UNIVERSIDAD TÉCNICA DE BABAHOYO FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

DICIEMBRE 2022 – ABRIL 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE: INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DE UN SISTEMA DE SEGURIDAD BASADO EN EL INTERNET DE LAS COSAS PARA VIVIENDAS URBANAS.

ESTUDIANTE:

JUAN FERNANDO SAA AYALA

TUTOR:

ING. CARLOS SOTO VALLE

AÑO 2023

RESUMEN

El internet de las cosas (IoT) se ha convertido en una parte integral de nuestra vida cotidiana, y está expandiéndose aún más a medida que el número de dispositivos inteligentes se incrementa. Esto plantea una serie de desafíos para la seguridad, ya que los dispositivos IoT se conectan a la red y comparten datos. Para abordar estos desafíos, un equipo de investigadores desarrolló un sistema de seguridad para viviendas urbanas basado en IoT. El sistema utiliza sensores inalámbricos para recopilar datos y almacenarlos en la nube. Además, una red inalámbrica de comunicación de datos se utiliza para transmitir datos de los sensores a un centro de control remoto. El sistema incluye un sistema de alerta que se puede configurar para enviar alertas al usuario si se detecta algún tipo de actividad anómala. El sistema también incluye un mecanismo de autenticación para garantizar que sólo los usuarios autorizados puedan acceder a los datos. Por último, el sistema proporciona una interfaz de usuario para que los usuarios puedan interactuar con el sistema. En conclusión, este sistema de seguridad para viviendas urbanas con IoT es una solución eficaz para mejorar la seguridad en entornos domésticos.

El objetivo de este análisis es desarrollar un sistema de seguridad para viviendas urbanas conectadas a Internet de las Cosas (IoT). El sistema de seguridad constará de una variedad de dispositivos conectados a la red de IoT, como sensores de movimiento, cámaras de videovigilancia, sensores de presencia de humo y de CO, detectores de intrusos, sistemas de alarma, etc. Estos dispositivos se conectarán a una plataforma en la nube que estará configurada para recibir notificaciones en caso de detectarse algún evento anómalo. La plataforma contará con un sistema de autenticación para proporcionar una seguridad adecuada y se permitirá a los usuarios acceder a los dispositivos desde cualquier lugar. El sistema también se diseñará para comprobar la integridad de los dispositivos conectados y permitir a los usuarios controlar el acceso a sus dispositivos. Se incluirá una aplicación móvil para permitir a los usuarios configurar y controlar los dispositivos de forma remota.

PALABRAS CLAVES

Alternativas, Monitoreados, Plataforma, Servicio, Factores

SUMMARY

The Internet of Things (IoT) has become an integral part of our daily lives, and it is expanding even more as the number of smart devices increases. This poses a number of security challenges as IoT devices connect to the network and share data. To address these challenges, a team of researchers developed an IoT-based security system for urban homes. The system uses wireless sensors to collect data and store it in the cloud. In addition, a wireless data communication network is used to transmit data from the sensors to a remote control center. The system includes an alert system that can be configured to send alerts to the user if any type of anomalous activity is detected. The system also includes an authentication mechanism to ensure that only authorized users can access the data. Finally, the system provides a user interface so that users can interact with the system. In conclusion, this security system for urban homes with IoT is an effective solution to improve security in domestic environments.

The objective of this analysis is to develop a security system for urban homes connected to the Internet of Things (IoT). The security system will consist of a variety of devices connected to the IoT network, such as motion sensors, video surveillance cameras, smoke and CO presence sensors, intrusion detectors, alarm systems, etc. These devices will be connected to a cloud platform that will be configured to receive notifications in case any anomalous event is detected. The platform will have an authentication system to provide adequate security and users will be allowed to access the devices from anywhere. The system will also be designed to check the integrity of connected devices, provide automatic firmware updates, and allow

users to control access to their devices. A mobile app will be included to allow users to remotely configure and control the devices.

KEYWORDS

Alternatives , Monitored , Platform , Service , Factors

CONTENIDO

PLANTEAMIENTO DEL PROBLEMA

Las redes de Internet de las Cosas (IoT) están cambiando la forma en que vivimos, trabajamos y nos comunicamos. Estas redes conectan dispositivos a la red, permitiendo a dispositivos como refrigeradores, termostatos, lavadoras, luces, sistemas de seguridad y más, comunicarse entre sí. Esta conectividad también ofrece nuevas oportunidades para proporcionar un entorno seguro y proteger los dispositivos de la red de manera efectiva. Uno de los principales riesgos de la IoT es la seguridad. Los dispositivos conectados a la red son vulnerables a ataques cibernéticos, ya que los dispositivos conectados a la red pueden ser utilizados para acceder a la información de la red o comprometer la seguridad de la red. Para contrarrestar estos riesgos, los sistemas de seguridad de la IoT deben proporcionar una capa de seguridad para proteger los dispositivos conectados a la red. Esto incluye la autenticación de usuarios, la protección contra amenazas externas, la criptografía para proteger la información transmitida, la autorización, el control de acceso, la detección de intrusiones y la prevención de amenazas. Además, los sistemas de seguridad de la IoT deben diseñarse para trabajar con dispositivos conectados a la red, lo que significa que deben ser capaces de identificar los dispositivos, autenticarlos, garantizar la comunicación segura entre los dispositivos y protegerlos de amenazas externas. Para implementar un sistema de seguridad eficaz en una vivienda urbana, es importante tener en cuenta los siguientes aspectos:

• Autenticación: Los sistemas de seguridad deben basarse en una autenticación fuerte para garantizar que los dispositivos sean accesibles solo por usuarios autorizados. Esto puede incluir la autenticación de dos factores, que requiere un segundo método de verificación para el acceso.

• Encriptación: Los sistemas de seguridad deben usar cifrado para proteger la información transmitida entre dispositivos. Esto evita que los atacantes puedan ver los datos en su forma cruda y los protege de la manipulación.

• Control de acceso: Los sistemas de seguridad deben proporcionar un control de acceso para garantizar que solo los usuarios autorizados puedan acceder a los dispositivos de la red. Esto incluye la autorización de usuarios para los dispositivos específicos de la red.

• Detección de intrusos: Los sistemas de seguridad deben proporcionar herramientas para detectar cualquier actividad sospechosa que pueda indicar un ataque a la red. Esto incluye la monitorización de la actividad de la red para detectar intentos de acceso no autorizados y el uso de algoritmos de detección de intrusiones para detectar actividades anómalas.

• Prevención de amenazas: Los sistemas de seguridad deben usar herramientas para prevenir amenazas externas antes de que puedan causar daños. Esto incluye la implementación de un firewall para bloquear el acceso no autorizado a la red y la instalación de software antivirus para detectar y prevenir el malware. En conclusión, los sistemas de seguridad de la IoT para viviendas urbanas deben incluir una serie de capas de seguridad para proteger los dispositivos conectados a la red. Esto incluye la autenticación de usuarios, la encriptación, el control de acceso, la detección de intrusiones y la prevención de amenazas. Estas capas de seguridad de la IoT ayudan a garantizar que los dispositivos conectados a la red sean seguros y protegidos.

Por ello el principal problema de investigación de este estudio es analizar el sistema de seguridad en el Internet de las Cosas (IoT) para viviendas urbanas. El estudio se centrará en la identificación de vulnerabilidades en el sistema de seguridad del IoT, evaluará la capacidad de los dispositivos conectados de detectar amenazas e identificará los mecanismos y estándares de seguridad que pueden ser implementados para aumentar la seguridad del sistema. Se evaluará el nivel de seguridad de los dispositivos conectados en la red de IoT, así como la capacidad de los usuarios de la red para implementar controles de seguridad adecuados.

.

JUSTIFICACIÓN

En la actualidad, el Internet de las Cosas (IoT) se ha convertido en una de las tecnologías más importantes para la modernización de nuestras vidas. Se trata de una red de dispositivos inteligentes que se conectan entre sí para proporcionar una variedad de servicios. Estos dispositivos inteligentes se usan en casi todas las áreas de la vida, incluyendo el hogar, la oficina, los vehículos, la salud, etc.

Sin embargo, el uso de estos dispositivos también conlleva riesgos, como la posibilidad de que los hackers puedan acceder a la red y robar información confidencial. Además, hay que tener en cuenta que los dispositivos conectados al IoT son generalmente más vulnerables a los ataques informáticos, ya que muchos de ellos no tienen dispositivos de seguridad incorporados.

Por esta razón, es necesario analizar los sistemas de seguridad que se utilizan para proteger los dispositivos conectados al IoT. Para ello, es importante entender cómo funcionan los sistemas de seguridad y qué medidas de seguridad se deben implementar para proteger los dispositivos conectados a la red.

Este análisis se centrará en el sistema de seguridad para viviendas urbanas conectadas al IoT. Se examinarán los principales riesgos asociados a la seguridad de los dispositivos, así como las mejores prácticas para prevenir estos riesgos. Además, se analizarán los principales protocolos de seguridad y se evaluarán los mecanismos de seguridad disponibles para proteger los dispositivos conectados al IoT.

El análisis de los sistemas de seguridad para viviendas urbanas conectadas al IoT es un tema de gran importancia debido a la creciente adopción de esta tecnología. El objetivo de este análisis es proporcionar información sobre los riesgos asociados con los dispositivos conectados al IoT, así como las mejores prácticas para prevenir estos riesgos. Esto permitirá a los usuarios implementar medidas de seguridad adecuadas para proteger sus dispositivos conectados al IoT.

La seguridad en el Internet de las Cosas (IoT) está evolucionando a un ritmo acelerado. Los dispositivos conectados a la red ofrecen un nuevo nivel de conectividad y comodidad, pero también presentan nuevos riesgos de seguridad. El aumento de dispositivos conectados a la red, en combinación con la naturaleza cada vez más remota de la gestión y control de estos dispositivos, hace que sea vital que los usuarios entiendan los riesgos potenciales y los beneficios que ofrecen los sistemas de seguridad IoT.

Realizar un análisis de seguridad de un sistema de seguridad en el Internet de las Cosas para viviendas urbanas es importante para determinar qué medidas de seguridad se deben implementar para proteger los dispositivos conectados. Un análisis de seguridad IoT puede ayudar a los usuarios a identificar y abordar los riesgos relacionados con la seguridad IoT, así como aprovechar las oportunidades de seguridad que ofrecen los dispositivos conectados.

Un análisis de seguridad IoT también puede ayudar a los usuarios a comprender mejor cómo pueden usar tecnologías de seguridad IoT para mejorar la seguridad de sus viviendas. Un análisis de seguridad IoT puede incluir una evaluación de las políticas de seguridad existentes, una evaluación de los dispositivos conectados en la red, una evaluación de los riesgos relacionados con la seguridad IoT y una evaluación de la infraestructura de seguridad IoT. Estos análisis pueden ayudar a los usuarios a comprender mejor el funcionamiento de los dispositivos conectados y cómo pueden usar estas tecnologías para mejorar la seguridad de sus viviendas.

OBJETIVOS

Objetivo General

Evaluar la eficacia de un sistema de seguridad en el Internet de las Cosas (IoT) para viviendas urbanas. El análisis se centrará en los componentes del sistema, la integración entre ellos, las medidas de seguridad implementadas y la capacidad del sistema para detectar y responder a amenazas de seguridad.

Objetivos Específicos

1. Identificar los principales riesgos de seguridad en el Internet de las Cosas para viviendas urbanas.

2. Estudiar los métodos de seguridad recomendados para proteger las viviendas urbanas de ciberataques.

3. Investigar las soluciones de seguridad actualmente disponibles en el mercado para la protección de viviendas urbanas.

LÍNEA DE INVESTIGACIÓN

Línea de investigación:

- Sistemas de información y comunicación, emprendimiento e innovación.

Sub línea de investigación:

- Redes y tecnologías inteligentes de software y hardware

MARCO CONCEPTUAL

Este proyecto de investigación se centrará en el análisis de un sistema de seguridad en el Internet de las cosas para viviendas urbanas. Se tomarán en consideración aspectos como seguridad informática, seguridad de dispositivos, privacidad, almacenamiento de datos, cumplimiento de normas, regulaciones, y otros factores.

ANTECEDENTES INVESTIGATIVOS

Ramos (2018) en su trabajo de tesis titulada “Sistema de control de llave digital con Raspberry PI3”, explica el diseñó de un software para el control de cerradura con llave digital controlada mediante vía web aplicando el internet de las cosas. El producto final efectivamente cumple con lo propuesto aplicando en un prototipo de cerradura.

El trabajo de grado desarrollado por Mahecha (2018) titulada “Diseño e implementación de una aplicación domótica para iluminación usando inteligencia artificial”, explica sobre el diseño de una aplicación domótica usando un controlador con el entorno de inteligencia artificial que será controlado vía WI-FI.

Por otro lado, Condori (2016) en su trabajo desarrollado cuyo título es “Sistema domótico de seguridad perimetral basado en arduino”, describiendo sobre la implementación de un sistema domótico de seguridad en un prototipo que tiene la funcionalidad de detectar y

alertar la intrusión de personas ajenas al hogar a lo largo del perímetro establecido usando el módulo GSM en el que se puede recibir o enviar datos desde un lugar remoto

La tesis desarrollada por Villca (2016) cuyo tema es "Sistema de seguridad domiciliaria basada en tecnología arduino y aplicación móvil", explica el desarrollo de una aplicación móvil con tecnología Bluetooth para el control automatizado del hogar con el uso de servomotores, sensores y otros medios inalámbricos para reducir costos, ofreciendo más comodidad y seguridad en el hogar.

La tesis desarrollada por Avilés y Cobeña (2015) titulada "Diseño e implementación de un sistema de seguridad a través de cámaras, sensores y alarma, monitorizado y controlado telemétricamente para el centro de acogida "Patio mi pana" perteneciente a la fundación proyecto salesiano", diseña un sistema de seguridad utilizando el microprocesador 18F4550 para el monitoreo del centro de acogida, por medio del módulo GSM, para la comunicación desde el celular hacia el sistema.

La tesis desarrollada por Coarite (2011) titulada "Integración de sistemas domóticos multimedia y comunicación en el hogar", explica la implementación de un sistema domótico para el control de dispositivos como sensores, actuadores y cámara web haciendo uso del micro controlador PIC-18F4550 integrando todos los dispositivos en un solo sistema controlado por vía web, aplicado en un prototipo.

La empresa "Control House", provee al mercado nacional sistema de casas inteligentes, que ofrece seguridad que tiene integrado cámaras de seguridad, alarmas, video porteros, control de acceso y chapas eléctricas. En la parte de automatización se tiene integrado la iluminación, cortinas, riego, climatización, audio/video. Como se muestra es un sistema completo, lo que nos limita a este servicio es el costo de la instalación que abarca entre los precios de 10000 a 15000 dependiendo el grado de complejidad en la parte de seguridad.

Criollo (2014), realiza un estudio respecto a la tecnología y su aplicación en la comunidad de Ambato-Ecuador, motivado por el problema de la inseguridad y los altos índices delictivos. Criollo presenta el diseño de un sistema electrónico para el hogar para vivienda, realizando la implementación de múltiples sensores electrónicos a los objetos del hogar e interconectados a través de la tecnología inalámbrica zigbee, dando como resultado la activación de alarmas cada vez que se presente un suceso inesperado en la vivienda. Se hace

referencia a sistemas domóticos, que son tecnologías que facilitan la convivencia en el hogar con equipos electrónicos y que son de bajo consumo de energía, ayuda a integrar la seguridad con sensores susceptibles al movimiento y que se encuentran integrados a internet. Las alarmas que se generan son de tipo detección de intrusos, detección de fugas de escape, gas entre otros, y alertas de asistencia y ayuda.

Álvarez (2005) en su obra Hablemos de seguridad- Elementos para la vigilancia y la protección se puede encontrar que el autor escribe en un lenguaje sencillo, sensible y reflexivo que transmite con cuidado los detalles para atender la seguridad, protección y vigilancia desde la residencia, los complejos residenciales, la empresa, el establecimiento comercial, instituciones oficiales, conglomerados humanos, las industrias y las grandes factorías, debido a que no se detiene en la aplicación puntual sino en el espectro de la modernidad globalizada donde reina el imperio del terror y el miedo, gracias al accionar de los belicistas o terroristas que durante décadas han medrado a expensas de gobiernos indolentes o permisivos, en detrimento de la sociedad, a la cual su accionar le ha restringido la libertad, el progreso, la tranquilidad, la estabilidad y el propio sentido de pertenencia y en no pocas situaciones hasta el de la patria. Álvarez trata de transmitir los valores de responsabilidad y respeto a través de todo el texto.

DEFINICIONES

Seguridad en el hogar

Según Simón (2018), cuando se habla de seguridad en el hogar se piensa en sistemas anti intrusión, en mecanismos que prevengan sufrir actos vandálicos, robos y otros percances procedentes principalmente del exterior. Se debe tener en cuenta estos asuntos, y considerar las amenazas que provienen del interior y que pueden poner en riesgo tanto a personas como a infraestructuras, bienes y componentes de cualquier vivienda, especialmente durante la ausencia del dueño.

Internet de las cosas

El Internet de las Cosas es una traducción de la expresión en inglés Internet of Things (IoT), que describe un escenario en el que diversas cosas están conectadas y se comunican. Esa

innovación tecnológica tiene como objetivo conectar los ítems que se usa diariamente a internet, con el objetivo de aproximar cada vez más el mundo físico al digital (Valois, 2018).

AMBIENTE DE SOFTWARE

MySQL

Desde la apreciación de (Luna, Peña, & Iacono, 2018) catalogan a MySQL como un sistema de gestión de base de datos multirelacional, con capacidades multiusuario y multihilo (refiriéndose a la capacidad de uso de varios usuarios y diferentes consultas en una misma línea de tiempo) y teniendo además como una de sus principales ventajas que es de código abierto, lo cual ha hecho que sea considerada por aplicaciones de millones de usuarios como Facebook y Twitter.

JavaScript

JavaScript es un lenguaje de programación que se utiliza principalmente para crear páginas web dinámicas. Una página web dinámica es aquella que incorpora efectos como texto que aparece y desaparece, animaciones, acciones que se activan al pulsar botones y ventanas con mensajes de aviso al usuario (Córdoa, 2015).

Css

CSS sirve para definir la estética de un sitio web en un documento externo y eso mismo permite que modificando ese documento (fichero CSS) podamos cambiar la estética entera de un sitio web, ese es precisamente el poder de CSS. (Criollo, 2015)

Html

Según (GAUCHAT, 2012) determina que:

“HTML usa un lenguaje de etiquetas para construir páginas web. Estas etiquetas HTML son palabras clave y atributos rodeados de los signos mayor y menor”.

De acuerdo con lo expresado por Gauchat (2012) argumentamos que permite estructurar un documento a través del uso de etiquetas de símbolo menor () permitiendo definir los elementos que se muestran a través del navegador ayudando a ordenar y etiquetar los documentos dentro de una lista. Admite la utilización de Script los cuales proporcionan información específica a los navegadores que son quienes interpretan el lenguaje, algunos scripts que se pueden anexar a HTML son JavaScript y PHP.

Node.js

Node.js, es el entorno de ejecución de JavaScript por el lado del servidor (server-side). Está construido sobre el motor JavaScript V8 de Google Chrome, utilizado generalmente para la creación de servidores web, pero no se limita sólo a ello (Vásquez, 2019).

Node.js es open source, multiplataforma, y desde su introducción en el año 2009, se hizo muy popular, entre los programadores de aplicaciones web.

Vue.js

Vue es un framework Javascript, es decir, es un conjunto de herramientas y funciones que permiten desarrollar páginas web de una manera más cómoda. Vue nace con la necesidad de no tener que escribir tanto código Javascript y sobre todo con la idea de ahorrar tiempo al programador (Coding Potions, 2019).

Json Web Token

JSON Web Token (JWT) es un estándar para transmitir información de forma segura en internet, por medio de archivos en formato JSON, que es un tipo de archivo de texto plano con el cual se pueden crear parámetros y asignarles un valor. Este sistema se utiliza para la autenticación de usuarios en aplicaciones y su función principal es la de validar la identidad de quien ingresa a la página, después de que ya haya iniciado sesión en el pasado. De esta forma, no es necesario hacer el proceso de *login* cada vez que se entra a la página. (KeepCoding, 2023)

¿Qué son los WebSockets?

Por definición, un WebSocket es un protocolo de comunicación de equipo bidireccional a través de un único TCP. WebSockets ayuda enormemente a manejar transferencias de datos a gran escala entre el cliente y el servidor. Los WebSockets son diferentes porque funcionan manteniendo abierta en todo momento la conexión entre el cliente y el servidor. Con este método, el servidor tiene la facultad de enviar información en cualquier momento, incluso cuando no fue iniciada por el cliente. (LaodView, 2020)

Firebase

Es una plataforma móvil creada por Google, cuya principal función es desarrollar y facilitar la creación de apps de elevada calidad de una forma rápida, con el fin de que se pueda aumentar la base de usuarios y ganar más dinero. La plataforma está subida en la nube y está disponible para diferentes plataformas como iOS, Android y web. Contiene diversas funciones para que cualquier desarrollador pueda combinar y adaptar la plataforma a medida de sus necesidades. (Pérez, 2016)

Arduino uno

Es una plataforma de creación de electrónica de código abierto, la cual está basada en hardware y software libre, flexible y fácil de utilizar para los creadores y desarrolladores. Esta plataforma permite crear diferentes tipos de microordenadores de una sola placa a los que la comunidad de creadores puede darles diferentes tipos de uso. (Hernández, 2022)

WhatsApp API

WhatsApp API es la solución para empresas con un número considerable de chats y marcas que necesitan expandir su línea de WhatsApp Business porque comienzan a perder ventas o demoran mucho sus servicios; ya que esto representa una pérdida de dinero día tras día. Por ello, WhatsApp entendió la necesidad de miles de sus usuarios empresas y diseñó una API que permite mantener un flujo optimizado de comunicación sin perder posibles ventas debido a la larga espera en respuesta. (Quiroz, 2021)

Sin embargo, es importante aclarar que la API de WhatsApp, a diferencia de WhatsApp Business y Messenger no es una aplicación que puedes descargar de una tienda de apps, es una

integración que permite hacer conexiones con otras herramientas y así lograr un alcance mucho mayor.

Qué es spiffs

Podemos decir que SPIFFS es un sistema de archivos destinado a dispositivos flash SPI NOR embebidos. Vamos a aprender en detalle cómo utilizar el SPIFFS (del inglés Serial Peripheral Interface Flash Fail System), como configurar nuestro IDE de Arduino y así, poder cargar archivos en el ESP8266, aunque el sistema de archivos flash SPIFFS se almacena en el mismo chip que el boceto, la programación de un nuevo boceto no modificará el contenido del sistema de archivos SPIFFS. Esto permite utilizar el sistema de archivos para almacenar datos del boceto, archivos de configuración o contenido para el servidor web. (García, 2019)

AMBIENTE DE HARDWARE

Buzzer

También conocido como zumbador es un pequeño transductor capaz de convertir la energía eléctrica en sonido. Para hacerlos funcionar solo basta conectar el positivo con el + y la tierra o negativo con el – de una batería o cualquier fuente de corriente directa. Se basa en el efecto piezoeléctrico de los materiales, este efecto funciona de tal manera que cuando se aplica un voltaje el volumen del material cambia ligeramente.

Están construidos con dos pequeñas placas una metálica y una cerámica, las cuales aprovechan este efecto, pero solo generan un click ya que los materiales cambiaron de forma, pero no regresan a su estado natural hasta que se les quita el voltaje. (Buzzer, 2020)

Cámara web

Una webcam es una cámara de pequeñas dimensiones que generalmente se encuentra integrada en ordenadores portátiles, pero que también se puede adquirir en una gran variedad de formatos para ordenadores de sobremesa, algo que las hace compatibles con todos aquellos dispositivos que cuenten con un puerto USB. (Bercial, 2023)

Sensor de movimiento PIR

Los detectores PIR (Passive Infrared) o Pasivo Infrarrojo, son sensores que reaccionan sólo ante determinadas fuentes de energía tales como el calor del cuerpo humano o animales. Básicamente reciben la variación de las radiaciones infrarrojas del medio ambiente que cubre. Es llamado pasivo debido a que no emite radiaciones, sino que las recibe. Estos captan la presencia detectando la diferencia entre el calor emitido por el cuerpo humano y el espacio alrededor. (Tecnoseguro, 2020)

El botón del pánico

Es un complemento de un sistema de alarmas, que se puede instalar junto a las alarmas para casa o alarmas para empresas. Consiste en un dispositivo que permite, con tan solo pulsarlo, notificar una emergencia a la Central Receptora Alarmas (CRA). El botón del pánico es capaz de emitir una señal silenciosa y existen varios tipos: botón de pared, de teclado (instalados en el panel de control de la alarma), o incluso inalámbrico. (Securitas Direct, 2022)

Sensor magnético M-38

Este sensor es esencialmente un interruptor de lengüeta magnético (*reed switch*), encerrado en una carcasa de plástico ABS. Normalmente una mitad del sensor está “abierto” (sin conexión entre los dos cables). La otra mitad es un imán. Cuando el imán está de menos de 13 mm (0.5 pulgadas) de distancia, el interruptor de lengüeta se cierra. Estos sensores se utilizan a menudo para detectar cuando una puerta o cajón está abierto, por lo que tienen pestañas de montaje y tornillos.

Sensor de humo

Llamado también detector de humo, es un sensor que detecta el humo como una indicación primaria de incendio. Proporciona una señal a un sistema de alarma contra incendios en un edificio grande, o produce una señal audible y visual localmente en una habitación o un hogar. Los detectores de humo generalmente se alojan en una pequeña caja de plástico de forma

redonda y se colocan en el techo donde hay riesgos de incendio o peligro de incendio. (Sensores, 2021)

MARCO METODOLÓGICO

Para realizar este proyecto de investigación, se utilizarán varias metodologías, como el análisis de documentos, entrevistas a expertos, encuestas a usuarios, análisis de datos, y pruebas de concepto. Los resultados obtenidos se compararán con los resultados de otros sistemas de seguridad existentes para determinar qué sistema es el mejor para satisfacer las necesidades de seguridad de los usuarios.

Investigación descriptiva

Se procede con la Identificación de Riesgos: Esta etapa involucra la identificación de todos los posibles riesgos que pueden afectar la seguridad de las viviendas urbanas. Algunos de estos riesgos pueden incluir el acceso no autorizado a dispositivos, la infección por malware, el robo o la interferencia en la comunicación entre dispositivos. Se pueden realizar entrevistas con expertos en seguridad, consultar informes de investigación y revisar publicaciones de seguridad para establecer una lista de riesgos.

2. Establecimiento de Requisitos de Seguridad: Esta etapa implica el establecimiento de los requisitos de seguridad para la solución propuesta. Esto incluye la definición de los niveles de seguridad necesarios para proteger los dispositivos, los datos y la comunicación. Se pueden consultar estándares de seguridad para ayudar a establecer los requisitos.

3. Diseño de la Solución de Seguridad: Esta etapa implica el diseño de la solución de seguridad para las viviendas urbanas. Esto incluye el diseño de una arquitectura de seguridad, el diseño de métodos de autenticación, el diseño de mecanismos de prevención de ataques y el diseño de métodos de detección y respuesta.

4. Implementación de la Solución de Seguridad: Esta etapa implica la implementación de la solución de seguridad diseñada. Esto incluye la instalación y configuración de los dispositivos,

la implementación de los mecanismos de seguridad, la configuración de los servicios y la implementación de políticas de seguridad.

5. Pruebas de Seguridad: Esta etapa implica la realización de pruebas de seguridad para asegurar que la solución diseñada cumple con los requisitos establecidos. Esto incluye pruebas de penetración, pruebas de rendimiento, pruebas funcionales y análisis de código.

6. Monitoreo de Seguridad: Esta etapa implica el monitoreo de los dispositivos, la comunicación y los datos para detectar amenazas y posibles vulnerabilidades. Esto incluye el uso de herramientas de monitoreo para recopilar información sobre el comportamiento de los dispositivos y la comunicación.

7. Evaluación de Seguridad: Esta etapa implica la evaluación de la solución de seguridad para asegurar que cumple con los requisitos establecidos. Esto incluye la evaluación de la arquitectura de seguridad, la evaluación del nivel de seguridad, la evaluación de los mecanismos de prevención y detección y la evaluación de los mecanismos de respuesta.

La entrevista.

Estimado experto.

- ¿Cuáles son los elementos más importantes que deben tener en cuenta al implementar un sistema de seguridad en el Internet de las Cosas para viviendas urbanas?
    - Los elementos más importantes que se deben tener en cuenta al implementar un sistema de seguridad en el Internet de las Cosas para viviendas urbanas son los siguientes:

1. Redes inalámbricas seguras: Las redes inalámbricas deben configurarse para protegerse contra los ataques cibernéticos, como la suplantación de identidad y los ataques de denegación de servicio. Esto requiere una configuración adecuada del servidor de autenticación y una selección cuidadosa de los protocolos de seguridad.

2. Autenticación de dispositivos: Todos los dispositivos que se conectan a la red IoT deben autenticarse antes de que puedan comunicarse con la red. Esto implica la

implementación de un mecanismo de autenticación robusto, como una contraseña o un token de seguridad.

3. Cifrado de datos: La información que se transmite a través de la red IoT debe cifrarse para prevenir que terceros no autorizados obtengan acceso a ella. Esto se puede lograr mediante la implementación de protocolos de cifrado de datos como TLS, SSL y VPN.

4. Detección y respuesta a amenazas: Un sistema de seguridad IoT eficaz debe contar con un mecanismo para detectar amenazas y responder a ellas de forma adecuada. Esto implica la implementación de herramientas de detección de intrusos y automatización para la respuesta a incidentes de seguridad.

5. Análisis de seguridad: El sistema de seguridad IoT debe realizar un análisis periódico de la seguridad de la red para garantizar que siga siendo segura. Esto implica la implementación de herramientas de análisis de vulnerabilidades y pruebas de penetración para detectar y corregir errores de seguridad.

Los propietarios de viviendas urbanas también deben asegurarse de que sus dispositivos IoT sean seguros y confiables. Esto significa usar dispositivos que estén actualizados con la última versión de firmware y que sean compatibles con el protocolo de seguridad de la red. También significa configurar los dispositivos correctamente para evitar la fuga de información, y usar contraseñas seguras para asegurarse de que los dispositivos no puedan ser accedidos por terceros.

Además de estas medidas de seguridad básicas, los propietarios de viviendas urbanas también pueden considerar la instalación de soluciones de seguridad avanzadas, como un sistema de monitorización remota. Esto permitirá a los propietarios monitorear sus dispositivos desde cualquier lugar con una conexión a Internet, lo que les proporcionará la tranquilidad de saber que sus dispositivos están seguros.

ANALISIS DE DOCUMENTACIÓN

El análisis de documentación de un sistema de seguridad en el Internet de las Cosas (IoT) para viviendas urbanas debe tener en cuenta varios factores clave. Primero, es necesario investigar cómo los dispositivos IoT se conectan a la red para garantizar que la seguridad de la red no se vea comprometida. Esto incluye la comprensión de cómo los dispositivos se comunican entre sí, el uso de protocolos de seguridad para la autenticación y encriptación de la comunicación, y el uso de medidas de seguridad tales como la autenticación de dos factores.

Además, es importante entender cómo se configuran y administran los dispositivos, incluyendo el uso de mecanismos de seguridad para garantizar que los dispositivos solo se conecten a la red de manera segura. Esto incluye el uso de contraseñas y otros métodos de autenticación, así como el uso de firewalls para limitar el tráfico entrante y saliente.

Otro factor clave para analizar es el uso de tecnologías de seguridad física, como sistemas de seguridad, alarmas, cámaras de seguridad y otros dispositivos para garantizar que los dispositivos IoT no sean manipulados maliciosamente. Esto incluye el uso de tecnologías como el reconocimiento facial, el sensor de huella digital y el sistema de identificación por radiofrecuencia (RFID).

Finalmente, el análisis de documentación debe incluir una comprensión de cómo los dispositivos IoT se integran con la infraestructura de la red para garantizar que los dispositivos funcionen correctamente. Esto incluye la configuración de la red para permitir la comunicación segura entre los dispositivos, así como el uso de tecnologías de análisis de datos para garantizar que los datos sean procesados de forma segura.

Metodología Scrum

Como metodología ágil, SCRUM se adapta al desarrollo de todo proyecto por ello, se ha seleccionado la misma para la presente propuesta porque su gestión permite reducir la complejidad en el desarrollo de proyectos tecnológicos e informáticos, esta metodología tiene como una de sus características centrarse en las necesidades del usuario y satisfacer sus necesidades en este caso, la seguridad de las viviendas a través de la automatización por ello, es ideal para este proyecto.

Según Díaz y Del Dago (2008), definen a SCRUM, como una colección de procesos para la gestión y control de proyectos donde prioriza la entrega de valor al cliente además, potenciar el trabajo de equipo logrando eficiencia en el trabajo dentro de un esquema de continuo mejoramiento.

LA ENCUESTA

Se desarrolló un escenario en el cual se determina la importancia de implementar una red segura en viviendas urbanas.

1. ¿Conoce usted lo qué es el internet de las cosas y su utilidad en la seguridad digital en las viviendas?
2. ¿Considera usted la posibilidad de implementar seguridad en su vivienda a través de las tecnologías informáticas?
3. ¿Qué nivel de seguridad considera usted que debe tener un sistema de seguridad para el Internet de las Cosas?
4. ¿Últimamente ha habido robos en las viviendas de su sector?
5. ¿Tiene alguna preocupación específica con relación a la seguridad del Internet de las Cosas para su vivienda urbana?
6. ¿Cree que el uso del sistema de seguridad para el Internet de las Cosas le hará sentirse más seguro en su vivienda urbana?
7. ¿Qué tan importante es para usted el tener un sistema de seguridad en el Internet de las Cosas para su vivienda urbana?

8. ¿Está usted de acuerdo realizar una inversión en tecnologías de internet de las cosas para proteger su vivienda?

RESULTADOS

Se espera que el proyecto de investigación determine cuál es el mejor sistema de seguridad en el Internet de las cosas para viviendas urbanas. Los resultados también se utilizarán para mejorar la seguridad de los dispositivos conectados y para garantizar la privacidad de los datos de los usuarios cuyo impacto se espera que los resultados de este proyecto de investigación mejoren la seguridad de los sistemas de seguridad en el Internet de las cosas para viviendas urbanas. Esto permitirá a los usuarios tener mayor confianza en la seguridad de sus dispositivos y garantizará que sus datos estén protegidos.

en la presente investigación la información fue utilizando metodología directa y entrevista, la misma que fue aplicada en la urbanización algunos usuarios para el análisis de un sistema de seguridad en el internet de las cosas para viviendas urbanas, ya que existe hoy en día herramientas útiles con la tecnología así poder obtener información y observar algún robo o fechorías que quieren hacer en dichas viviendas y realizar una mejor investigación y análisis.

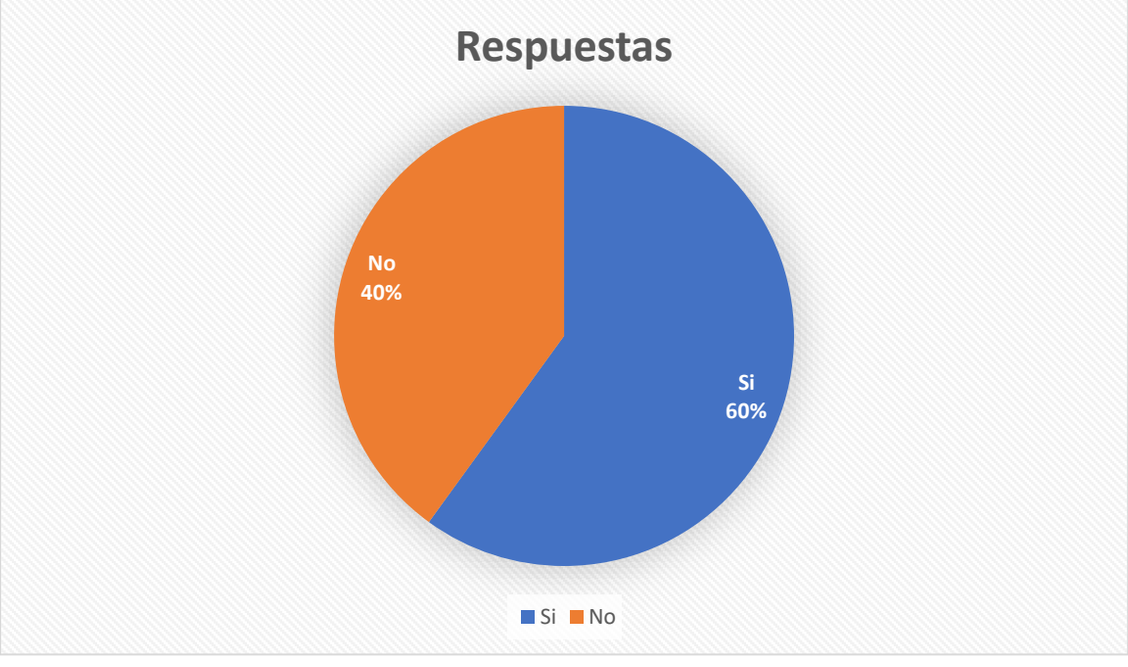
Esta entrevista se pudo obtener de que si es necesario conocer un sistema de seguridad para poder monitorear nuestras viviendas y evitar cualquier acontecimiento que deseen realizar cualquier individuo, de esta manera poder tener información en cualquier lugar o parte del mundo que se encuentre este análisis es con el objetivo de tener mejor seguridad.

Tabla 1

¿Conoce usted lo qué es el internet de las cosas y su utilidad en la seguridad digital en las viviendas?

CATEGORÍAS	FRECUENCIA ABSOLUTA	FRECUENCIA ABSOLUTA PORCENTUAL
SI	15	60%
NO	10	40%
TOTAL		100%

PREGUNTA 1



Elaborado por: Juan Saa Ayala

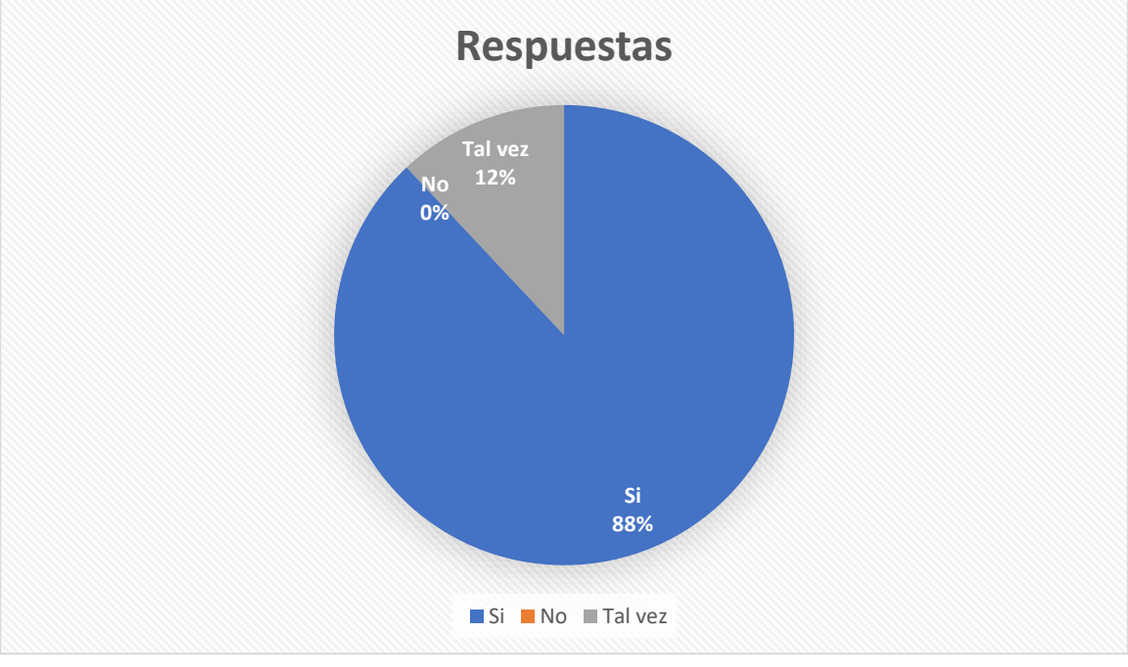
Podemos indicar que los resultados obtenidos mediante la encuesta en algunos habitantes se pudo constatar que el 60% si conoce sobre las tecnologías del internet de las cosas mientras que, el 40% mencionó que no conoce, estos resultados afianzan este estudio porque la mayoría tiene conocimiento de esta important etemática y sus usos en la seguridad de las viviendas.

Tabla 2

¿Considera usted la posibilidad de implementar seguridad en su vivienda a través de las tecnologías informáticas?

CATEGORÍAS	FRECUENCIA ABSOLUTA	FRECUENCIA ABSOLUTA PORCENTUAL
Si	22	88%
No	0	0%
Tal vez	3	12%
TOTAL		100%

PREGUNTA 2



Elaborado por: Juan Saa Ayala

Podemos indicar que los resultados obtenidos mediante la encuesta revelan que, el 88% de las personas encuestadas, consideran que si es posible implementar estas tecnologías para al seguridad del hogar. El 12% dijo que tal vez. Estos resultados son importantes permite la aceptación de este casod ee studio y su importancia para la seguridad privada de viviendas urbanas.

Tabla 3

¿Qué nivel de seguridad considera usted que debe tener un sistema de seguridad para el Internet de las Cosas?

CATEGORÍAS	FRECUENCIA ABSOLUTA	FRECUENCIA ABSOLUTA PORCENTUAL
Alto	21	84%
Medio	4	16%
Bajo	0	0%
TOTAL		100%

PREGUNTA 3

Elaborado por: Juan Saa Ayala

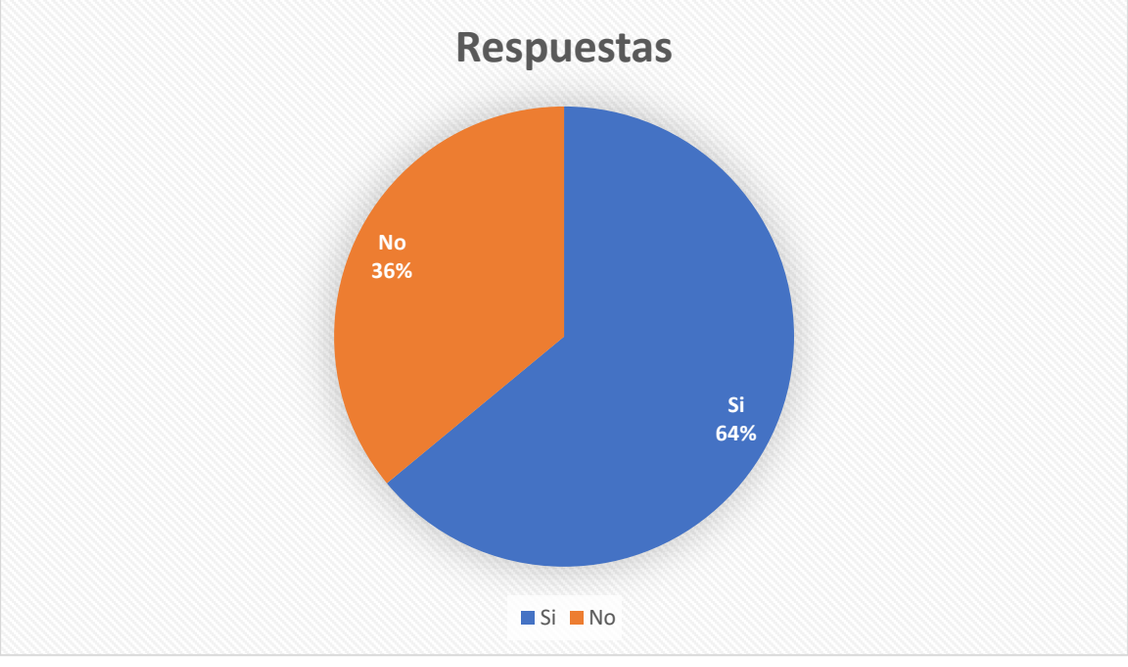
Las respuestas de esta preguntas revelan que los encuestados exigen seguridad alta al momento de usar mecanismos apra proteger sus viviendas. Así, el 84% mencionó que la seguridad del internet de las coss debe ser alta, y 16% dijo que debe sr ser seguridad media y ninguno optó por la opción baja.

Tabla 4

¿Últimamente han habido robos en las viviendas de su sector?

CATEGORÍAS	FRECUENCIA ABSOLUTA	FRECUENCIA ABSOLUTA PORCENTUAL
Si	16	64%
No	9	36%
TOTAL		100%

PREGUNTA 4



Elaborado por: Juan Saa Ayala

Podemos indicar que los resultados obtenidos en esta pregunta, revelan la inseguridad que vive la población y la vulnerabilidad de las viviendas ante hechos delictivos. El 64% de los encuestados mencionó que si ha existio robos de viviendas en su sector mientras que el 36% dijo que no. Estos datos afianzan los objetivos de este caso de estudio.

Tabla 5

¿Tiene alguna preocupación específica con relación a la seguridad del Internet de las Cosas para su vivienda urbana?

CATEGORÍAS	FRECUENCIA ABSOLUTA	FRECUENCIA ABSOLUTA PORCENTUAL
Si	10	40%
No	7	28%
Tal vez	8	32%
TOTAL		100%

PREGUNTA 5

Elaborado por: Juan Saa Ayala

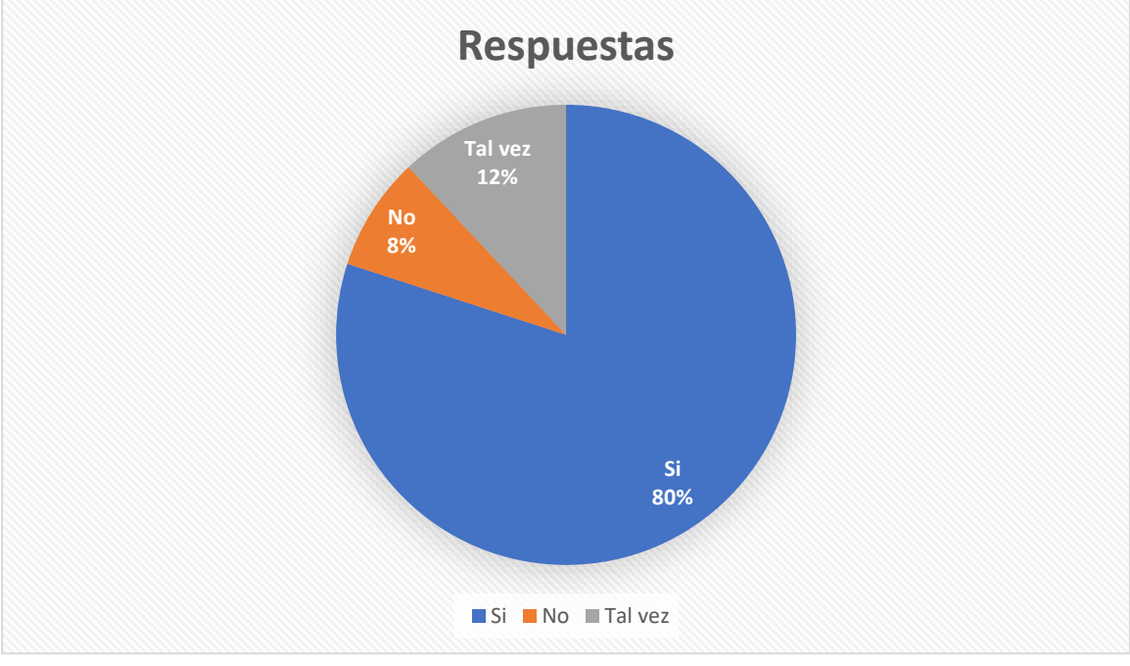
Podemos indicar que los resultados obtenidos mediante la encuesta revelan que el 40% mencionaron que si tienen preocupación al posible uso de estas tecnologías del internet de las cosas. El 28% dijo que no y el 32% mencionó que talvez. Esta pregunta revela que todavía puede existir resistencia en el uso de tecnologías por parte de la población.

Tabla 6

¿Cree que el uso del sistema de seguridad para el Internet de las Cosas le hará sentirse más seguro en su vivienda urbana?

CATEGORÍAS	FRECUENCIA ABSOLUTA	FRECUENCIA ABSOLUTA PORCENTUAL
Si	20	80%
No	2	8%
Tal vez	3	12%
TOTAL		100%

PREGUNTA 6



Elaborado por: Juan Saa Ayala

Podemos indicar que los resultados obtenidos mediante la encuesta, se puede observarque el 80% menciona que el uso de seguridades para sus viviendas a través el internet de las cosas los puede hacer sentir más seguros, el 12% dijo que tal vez y sólo el 8% dijo que no. Estos resultados permiten conocer el nivel de confianza de las personas en als tecnologías.

Tabla 7

¿Qué tan importante es para usted el tener un sistema de seguridad en el Internet de las Cosas para su vivienda urbana?

CATEGORÍAS	FRECUENCIA ABSOLUTA	FRECUENCIA ABSOLUTA PORCENTUAL
Mucho	21	84%
Poco	4	16%
No es importante	0	0
TOTAL		100%

PREGUNTA 7

Elaborado por: Juan Saa Ayala

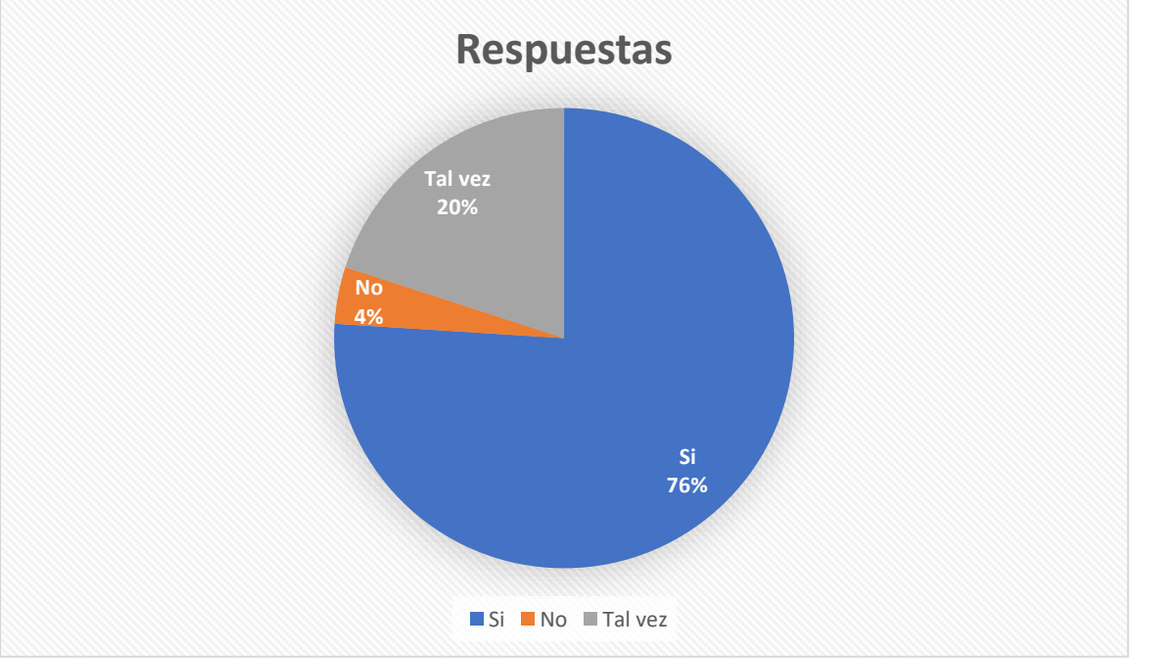
Los resultados de esta pregunta permiten conocer la importancia de tener seguridades en sus viviendas a travez de las tecnologías. El 84% de los encuestados mencionó que es mucha la improtancia, el 16% dijo que poco y ninguno que no es importante.

Tabla 8

¿Está usted de acuerdo realizar una inversión en tecnologías de internet de las cosas para proteger su vivienda?

CATEGORÍAS	FRECUENCIA ABSOLUTA	FRECUENCIA ABSOLUTA PORCENTUAL
Si	19	76%
No	1	4%
Tal vez	5	20%
TOTAL		100%

PREGUNTA 8



Elaborado por: Juan Saa Ayala

Podemos indicar que los resultados obtenidos mediante la encuesta indican que el 76% de las personas Si está de acuerdo en invertir en seguridad de sus viviendas mediante tecnologías del internet de las cosas, el 20% dijo que talvés y solamente el 4% mencionó que No. Estos resultados son muy importantes porque cumplen los propósitos de este caso de estudio en dar a conocer y usar los beneficios de las tecnologías en amteria de seguridad privada.

DISCUSIÓN Y RESULTADOS

A pesar el mecanismo de la inseguridad que hay un alto índice delincuencial aumentado esto hace que afecte a la ciudadanía en el cual se ha propuesto un análisis de sistema de seguridad con internet de las cosas para viviendas urbanas, permaneciendo evidencias que no tenemos seguridad. Esta investigacion nos ayudara analizar como optimizar las herramientas tecnologicas con el fin de dar un buen eso a esta inseguridad que vivimos al diario en las urbanizaciones .

El cual nos a obligado buscar y analizar herramientas informaticas para el uso diario, por que el aumento delincuencial mantiene preocupada a la poblacion asi poder monitorear con sistema poder tener datos exactos en el momento que se de una emergencia de robos en la urbanizacion

Los moradores encuestados manifestaron que siempre sucitan actos delictivos en las urbanizaciones no tenemos un resguardo que nos de seguridad con un sistema lograriamos por lo menos tener la hora y el momento exacto donde estan cometiendo un delito .

Con mejoras de un sistema de seguridad es la finalidad de enriquecer para un sector seguro poder utilizar componentes a un bajo costo así poder adquirir la mayoría de la población, además este tipo de herramientas debe ser consciente el usuario este tipo de tecnología puede ayudar mucho en cualquier ambiente que se implemente con el debido cuidado de quien le de uso también debemos tener en cuenta la confidencialidad de la información con responsabilidad y durabilidad del sistema de seguridad en las urbanizaciones

Gracias a estos resusltados obtenidos mediante encuestas y ala ciudadania en comun se pudo constatar que el 100% esta de acuerdo con el uso de un sistema de seguridad se puede bajar el índice de la delincuencia.

Mediante esta entrevitas podemos analizar Mediante esta entrevista aplicada podemos analizar que el 100% de usuarios considera que un sistema de seguridad será favorable para las viviendas urbanas.

Como podemos observar que la opción si es el índice más alto del 100% se ve que es necesario el sistema para el control y monitoreo de la vivienda.

El índice de usuarios está de acuerdo con el 100% de implementar un sistema de seguridad basado para e l monitoreo de las viviendas y tener un mejor control.

Como podemos visualizar que el 75% de los usuarios podrían adquirir un sistema de seguridad si fuera a bajo costo y el 25% no está seguro de adquirir una herramienta tecnológica

RECOMENDACIONES

- Es recomendable que en futuras investigaciones se logre mejorar o añadir el prototipo de sistema de seguridad propuesto, debido ante los avances de la tecnología se puede el ir mejorando muchos aspectos
- Además, es importante que el usuario utilice y actualice cada cierto tiempo sus contraseñas y los mantenga de manera anónima y no lo llegue a compartir o anotar en cualquier lado.
- Se debe tener siempre actualizados con la última versión de firmware a medida que las nuevas amenazas de seguridad evolucionan, los fabricantes de dispositivos y los operadores de redes responden para hacer frente a las nuevas amenazas.

.

CONCLUSIONES

El análisis de un sistema de seguridad para el Internet de las Cosas para viviendas urbanas ha demostrado que un sistema de seguridad robusto y confiable es la clave para proteger las viviendas urbanas modernas. La seguridad debe ser la prioridad en el diseño, desarrollo e implementación de todos los dispositivos IoT, al igual que en la configuración de los sistemas de seguridad para el hogar. El uso de cifrado, autenticación, seguridad de la red y controles de acceso como parte de la solución de seguridad es esencial para la protección de los dispositivos IoT y las viviendas urbanas. El uso de tecnologías de seguridad avanzadas, como la Inteligencia Artificial, también puede ayudar a aumentar la seguridad y proteger los dispositivos y la red de los ataques cibernéticos.

- El sistema de seguridad en el Internet de las cosas para viviendas urbanas debe abordar el control de acceso, el almacenamiento seguro de datos, la prevención de intrusiones y la detección de anomalías.
- Los sistemas de seguridad en el Internet de las cosas para viviendas urbanas deberían incluir los protocolos de seguridad adecuados para garantizar la seguridad de los dispositivos y los datos que se almacenan.
- El sistema de seguridad en el Internet de las cosas para viviendas urbanas debe ser robusto para resistir varios tipos de ataques, incluyendo ataques remotos y locales.
- Los dispositivos de seguridad en el Internet de las cosas para viviendas urbanas deben estar equipados con medidas de seguridad para prevenir la manipulación o el uso indebido de los datos.
- El sistema de seguridad en el Internet de las cosas para viviendas urbanas debe proporcionar una gestión de seguridad adecuada para garantizar que los dispositivos y los datos estén seguros.

- El sistema de seguridad en el Internet de las cosas para viviendas urbanas debe proporcionar una auditoría adecuada para detectar y registrar cualquier actividad sospechosa.
- El sistema de seguridad en el Internet de las cosas para viviendas urbanas debe permitir a los usuarios configurar los niveles de seguridad adecuados para cada dispositivo.

En conclusión, un sistema de seguridad en el Internet de las cosas para viviendas urbanas debe abarcar una amplia gama de medidas de seguridad para garantizar la seguridad de los dispositivos y los datos. Estas medidas incluyen el control de acceso, el almacenamiento seguro de datos, la prevención de intrusiones, la detección de anomalías, la seguridad de la red y los protocolos de seguridad adecuados, así como la auditoría.

.

REFERENCIAS BIBLIOGRÁFICAS

Aguilera, Echeverria, & Velez. (2013). *Implementación de un componente para el préstamo de material bibliográfico digital para la biblioteca virtual en el cib-ESPOL*. Obtenido de http://www.dspace.espol.edu.ec/handle/123456789/24535

Álvarez, A. (2005). *Hablemos de seguridad Elementos para la vigilancia y protección.* Cartagena: Pluma de Mompox.

Aviles, A., & Cobeña, K. (2015). *Diseño e implementación de un sistema de seguridad a través de cámaras, sensores y alarma, monitorizado y controlado telemétricamente para el centro de acogida "Patio mi pana" perteneciente a la fundación proyecto salesiano.* Ecuador: Ingenieria Electronica.

Bercial, J. (2023). *¿Qué es una webcam y para qué sirve?* Obtenido de https://www.geeknetic.es/Webcam/que-es-y-para-que-sirve

Buzzer. (2020). *Buzzer*. Obtenido de http://ceca.uaeh.edu.mx/informatica/oas_final/OA4/buzzer.html

Coding Potions. (2019). *Introducción a Vue JS ≫ Qué es y sus características*. Obtenido de https://codingpotions.com/que-es-vue

Córdoa, A. (2015). *Portal web para mejorar la gestión de integración de los miembros de la Iglesia Divino Maestro de Galilea*. Recuperado el 15 de Diciembre de 2020, de http://dspace.uniandes.edu.ec/bitstream/123456789/3502/1/TUASIS001-2016.pdf

Criollo, A. (2015). *El poder de HTML5 Y CCS3*. Recuperado el 23 de Septiembre de 2020, de https://prezi.com/5pa2ucuodgr_/el-poder-de-html5-y-ccs3/

Criollo, W. (2014). *Aplicación de tecnología inalámbrica ZIGBEE en inmuebles residenciales y su incidencia en la seguridad en el Caserío Tangaiche del Cantón Ambato* . Obtenido de http://repo.uta.edu.ec/bitstream/123456789/7795/1/Tesis_t904ec.pdf

Díaz, M., & Del Dago, S. (2008). Educación a Distancia en el. *Anales del Encuentro Internacional BTM 2008: Educación, Formación y Nuevas Tecnologías*, (págs. 1-7). Punta de Este, Uruguay.

Emailengine. (2020). *Nodemailer*. Obtenido de https://nodemailer.com/about/

FAZT. (2018). *Desarrollo Web en Visual Studio Code*. Obtenido de https://blog.faztweb.com/2018/05/desarrollo-web-en-visual-studio-code.html

García, V. (2019). *Funcionalidad de SPIFFS.* Obtenido de https://www.diarioelectronicohoy.com/blog/funcionalidad-de-spiffs

GAUCHAT, J. (2012). *El gran libro de Html5, Css3 y Javascript.* Marcombo.

Guerrero, D., Jiménez, D., & Torres, L. (2017). *Elaboración de un marco de referencia para la implementación de prácticas ágiles en la gestión de portafolios en empresas del sector TI.*

Hernández, Y. (2022). *Qué es Arduino, cómo funciona y qué puedes hacer con uno*. Obtenido de https://www.xataka.com/basics/que-arduino-como-funciona-que-puedes-hacer-uno

KeepCoding. (2023). *¿Qué es JSON Web Token?* Obtenido de https://keepcoding.io/blog/que-es-json-web-token/

LaodView. (2020). *Aplicaciones WebSocket de pruebas de carga*. Obtenido de https://www.loadview-testing.com/es/blog/pruebas-de-carga-de-aplicaciones-basadas-en-websocket/

Luna, F., Peña, C., & Iacono, M. (2018). *Programacion Web Full Stack 14 - MySQL: Desarrollo frontend y backend.* RedUsers.

Mahecha, J. (2018). *Diseño e implementacion de una aplicacion domotica para iluminacion usando inteligencia artificial.* Bogotá: Universidad de la Salle.

Pérez, M. (2016). *Firebase, qué es y para qué sirve la plataforma de Google*. Obtenido de https://www.iebschool.com/blog/firebase-que-es-para-que-sirve-la-plataforma-desarroladores-google-seo-sem/

Proyectos ágiles. (2019). *Qué es SCRUM*. Recuperado el 02 de Octubre de 2021

Quiroz, A. (2021). *API WhatsApp: ¿Qué es, cómo funciona y para qué sirve?* Obtenido de https://www.b2chat.io/blog/whatsapp/que-es-y-como-funciona-la-api-de-whatsapp/

Securitas Direct. (2022). *¿Qué es el botón del pánico y para qué sirve?* Obtenido de https://www.securitasdirect.es/blog/boton-del-panico-que-es/

Sensores. (2021). *Sensor de Humo – Información y Características*. Obtenido de https://sensores.top/sensor-de-humo-informacion-y-caracteristicas/

Suárez, R. (2021). *Quasar - El Framework todo terreno de VueJS*. Obtenido de https://roylans.dev/quasar-framework-todo-terreno-de-vuejs

Tecnoseguro. (2020). *¿Qué es un detector de movimiento pasivo o PIR y cómo funcionan los sensores de movimiento?* Obtenido de https://www.tecnoseguro.com/faqs/alarma/que-es-un-detector-de-movimiento-pasivo-o-pir

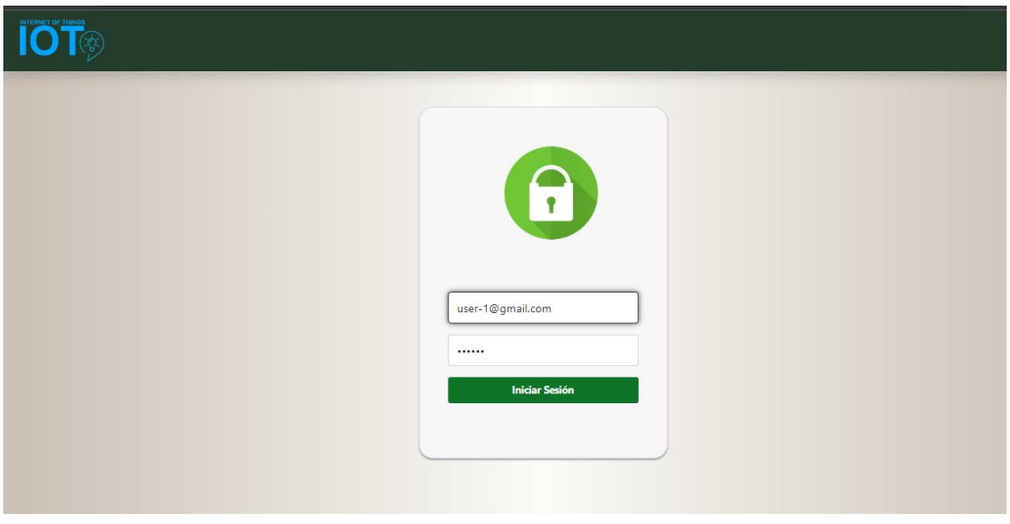
Trigas Galego, M. (2015). *«Gestion de Proyectos Informaticos,» Metodología Scrum.*

Vásquez, G. (2019). *Node.js – La introducción perfecta*. Recuperado el 12 de Mayo de 2020, de https://codigoonclick.com/nodejs-introduccion/

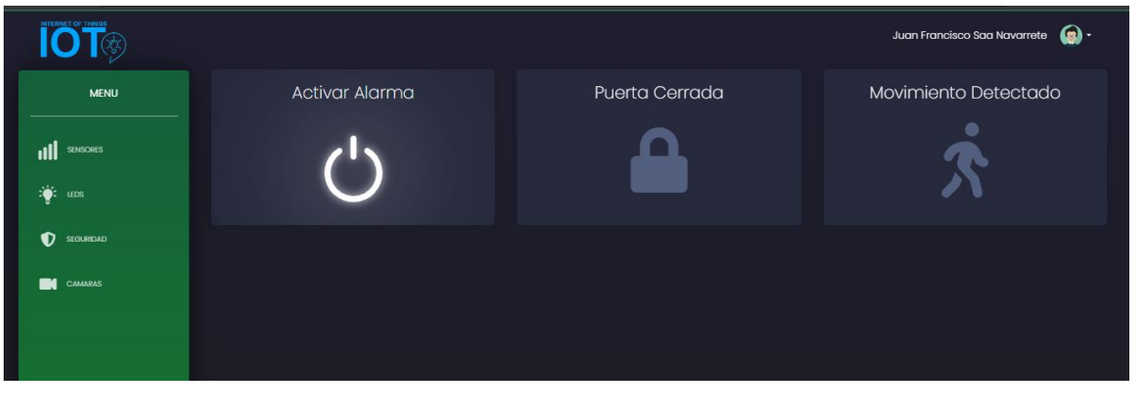
ANEXOS

Prototipo del aplicativo web basado en IOT para seguridad de vivienda urbana

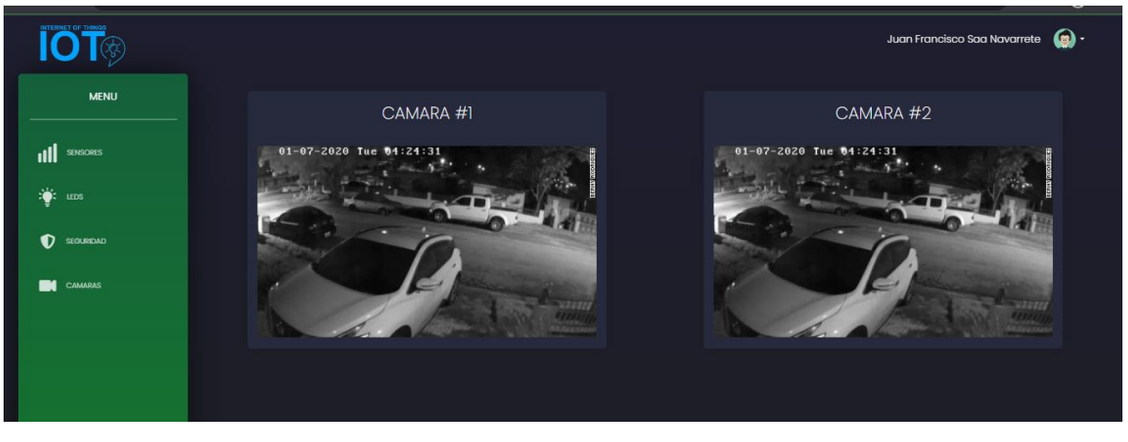
Login



Modulo Seguridad



Módulo de cámaras de vigilancia



CERTIFICADO DE ANÁLISIS

magister

JUAN FERNANDO SAA AYALA

9% Similitudes

1% Texto entre comillas

< 1% similitudes entre comillas

< 1% Idioma no reconocido

Nombre del documento: JUAN FERNANDO SAA AYALA .docx
ID del documento: [illegible]
Tamaño del documento original: 352,32 ko

Depositante: SOTO VALLE CARLOS JULIO
Fecha de depósito: 5/4/2023
Tipo de carga: interface
fecha de fin de análisis: 5/4/2023

Número de palabras: 7216
Número de caracteres: 48.019

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.ingmecafenix.com | Qué es el buzzer y cómo funciona (zumbador) - Ingeniería... [illegible]	1%		Palabras idénticas : 1% ([illegible] palabras)
2	www.diarioelectronicohoy.com | Funcionalidad de SPIFFS. – Electrónica Práctica Apl... [illegible] 1 fuente similar	1%		Palabras idénticas : 1% ([illegible] palabras)
3	www.ilelschool.com | Firebase, qué es y para qué sirve la plataforma de Google [illegible]	1%		Palabras idénticas : 1% ([illegible] palabras)
4	MI CASO DE ESTUDIO JOEL SANCHEZ.docx | MI CASO DE ESTUDIO JOEL SAN... El documento proviene de mi grupo 4 fuentes similares	< 1%		Palabras idénticas : < 1% ([illegible] palabras)
5	codigoonclick.com | Node.js - La introducción perfecta - Código OnClick [illegible]	< 1%		Palabras idénticas : < 1% ([illegible] palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	Tamaquiza Proyecto final para revisión.docx | Tamaquiza Proyecto final pa... El documento proviene de mi grupo	< 1%		Palabras idénticas : < 1% ([illegible] palabras)
2	1library.co | Diseño e implementación de una aplicación domótica para ... [illegible]	< 1%		Palabras idénticas : < 1% ([illegible] palabras)
3	Documento de otro usuario [illegible] El documento proviene de otro grupo	< 1%		Palabras idénticas : < 1% ([illegible] palabras)

Fuentes ignoradas

Estas fuentes han sido retiradas del cálculo del porcentaje de similitud por el propietario del documento.

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	dspace.ulb.edu.ec | La tecnología android y su incidencia en el desarrollo de una ap... [illegible]	2%		Palabras idénticas : 2% ([illegible] palabras)
2	keepcoding.io | ¿Qué es JSON Web Token? | KeepCoding Bootcamps [illegible]	1%		Palabras idénticas : 1% ([illegible] palabras)
3	MULLO MULLO EDISON GABRIEL.docx | MULLO MULLO EDISON GABRIEL El documento proviene de mi biblioteca de referencias	1%		Palabras idénticas : 1% ([illegible] palabras)
4	Estudio de caso Steven Naranjo.docx | documento corregido El documento proviene de mi grupo	< 1%		Palabras idénticas : < 1% ([illegible] palabras)
5	localhost | Aplicación web para la gestión de incidencias en el soporte de T.I. a los cl... [illegible]	< 1%		Palabras idénticas : < 1% ([illegible] palabras)
6	infohardwaresdk.blogspot.com | Arduino [illegible]	< 1%		Palabras idénticas : < 1% ([illegible] palabras)
7	repositorio.espe.edu.ec | Implementación de un sistema de seguridad automático c... [illegible]	< 1%		Palabras idénticas : < 1% ([illegible] palabras)
8	disenowebakus.net | Aprender JavaScript - Creación de páginas Web dinámicas [illegible]	< 1%		Palabras idénticas : < 1% ([illegible] palabras)
9	bricoladores.simonelectric.com | Seguridad en el hogar: qué debemos proteger [illegible]	< 1%		Palabras idénticas : < 1% ([illegible] palabras)
10	Documento de otro usuario [illegible] El documento proviene de otro grupo	< 1%		Palabras idénticas : < 1% ([illegible] palabras)