura de cinco capas

Fuente: (Fernández & Noguera, 2017)

Capa de transporte

Esta capa solía transportar datos desde la capa de percepción a la capa de procesamiento y viceversa a través de redes como inalámbricas, 3G, red de área local (LAN), Bluetooth, RFID y comunicación de archivo cercano (NFC) (Salazar & Silvestre, 2018).

Capa de procesamiento

Esta capa también se considera como capa de software intermedio, ya que almacena, analiza y procesa datos que provienen de la capa de transporte (Rose, Eldridge, & Chapin, 2018). Consecuentemente, representa un proceso adecuado para proporcionar servicios específicos que se adaptan a las especificaciones de los requirentes.

Esta capa también es responsable de proporcionar diferentes servicios a las capas inferiores; por tanto, en esta capa también se implementan diferentes tecnologías, y elementos adecuados al escenario que requiere, como bases de datos, computación en la nube y módulos de procesamiento de *big data*.

Capa de negocios

Esta capa administra todo el sistema IoT, administra todas las aplicaciones, los modelos comerciales y de ganancias, y la privacidad del usuario, maximizando de esta forma los beneficios para su aplicación en escenarios empresariales en el fomento de la seguridad en los procesos de crecimiento comercial y productivo (Alcázar, 2018).

Dispositivos de Internet de las Cosas (IoT)

El IoT, consta de muchas redes en las que los dispositivos pueden interactuar entre sí a través de Internet, mejorando con ello, los procesos de comunicación y coordinación de manera integral entre todos los elementos integrados. Estos dispositivos generalmente se denominan cosas y se presentan en la figura 7, cada una de estas cosas tiene sus oportunas propiedades que lo identifican.

Tecnologías de código abierto para el Internet de las Cosas (IoT)

Arduino

Es una plataforma de creación de electrónica de código abierto, que está basada en hardware y software libre, flexible y fácil de usar tanto para los creadores y desarrolladores. La plataforma permite crear diferentes tipos de tareas en una sola placa y que se le puede darle diferentes tipos de uso. Existe una gran variedad de placas de Arduino que son capaces de tomar datos a través de sus pines de entrada de los diferentes sensores que poseen.

El microcontrolador Arduino es una placa basada en ATMEL en la que se la puede programar con el entorno Arduino IDE en donde se le puede asignar instrucciones que permiten crear programas e interactúan con los circuitos de la placa. El software que ofrece Arduino es fácil de usar por usuarios principiantes, pero a su vez es flexible para usuarios ya avanzados.

Los diferentes Arduino que existen son relativamente baratos a comparación de otros microcontroladores, la variedad que tiene permite la creación de un sin número de aplicaciones específicas como para el Internet de las Cosas.

Figura 10. Tipos de placa Arduino.

Arduino Uno es una de las placas diseñadas para la implementación basada en el Internet de las Cosas, esta placa incorpora el microcontrolador ATMEGA328P que permite controlar los diferentes dispositivos electrónicos es un equipo de baja potencia ya que se le puede ejecutar potentes instrucciones en un solo ciclo de reloj.

NodeMCU-32, es una herramienta muy potente para el prototipado rápido de proyectos relacionados con el Internet de las Cosas (IoT) funciona con la plataforma ESP32 que posee conectividad vía Wifi y Bluetooh, además de un procesador CPU de 32 bits de doble núcleo de procesamiento cuyas frecuencias operativas pueden controlarse independientemente entre 80 MHZ y 240 MHZ.

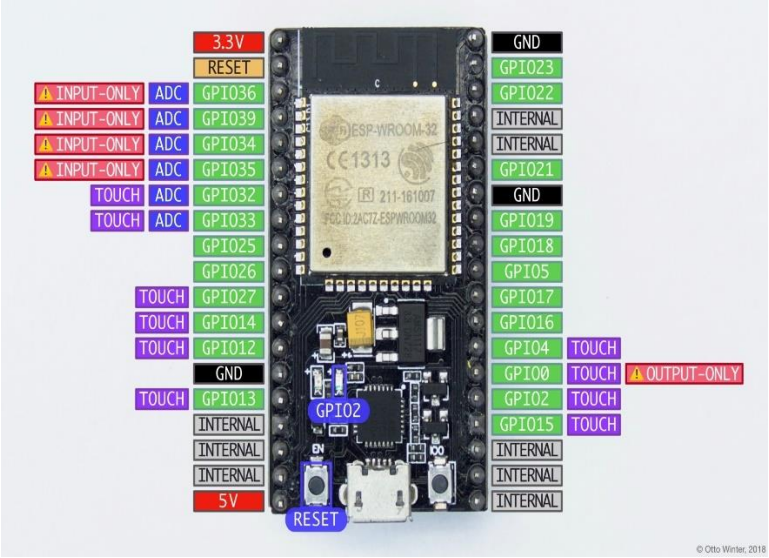


Figura 11. Microcontrolador NodeMCU-32

Lector RFID-RC522, en la actualidad están teniendo bastante popularidad en los sistemas de identificación, su principal uso abarca desde sistemas de seguridad, control de acceso, identificación y logística de productos como llaves o tarjetas de puertas eléctricas, portales de acceso a un edificio u organización entre otras aplicaciones. Su principal funcionamiento se basa en pasar una tarjeta o llavera cerca de un lector

RFID y el TAG tiene la capacidad de enviar la información al lector dicha información puede ser un código de números o hexadecimal, la información dependerá de cómo se guarde en memoria.

ILI9341, es un display LCD que permite mostrar texto o gráficos en proyectos relacionados con el Internet de las Cosas (IoT) o que tengan relación con los distintos microcontroladores como el Arduino Uno, ESP32 o Raspberry PI. La pantalla posee una resolución de 240x320 pixeles, se puede implementar de una manera muy fácil con el microcontrolador ESP32 permitiendo una comunicación y la transmisión de los datos.

Tecnologías de Internet de las Cosas (IoT)

IoT se utiliza para conectar diferentes productos con el mundo digital, esta interconexión entre los dispositivos está creciendo con el avance de las tecnologías como sensores, teléfonos inteligentes, computación en la nube, capacidades de comunicación, etc.

Estos dispositivos integrados a través de las tecnologías IoT, representan un gran avance en el control, manejo y seguridad integrada de los procesos de comunicación, transmisión de datos e información, de manera constante y continua, aportando al desarrollo operativo y tecnológico en tiempo real.

Este aporte de innovación y tecnología, constituye un avance en desarrollo de aplicaciones digitales y herramientas tecnológicas que pueden ser aplicadas y maximizadas en recursos para las organizaciones, mejorando así, sus procesos de control y seguridad, con revisión y monitoreo de sus escenarios de manera oportuna.

Consecuentemente, esta es una red de diferentes objetos físicos como vehículos, máquinas, electrodomésticos y más que utilizan diferentes tecnologías para intercambiar datos a través de Internet. La tabla 2 explica las tecnologías que respaldan el concepto de IoT.

Tabla 3.

Tecnologías de Internet de las Cosas (IoT)

Tecnologías IoT	***Tecnologías de apoyo***
Tecnologías de identificación	Identificación por radiofrecuencia (RFID), Red de sensores inalámbricos (WSN)
Redes y tecnologías de la comunicación	GSM, Sistema Universal de Telecomunicaciones (UMTS), Wi-Fi, Bluetooth, Zigbee.
Tecnologías de software y hardware	Dispositivos inteligentes con comunicación entre dispositivos mejorada

Fuente: (Molano, Lovelle, & Montenegro, 2017)

Tecnologías de identificación

Los dispositivos conectados en el entorno de IoT deben definirse de forma única para posicionar elementos de seguridad en el entorno de aplicación digital, en previsión de la identificación de las tecnologías que se estructuran según los requerimientos del desarrollador al momento de la aplicación en el sistema (Alcázar, 2018). Las tecnologías de identificación como RFID y WSN se utilizan para la identificación única de los dispositivos conectados.

Tecnologías de red y comunicación

Tecnologías como el Sistema de Posicionamiento Global (GSM), Sistema Universal de Telecomunicaciones (UMTS), internet inalámbrico (Wi-Fi), Bluetooth, ZigBee, permiten que los dispositivos se conecten entre sí (Ramírez, Hernández, & Duarte, 2019). La comunicación entre los dispositivos conectados debe ser segura para que el usuario pueda utilizar la red con total confianza y seguridad.

Tecnologías de software y hardware

Los dispositivos inteligentes con alta comunicación entre dispositivos, representados en tecnología de interacción digital, darán lugar a sistemas inteligentes que proporcionen altos grados de inteligencia y autonomía, lo que facilitará la implementación rápida de aplicaciones de IoT (Martínez-Santander & Cruz, 2021).

Síntesis referencial del estudio teórico

Los trabajos referenciales que justifican el presente estudio teórico del capítulo, se presentan sobre autores como Alcázar (2018), en su estudio denominado: La Internet de las Cosas (IoT), Big Data y los nuevos problemas de comunicación en el siglo XXI, el cual se realizó como un análisis de las nuevas tecnologías en el desarrollo de la seguridad y maximización de recursos, donde se expone la importancia de estas tecnologías para promover el crecimiento empresarial y rendimiento operativo, que puede ser promovido desde los entornos corporativos para un control en tiempo real.

Asimismo, el estudio presentado por Bernal (2020), denominado Diseño de una red IoT para el hogar, presenta cómo las nuevas herramientas tecnológicas son utilizadas para promover la seguridad y control de los hogares inteligentes, con una revisión continua de las actividades que acontecen en el lugar, para incrementar los controles habitacionales y maximizar los recursos en las casas, principalmente presentado para el uso en edificios inteligentes y conjuntos residenciales.

La Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (2021), en su informe de tecnología e información, presentado como resultado de los avances y utilización de las herramientas tecnológicas a causa de la pandemia por Covid-19, expone el fomento y difusión que se ejecutó en el distanciamiento social, que obligó a las empresas de todos los tamaños a implementar y/o adaptarse a la utilización de estas

herramientas, integrando al IoT en el desempeño operativo de todos los ámbitos de control y seguridad, entre otros.

El estudio presentado por Cisneros y Altamirano (2021), denominado Estudios de mecanismos de aseguramiento de la información para internet de las cosas IoT en Smart Home, presenta un escenario donde los datos e información sensibles son tratados a través de las nuevas tecnologías para fomentar la seguridad y control en los hogares inteligentes, promoviendo con ello, la integración y uso de estas nuevas herramientas en todos los entornos habitacionales.

Es así, que el presente marco teórico investigó la importancia y desarrollo del IoT y la computación en la nube como un elemento de integración para la seguridad y control en los conjuntos residenciales, especialmente para este documento en la etapa Cosmos de la urbanización Villa Club, considerando que en la localidad y el país se deben fomentar nuevas herramientas tecnológicas que integren a las tecnologías informáticas en la seguridad y control y así promover lugares seguros y vigilados en tiempo real, maximizando la confianza y los recursos de sus habitantes.

Conclusión del capítulo

A partir de los elementos teóricos descritos anteriormente el autor considera utilizar el protocolo MQTT, considerando que es un protocolo ligero de colas y transporte de mensajes, adecuado para el transporte de datos de telemetría (datos de sensores y actores). Además, es muy liviano y, por lo tanto, es coherente para escenarios M2M (*Machine to Machine*), WSN (*Wireless Sensor Networks*) y también IoT (Internet de las Cosas) donde los nodos de sensores y actores se comunican con aplicaciones a través del intermediario de mensajes. Sus características claves centran la consideración para su utilización en el presente proyecto, entre las cuales están:

a. Protocolo de transporte y colas de mensajes ligeros
b. Modelo de comunicación asíncrona con mensajes (eventos)
c. Baja sobrecarga (encabezado de 2 bytes) para aplicaciones de bajo ancho de banda de red
d. Modelo de publicación/suscripción (PubSub)
e. Desacoplamiento del productor de datos (editor) y el consumidor de datos (suscriptor) a través de temas (colas de mensajes)
f. Protocolo simple, dirigido a implementaciones de baja complejidad, baja potencia y bajo espacio físico (por ejemplo, WSN – Wireless Sensor Networks)
g. Se ejecuta en transporte orientado a conexión (TCP). Para usar junto con 6LoWPAN (compresión de encabezado TCP)
h. MQTT atiende las interrupciones de la red (inalámbrica).

Por esta razón se prevé su utilización, estimando que los dispositivos de Internet de las cosas (IoT) se utilizan cada vez más en la vida actual, sin embargo, a medida que aumenta la cantidad de dispositivos conectados, las comunicaciones entre ellos son cada vez más difíciles de escalar. Por tanto, el protocolo de comunicación MQTT ha venido a solucionar este problema ya que es un protocolo de comunicación entre dispositivos IoT que tiene como objetivo centralizar las comunicaciones dentro de un corredor.

Por tanto, una comunicación MQTT típica implica cientos de mensajes por minuto; entonces es difícil analizar una comunicación MQTT con herramientas de rastreo de paquetes. El propósito es proporcionar una herramienta adecuada y disponible públicamente para visualizar y analizar las comunicaciones MQTT con fines de depuración que fomenten procesos operativos para el control y seguridad.

Una de las ventajas se prevé sobre la arquitectura, donde se puede analizar el sistema de complementos que permite extender el visor, cómo se deben almacenar y representar los datos MQTT en el visor y cómo el usuario debe tener acceso a las funciones requeridas. La previsión de los

resultados se prevén revisar con las latencias encontradas cuando el corredor enfrenta mucho tráfico y algunas capturas de pantalla del visor.

En síntesis, es claro que el Internet de las cosas (IoT) está evolucionando y revolucionando la forma en cómo se desenvuelven las personas y las cosas en interactividad funcional digitalizada, por lo cual, su desarrollo en el control continuo de una diversidad de cosas, como casas, urbanizaciones, ciudades, etc., representa una oportunidad para maximizar recursos y promover seguridad y control en tiempo real usando los servicios de la nube como complemento de ejecución.

Consecuentemente, Internet tiene un impacto en escenarios como la educación, comunicación, negocios, ciencia, gobierno y en general toda la humanidad. Claramente, Internet es una de las creaciones más importantes y poderosas en toda la historia humana y ahora, con el concepto de Internet de las cosas, Internet se vuelve más favorable para tener una vida inteligente en todos los aspectos.

Mediante el Internet de las Cosas, los objetos se reconocen a sí mismos y obtienen un comportamiento inteligente al tomar o habilitar decisiones relacionadas con el hecho de que pueden comunicar información sobre sí mismos.

Estos objetos pueden acceder a información que ha sido agregada por otras cosas, o pueden agregarse a otros servicios. La tabla 4 muestra que, con el Internet de las cosas, cualquier cosa podrá comunicarse en cualquier momento y desde cualquier lugar para proporcionar cualquier servicio a través de cualquier red a cualquier persona.

Este concepto creará nuevos tipos de aplicaciones que pueden involucrar elementos tales como vehículos inteligentes y hogares inteligentes, para brindar muchos servicios, como seguridad de notificaciones, ahorro de energía, automatización, comunicación, computadoras y entretenimiento.

La computación en la nube, el modelo de computación de la futura generación como utilidad, tiene la capacidad de hacer que el *software* basado en la nube sea más atractivo como servicio. Los desarrolladores que tienen ideas innovadoras para mejorar los servicios de Internet ya no necesitan configurar una gran cantidad de máquinas físicas o requieren expertos y soporte técnico para operar las infraestructuras. Sobre ello, se presenta el contrate/complemento entre IoT y la nube.

Tabla 4.

Distinción de Internet de las Cosas y la Nube

Internet de las Cosas	***Servicios en la Nube***
Situacional	Ubicuo
Mundo real	recursos virtuales
Limitado	Ilimitado
Almacenamiento limitado	Almacenamiento ilimitado
Punto de convergencia	Prestación de servicios
Fuente de Big data	Medios para gestionar Big data

La tecnología de computación en la nube tiene varias ventajas, como flexibilidad, automatización, bajo costo, servicio rápido y capacidad de almacenamiento ilimitada. Con ello, proporciona a los usuarios una gran flexibilidad, tal como que los usuarios pueden ver sus datos y modificarlos desde cualquier lugar y en cualquier momento utilizando diferentes tipos de dispositivos (como computadoras, teléfonos inteligentes y computadoras portátiles) y diferentes tipos de sistemas operativos (como Windows, Mac y Android).

Este modelo de nube e Internet de las Cosas, promueve la disponibilidad y a partir de ello, se puede categorizar una infraestructura en

la nube a través de sus modelos de implementación, como nube privada, nube comunitaria, nube pública y nube híbrida.

Con ello, el desarrollo de un sistema IoT usando servicios en la nube, se complementa de manera adecuada, en términos de velocidad de cómputo, capacidad de almacenamiento y recursos de comunicación. En síntesis, la distinción de IoT y la nube representan un avance en el desarrollo tecnológico y el uso de las nuevas tecnologías para beneficiar a la sociedad en conjunto.

CAPÍTULO 2

MARCO METODOLÓGICO

MARCO METODOLÓGICO

Tipo de estudio

El tipo de estudio será descriptivo, considerando que se describirá el desarrollo del sistema IoT para el control de acceso y seguridad en la etapa Cosmos de Villa Club en el cantón Durán, usando servicios en la nube. Consecuentemente, el método descriptivo se adapta de manera adecuada al enfoque de investigación.

El tipo de investigación, además se adecua al estudio explicativo, ya que busca detallar el funcionamiento del control de acceso; y es de tipo exploratorio, debido a las nuevas tendencias y gestión de los datos. Por tanto, el estudio descriptivo ha tomado como referencia a las investigaciones, estudios y artículos científicos referenciados en este documento, como elementos que fundamentan la propuesta del proyecto.

Basados en ello, se explicarán los procesos y funciones para la implementación de un sistema de Internet de las Cosas para la gestión de los servicios en la nube AWS (*Amazon Web Services*), considerando que es el elemento oportuno de adaptación para la consecución de la presente investigación.

Enfoque de Investigación

La investigación tiene un enfoque cualitativo, dado que la información denominada incluye datos escritos que se ha analizado anteriormente, en base a los requerimientos operativos obtenidos durante el proceso de investigación proporcionados por la Administración de la Etapa Cosmos de Villa Club, sobre lo que se han fundamentado los datos para la revisión del escenario presentado.

El enfoque cualitativo proporciona los elementos adecuados para cualificar la información necesaria, que es relevante a considerar en la toma de decisiones para la implementación de una propuesta de desarrollo del

sistema IoT para el control y acceso en la seguridad del conjunto habitacional.

Instrumentos para la recolección de información

La herramienta de recolección de información está representada en el informe de control de acceso y seguridad de la etapa Cosmos de Villa Club, proporcionado por la Administración de la Corporación Samborondón Cía. Ltda., CORSAM, en el período 2020 – 2021 para poder analizar los datos de seguridad operativa (Corporación Samborondón Cía. Ltda. CORSAM, 2022).

En referencia a ello, se realiza una encuesta al personal administrativo de la empresa que labora para la etapa Cosmos en la urbanización Villa Club, con el propósito de conocer de manera específica su criterio en referencia a los procedimientos inadecuados que se suscitan en el control de acceso y seguridad. La encuesta se ha predeterminado en 10 preguntas cerradas, con escala Likert para su tabulación y análisis de la información.

Consecuentemente, a partir de los resultados presentados de los criterios recogidos del personal administrativo en referencia al control de acceso y seguridad en la etapa Cosmos, para la urbanización Villa Club, se presentan los resultados como un elemento de sustentación en la propuesta de desarrollo del sistema IoT, en el entorno situacional que prevé una solución para el problema presentado inicialmente.

Población y muestra

La población y muestra han sido representadas en un mismo número de personas, que se han tomado de la administración de la empresa en la etapa Cosmos, en 17 personas del departamento administrativo del

conjunto residencial, las cuales son centrales para el control operativo de acceso y seguridad, para fomentar una toma de decisiones adecuada.

Tabla 5.

Población y muestra de investigación

Descripción	***Número de personas***	***Lugar y fecha***
Muestra de investigación	17 miembros del personal de Departamento Administrativo en área de control de acceso para la etapa Cosmos.	26 a 30 de agosto de 2022 10H00 a 16H30 Urbanización Villa Club, oficina central para etapa Cosmos.

Siendo así, se ha presentado en la tabla 5 a los datos para la recolección de información que se establece sobre 17 miembros del personal administrativo para el control de acceso de la etapa Cosmos, con ello, a continuación, se pueden revisar los datos sobre las interrogantes que dan inicio a la encuesta de investigación para conocer el criterio del personal administrativo.

Encuesta

La encuesta se ha realizado sobre un cuestionario de 10 preguntas cerradas en escala Likert para poder realizar un análisis y tabulación de la información de manera apropiada (cuestionario de preguntas en Anexo 1). Por tanto, a continuación, se procede a la consecución de la encuesta de investigación para conocer el criterio referente al control de acceso y seguridad para la etapa Cosmos de la urbanización Villa Club.

Primera pregunta

¿Cómo calificaría usted el nivel para el control de acceso y seguridad de la etapa Cosmos en la urbanización Villa Club?

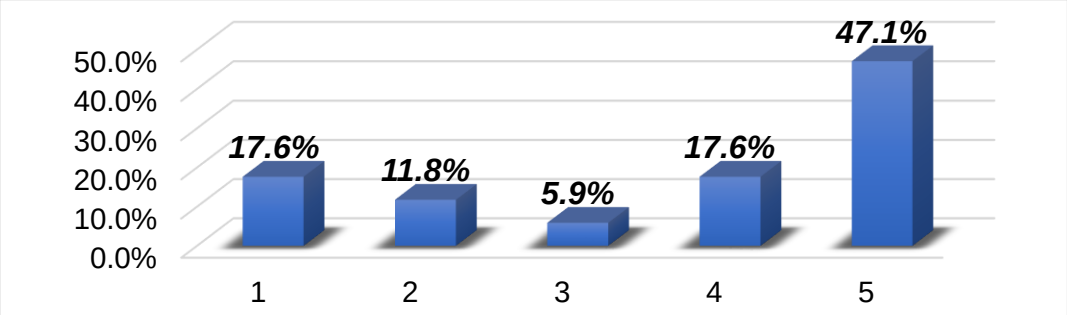


Figura 12. Metodología de procesos operativos actuales

Tabla 6**.**

Escenario metodológico de procesos operativos

Opción	***No.***	***Frecuencia (Fr=17)***	***Porcentaje (%)***
Muy Bueno	***1***	3	17,6%
Bueno	***2***	2	11,8%
Regular	***3***	1	5,9%
Malo	***4***	3	17,6%
Muy Malo	***5***	8	47,1%
Total		**17**	**100%**

Análisis

El 47,1% de los encuestados dijo estar totalmente en desacuerdo respecto al nivel actual para los procesos operativos de control de acceso y seguridad en la etapa Cosmos, considerando que no existe un control integrado y coordinado entre los registros de entradas y salidas de personas, debido a una coordinación y comunicación inadecuada entre todos los miembros del personal.

Segunda pregunta

¿Considera usted que se requiere la implementación de nuevos procesos de seguridad tecnológica e innovación en la gestión de control de acceso a la etapa Cosmos?

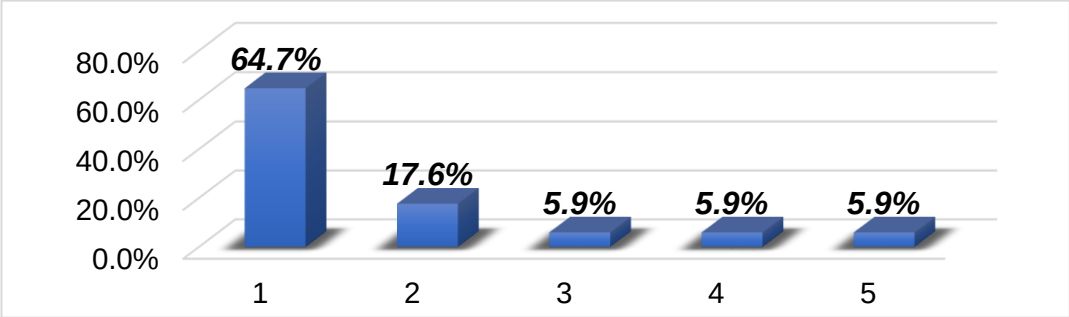


Figura 13. Seguridad tecnológica e innovación en el control de acceso y seguridad

Tabla 7**.**

Resultados de seguridad tecnológica e innovación

Opción	***No.***	***Frecuencia (Fr=17)***	***Porcentaje (%)***
Totalmente de acuerdo	***1***	11	64,7%
Parcialmente de acuerdo	***2***	3	17,6%
Indiferente	***3***	1	5,9%
Parcialmente en desacuerdo	***4***	1	5,9%
Totalmente en desacuerdo	***5***	1	5,9%
Total		**17**	**100%**

Análisis

El 64,7% dijo estar totalmente de acuerdo en que se requiere la implementación de nuevos procesos de seguridad tecnológica e innovación en la gestión de control de acceso a la etapa Cosmos, considerando que el uso, implementación y desarrollo de nuevas herramientas tecnológicas para los sistemas de seguridad, representan un avance y mejoramiento de la coordinación y comunicación en tiempo real para las partes interesadas.

Tercera pregunta

¿Cuál considera usted el principal problema de seguridad en la etapa Cosmos Villa Club?

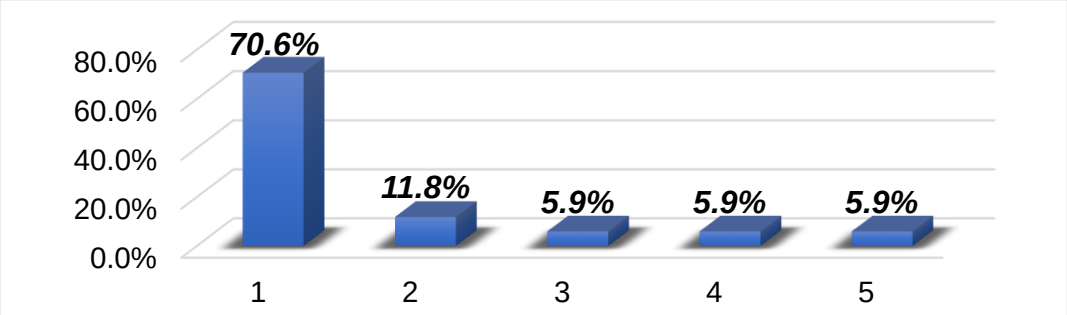


Figura 14. Desarrollo de nuevos sistemas para comunicación y coordinación de seguridad

Tabla 8**.**

Resultados de desarrollo de nuevos sistemas tecnológicos

Opción	***No.***	***Frecuencia (Fr=17)***	***Porcentaje (%)***
Falta de control en las entradas y salidas	***1***	12	70,6%
Falta de vigilancia	***2***	2	11,8%
Robos	***3***	1	5,9%
Homicidios	***4***	1	5,9%
otros	***5***	1	5,9%
Total		**17**	**100%**

Análisis

El 70,6% de los encuestados indicó la falta de control en las entradas y salidas dentro de la urbanización en lo que se demuestra la falta de seguridad por parte del personal administrativo.

Cuarta pregunta

¿De las siguientes soluciones tecnológicas cual considera usted que mejoraría la seguridad en la ciudadela Villa Club Etapa Cosmos?

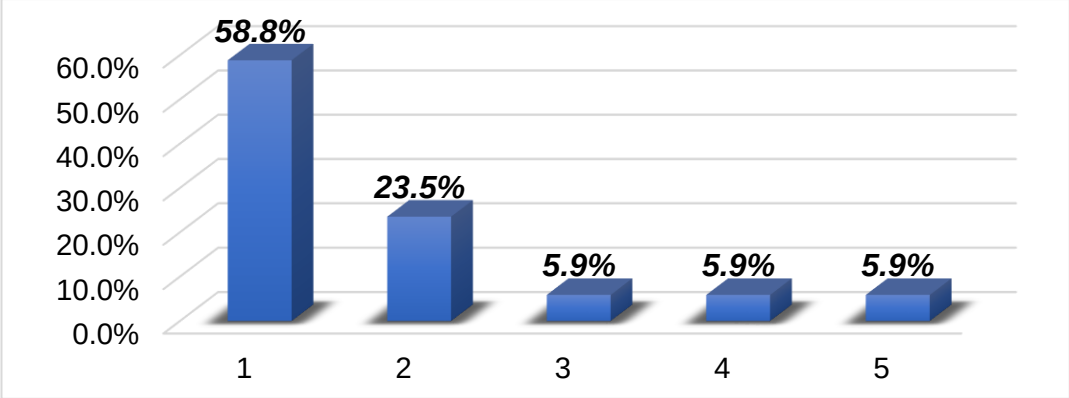


Figura 15. Implementación de nuevos procedimientos a través de herramientas tecnológicas

Tabla 9**.**

Resultados de implementación de nuevos procedimientos

Opción	***No.***	***Frecuencia (Fr=17)***	***Porcentaje (%)***
Lector RFID	***1***	10	58,8%
Lector de huellas digitales	***2***	4	23,5%
Biométrico por teclado	***3***	1	5,9%
Reconocimiento facial	***4***	1	5,9%
Lector de proximidad	***5***	1	5,9%
Total		**17**	**100%**

Análisis

El 58,8% indicó estar totalmente de acuerdo en que la implementación de un lector RFID mejorara los procedimientos de control de acceso para la seguridad, promueven el desarrollo tecnológico para la urbanización, fomentando la innovación y mejores prácticas al momento de realizar el control de acceso en la etapa Cosmos.

Quinta pregunta

¿Considera usted que el desarrollo e implementación de sistemas IoT para el control y seguridad en las urbanizaciones, constituye un beneficio operativo?

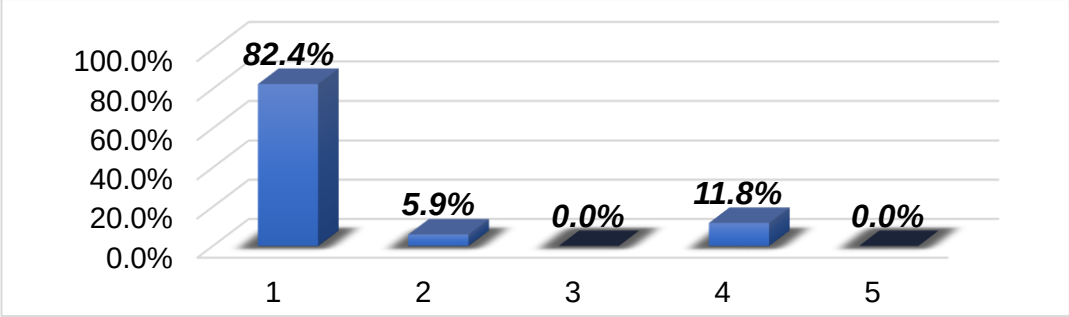


Figura 16. Implementación de sistemas IoT como beneficio operativo

Tabla 10**.**

Resultados de implementación IoT como beneficio operativo

Opción	***No.***	***Frecuencia (Fr=17)***	***Porcentaje (%)***
Totalmente de acuerdo	***1***	14	70,6%
Parcialmente de acuerdo	***2***	1	5,9%
Indiferente	***3***	-	-
Parcialmente en desacuerdo	***4***	2	11,8%
Totalmente en desacuerdo	***5***	-	-
Total		**17**	**100%**

Análisis

El 70,6% dijo estar totalmente de acuerdo en que el desarrollo e implementación de sistemas IoT para el control y seguridad en la etapa Cosmos para la urbanización Villa Club, representa un beneficio operativo, ya que integrará la información en tiempo real, mejorando los procesos de comunicación y coordinación entre el personal y los administradores podrán mantener actualizados los datos sobre entradas y salidas de personas de manera segura.

Sexta pregunta

¿Está usted de acuerdo qué ante los errores de control de acceso y seguridad en la etapa Cosmos, se deben implementar nuevos procesos operativos con sistemas integrados IoT?

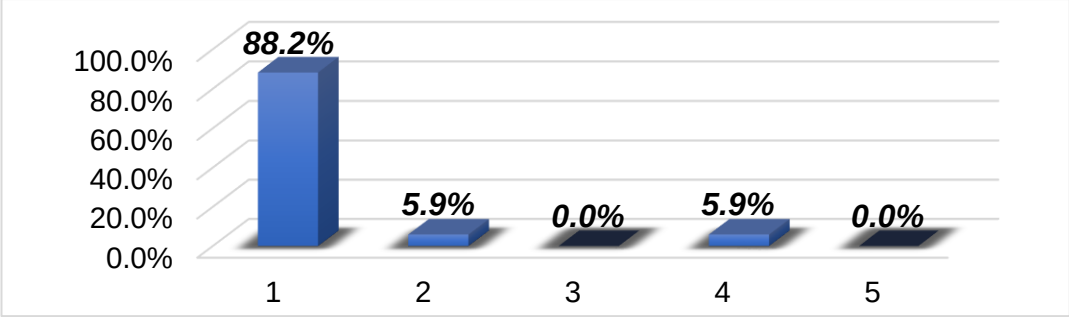


Figura 17. Fortalecimiento de control de acceso y seguridad

Tabla 11**.**

Resultados de fortalecimiento de control de acceso y seguridad

Opción	***No.***	***Frecuencia (Fr=17)***	***Porcentaje (%)***
Totalmente de acuerdo	***1***	15	88,2%
Parcialmente de acuerdo	***2***	1	5,9%
Indiferente	***3***	-	-
Parcialmente en desacuerdo	***4***	1	5,9%
Totalmente en desacuerdo	***5***	-	-
Total		**17**	**100%**

Análisis

El 88,2% indicó estar totalmente de acuerdo en que ante los errores presentados en el informe administrativo enero – enero 2021 a 2022, sobre el control de acceso y seguridad, sí se deben implementar nuevos procesos operativos con sistemas integrados IoT, considerando que la tecnología ya se ha vuelto parte de la vida diaria, y el personal puede adherirse a los beneficios que brinda el internet de las cosas para una coordinación de control en tiempo real en el registro de entradas y salidas de personas.

Séptima pregunta

¿Actualmente considera usted que los porcentajes de errores en los procesos de control de acceso a la etapa Cosmos, incrementan la inseguridad de los residentes?

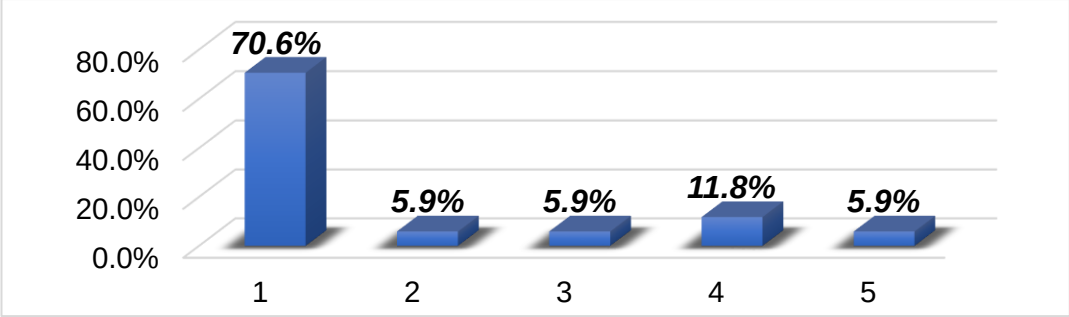


Figura 18. Inseguridad en el control de acceso

Tabla 12**.**

Resultados de inseguridad en el control de acceso

Opción	***No.***	***Frecuencia (Fr=17)***	***Porcentaje (%)***
Totalmente de acuerdo	***1***	12	70,6%
Parcialmente de acuerdo	***2***	1	5,9%
Indiferente	***3***	1	5,9%
Parcialmente en desacuerdo	***4***	2	11,8%
Totalmente en desacuerdo	***5***	1	5,9%
Total		**17**	**100%**

Análisis

El 70,6% indicó estar totalmente de acuerdo en considerar que los porcentajes de errores en los procesos de control de acceso a la etapa Cosmos (ver tabla 1), sí incrementan la inseguridad de los residentes, considerando que de las 12,726 personas que circularon en el conjunto residencial, el 26,8% presentó errores de identificación, que no se registró, y una incidencia de 44,2% de personas que ingresaron sin ser registradas, lo cual expone los errores de seguridad en la actualidad.

Octava pregunta

¿Estima usted que el desarrollo e implementación de un sistema IoT a través de servicios en la nube, maximizará la operatividad y seguridad?

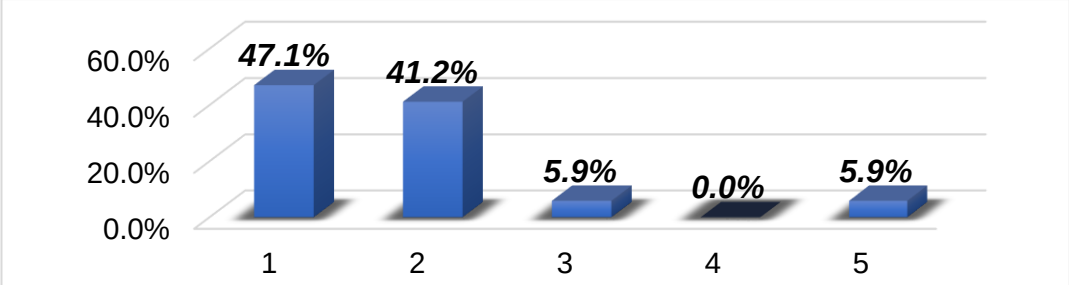


Figura 19. Sistema IoT para maximización de operatividad

Tabla 13**.**

Resultados de Sistema IoT para maximización de operatividad de control

Opción	***No.***	***Frecuencia (Fr=17)***	***Porcentaje (%)***
Totalmente de acuerdo	***1***	8	47,1%
Parcialmente de acuerdo	***2***	7	41,2%
Indiferente	***3***	1	5,9%
Parcialmente en desacuerdo	***4***	-	-
Totalmente en desacuerdo	***5***	1	5,9%
Total		**17**	**100%**

Análisis

El 47,1% indicó estar totalmente de acuerdo, aunque un 41,2% dijo estar parcialmente de acuerdo, esto se debe a que el escenario del control de acceso y seguridad, sí se fortalecería mediante la implementación de un sistema IoT para fomentar un mejor control en tiempo real, más la práctica de revisión y operatividad de control siempre se realiza de manera física entre los guardias y aquellos que ingresan y salen; por ello, consideraron que aunque sí se beneficia su implementación, indicaron que el personal desempeña un papel central en la práctica.

Novena pregunta

¿Está usted de acuerdo en que los avances tecnológicos para el control y seguridad en el acceso de personas a la urbanización, debe fomentar una innovación continua de actualización?

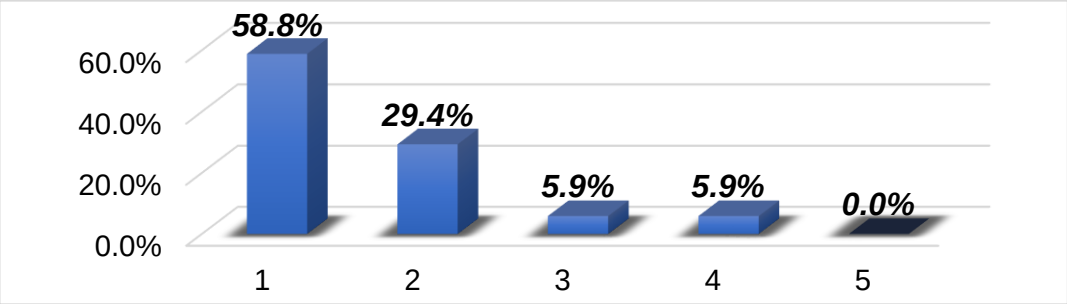


Figura 20. Fomento de avances tecnológicos como innovación continua

Tabla 14**.**

Resultados de fomento de avances tecnológicos

Opción	***No.***	***Frecuencia (Fr=17)***	***Porcentaje (%)***
Totalmente de acuerdo	***1***	10	58,8%
Parcialmente de acuerdo	***2***	5	29,4%
Indiferente	***3***	1	5,9%
Parcialmente en desacuerdo	***4***	1	5,9%
Totalmente en desacuerdo	***5***	-	-
Total		**17**	**100%**

Análisis

El 58,8% indicó estar totalmente de acuerdo en que los avances tecnológicos para control de acceso y seguridad representan un elemento central en la operatividad para la urbanización, por lo que se debe fomentar un proceso de innovación continua en las constantes actualizaciones a las que está sometida la tecnología. Un 29,4% indicó estar parcialmente de acuerdo, ya que consideraron que, aunque es importante mantener un proceso de innovación continua, los cambios constantes pueden causar inconsistencia en la continuidad del proceso diario de control de acceso.

Décima pregunta

¿Estima usted que el desarrollo de un sistema IoT para el control de acceso y seguridad en la etapa Cosmos, mejorarán las capacidades operativas de seguridad y coordinación de información en tiempo real?

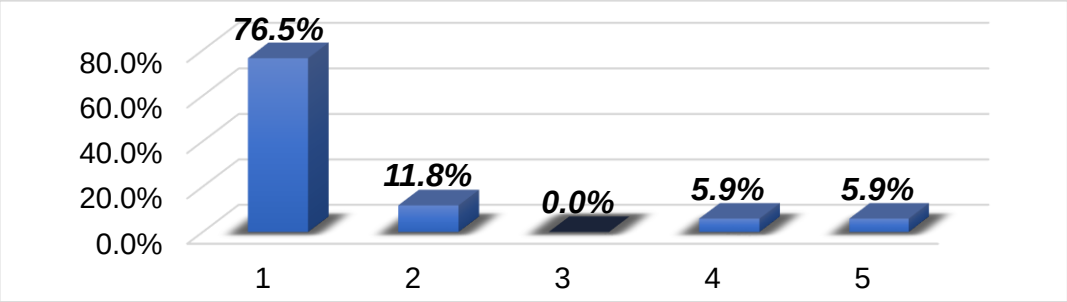


Figura 21. Desarrollo de un sistema IoT para control de acceso y seguridad de etapa Cosmos

Tabla 15**.**

Resultados de desarrollo de sistema IoT para control de acceso

Opción	***No.***	***Frecuencia (Fr=17)***	***Porcentaje (%)***
Totalmente de acuerdo	***1***	13	76,5%
Parcialmente de acuerdo	***2***	2	11,8%
Indiferente	***3***	-	-
Parcialmente en desacuerdo	***4***	1	5,9%
Totalmente en desacuerdo	***5***	1	5,9%
Total		**17**	**100%**

Análisis

El 76,5% dijo estar totalmente de acuerdo en que el desarrollo de un sistema de internet de las cosas usando los servicios en la nube, beneficiarán a las capacidades operativas de la seguridad y coordinación de información en tiempo real, estimando que la utilización de las nuevas herramientas tecnológicas beneficia y agilizan los procesos de control de acceso y efectivizan a la seguridad en tiempo real, por lo que están de acuerdo en su implementación como proyecto propuesto.

Resultados

A continuación, se presentan los resultados sobresalientes de las preguntas revisadas en la encuesta para el fundamento de estudio.

Tabla 16.

Resultados principales de estudio

No.	***Pregunta***	***Opción***	***Frecuencia (Fr = 17)***	***Porcentaje (%)***
1	¿Cómo calificaría usted el nivel para el control de acceso y seguridad de la etapa Cosmos en la urbanización Villa Club?	Muy Malo	8	47,1%
2	¿Considera usted que se requiere la implementación de nuevos procesos de seguridad tecnológica e innovación en la gestión de control de acceso a la etapa Cosmos?	Totalmente de acuerdo	11	64,7%
3	¿Cuál considera usted el principal problema de seguridad en la etapa Cosmos Villa Club?	Falta de control de entrada y salida	12	70,6%
4	¿De las siguientes soluciones tecnológicas cual considera usted que mejoraría la seguridad en la ciudadela Villa Club Etapa Cosmos?	Lector RFID	10	58,8%

5	¿Considera usted que el desarrollo e implementación de sistemas IoT para el control y seguridad en las urbanizaciones, constituye un beneficio operativo?	Totalmente de acuerdo	14	70,6%
6	¿Está usted de acuerdo qué ante los errores de control de acceso y seguridad en la etapa Cosmos, se deben implementar nuevos procesos operativos con sistemas integrados IoT?	Totalmente de acuerdo	15	88,2%
7	¿Actualmente considera usted que los porcentajes de errores en los procesos de control de acceso a la etapa Cosmos, incrementan la inseguridad de los residentes?	Totalmente de acuerdo	12	70,6%
8	¿Estima usted que el desarrollo e implementación de un sistema IoT a través de servicios en la nube, maximizará la operatividad y seguridad?	Totalmente de acuerdo	8	47,1%
9	¿Está usted de acuerdo en que los avances tecnológicos para el control y seguridad en el acceso de personas a la urbanización, debe fomentar una innovación continua de actualización?	Totalmente de acuerdo	10	58,8%
10	¿Estima usted que el desarrollo de un sistema IoT para el control de acceso y seguridad en la etapa Cosmos, mejorarán las capacidades operativas de seguridad y coordinación de información en tiempo real?	Totalmente de acuerdo	13	76,5%

Conclusión del capítulo

Para concluir, el análisis situacional actual del control de acceso y seguridad en la etapa Cosmos de la urbanización Villa Club, en el que se pudo evidenciar falencias operativas en el control de acceso, las cuales hacen referencia a las entradas y salidas en la etapa. Estos datos se reflejaron de la siguiente manera:

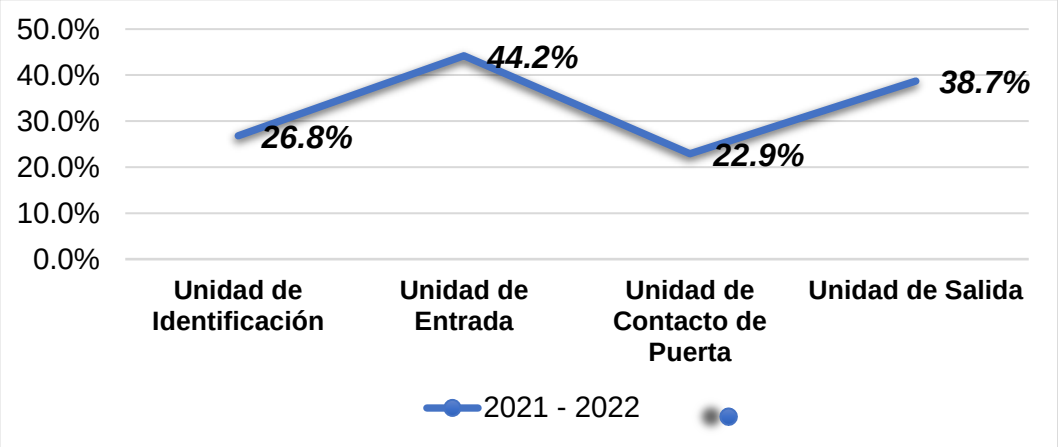


Figura 22. Identificación de problemas en el control de acceso de la etapa Cosmos, Villa Club

Fuente: (Corporación Samborondón Cía. Ltda. CORSAM, 2022)

Por ello, el personal administrativo, encargado del mantenimiento operativo de la seguridad de acceso a la etapa Cosmos, indicó que no está de acuerdo (47,1%) con los procesos actuales para el control de acceso y seguridad, considerando que mantiene elementos de registro y control realizados de manera escrita a mano, con una bitácora física, que según los datos de problemas presentados entre enero a enero de 2021 a 2022, existen errores en registros y control para la unidad de identificación, entrada, contacto de puerta y unidad de salida, lo que constituye un problema a abordar para la empresa y su administración.

En consecuencia, dentro de los puntos sobresalientes de la anterior encuesta presentada para la etapa metodológica, el 64,7% consideró que la urbanización sí requiere de la implementación de nuevos procesos de seguridad adaptados a las nuevas tecnologías e innovación, como parte de

una gestión de control de accesos adecuada, y acorde a los requerimientos y desafíos administrativos de control, que lo demanda tanto el personal como los residentes de la etapa Cosmos.

El desarrollo de nuevos sistemas de IoT con servicios en la nube, constituye un avance tecnológico necesario para la empresa, para beneficio de su gestión de control y seguridad en la urbanización, por lo que, el 70,6% estimó que mejorarían con ello, la comunicación y la coordinación de manera integral en la operatividad administrativa para las entradas y salidas de personas, con lo que se prevé incrementar así la seguridad de los residentes.

Finalmente, el 76,5% indicó estar totalmente de acuerdo en que el desarrollo de un sistema IoT para el control de acceso y seguridad en la etapa Cosmos, usando los servicios en la nube, maximizarían las capacidades operativas y de seguridad y coordinación de la información transmitida en tiempo real, proyectando con ello datos e información clara y precisa para todos los actores involucrados, tanto residentes como personal administrativo, generando una revisión continua del escenario de seguridad para la etapa.

En consecuencia, La tecnología basada en IoT proporciona seguimiento, análisis y alternativas en tiempo real para aumentar la seguridad en la etapa Cosmos de la urbanización Villa Club. Con ello, los sistemas de seguridad pueden predecir elementos preventivos al combinar estadísticas de sensores y cámaras con datos de lecturas y fuentes de redes, alertando a la administración del conjunto residencial y a sus residentes, con lo cual, la implementación de la propuesta representa un avance y aporte al desarrollo de ciudades y urbanizaciones seguras, tanto para la localidad como para el país.

CAPÍTULO 3

PROPUESTA

PROPUESTA

La propuesta del presente proyecto, se ha desarrollado en consecución del objetivo de investigación, de diseñar un sistema IoT, usando los servicios en la nube para el control de acceso y seguridad en la etapa Cosmos de la urbanización Villa Club, del cantón Daule, validando los resultados a partir de su implementación. Por tanto, a continuación, se presenta el desarrollo de la propuesta de estudio.

Desarrollo de la propuesta

La propuesta integra el desarrollo del proyecto, para el diseño del sistema de internet de las cosas, iniciando con la descripción de los componentes de hardware y software. A continuación, se presenta la descripción para el desarrollo de la propuesta.

Componentes de Hardware

Los dispositivos utilizados para la conectividad de datos y la comunicación en la nube son dispositivos IoT, con las siguientes características:

1. NODEMCU-32-30-PIN ESP32 WIFI
2. Arduino Uno
3. Modulo RFID RC522
4. Display LCD ILI9341

Componentes de Software

Los diferentes softwares a utilizar son los siguientes:

1. Atom V 1.60.0
2. Terminal Putty V 0.77

3. Visual Studio Code V 1.69.2
4. Base de datos HeidiSQL V 12.0.0
5. Base de datos MyBuilder V 1.20
6. Arduino V1.8.19
7. Servicio NodeJs V 10.24.1
8. AWS (Amazon Web Service)
9. Vesta Control Panel V 0.9.8
10. EMQX (MQTT) V 3.0.1

De acuerdo a lo estudiado dentro del marco teórico, la tecnología que mejor se adapta a los objetivos planteados a este trabajo, se optó por utilizar los componentes de *hardware* y *software* descritos anteriormente, ya que aseguran el pleno aprovechamiento del Internet de las Cosas componentes con el protocolo MQTT.

Este último facilita la conexión de una gran cantidad de dispositivos y es capaz de verificar que el mensaje alcanza su objetivo, proporciona seguridad a través de certificados electrónicos. Además de todo lo anterior, la selección de componentes de *hardware* y *software* se debe a la disponibilidad de equipos de proveedores existentes en el país y también a su costo, ya que existen aproximadamente dispositivos similares de diferentes marcas.

Por tanto, en la relación calidad – precio, los equipos Arduino cumplen con los requisitos técnicos expuestos en este trabajo. Después de la selección de los componentes, se procede a realizar la instalación de Vesta Control Panel que se utilizará para administrar un Web Hosting y que a su vez se puede instalar servicios como Firewall, servicios web, servidor de mail, motor de base de datos y un motor de FTP que ayudará a transferir y subir archivos, y que se conecta con la nube de AWS para él envío de datos.

Consecuentemente, para entrar a los servicios de *Amazon Web Service (*AWS), se realiza mediante la siguiente dirección URL: https://aws.amazon.com/, En base a ello, se prevé la utilización del método

para conectarse entre el servidor *Amazon Web Service* y las diferentes aplicaciones que se mencionó anteriormente.

Diagrama de caso de uso

En el presente proyecto, para poder construir su uso se toma apuntes de referencia a la Ingeniería de Software.

En el siguiente diagrama se presenta El sistema IoT que incluye el uso general del dispositivo.

En base a lo establecido se tendrá un sistema en donde el microcontrolador recolectará la información y posteriormente transmitirá dicha información y a su vez, la aplicación web transmitirá la información y, por consiguiente, presentará los datos que se recolectaron. Por otro lado, el usuario y el administrador visualizarán la información.

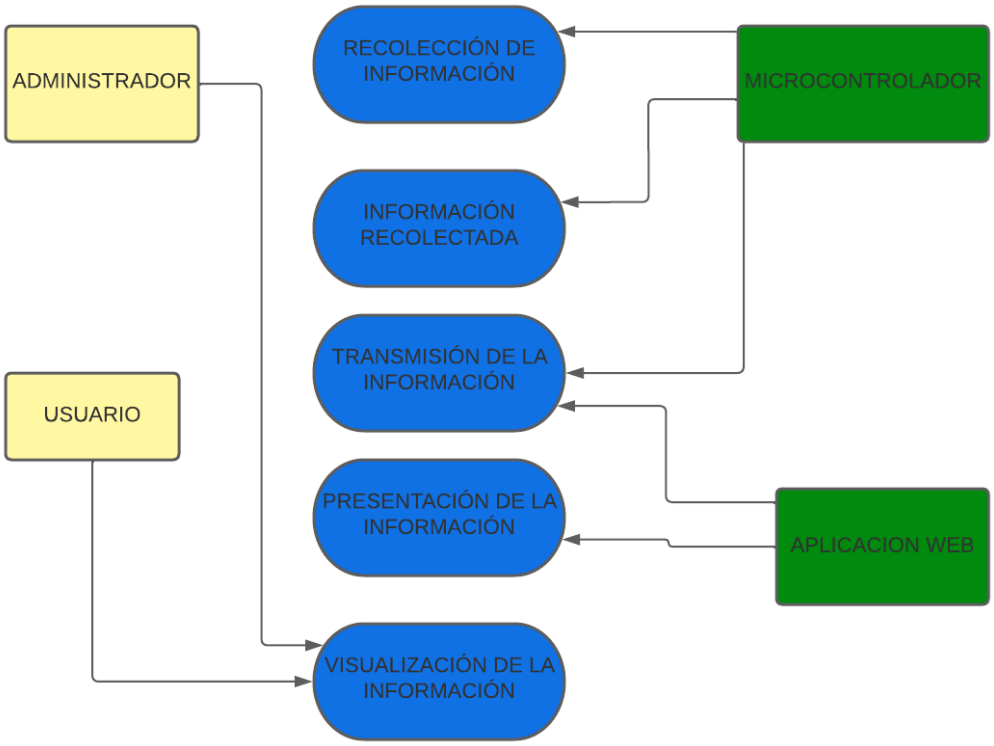


Figura 23. Uso general del Sistema del Internet de las Cosas (IoT).

A continuación, se presentará información que permitirá una mejor comprensión acerca de las funcionalidades y comportamiento que tendrá los distintos componentes en el proyecto.

En el siguiente diagrama que se muestra el uso del Sistema para presentar la información desde la aplicación web tanto el administrador como el usuario puede ingresar en el aplicativo web en donde se presenta la información y posteriormente se visualiza.

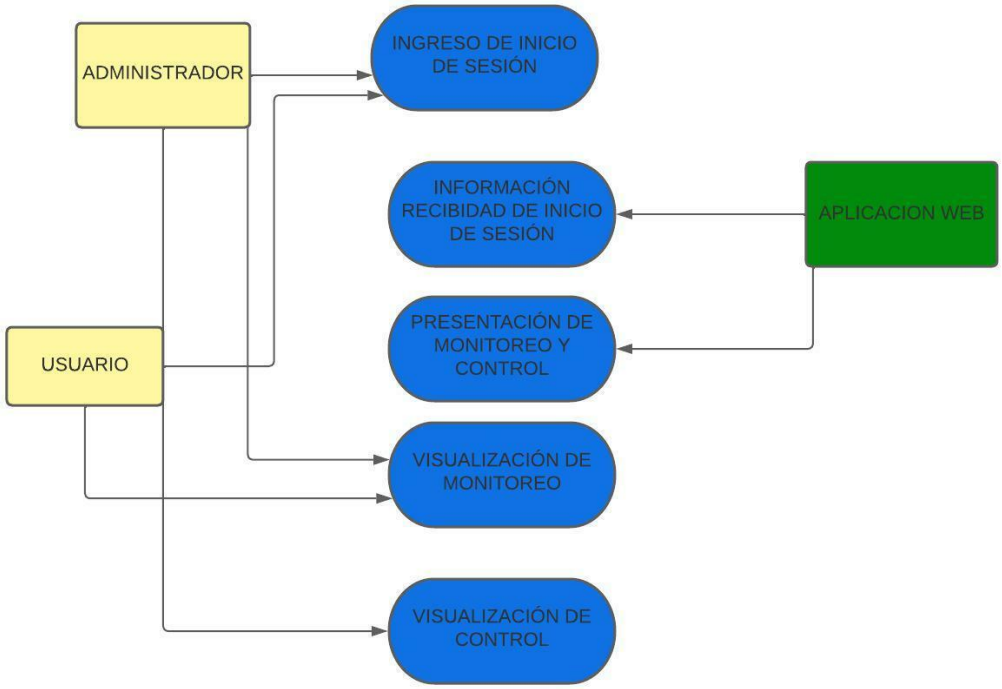


Figura 24. Sistema de presentación de la información.

En la aplicación web se realiza la verificación de identidad de usuarios (Administrador o Usuario final), esto corresponde al sistema de inicio de sesión, luego la aplicación web recibe el usuario y contraseña en donde se verifica los datos y finalmente, permitir el acceso en la aplicación web.

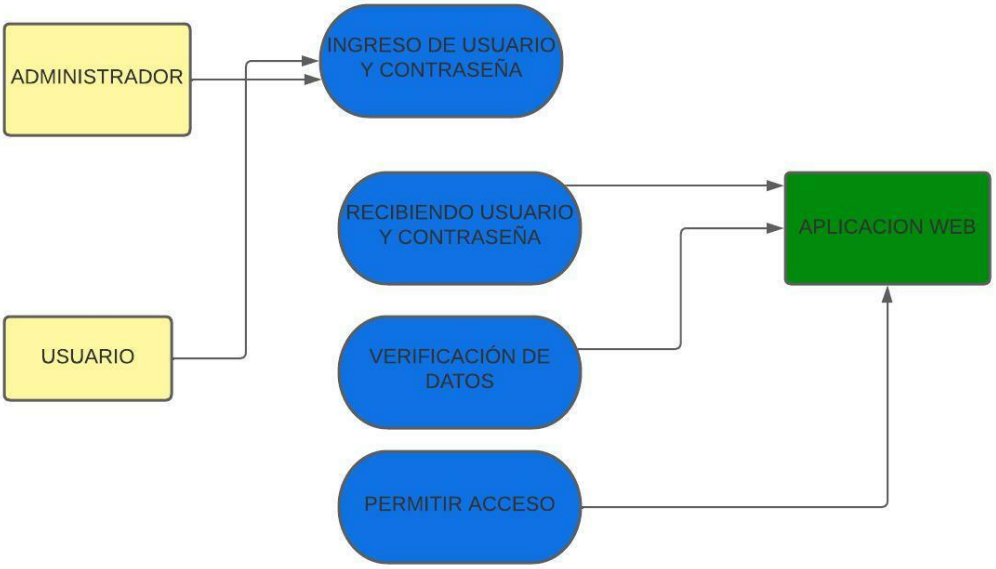


Figura 25. Sistema de Inicio de Sesión.

En la aplicación web tendrá la posibilidad de monitorear la temperatura del dispositivo y a su vez en la plataforma podrá gestionar los dispositivos que el único que puede hacer eso es el administrador y el microcontrolador se encarga de los procesos de control. Esta funcionalidad se detallará con el siguiente diagrama.

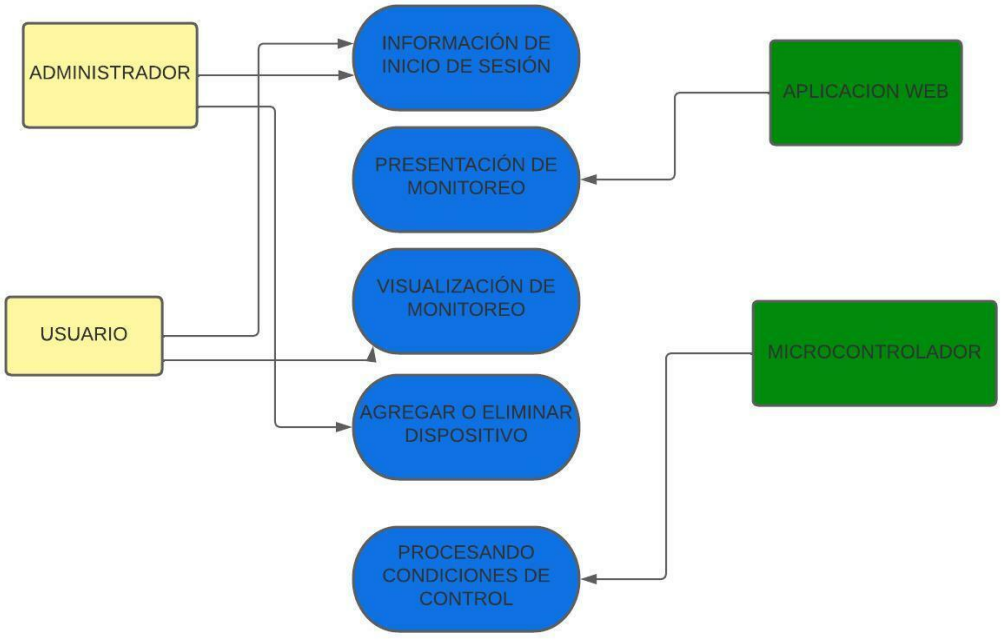


Figura 26. Uso del Sistema con el dispositivo IoT.

Diagrama principal del dispositivo para el control de acceso

En el siguiente flujograma se describe las funcionalidades para el control de acceso mediante el dispositivo. Primero se da inicio a las declaraciones globales mediante el dispositivo IoT en el que tenemos un lector de tarjeta RFID encargado de detectar las tarjetas, una vez que dicho usuario una tarjeta o llavero se validará la información o los datos que fueron almacenados en la base de datos y si el usuario existe permite el acceso caso contrario se le denegará el acceso por el dispositivo que quiere entrar de esa forma se tiene un mejor control de acceso y seguridad con el dispositivo.

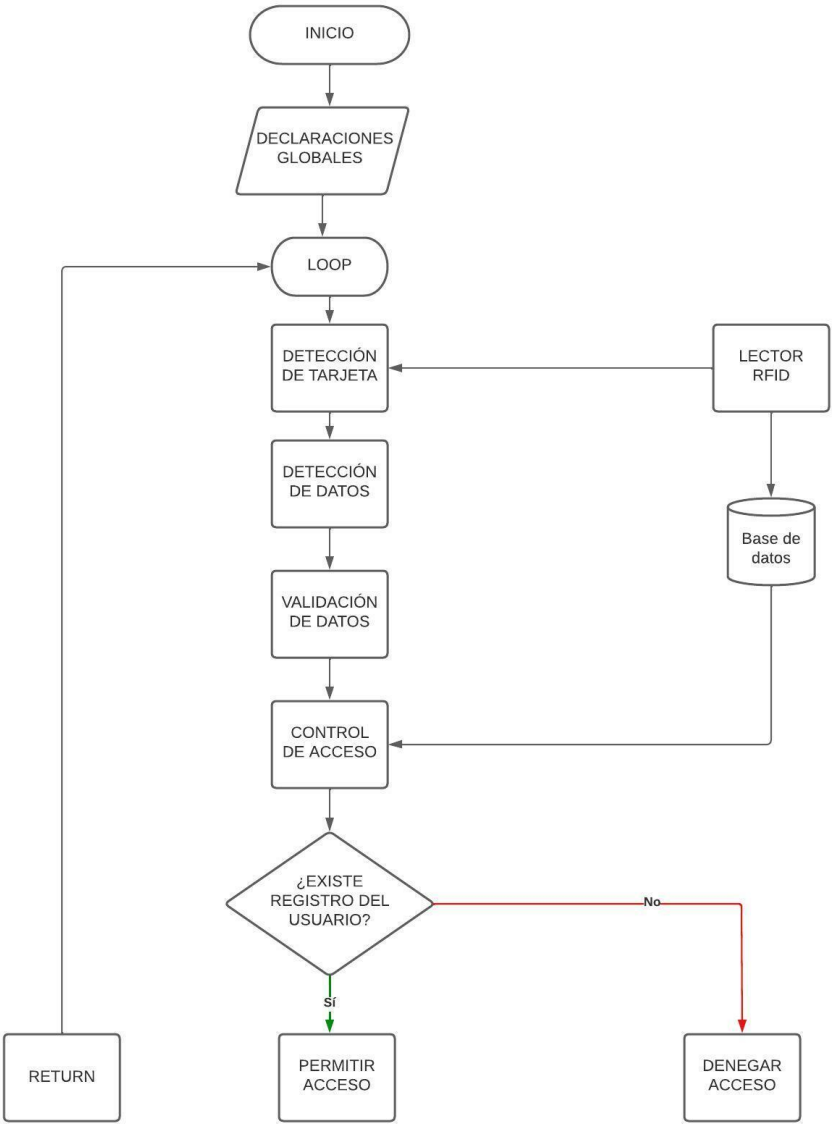


Figura 27. Flujograma del dispositivo en general.

Configuración de servicios en la nube AWS

La configuración de los servicios en la nube AWS, presentan las siguientes etapas:

Desarrollo de etapas de configuración de servicios en la nube

Etapa uno

Se procede a direccionar a la página de Amazon Web Services.

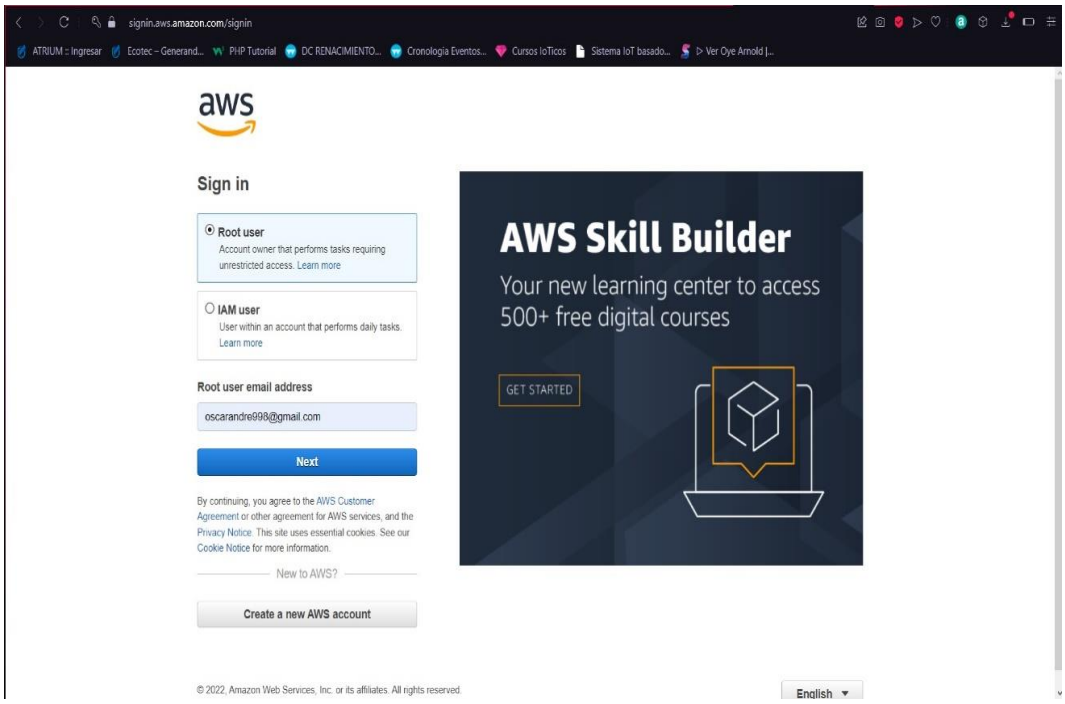


Figura 28. Amazon Web Services (AWS)

En esta etapa se procede al registro de usurario para el desarrollo de los servicios en la nube, considerando los beneficios presentados por AWS en la consecución del objetivo específico de esta propuesta.

Etapa dos

Se procede a la creación de un usuario para acceder a la consola de AWS.

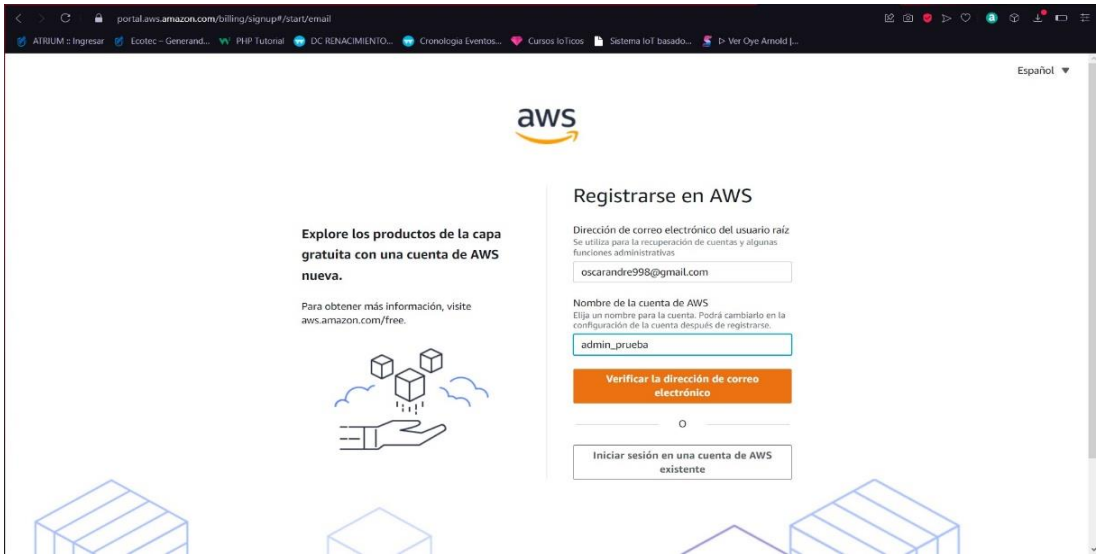


Figura 29. Creación de cuenta AWS.

Etapa tres

Se procede a ingresar al inicio de la consola.

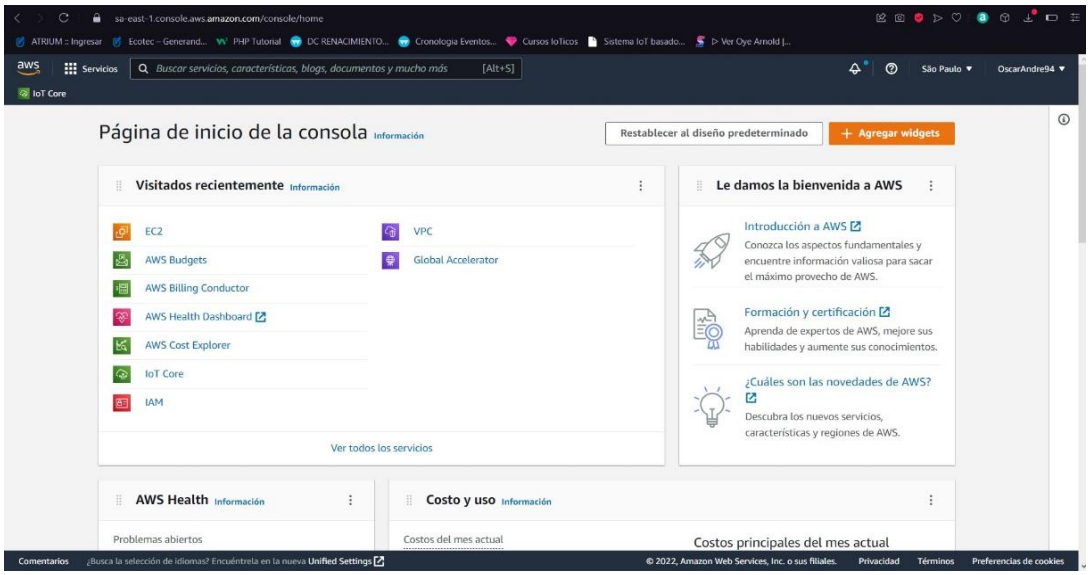


Figura 30. Página de inicio de la consola**.**

Etapa cuatro

Se procede a la selección de servicio de nube, seguridad y conformidad, se procede a seleccionar EC2.

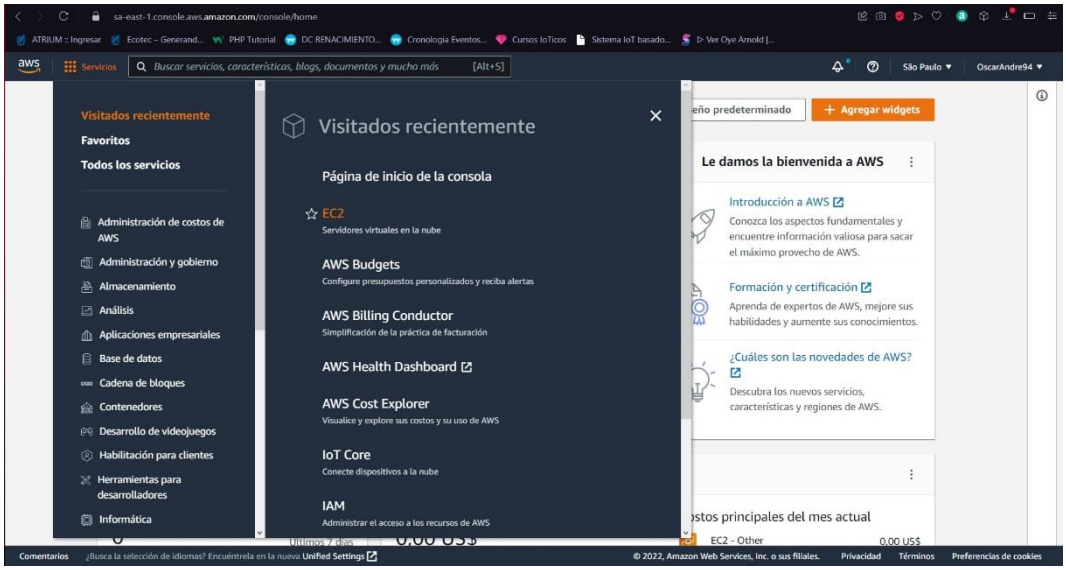


Figura 31. **Selección de servicio**

Etapa cinco

Se procede a la creación de una nueva instancia dentro del servicio.

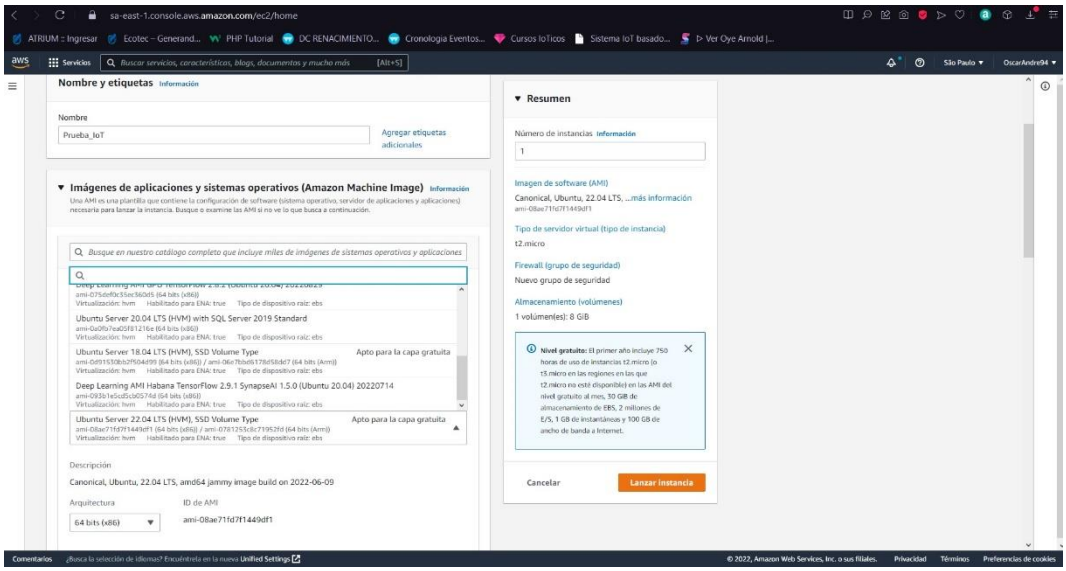


Figura 32. **Creación de instancia**

Posteriormente, el servicio de Amazon Web Services nos asigna una IP elástica y, por consiguiente, le asignamos un dominio. En el siguiente sitio web, www.freenom.com adquirimos un dominio de forma gratuita en el que con la IP asignada la reservamos con la terminal Putty.

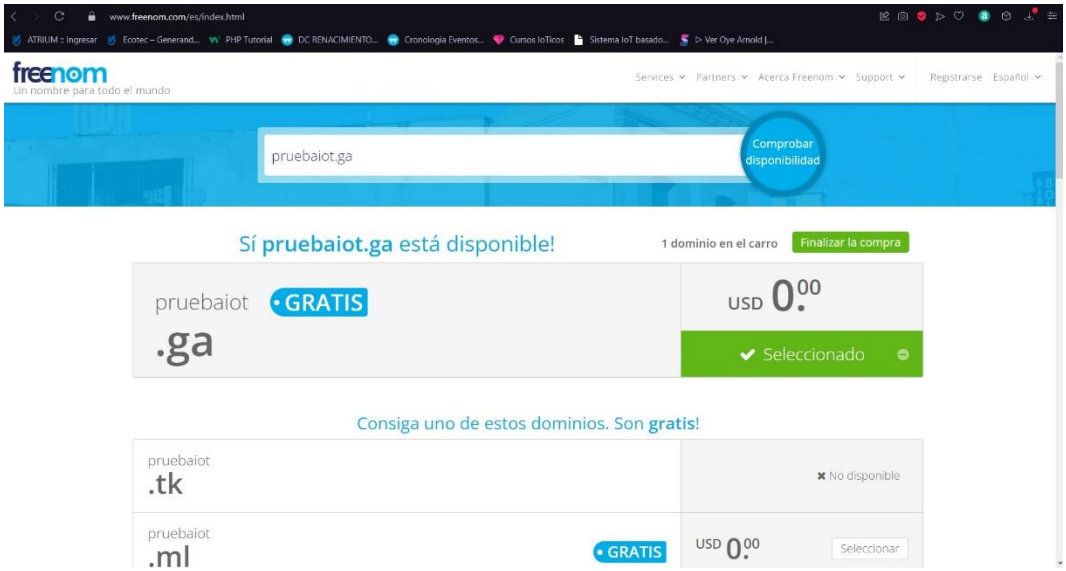


Figura 33. **Registro de dominio web**

En la terminal Putty se procede a configurar y a conectar mediante SSH, ya con la llave privada y con la IP fija que se reservan en los pasos anteriores.

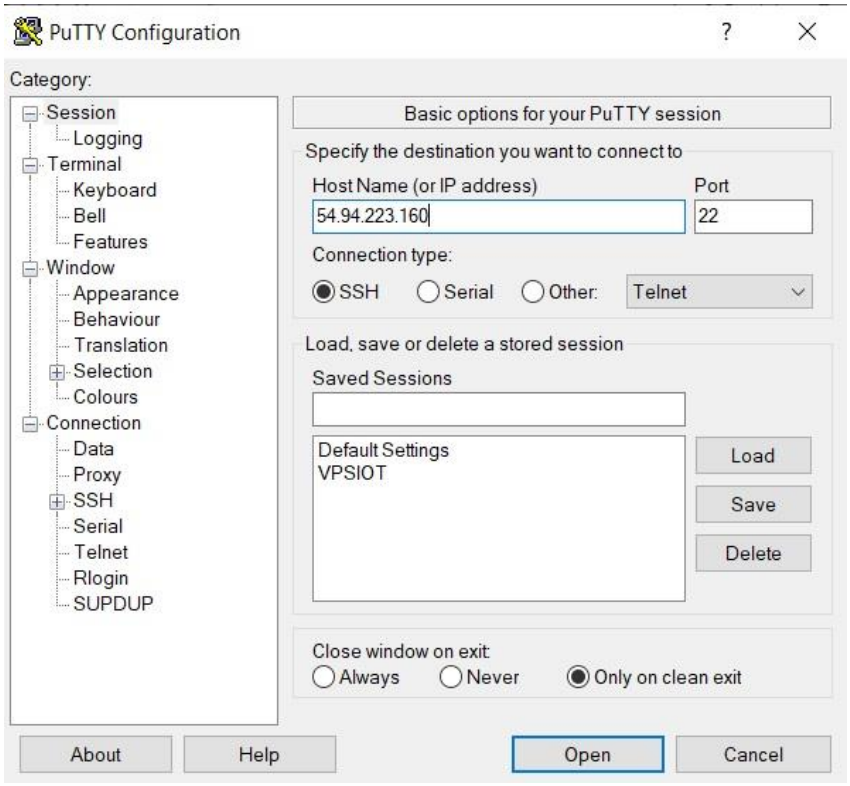


Figura 34. Conexión por SSH y se reserva la IP.

Vesta Control Panel

VestaCP es un panel de control en el que alojamos el hosting web y que se genera un usuario administrativo para la web. La instalación de VestaCP es sencilla se efectúa de la siguiente manera: mediante comandos que se ingresan en la terminal Putty.

```
1  # Connect to your server as root via SSH
   ssh root@your.server

2  # Download installation script
   curl -O http://vestacp.com/pub/vst-install.sh

3  # Run it
   bash vst-install.sh --nginx yes --apache yes --phpfpm no --named yes --remi yes --vsftpd yes --proftpd no --iptables
   yes --fail2ban yes --quota no --exim yes --dovecot yes --spamassassin yes --clamav yes --softaculous no --mysql
   yes --postgresql no --hostname jonsuiot.ga --email oscarandre998@gmail.com --password 121212
```

Figura 35. Instalación de VestaCP mediante comandos.

Después de hacer el paso anterior procedemos a ingresar a nuestro dominio www.jonsuiot.ga:8083 el protocolo con el que podemos entrar es para el usuario administrativo que ingresamos con un usuario y contraseña.

Figura 36. VestaCP Inicio de Sesión.

En la siguiente ilustración tenemos un Dashboard que pertenece a VestaCP en donde se podrá administrar y configurar como el dominio que

mencionamos anteriormente, la base de datos y los cortafuegos que se le dará seguridad a la aplicación web que se mostrará más adelante.

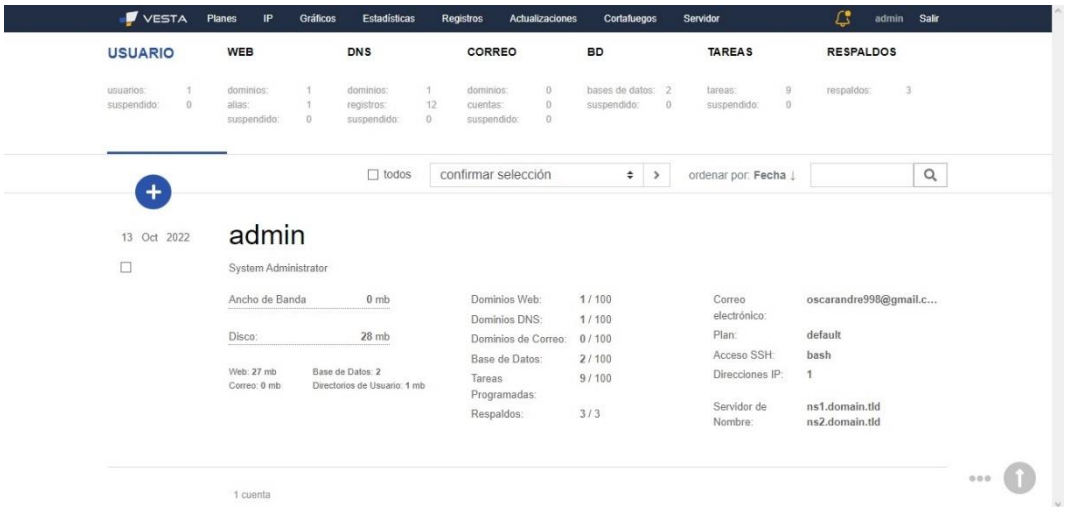


Figura 37. **Dashboard de VestaCP y su funcionalidad**.

Como última instancia, para aplicar la seguridad se asignará cortafuegos tanto en Amazon Web Services (AWS) y en el Vesta Control Panel en lo que se abrirá diferentes protocolos como de MQTT 8093, 8094, 1883, 18083, 8883 y 8090. Los protocolos mencionados ayudarán en la seguridad que protegerá el dispositivo, la base de datos y la aplicación web, así como los servicios mencionados como VestaCP y AWS.

Función de la Base de Datos.

En el siguiente diagrama muestra la función que cumple la base de datos con los diferentes actuadores (Microcontrolador, aplicación web, servicio en la nube y el protocolo MQTT) y como se comunican, transmitirá la información a la base datos MYSQL.

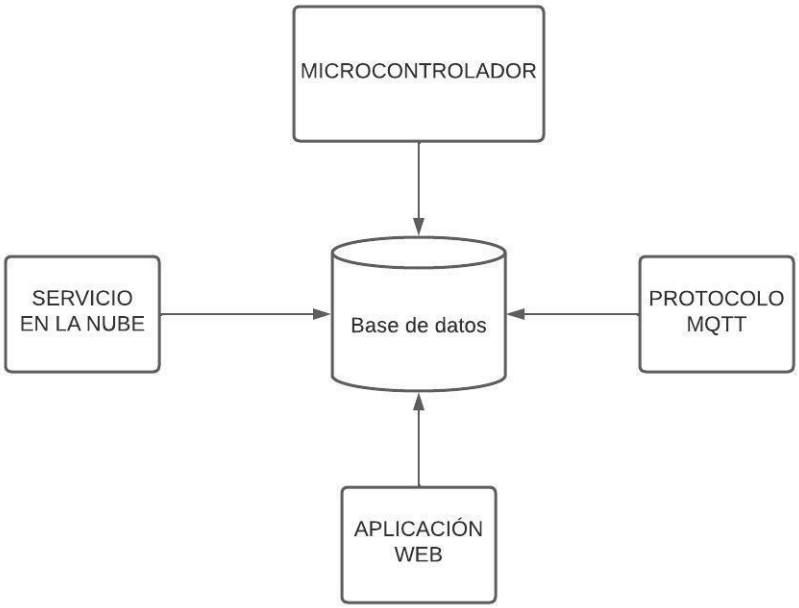


Figura 38. Flujograma para él envió de datos a la BDD.

La función de la base de datos es almacenar la información registrada como la de los usuarios o la temperatura del dispositivo.

Gestor de la Base de Datos.

Al momento de elegir la base de datos se elegirá relacional, debido a que son las más populares y las más usadas. Se usará HeidiSQL ya que facilitará las tareas, ya que permite organizar la información mediante tablas estructuradas, además que es liviana al momento de realizar el desarrollo IoT.

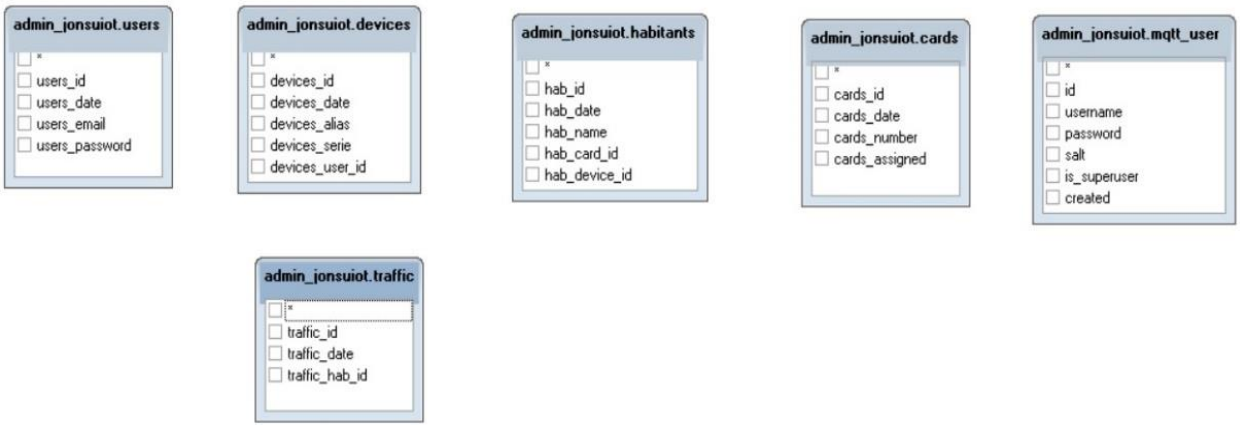


Figura 39. Base de datos HeidiSQL con las diferentes tablas relacionadas.

Posteriormente, en VestaCP se tendrá que crear la base en donde se le asignará un nombre a la base, un usuario y una contraseña para poder administrarla.

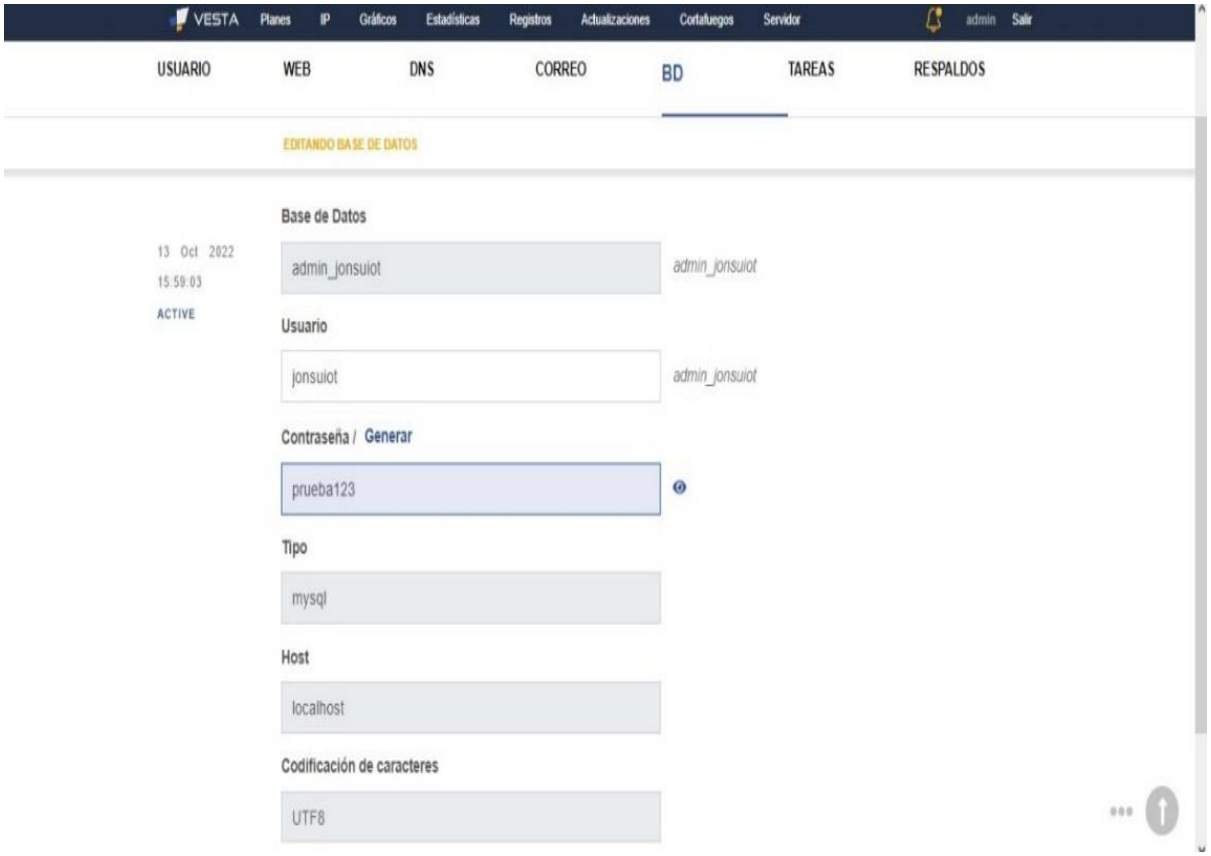


Figura 40. Creación de base de datos en VestaCP.

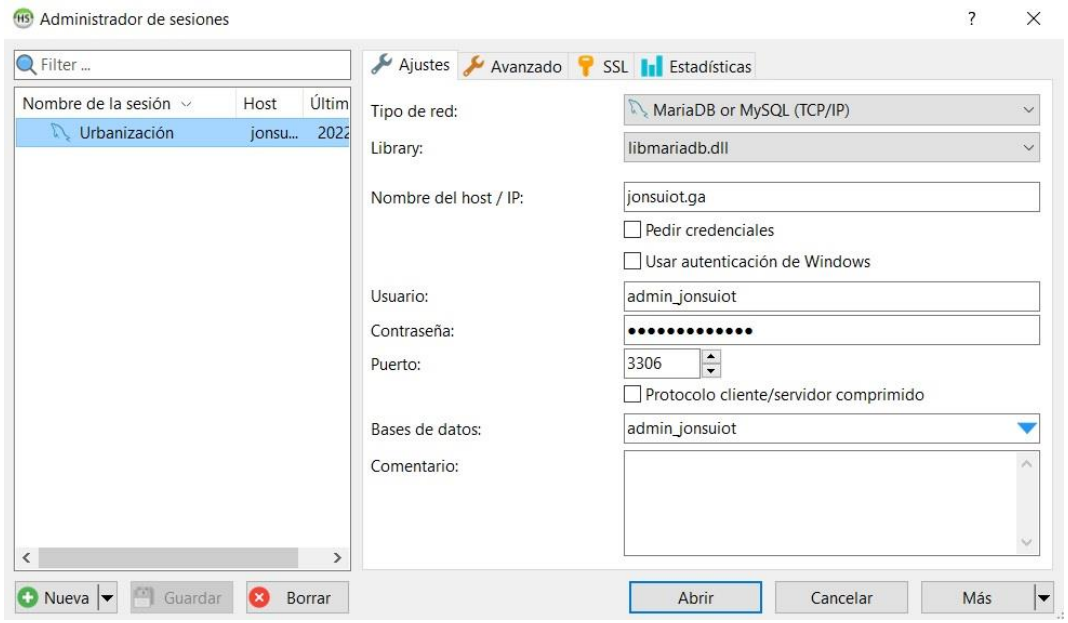


Figura 41. Inicio de sesión en HeidiSQL con las credenciales.

Desarrollo de la aplicación Web

Para el desarrollo de la aplicación web se ha utilizado el editor de código Atom que servirá como sugerencia, sin embargo, se puede decir que es muy completo y muy potente, debido a que es de código abierto que servirá para llevar a cabo la aplicación web. Además, existe otros editores de código como Sublime Text o Visual Studio Code que son más livianos, pero Atom posee un plugin de FTP para poder administrar los archivos y permitirá la conexión al servidor y se podrá visualizar de manera local o remota.

Como primera instancia se debe añadir la carpeta y posteriormente se comienza hacer el desarrollo de la aplicación web que se realiza con el lenguaje PHP para el proyecto. En primer lugar, se realiza la página donde se podrá registrar mediante un email y una contraseña en la aplicación web y la información se almacena en la base de datos.

En segundo lugar, en otra sección de la aplicación web con el email va poder iniciar sesión mediante una contraseña.

Por otro lado, el usuario podrá visualizar un Dashboard que se tendrá la facilidad de comunicarse con el dispositivo y que podremos administrar y hacer diferentes funciones como el de agregar y eliminar dispositivos sin necesidad de ir a la base de datos.

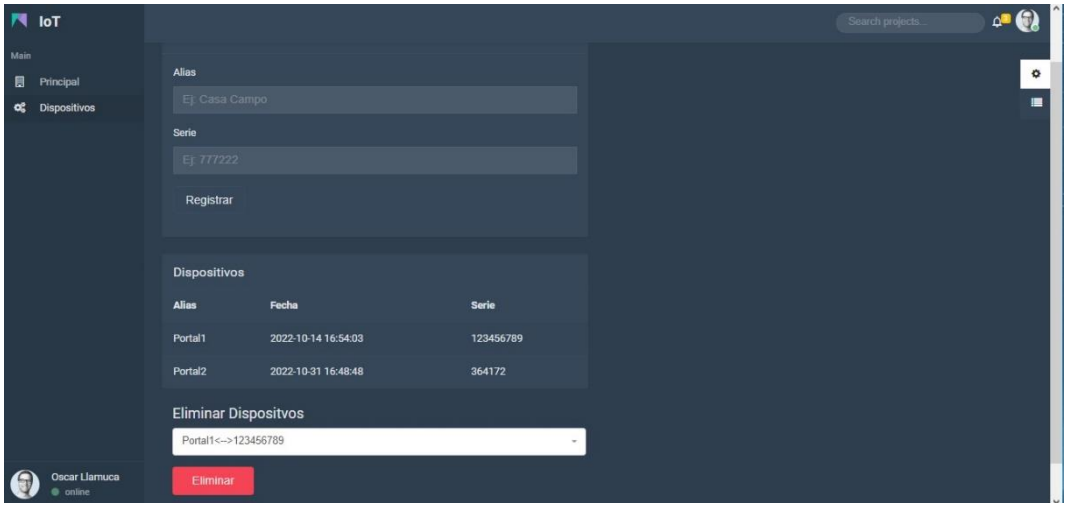


Figura 42. Dashboard de la aplicación web.

Desarrollo de etapas para la configuración de EMQX mediante protocolo MQTT

De manera que, montar el bróker EMQX es vital para la implementación de Internet de las Cosas (IoT), por el motivo de que es el líder en mensajería IoT de código abierto y que es lo más complejo y más potente que hay actualmente. Es altamente escalable para la plataforma y las aplicaciones IoT.

Cada día usamos protocolos de comunicación como HTTPS para la conexión a Internet, pero ahora se dispondrá a usar protocolos IoT debido a su bajo consumo de recursos.

Para ello, los protocolos que vamos a utilizar es MQTT actualmente, es el protocolo predilecto para la implementación de un sistema IoT. MQTT tiene diversas ventajas como la comunicación entre la aplicación web, el dispositivo, la base de datos y los servicios en la nube que funciona en tiempo real. En el siguiente flujograma podemos entender cómo se comunicarán los diferentes actuadores con el bróker MQTT que es el intermediario.

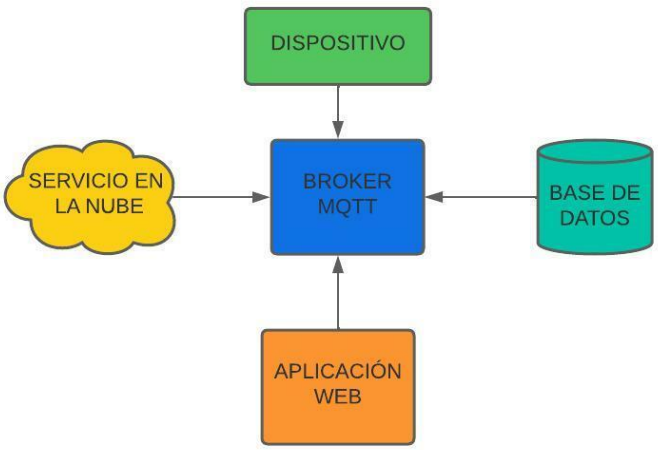


Figura 43. Diagrama de flujo general del protocolo MQTT.

Procederemos a descargar e instalar MQTT en el servidor desde el sitio web oficial en donde ejecutaremos comandos para la instalación mediante la terminal Putty.

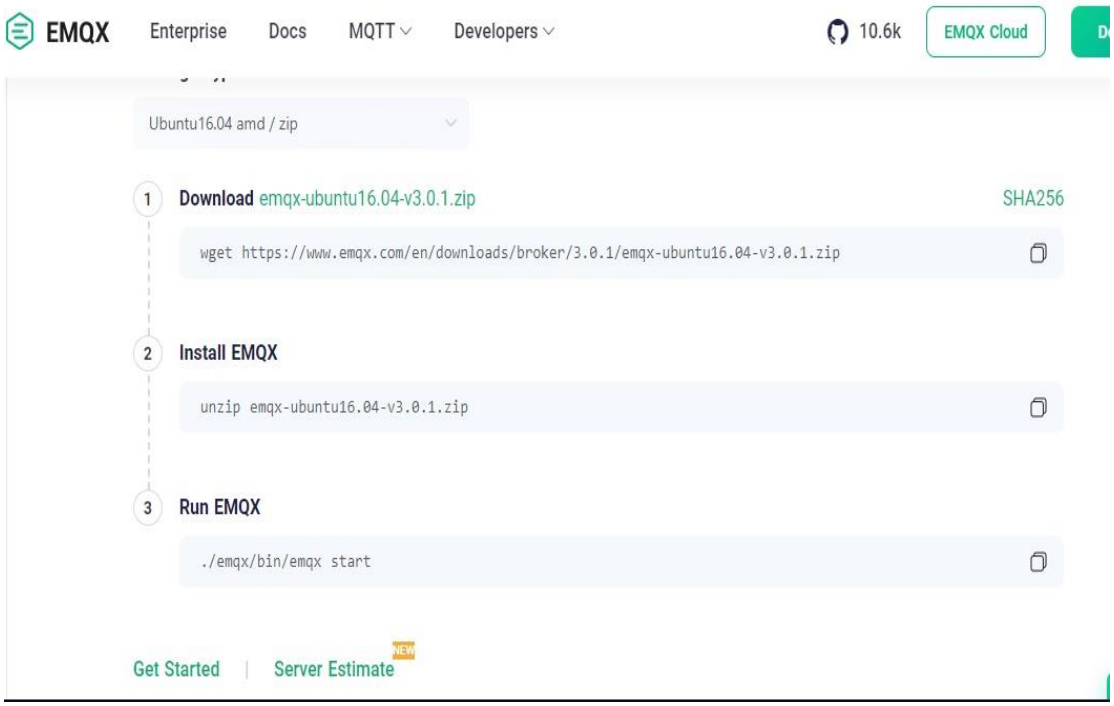


Figura 44. Instalación del bróker MQTT.

Luego haremos diferentes configuraciones como asignar protocolos pertenecientes al bróker MQTT que ayudara en la seguridad y como se comunican entre sí para poder visualizar la información. Para ello, los puertos se agregaron tanto en el Amazon Web Services (AWS) y Vesta Control Panel como veremos a continuación.

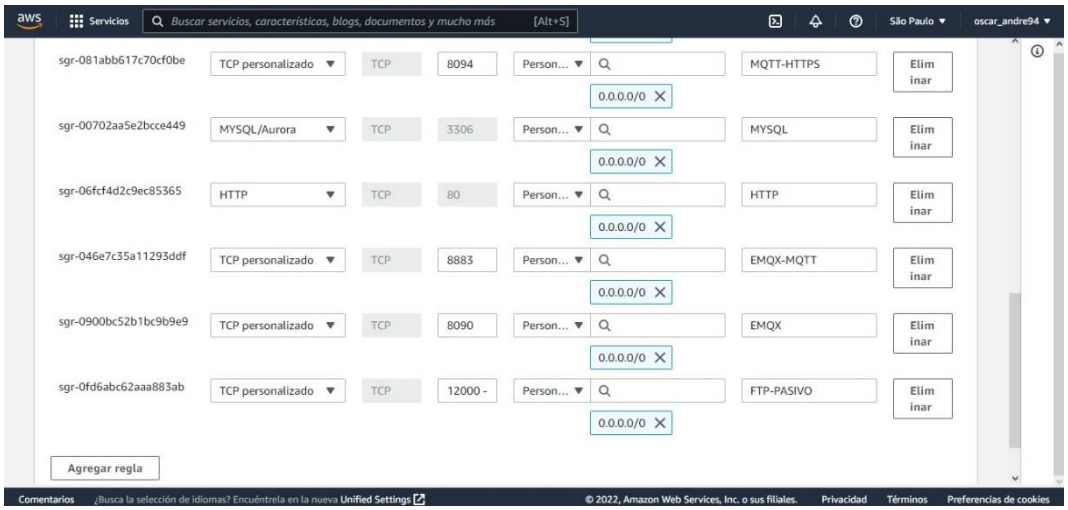


Figura 45. Protocolos MQTT asignados en AWS.

Finalmente, EMQX ofrece un dashboard en donde podemos acceder con los protocolos asignados anteriormente en donde aquí podemos administrar el dispositivo que esté conectado y podremos mandar y recibir mensajes.

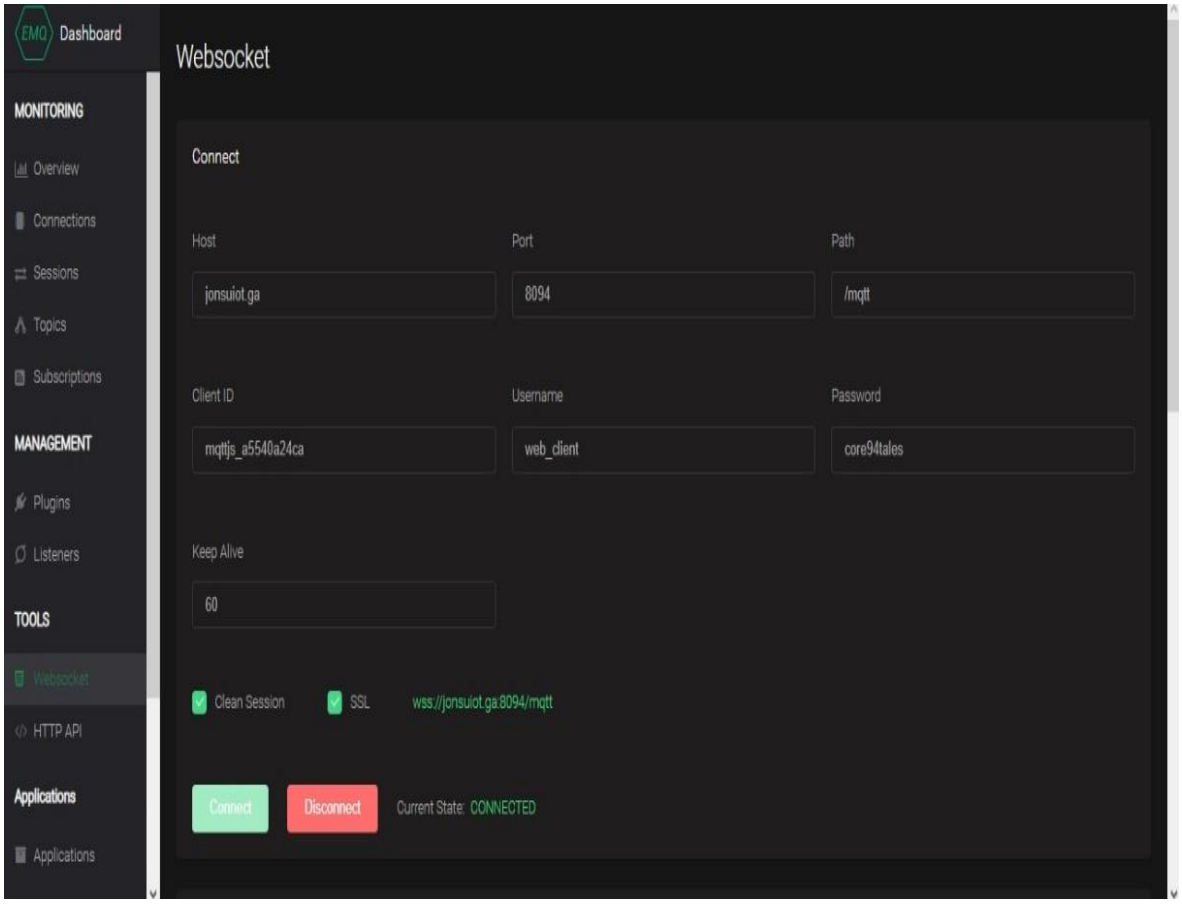


Figura 46. Dashboard de Emqx.

Desarrollo del prototipo IoT

Para el diseño del dispositivo se opta de armarlo y de cómo los diferentes microcontroladores ya mencionados con anterioridad se comunican entre sí para poder determinar su funcionamiento.

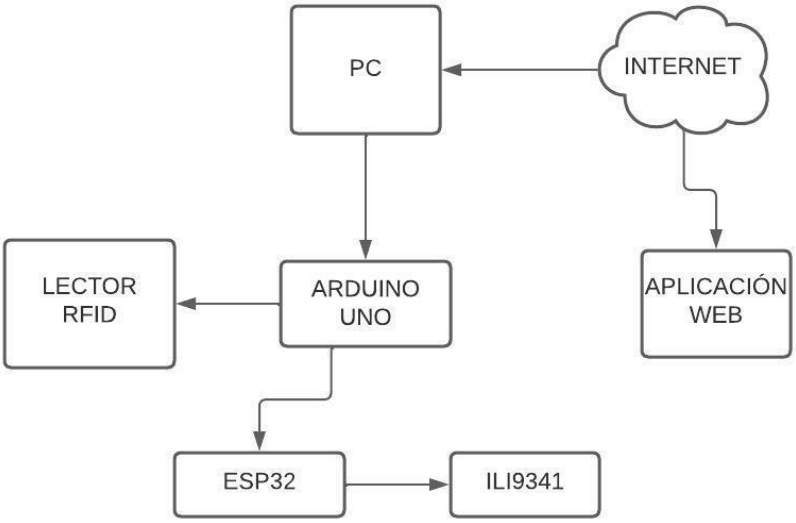


Figura 47. **Flujograma del dispositivo IoT para el proyecto**.

El dispositivo cuenta con diferentes componentes que va servir para el control de acceso como el lector RFID-RC522 que va hacer comunicación con el Arduino Uno y que va tener el programa cargado en la memoria y que tendrá la facilidad de leer los identificadores de las tarjetas o llaveros. Del mismo modo, se hará comunicación con el microcontrolador NodeMCU-32 y se le cargará el programa en memoria, por lo tanto, podrá realizar diferentes funcionalidades como mostrar los accesos mediante una pantalla ILI9341 encargada de mostrar mensajes de los usuarios que ingresen por el dispositivo.

.

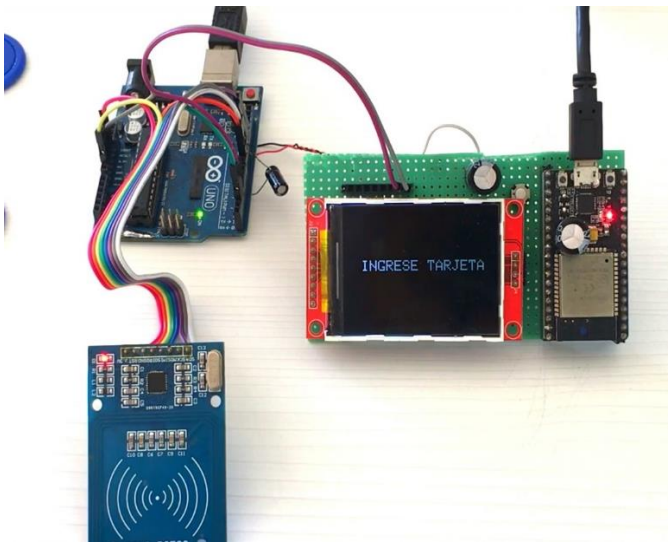


Figura 48. **Configuración del hardware del dispositivo**.

En el siguiente flujograma podemos observar cómo se va comunicar los distintos dispositivos que harán funcionar el dispositivo en general.

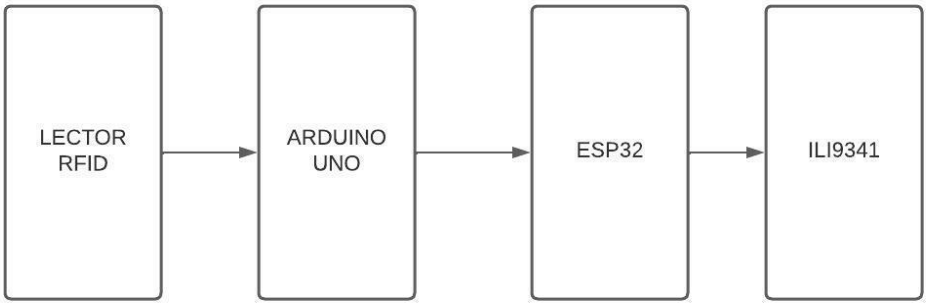


Figura 49. **Diagrama del flujo del dispositivo en general**.

Entorno de programación y software utilizado

Para elaborar el entorno de desarrollo utilizamos el siguiente IDE de Arduino ya que es sencillo y fácil de implementar en él lo descargamos desde la página oficial de Arduino (https://www.arduino.cc/en/software) es multiplataforma ya que funciona con los distintos Sistemas Operativos.

En la placa de Arduino Uno se realizó la codificación para comunicarse con el lector RFID y cada vez que pase una tarjeta nueva nos muestre el código de dicha tarjeta.

Del mismo modo, el microcontrolador NodeMCU-32 se utilizará el IDE de Visual Studio Code, en donde de manera constante se le dará un nombre o código al dispositivo que anteriormente ya fue asignado en la base de datos que se comunica con la aplicación web para que tengan la relación.

Por consiguiente, pasaremos credenciales como las de MQTT para hacer la conexión y a su vez los parámetros para la conexión Internet que se usará vía Wifi y se le asignará una IP fija.

```
//*****************************
//***   CONFIGURACION MQTT   ***
//*****************************

const char *mqtt_server = "jonsuiot.ga";
const int mqtt_port = 1883;
const char *mqtt_user = "web_client";
const char *mqtt_pass = "core94tales";

WiFiClient espClient;
PubSubClient client(espClient);

long lastMsg = 0;
char msg[25];
bool send_access_query = false;

//*******************************
//***   CONFIGURACION DISPLAY  ***
//*******************************
#define TFT_DC 10
#define TFT_CS  9
```

Figura 50. **Configuración MQTT**.

```
#include "SPI.h"
#include <Arduino.h>
#include <WiFi.h>
#include <PubSubClient.h>
#include <Adafruit_ILI9341.h>

const String serial_number = "123456789";

#define RXD2 16
#define TXD2 17

TaskHandle_t Task1;

const char* ssid     = "OscarRoom";
const char* password = "oscar94tales";

//para evitar que el dhcp nos asigne ip, o si el ruter no cuenta con dhcp
//podemos seleccionar una ip fija si no lo usas comentar las 5 líneas
IPAddress local_IP(192, 168, 0, 184);
IPAddress gateway(192, 168, 0, 1);
IPAddress subnet(255, 255, 255, 0);
IPAddress primaryDNS(8, 8, 8, 8);
IPAddress secondaryDNS(8, 8, 4, 4);
```

Figura 51. **Credenciales de conexión a Internet**.

A continuación, la configuración de la pantalla LCD ILI9341 en el que se mostrará los mensajes, las suscripciones y los tópicos con el cual se comunicará con el dispositivo en general.

```
void callback(char* topic, byte* payload, unsigned int length){
    String incoming = "";
    Serial.print("Mensaje recibido desde -> ");
    Serial.print(topic);
    Serial.println("");
    for (int i = 0; i < length; i++) {
        incoming += (char)payload[i];
    }
    incoming.trim();
    Serial.println("Mensaje -> " + incoming);

    String str_topic(topic);

    if (str_topic == serial_number + "/command"){

        if ( incoming == "open") {
            digitalWrite(BUILTIN_LED, HIGH);
            opening();
        }

        if ( incoming == "close") {
            digitalWrite(BUILTIN_LED, LOW);
            closing();
        }

        if ( incoming == "granted") {
            digitalWrite(BUILTIN_LED, HIGH);
            access_screen(true);
        }

        if ( incoming == "refused") {
            digitalWrite(BUILTIN_LED, LOW);
            access_screen(false);
```

Figura 52. **Tópicos y comandos que se suscribe el dispositivo**.

```
//***************************
//*** PANTALLAS ACCESO      ***
//***************************

void access_screen(bool access) {

    if (access) {
        tft.fillRect(0, 0, 320, 240, ILI9341_BLACK);
        tft.setTextSize(3);
        tft.setCursor(20, 30);
        tft.setTextColor(ILI9341_GREEN);
        tft.println("Hola Bienvenido " + user_name);
        tft.println("");
        tft.print(" ACCESO PERMITIDO");

        delay(2000);
        opening();
    }else{
        tft.fillRect(0, 0, 320, 240, ILI9341_RED);
        tft.setTextSize(3);
        tft.setCursor(20, 100);
        tft.setTextColor(ILI9341_WHITE);
        tft.print("ACCESO DENEGADO");
        delay(2000);
        iddle();
    }
}
```

Figura 53. **Mensajes mostrados en la pantalla ILI9341**.

Prueba General del dispositivo

A continuación, cada vez que un usuario o el residente pase la tarjeta por el lector RFID mediante un mensaje se le mostrará un saludo cordial de bienvenida y posteriormente le dará acceso. Debido a que el habitante existe en la base de datos y, por lo tanto, tiene derecho a pasar.

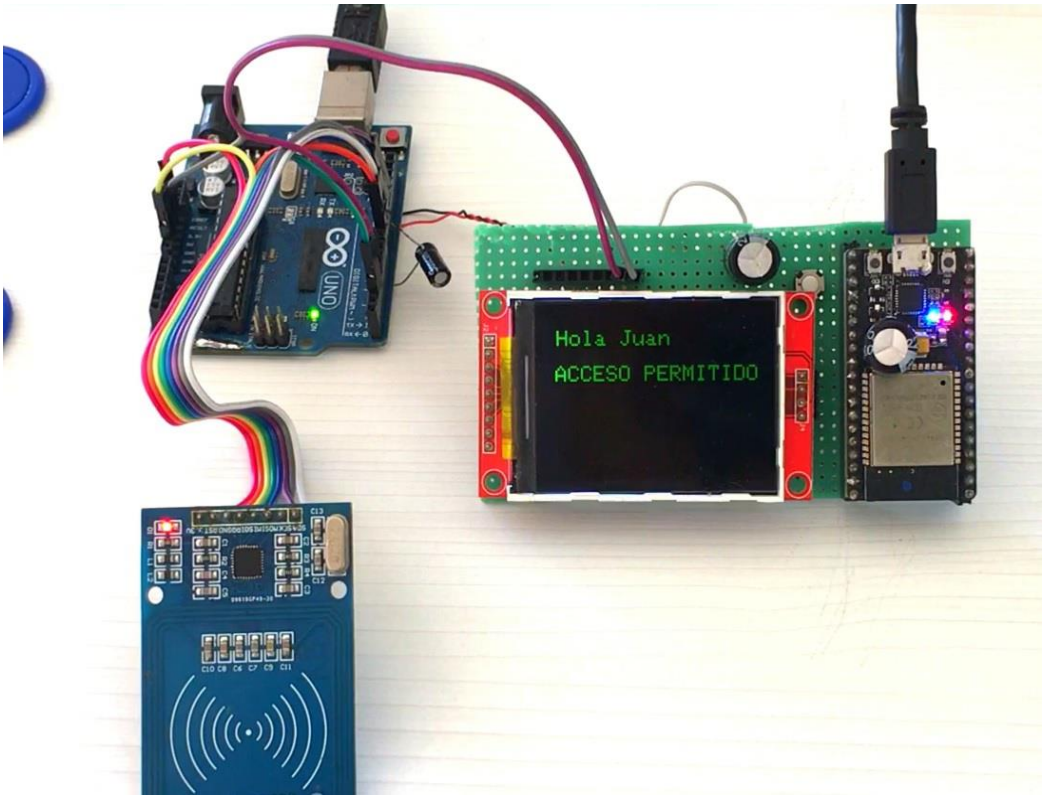


Figura 54. **Mensaje de bienvenida al usuario**.

Por otro lado, cuando el usuario pase otra tarjeta por el lector RFID y dicha tarjeta no pertenezca a la base de datos o no tenga la relación con el dispositivo mediante la pantalla se visualizará un mensaje que no tiene acceso y por esta razón, no podrá pasar por el dispositivo.

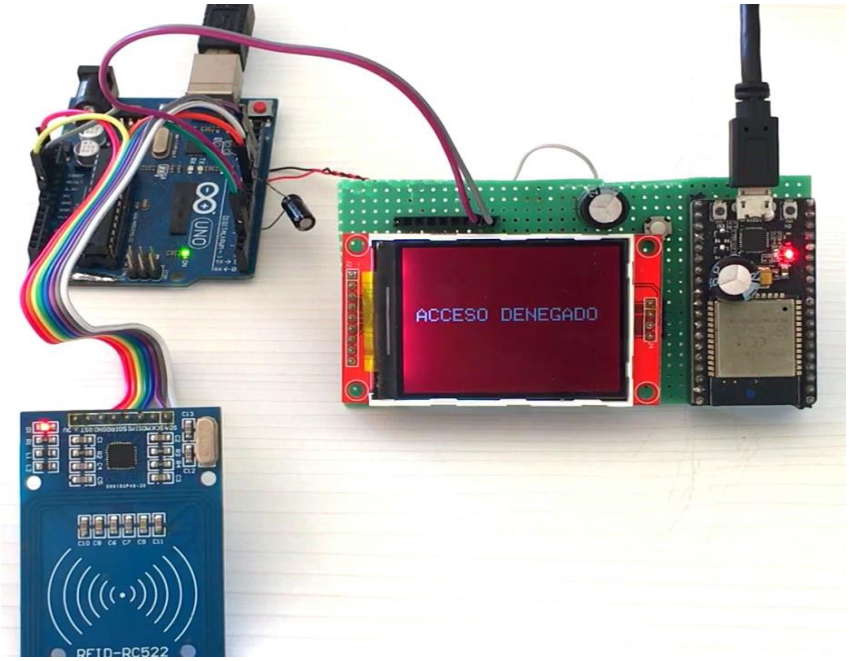


Figura 55. **Acceso denegado al usuario**.

Desarrollo para la configuración de servicio Node js

Node JS es un entorno de tiempo de ejecución de Javascript y que facilitará la tarea resulta que, su ejecución es en tiempo real y que se comunica con el bróker MQTT y que se podrá suscribir a todos los tópicos en el sistema implementado del Internet de las Cosas (IoT) igualmente, hará conexión a la base de datos.

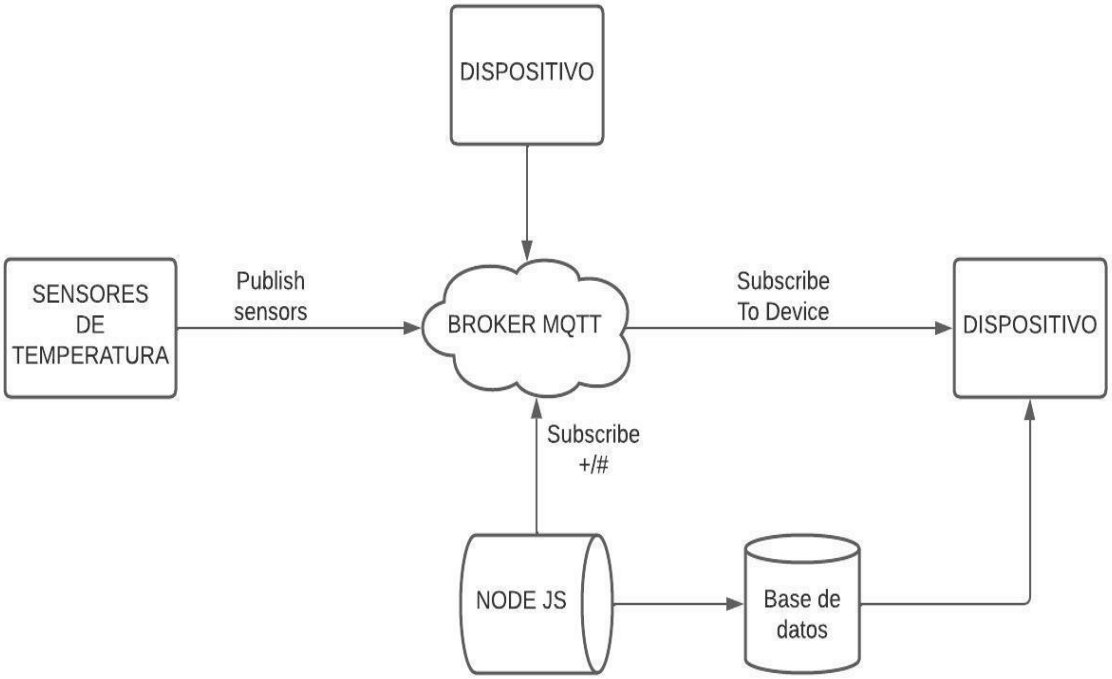


Figura 56. **Funcionalidad del servicio de Node Js**.

Para implementar el servicio de Node Js lo haremos de la siguiente manera: primero hará comunicación con la base de datos en donde esta guardado los datos que pertenecen al dispositivo e interviene el bróker MQTT, no obstante, si el usuario pasa la tarjeta por el lector RFID, se validará si tiene derecho a pasar o no por el portal.

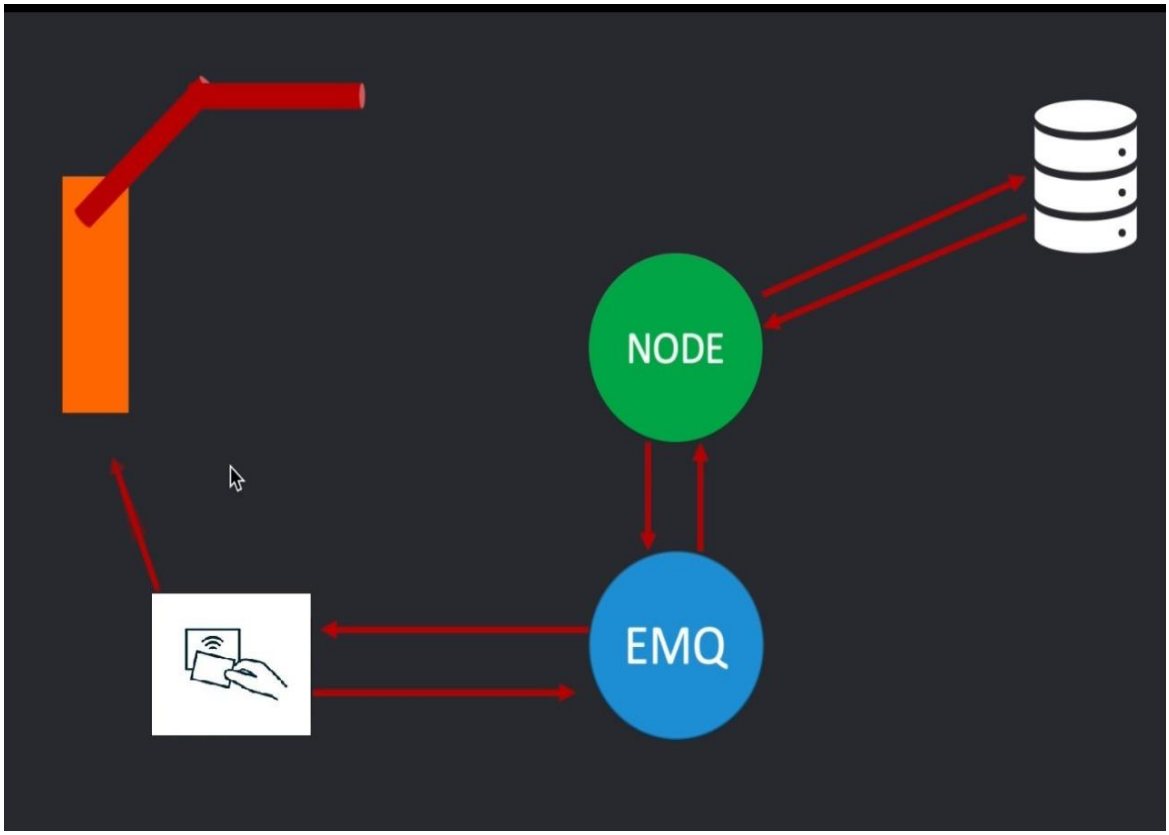


Figura 57. **Servicio Node Js para el proyecto**.

Para poder usar el servicio de Node Js procederemos a descargar y a instalar mediante comandos en la terminal luego, se añadirá las librerías de MQTT, así como protocolos para la comunicación y las credenciales de la base de datos MYSQL y finalmente, se pueda sincronizar el dispositivo y la aplicación web.

```
# Remove the version that is currently installed
sudo apt remove -y nodejs
#Setup sources for the version you want
curl -SL https://deb.nodesource.com/setup_10.x | sudo -E bash -
# (Re ) Install Node
sudo apt-get install -y nodejs
```

Figura 58. **Instalación de Node Js**.

```
var mysql = require('mysql');
var mqtt = require('mqtt');

//CREDENCIALES MYSQL
var con = mysql.createConnection({
  host: "jonsuiot.ga",
  user: "admin_jonsuiot",
  password: "ellalabotella",
  database: "admin_jonsuiot"
})

//CREDENCIALES MQTT
var options = {
  port: 1883,
  host: 'jonsuiot.ga',
  clientId: 'acces_control_server_' + Math.round(Math.random() * (0- 10000) * -1) ,
  username: 'web_client',
  password: 'core94tales',
  keepalive: 60,
  reconnectPeriod: 1000,
  protocolId: 'MQIsdp',
  protocolVersion: 3,
  clean: true,
  encoding: 'utf8'
};

var client = mqtt.connect("mqtt://jonsuiot.ga", options);
```

Figura 59. **Configuración MQTT y MYSQL en Node Js**.

Mediante el servicio Node Js se procederá a realizar la comunicación con el dispositivo IoT luego, se validará los usuarios que ingresen con la tarjeta que les pertenece inmediatamente, realizará una consulta sencilla en MYSQL cada vez que ingresen o pasen la tarjeta por el dispositivo.

Con el objetivo de, validar los usuarios que pueden ingresar y posteriormente, el dato se registrará y será almacenado en la base de datos.

```
if(query=="access_query"){
  var rfid_number = message.toString();

  //HACEMOS LA CONSULTA
  var query = "SELECT * FROM cards_habs WHERE cards_number = '" + rfid_number + "' AND devices_serie = '" + serial_number + "'";
  con.query(query, function (err, result, fields){
    if(err) throw err;

    //console.log(result);
    if(result.length==1){
      //GRANTED
      client.publish(serial_number + "/user_name", result[0].hab_name);
      client.publish(serial_number + "/command", "granted");
      console.log("Acceso permitido a..." + result[0].hab_name);

      var query = "INSERT INTO `traffic` (`traffic_hab_id`) VALUES (" + result[0].hab_id + ");";
      con.query(query, function (err, result, fields) {
        if (err) throw err;
        console.log("Ingreso registrado con exito en 'TRAFFIC' ");
      });

    }else{
      //REFUSED
      client.publish(serial_number + "/command", "refused");

    }
  });

}
```

Figura 60. **Validación y registro de ingreso en la BDD**.

Desde la terminal se ejecutará Node Js y se visualizará los mensajes y validaciones cuando un residente o habitante ingrese por el dispositivo, y el usuario tengo acceso, por último, se registra con éxito en la base de datos.

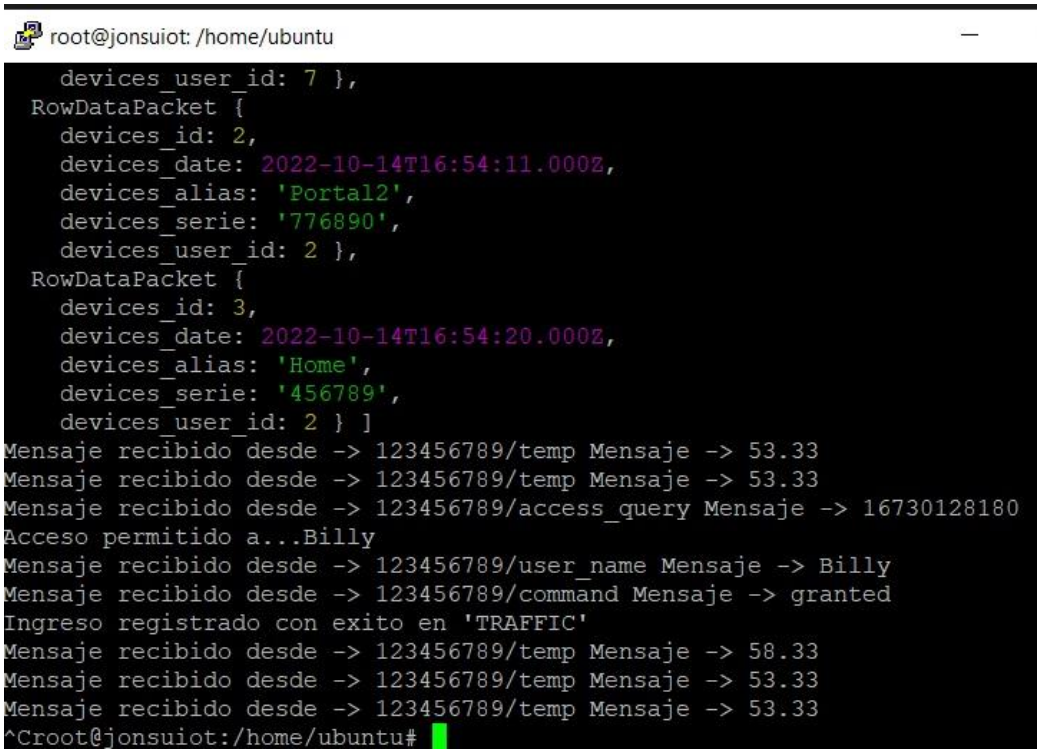


Figura 61. **Node Js en la terminal Putty**.

Por último, en la aplicación web que se desarrolló en el Dashboard se tendrá a disposición el registro que tenemos en HeidiSQL almacenada y se podrá visualizar, posteriormente, la comunicación no se pierde y que todos los servicios para el proyecto se siguen manteniendo en correcto funcionamiento.

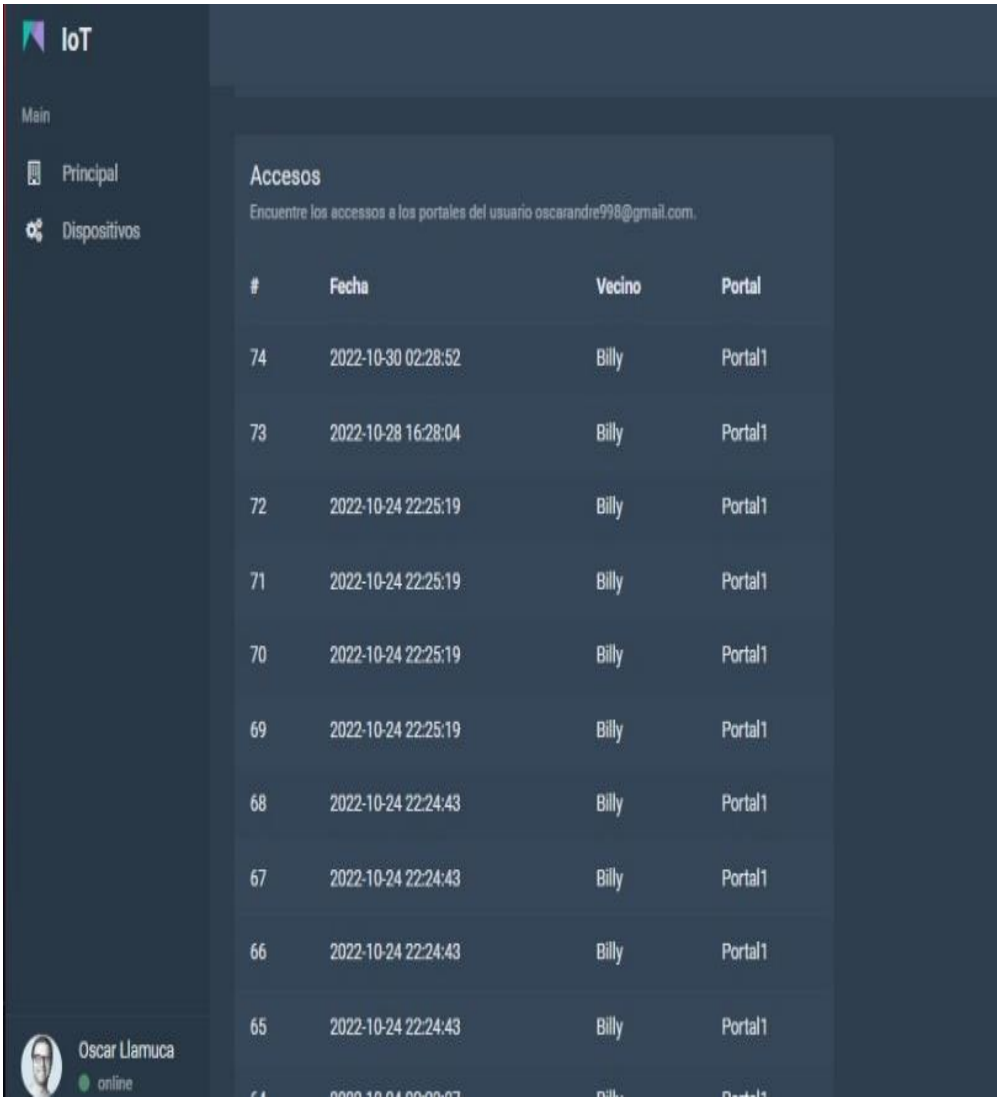


Figura 62. **Accesos registrados en la aplicación web**.

En esta sección se describió el método a utilizar y los pasos a seguir para la conexión entre los dispositivos IoT con la nube de AWS por consiguiente se pudo evidenciar el funcionamiento para el envío de los datos a través de internet en tiempo real que dará un mejor control de la información y que puede beneficiar de una u otra manera al curso regular de las actividades.

Validación de los resultados para control de acceso

La presente propuesta se fundamentó en la creciente comunicación inteligente entre las cosas, especialmente el sensor equipado, bajo el alcance de IoT que está dando como resultado la producción de una

cantidad increíblemente grande de Big Data. Con el respaldo de la computación consciente del contexto, esta es suficiente para abordar las tareas integrales y no triviales con un alto grado de automatización, especialmente para el control de acceso y seguridad en la etapa Cosmos.

Por ello, el siguiente esquema presentado en la figura 48 expone el rol del dispositivo, en este caso el lector RFID que se va a enviar al bróker, y este a su vez considerando que tiene una suscripción por parte de la plataforma en Node.js y node por su cuenta, consultará a la base de datos, el cual recibirá una respuesta y a partir de ello, evaluará oportunamente si la persona tiene derecho a pasar o no en la etapa Cosmos de la urbanización Villa Club, con lo que, se prevé el fortalecimiento del control de acceso y seguridad en el lugar.

Por tanto, mediante la validación de los resultados en el control de acceso, se estima la corrección de los errores de seguridad que anteriormente en el periodo enero – enero (2021 – 2022), presentaron alto margen porcentual de falencias, específicamente en la unidad de identificación, unidad de entrada, unidad de puerta de contacto y unidad de salida, lo cual se prevé mejorar en la corrección de la problemática descrita y la implantación de herramientas tecnológicas como elementos de innovación y desarrollo en la operatividad de la urbanización.

Asimismo, en la actualidad, la computación en la nube es la solución más recomendada para los problemas mencionados anteriormente en el control de acceso, y a través de ello, promete brindar servicios eficientes como los productos básicos tradicionales. Los servicios en la nube emergentes están siendo apreciados por respaldar los análisis de integración de sistemas, para todas las partes interesadas, en sus tareas de rutina.

Por tanto, las necesidades de servicios informáticos y analíticos altamente robustos para abordar y analizar los desafíos relacionados con los datos con un costo extremadamente reducido han llevado aún más a la vanguardia la computación en la nube rica en servicios, que para este

proyecto puede aprovechar las ventajas del IoT y servicios en la nube para el control de acceso y seguridad en la etapa Cosmos.

Finalmente, el creciente interés en IoT y el sistema de aprovisionamiento en la nube ha desencadenado el aumento de los análisis integrales alojados en la nube como un elemento de innovación tecnológica y fortalecimiento de la operatividad en tiempo real.

CONCLUSIONES

El presente estudio ha concluido con el cumplimiento de los objetivos de investigación, a través de lo cual, se ha proporcionado una ilustración completa del sistema de internet de las Cosas sobre el análisis y el servicio emergente basado en la nube, especialmente para el control de acceso y seguridad en la etapa Cosmos de la urbanización Villa Club, que se ha basado en la selección de los servicios de interés que está influenciada principalmente por su utilidad y aplicabilidad en el ecosistema IoT.

Se determinó la teoría relacionada con la implementación de sistemas IoT, como soluciones de seguridad usando los servicios en la nube; para ello, se utilizó AWS que se ajustó a la necesidad del presente proyecto debido a su bajo costo, consumo y rentabilidad, a su vez se utilizó el protocolo MQTT ya que tiene la facilidad de enviar datos en tiempo real y con ayuda del dispositivo con el que interviene, con el servicio en Node JS y con la comunicación a la base datos que tiene la facilidad de enviar dichos datos al dispositivo con el cual se puede comunicar, que representan estos elementos para el desarrollo e implementación del sistema IoT.

Asimismo, se presentó el escenario situacional actual, referente al control de acceso y seguridad en la etapa Cosmos para el desarrollo de un sistema IoT, a través de los servicios en la nube, el cual se realizó mediante una encuesta al personal administrativo integrado por 17 personas, las

cuales están a cargo del control de acceso, registros, revisión de bitácoras de entrada y salida de personas.

En esta etapa se pudo obtener como resultado de la encuesta, que el escenario situación presenta un control deficiente con 26,8% de errores en la unidad de identificación, 44,2% en la unidad de entrada, 22,9% en la unidad de contacto de puerta y 38,7% en la unidad de salida, lo cual es contrastado con las respuestas que indicaron que el 47,1% indicó que no están conformes con la metodología actual de procesos operativos, ya que no existe un control integrado en el acceso de personas.

Por ello, el 76,5% indicó que sí estarían de acuerdo en el desarrollo e implementación de un sistema IoT para el control de acceso y seguridad en la etapa Cosmos, considerando que esto mejoraría los procesos de control y maximizaría los elementos de seguridad y manejo de entradas y salidas de personas, con revisiones y control en tiempo real; lo cual integra los procesos de innovación y tecnología en la administración de la etapa Cosmos para la urbanización Villa Club.

En concordancia con lo expuesto, se presentó el diseño del sistema IoT, usando los servicios de la nube para el control de acceso y seguridad basado en los servicios de Amazon Web Services (AWS), el cual fue desarrollado en diferentes etapas para la configuración de servicios en la nube; una de las etapas es para la configuración de base de datos, para la construcción del panel de control en PHP; otra de las etapas importantes es la configuración EMQX mediante protocolo MQTT; la configuración del dispositivo IoT y también se realizó la configuración del servicio Node JS, para concluir, las diferentes etapas que se mencionaron sirvieron para la implementación IoT, y que tiene como finalidad demostrar la seguridad y el control de acceso mediante los datos y demostrar que realmente se cumple las medidas mediante la práctica para la etapa Cosmos de la Urbanización Villa Club.

Para ello, se presentó la validación de los resultados a partir de la implementación propuesta en el esquema IoT para el control de acceso a la etapa Cosmos de la urbanización Villa Club, en ello, el lector RFID se envía al bróker y este a su vez como tiene una suscripción por parte de la plataforma en Node JS, consulta a la base de datos que recibe una respuesta, evaluando de manera oportunamente si esa persona tiene derecho a pasar o no, de una manera más clara y sencilla se ha demostrado que los datos que generamos al utilizar nuestro dispositivo es aprovechado por los programas que lo tenemos sincronizados.

En consecuencia, se ha concluido con el presente proyecto, considerando que, los desarrollos de servicios emergentes de próxima generación están cerrando la brecha y ayudando a la computación en la nube a adaptarse gradualmente a los desafíos de IoT por completo y brindando las abundantes herramientas de análisis a los usuarios finales, como en este caso para mejorar el control de acceso y seguridad en la etapa Cosmos de la urbanización Villa Club, como un modo de aporte en el desarrollo tecnológico para Guayaquil, Daule y el Ecuador.

RECOMENDACIONES

- Se recomienda el desarrollo de pautas estructurales sobre el escenario actual para el análisis y toma de decisiones en cuando a la implementación continua de herramientas tecnológicas y elementos de innovación en la gestión de control y seguridad de las urbanizaciones, considerando que es fundamental mantener un control integrado y en tiempo real, que monitoree constantemente las actividades en el control de acceso de personas, a través de IoT y servicios en la nube AWS, tomando en cuenta las ventajas operativas y de productividad que ofrecen a la comunidad.
- Se recomienda una supervisión estricta del uso de datos, ya que el control de acceso y seguridad en las urbanizaciones pueden manejar información sensible de los residentes, los cuales necesitan el mantenimiento de reserva de datos y cuidado continuo, para mantener un control efectivo de acuerdo a la operatividad y manejo de protocolos de seguridad en la administración local.
- Se recomienda implementar procesos de autorregulación corporativa referente al uso de la tecnología de sistemas IoT y servicios en la nube, que fortalezca la gestión de datos e información de aquellos que entran y salen y demás

elementos de los residentes, para promover la reserva y la seguridad de la información y datos de quienes habitan la etapa cosmos, desde una administración corporativa responsable.

BIBLIOGRAFÍA

Alcázar, M. P. (3 de Agosto de 2018). La Internet de las Cosas, el Big Data y los nuevos problemas de la comunicación en el Siglo XXI. (U. C. Madrid, Ed.) *Revista Ediciones Complutense. Mediaciones Tecnológicas, 10*(52), 12.

Amazon.com, Inc. (2022). *Informe anual de AWS Amazon Web Services en el desarrollo y expansión tecnológica.* Informe anual, Departamento de Servicios de Amazon, Seattle.

Augé, A. C. (2018). *Demostrador arquitectura publish/suscribe con MQTT.* Investigación científica, Universidad de Barcelona, Centro de Investigación en Ingeniería de las Telecomunicaciones, Barcelona.

Ávila, Ó. (Julio de 2016). Computación en la Nube. *Revista de Ingeniería Eléctrica de la Universidad Nacional Autónoma de México, 04*(19), 48.

Banco Mundial. (2021). *Número de dispositivos conectados al internet de las cosas (IoT) en todo el mundo de 2019 - 2021, con previsiones de 2022 - 2030.* Departamento de Desarrollo y Tecnología. París: Banco Mundial.

Barrio, M., & Leroux, I. A. (2018). *Internet de las Cosas.* Universidad Carlos III de Madrid, Centro de Desarrollo Tecnológico. Madrid: Editorial Reus.

Bernal, Y. E. (2020). *Diseño de una red IoT para el hogar.* Investigación científica, Universidad Nacional de Colombia, Programa de Maestría en Redes y Telecomunicaciones, Bogotá.

Berreño, R., Herrera, A. K., & Alarcón, D. M. (2020). *Revisión sistemática del estándar ISO/IEC 30141:2018 como arquitectura de referencia para la seguridad en entornos IoT.* Investigación científica, Universidad Católica de Colombia, Departamento de Especialistas en Seguridad de la Información , Bogotá.

Bonilla-Fabela, I., Tavizon, A., Escobar, M. M., Muñoz, L. T., & Laines, I. C. (2016). *IoT, El Internet de las Cosas y la innovación de sus aplicaciones.* Universidad Autónoma Nacional de México, Programa de Maestría en Desarrollo Tecnológico e Innovación Digital. México D.F.: UNAM.

Brañes, R. E., & Osoria, S. H. (2019). *Arquitectura de back end con Amazon Web Services para sistemas .* Investigación científica, Universidad de Montemorelos, Programa de Maestría en Ciencias Tecnología Informática, México D.F.

Calva, J., Rojas, D., Román, R. E., & Radicelli, C. (Agosto de 2020). Seguridad IoT. Principales amenazas en una taxonomía de activos. *Revista de Tecnología y Desarrollo de Sistemas Integrados de la Universidad Alas Peruanas, 7*(3), 54.

Carrillo, M. J., & Marroquín, M. R. (2016). *Amazon Web Services: Amazon EC2. Cambiando paradigmas, análisis, uso e implementación.* Investigación científica, Universidad de San Carlos de Guatemala, Programa de Ingeniería en Ciencias y Sistemas, Ciudad de Guatemala.

Castillo, Á. A., & Navarro, J. (2019). *Diseño e Implementación de un Sistema MQTT sin bróker basado en SDN.* Investigación científica, Universidad de Granada, Programa Máster en Ingeniería de Tecnologías de Telecomunicación, Madrid.

Cisneros, C. R., & Altamirano, J. F. (2021). *Estudio de mecanismos de aseguramiento de la información para internet de las cosas IoT en Smart Home.* Pontificia Universidad Católica del Ecuador, Programa de Maestría en Tecnologías de la Información. Mención en Redes de Comunicaciones. Quito: PUCE.

Comisión Económica para América Latina y el Caribe. (2021). *Informe de desarrollo IoT en el mundo, con referencia comparativa en la región. Transformaciones tecnológicas en América Latina.* Informe anual, CEPAL, Departamento de Desarrollo en Tecnologías e Información, Santiago de Chile.

Condori, G. T. (2019). *El Internet de las Cosas IoT.* Investigación científica, Escuela Superior Profesional de Electrónica y Telecomunicaciones, Programa de Maestría en Telecomunicaciones e Informática, Lima.

Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. (2021). *Informe sobre Tecnología e Información.* Organización de las Naciones Unidas, Área de Desarrollo Tecnológico. Nueva York: UNCTAD.

Corporación Samborondón Cía. Ltda. CORSAM. (2022). *Informe administrativo de: Villa Club, etapa Cosmos: Informe de seguridad y control de accesos.* Informe administrativo, CORSAM, Departamento Administrativo, Guayaquil.

Cortés, P., & Cabero, M. M. (2017). *Computación en la Nube.* Investigación científica, Universidad de Salamanca, Programa de Investigación en Información y Desarrollo Tecnológico, Salamanca.

Cosin, A. L., & Manzoni, P. (2021). *Uso de MQTT para el control de dispositivos de IoT.* Investigación científica, Universidad Politécnica de Valencia, Programa de Investigación en Ingeniería Informática, Valencia.

Cruz, M. d., Ortega, J. P., Demera, G., & Zambrano, D. (30 de Abril de 2018). Tecnologías de internet de las cosas en la obtención de información. *Revista Científica Dominio de las Ciencias, 4*(2), 160.

Estévez, M. E., & Castro, M. (2016). *Internet de las Cosas (IoT). Privacidad y seguridad.* Investigación científica, Universidad de Jaén. Escuela Politécnica Superior de Jaén, Programa Máster en Seguridad Informática, Jaén.

Fernández, A. M., & Noguera, P. I. (2017). *Lineamientos de Seguridad IoT para el Ecosistema de Dispositivos Periféricos IoT.* Centro de Desarrollo Tecnológico de la Universidad Nacional Autónoma de México, Ecosistemas de Desarrollo en Tecnología. México D.F.: GSMA-UNAM.

González, A., García, Y., Gallego, D. E., & Sastoque, J. (2016). *Impacto medioambiental de la integración de la computación en la nube y la Internet de las Cosas IoT.* Universidad Nacional Mayor de San Marcos, Programa de Desarrollo Tecnológico e Informática de Seguridad. Lima: UNMSM.

Gutiérrez, Á. (Marzo de 2018). Almacenamiento en la Nube. *Revista ACTA de Tecnologías de Información, 16*(7), 81.

Hernández, N. L., & Fuentes, A. S. (2018). *Computación en la Nube.* Artículo científico, Universidad de Pamplona, Programa de Maestría en Ingenierías y Arquitecturas de Sistemas Informáticos, Pamplona.

Joyanes, L. (2021). *Internet de las Cosas. Un futuro hiperconectado: 5G, inteligencia artificial, Big Data, Cloud, Blockchain y ciberseguridad*

(Segunda ed., Vol. 16). (Marcombo, Ed.) Lima, Perú: Computación y Ciencia General.

Kezherashvili, B. (2017). *Comutación en la Nube. Internet de las Cosas IoT y desarrollo tecnológico.* Investigación científica, Universidad de Almería, Programa Máster en Administración, Comunicaciones y Seguridad Informática, Almería.

Laguna, J. A., Rosales, A. B., Balbuena, J. A., Zamora, A. R., & Frías, C. U. (Enero de 2020). Big Data e Internet de las Cosas (IoT) para los sistemas inteligentes. Características y áreas de oportunidad. *Revista del Instituto Mexicano de Tecnología, 626*(17), 71.

Marcet, N. C., & Martínez, G. (2019). *Implementación y evaluación de plataformas en la nube para servicios de IoT (Interner de las Cosas).* Investigación científica, Universidad Politécnica de Valencia, Programa de Maestría en Telecomunicaciones, Valencia.

Martínez-Santander, C., & Cruz, Y. (Marzo de 2021). Tendencias tecnológicas y desafíos de la seguridad informática. *Revista Polo de Conocimiento: Sección de Desarrollo Tecnológico de Sistemas de Seguridad IoT, III*(V), 16.

Molano, J. I., Lovelle, J. M., & Montenegro, C. E. (2017). *Metamodelos para la integración del Internet de las Cosas (IoT) .* Investigación científica, Universidad de Oviedo, Programa de Investigación en Ingeniería de Sitemas Informáticos y Seguridad Tecnológica, Oviedo.

Norero, Y. C., & Salazar, G. D. (2019). *Análisis comparativo de desempeño entre Protocolos MQTT y COAP para Internet de las Cosas (IoT) con Raspberry PI 3 en ambientes IEEE 802.11.* Universidad de las Fuerzas Armadas, Centro de Posgrados. Maestría en Gerencia de Sistemas. Quito: ESPE.

Norma ISO/IEC 30141 . (2018). *Normas ISO/IEC 30141 sobre Internet de las Cosas (IoT).* Informe normativo, Normas ISO, París.

Paternina, F. J., & Henríquez, C. (Diciembre de 2016). La computación en la nube. Un modelo para el desarrollo de las empresas. (Scielo, Ed.) *Revista Semillero de Ingeniería de Sistemas de la Universidad Autónoma del Caribe, 13*(2), 87.

Piedra, C. D., Sari, P. A., & Cedillo, I. P. (2018). *Una arquitectura de integración tecnológica de Internet de las Cosas (IoT) y computación en la nube.* Universidad San Francisco de Quito, Programa de Maestría en Sistemas Integrados de Tecnología. Quito: USFQ.

Pisano, A., & Hoffman, E. (2018). *Internet de las Cosas (IoT).* Investigación científica, Universidad San Andres, Tesis de Maestría en Gestión de Servicios Tecnológicos y de Telecomunicaciones, Buenos Aires.

Ramírez, X. G., Hernández, J., & Duarte, M. A. (2019). *Seguridad en la nube: Internet de las Cosas (IoT) evolución indispensable en el siglo XXI.* Investigación científica, Universidad Distrital Francisco José de Caldas, Centro de Investigación en Tecnología , Bogotá.

Rose, K., Eldridge, S., & Chapin, L. (2018). *La Internet de las Cosas. Una breve reseña para entender mejor los problemas y desafíos de un mundo más conectado* (Vol. II). (McGraw-Hill, Ed.) Buenos Aires, Argentina: Sociedad de Internet; McGraw-Hill.

Salazar, J., & Silvestre, S. (2018). *Internet de las Cosas.* Investigación científica, Centro de Investigación y Desarrollo Tecnológico TechPedia, Programa de Ingeniería en Plataformas Virtuales e Información, Barcelona.

Sapién, A. L., Diez, M. d., & Piñón, L. C. (2021). *Computación en la Nube. Una estrategia competitiva para las pequeñas y medianas empresas en México.* Artículo científico, Universidad Autónoma de Chihuahua,

Programa de Maestría en Tecnologías de la Información y Comunicación, México D.F.

Tejada, J. C. (2020). *Internet de las Cosas. Aliado de la transformación digital.* Investigación científica, Universidad EIA. Escuela de Ingeniería de Antioquia, Programa Máster en Ingeniería Informática y Desarrollo Tecnológico, Medellín.

Tello, M. A., & Velásquez, F. C. (2017). *Diseño de un esquema de integración de tecnologías IoT de los Sistemas de Seguridad Informática.* Investigación científica, Universidad del Pacífico de Colombia, Programa de Ingeniería en Sistemas, Bogotá.

Toledo, A. H., Nogales, E. D., & Zaragoza, J. J. (2017). *Amazon Web Services (AWS). Solución de infraestructura aplicativa en la nube para pequeñas y medianas empresas.* Instituto Politécnico Nacional, Programa de Investigación de Ingeniería en Sistemas. México D.F.: UPIICSA.

Unión Internacional de Telecomunicaciones. (2012). *Interconexión de cosas físicas y virtuales. Internet de las Cosas IoT integrado en las telecomunicaciones.* Informe de Desarrollo Tecnológico, UIT, Oficina de Normalización de las Telecomunicaciones, Ginebra.

Vecchio, R., Martínez, E., & Cosentino, J. P. (Agosto de 2018). Internet de las Cosas (IoT) en el desarrollo de la seguridad y manejo estructural de la ciudad. *Revista de Investigación Tecnológica Belgrano, 16*(4), 98.

ANEXOS

Anexo 1. Cuestionario de preguntas

 **INGENIERÍA EN SISTEMAS INTELIGENTES CON ÉNFASIS EN ADMINISTRACIÓN DE REDES**	
Tema	Desarrollo de un sistema IoT para el control de acceso y seguridad en la etapa Cosmos de Villa Club, usando los servicios en la nube.
Objetivo	Conocer el escenario situacional, referente al control de acceso y seguridad en la etapa Cosmos para el desarrollo de un sistema IoT a través de los servicios en la nube.
Muestra	17 miembros del Departamento Administrativo CORSAM, para la etapa Cosmos de Villa Club.

Lugar	Daule, Guayas.					
Fecha	26 a 30 de agosto de 2022					
Horario	8am a 4:30pm, de lunes a viernes.					
Indicaciones	Responda la respuesta adecuada marcando con una X.					
ENCUESTA						
Datos	1 = Totalmente de acuerdo		2 = Parcialmente de acuerdo			
	3 = Indiferente	4 = Totalmente en desacuerdo		5 = Parcialmente en desacuerdo		
No.	**Pregunta**	**1**	**2**	**3**	**4**	**5**
1	¿Está usted de acuerdo en la metodología de procesos operativos desarrollada actualmente (2021 – 2022 enero a enero) para el control de acceso y seguridad de la etapa Cosmos en la urbanización Villa Club?					
2	¿Considera usted que se requiere la implementación de nuevos procesos de seguridad tecnológica e innovación en la gestión de control de accesos a la etapa Cosmos?					
3	¿Cree usted que el desarrollo de nuevos sistemas de internet de las cosas con servicios digitales (en la nube), mejoraría los procedimientos de comunicación y coordinación en la seguridad de la etapa Cosmos?					
4	¿Está usted de acuerdo en la implementación de nuevos procedimientos de control de acceso para la seguridad de la					

	etapa Cosmos, mediante herramientas de tecnologías de innovación?					
5	¿Considera usted que el desarrollo e implementación de sistemas IoT para el control y seguridad en las urbanizaciones, constituye un beneficio operativo?					
6	¿Está usted de acuerdo que, ante los errores de control de acceso y seguridad en la Etapa Cosmos, se deben implementar nuevos procesos operativos con sistemas integrados IoT?					
7	¿Actualmente considera usted que los porcentajes de errores en los procesos de control de acceso a la etapa Cosmos, incrementan la inseguridad de los residentes?					
8	¿Estima usted que el desarrollo e implementación de un sistema IoT a través de servicios en la nube, maximizará la operatividad y seguridad?					
9	¿Esta uste de acuerdo en que los avances tecnológicos para el control y seguridad en el acceso de personas a las urbanizaciones, debe fomentar una innovación continua de actualización?					
10	¿Estima usted que el desarrollo de un sistema IoT para el control de acceso y seguridad en la etapa					

	Cosmos, usando los servicios en la nube, mejorarán las capacidades operativas de seguridad y coordinación de información en tiempo real?					

Anexo 2. Etapa Cosmos

Anexo 3. Etapa Cosmos, urbanización Villa Club