UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Sistema basado en internet of thinks para mejorar la seguridad física en la Empresa Dr. PC Tarapoto, San Martin 2022

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTORES:

Cigüeñas Piña, Edwin Alcides (orcid.org/0000-0002-2718-6314)

Coronel Davila, Luis Humberto (orcid.org/0000-0003-4303-6321)

ASESORA:

Dra. Mescua Ampuero, Lizeth Erly (orcid.org/0000-0003-2748-479X)

LÍNEA DE INVESTIGACIÓN:

Infraestructura de Servicio de Redes y Comunicaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

TARAPOTO – PERÚ

2022

DEDICATORIA

Nuestro proyecto de tesis está dedicado a todos los maestros quienes nos han acompañado a lo largo de la carrera universitaria ya que han sido nuestros mentores y amigos, además por haber compartido sus conocimientos y brindarnos una formación de calidad como profesionales y personas.

A nuestros progenitores los cuales nos permitieron existir y han estado presente con nosotros inculcándonos buenas costumbres y valores, los queremos demasiado gracias por estar en todo momento y lugar apoyándonos siendo la guía y soporte en las circunstancias que nos presenta la vida.

AGRADECIMIENTO

A Dios por ser nuestro apoyo espiritual y guía en los momentos difíciles, por las oportunidades que se nos presenta durante nuestra vida y por permitirnos estar presentes en la realización de nuestro proyecto de tesis.

A la **Universidad César Vallejo** por darnos las herramientas para desarrollarnos como profesionales y de esa manera estar más capacitados con nuevos conocimientos que estaremos aplicando en la realización de nuestro proyecto de tesis.

A la empresa Dr. PC por darnos la oportunidad de desarrollar nuestros conocimientos en su establecimiento y ayudarnos con el informe para el progreso de nuestro proyecto de tesis.

A nuestros asesores el Doctor Romero Ruiz, Hugo José Luis y la Doctora Mescua Ampuero Lizeth Erly por la guía y paciencia brindada en el presente proyecto de tesis ya que sin su soporte no hubiéramos podido desarrollar nuestro proyecto de tesis.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS Y FIGURAS

RESUMEN

La tesis tuvo como objetivo general mejorar la seguridad física en la empresa Dr. PC por medio de la instalación de un sistema basado en internet of thinks. Esta investigación fue de enfoque cuantitativo – aplicada con un diseño experimental de tipo preexperimental. Se uso como herramientas para recolectar datos guías de observación y una encuesta que se aplicó a 12 usuarios estando apoyados por fuentes, trabajos de investigación y artículos científicos de revistas indexadas. La implementación del sistema basado en internet of thinks tuvo un efecto positivo en los indicadores de la investigación primero se mejoró en un 94.13% el tiempo que se emplea para activar los dispositivos de seguridad, segundo se mejoró en un 96.08% el tiempo de comprobación de acceso de seguridad, tercero se redujo en un 98.84% el tiempo de envió de alertas de incidencias, cuarto se redujo la vulnerabilidad de los accesos de seguridad en un 83.30% y quinto se mejoró el nivel de satisfacción del usuario en un 53.93% con el sistema en la empresa Dr. PC, San Martin, 2022. Lo cual nos permitió llegar a la conclusión que, si se mejora significativamente la seguridad en la empresa Dr. PC a través de la implementación de un sistema basado en internet of thinks.

Palabras clave: Sistema de seguridad, Internet de las Cosas, Seguridad física, Innovación, Tecnología.

ABSTRACT

The general objective of the thesis was to improve physical security in the company Dr. PC through the installation of a system based on the internet of thinks. This research was of a quantitative approach - applied with a pre-experimental experimental design. Observation guides and a survey that was applied to 12 users were used as tools to collect data, being supported by sources, research papers and scientific articles from indexed journals. The implementation of the system based on the Internet of Thinks had a positive effect on the research indicators. First, the time used to activate the security devices was improved by 94.13%, second, the verification time was improved by 96.08%. security access, thirdly, the time for sending incident alerts was reduced by 98.84%, fourthly, the vulnerability of security accesses was reduced by 83.30% and fifthly, the level of user satisfaction was improved by 53.93% with the system in the company Dr. PC, San Martin, 2022. Which allowed us to conclude that, if security is significantly improved in the company Dr. PC through the implementation of a system based on the Internet of thinks.

Keywords: Security system, Internet of Things, Physical security, Innovation, Technology.

I. INTRODUCCIÓN

Las redes de los sistemas de información han gobernado las diferentes compañías comerciales y más de las tecnologías de información que generalmente se ven inmersas en casos de ataques que permite poner las redes en los suelos permitiendo a los vándalos cibernéticos robar información y encriptarlas para pedir recompensa por desencriptar sus datos. Debido a lo antes expuesto las nuevas tecnologías son el componente clave para que las empresas alcancen un eje productivo, innovador y sobre todo sean competitivas en su rubro laboral. Las tecnologías constituyen un elemento fundamental que diferencia a las empresas, enfocándose en mejorar sus procesos e incorporando nuevas tecnologías, las cuales sean capaces de hacer nuevos productos y/o servicios y finalmente permitiendo a la empresa entrar en nuevos mercados. El valor agregado que le da la tecnología a una empresa, crea un componente central en virtud que permite a los gerentes y compañías usar los medios que tiene la empresa de una manera eficaz, según los autores (Sebastián, y otros, 2022).

Según el artículo de (Carreras, y otros, 2020) señalan que las organizaciones deberían adquirir mejoras tecnológicas que, al implementarlas sostengan las áreas y servicios que tengan más problemas, puesto que, al encontrarlas y despejarlas, se estarían disminuyendo los peligros y manteniendo una mejoría como empresa de servicios. Según las estadísticas de crímenes del Ministerio del interior 2019, en España se denunciaron 6,032 casos al día, de los cuales, entre 270 y 391 están concretamente reservados como robos de fuerza mayor en establecimientos, esto sin tomarse en cuenta la cantidad no cuantificada, de robos y hurtos de automóviles, que estarían directamente relacionados con los hogares privados, para el Perú según las Estadísticas de Criminalidad, Seguridad Ciudadana y Violencia del 29/03/2022 del INEI entre Setiembre - octubre, 2019 – 2021 las denuncias por comisión de delitos en el departamento de San Martin han tenido un aumento del 13.7% de acuerdo con él (Instituto Nacional de Estadistica e Informatica, 2022).

Por lo tanto, surge la importante necesidad de salvaguardar la integridad personal y material de los individuos, para lo que se propuso para concretar el proyecto de tesis, una solución basada en Internet of Thinks el cual pueda mejorar la seguridad en la empresa Dr. PC en donde se identificó la realidad problemática que vendría

a ser la falta de implementos tecnológicos que le permitan tener una buena seguridad además de una herramienta que sea capaz de comprobar quienes acceden a la empresa, al mismo tiempo automatice el proceso de control ya que el sistema actual solo tiene cámaras de seguridad que si bien son muy afectivas para vigilancia no tanto para enviar alertas y otras funciones de algún suceso que está aconteciendo en la empresa Dr. PC adjunto a eso la inseguridad que está en aumento en la ciudad de Tarapoto y la insuficiencia del personal de seguridad municipal (serenazgo).

Para este proyecto de tesis se estableció el siguiente problema general: ¿De qué manera un sistema basado en internet of thinks mejora la seguridad física en la empresa Dr. PC Tarapoto, San Martin 2022?

Además de los problemas específicos: ¿De qué manera un sistema basado en internet of thinks mejora el tiempo de activación de dispositivos de seguridad en la empresa Dr. PC, Tarapoto, San Martín 2022?, ¿De qué manera un sistema basado en internet of thinks mejora el tiempo de comprobación de accesos de seguridad en la empresa Dr. PC, Tarapoto, San Martín 2022?, ¿De qué manera un sistema basado en internet of thinks mejora el tiempo de enviar alertas de incidencias en la empresa Dr. PC, Tarapoto, San Martín 2022?, ¿ De qué manera un sistema basado en internet of thinks reduce las vulnerabilidades de accesos de seguridad en la empresa Dr. PC, Tarapoto, San Martín 2022?, ¿De qué manera un sistema basado en Internet of thinks mejora el nivel de satisfacción del usuario en la empresa Dr. PC, Tarapoto, San Martín 2022?.

Este proyecto de tesis tiene gran importancia para el ambiente universitario de la facultad de ingeniería de sistemas porque, nos permite aplicar todo el contenido de aprendizajes teóricos y prácticos alcanzados en los años de formación académica y probar de manera experimental dichos aprendizajes en la empresa Dr. PC, demostrando su aplicación final en casos cotidianos que ocurren diariamente para beneficio de la sociedad Tarapotina, como institución representativa en el ámbito tecnológico de la región San Martin.

Este trabajo se justificó académicamente porque la Universidad César Vallejo, establece como uno de los productos académicos de la carrera universitaria en desarrollo de investigación, la presentación de un producto final, el presente es

realizar el desarrollo del proyecto de tesis todo lo que concierne con toda la parte teórica y práctica que involucra al proyecto final.

Como justificación tecnológica, se planteó a la empresa Dr. PC ubicada en la ciudad de Tarapoto, la inserción de un sistema de seguridad que logre aumentar la seguridad física en la compañía con la aplicación de nuevas tecnologías basadas en Internet of thinks, más conocidas como IoT por sus palabras en inglés.

Como objetivo general de este proyecto de tesis se planteó; Mejorar la seguridad en la empresa Dr. PC con la inserción de un sistema basado en internet of thinks. Además de cinco específicos; 1) mejorar el tiempo de activación de dispositivos de seguridad (puertas de acceso y alarmas de la empresa) en la empresa Dr. PC, 2) mejorar el tiempo de comprobación de acceso de seguridad en la empresa Dr. PC, 3) mejorar el tiempo de envió de alertas de incidencias en la empresa Dr. PC, 4) reducir la vulnerabilidad de los accesos de seguridad en la empresa Dr. PC y 5) mejorar el nivel de satisfacción del usuario (directivos y responsables de seguridad) en la empresa Dr. PC con un sistema basado en internet of thinks.

Con el objetivo general y la realidad problemática establecida para el estudio se plantea la hipótesis general:" Con un sistema basado en internet of thinks se mejora la seguridad en la empresa Dr. PC Tarapoto, San Martin 2022"

Además de las hipótesis especificas: "Con un sistema basado en internet of thinks se mejora el tiempo de activación de dispositivos de seguridad en la empresa Dr. PC Tarapoto, San Martin 2022", "Con un sistema basado en internet of thinks se mejora el tiempo de comprobación de acceso de seguridad en la empresa Dr. PC Tarapoto, San Martin 2022", "Con un sistema basado en internet of thinks se mejora el tiempo de envió de alertas incidencias en la empresa Dr. PC Tarapoto, San Martin 2022", "Con un sistema basado en internet of thinks se disminuyen las vulnerabilidades de los accesos de seguridad en la empresa Dr. PC Tarapoto, San Martin 2022" y "Con un sistema basado en internet of thinks se mejora el nivel de satisfacción del usuario en la empresa Dr. PC Tarapoto, San Martin 2022

II. MARCO TEÓRICO.

Al inicio de esta nueva sección de este informe se señalan algunas referencias acerca del estado del arte del IoT en esta rama del conocimiento científico a nivel internacional tenemos al artículo de (Zambrano, y otros, 2019) que gracias a la implementación de una cantidad de sensores y su sincronización y coordinación en tiempo real en el sistema basada en IoT se obtuvieron óptimos resultados detallados en los acontecimientos estudiados, se puede observar que el 60% fueron solucionados por el sistema. Además, la participación comunitaria agrega un 37%, de valor agregado en la recuperación de personas desaparecidas. Al igual que el artículo de (Agudelo, y otros, 2019) que presenta una propuesta de arquitectura IoT enfocada en la seguridad física, con el objetivo de comparar y distinguir los distintos tiempos de respuesta y procesamiento. De esta manera los componentes usan entre el 15% y 23% referente a la capacidad de memoria, por lo cual se concluye que la propuesta arquitectónica utiliza un bajo uso de recursos de memoria, dado que no sobrepasa el 50%. También se determinó el porcentaje de memoria RAM empleado para la función evaluada determinando que existen unos picos altos de hasta 93.5% y otros muy bajos de 5%. Lo que permite evidenciar que el proceso de recolección de imágenes no es estable.

Like the article (Mbarek, y otros, 2020) they proposed a self-adaptive mutual key access authentication system that solves security problems. Resulting that we can detect about 80% of spoofed packets while only 60% fail with SAM (Secure Access Module) and TAP (Terminal Access Point) because it uses two forms of authentication which are current and previous keys. As well as the article (Fayez, y otros, 2020) who designed a trust-based monitoring (TBM) scheme using middleware and intelligent agents. The results show that lower response times (0.006 seconds) and higher detection rate (50 devices) were achieved.

Así como el artículo de (Koohang, y otros, 2022) que propone un modelo de cinco constructos para la elaboración de un software de seguridad comunitaria donde se midieron la privacidad = 59%, la seguridad = 66%,la confianza = 14% y la intención = 0,60%, lo que sugiere valores colectivos de moderados a altos, por lo que contribuye a construir una mejor comprensión de cómo el IoT puede cumplir un convertirse en un factor necesario para mejorar la seguridad y privacidad que a su vez, afecta la confianza de IoT y, en consecuencia, conduce al uso continuo de IoT

para la seguridad. Al igual que el artículo de (Toledo, y otros, 2019) que plantean un sistema de monitorización que concluyo con satisfacer las carencias de una población especifica, arrojando alertas establecidas en tiempos oportunos para informar a las autoridades inmediatamente después de activar las alarmas, el sistema les permite resguardar su integridad física generando un grado de confianza de 46.3% en los moradores, ya que, los datos almacenados por los teléfonos celulares son de gran ayuda para avisar a la población de cualquiera de los tipos de incidencias riesgosas. Así como también en artículo de (Cuervo, y otros, 2018) que plantea un sistema de monitoreo de alarmas que busca optimizar los tiempos de respuestas y monitoreo por cada 750 metros. Los resultados externos capturados en imágenes y videos ante cualquier caso de robo generando lograron cuantificar los tiempos de respuesta y supervisión, de un modo favorable en el monitoreo.

In addition to the article (Deebak, y otros, 2020) which focuses on providing flexible security with an authentication and encryption protocol to resist vulnerability to attacks. The result shows that it resists multiple attacks such as wormholes and IP impersonations which generates a detection radius of 80%; and, therefore, guarantees the delivery and security of multiple routes. As well as the article (Sani, y otros, 2019) In the 21st century, security systems are undergoing improvements thanks to the implementation of IoT, which can provide effective security and management support by verifying through analysis of security issue improvements for Energy Internet (IE) together with IoT. Like (Manjia, y otros, 2020) the internet of things every day is becoming a necessary part of our lives due to the ease of use it faces challenges that try to violate its security, so it is necessary devices that provide confidence to the user, which led us to present solutions that are based on machine learning algorithms for continuous improvement. Resulting in 32% using this method for IoT security compared to other methods.

(Rasim, y otros, 2018) creating cyber-physical security systems represents a challenge for people since they face multiple threats in both architecture and physical security, this work seeks to solve these difficulties and show lines of future research. Like the article (Noor, y otros, 2019) according to the article, between 2016 and 2018 IoT security studies are important because they aim to maintain data security and integrity, as well as user trust. For this reason, tools such as analysis

simulators have emerged that provide a description of the current state of the investigation.

(Alqahtani, y otros, 2020) This article presents a model for enhancing security capabilities in a cloud-enabled IoT environment, employing middleware and intelligent agents to manage security at the user level. The results indicate that only 1.51 joules are required for processing and authentication, generating low error rates, as well as reducing power consumption. Like the article (Balakrishnan, y otros, 2021) This research presents a methodology to defend against the security breach using IoT, and with the aim of detecting malicious intruders within a network. giving as results that the scores of DGA (Domain Generation Algorithm) are higher than 0.85 which means that improvements are needed against malicious attacks on the network. As well as the article (Yang, y otros, 2022) this article seeks to provide a guide on what concerns physical security and protection of IoT equipment as well as to summarize a set of solutions based on artificial intelligence which conclude in four future research opportunities.

(Lata, y otros, 2022) The future of the IoT in the web interconnection faces one of the challenges that is physical security, so this research seeks to describe the countermeasures following various security models. determining that truly innovative network designs are required to be resistant to theft and other malevolent threats. Like the article (Sarker, y otros, 2022) the research seeks to implement AI within IoT in order to improve its security from cyber-attacks based on studies highlights the research problems which leads the article to serve as a guide from a technical point of view for people who are experts in cybersecurity and IoT.

(Memos, y otros, 2022) According to the article, the new 4.0 standard seeks to integrate physical cyber systems, IA, IoT to reduce costs, minimize time and increase the quality of products, however this generates a security problem. Through the results obtained in the investigation, there are encouraging results in terms of accuracy, precision, recovery, crash, against known and unknown bot attacks.

(Miloslavskaya, y otros, 2019) With the aim of developing a taxonomy that identifies the risks in IoT-based security systems and also the directions to counteract them, a security intelligence approach is proposed. Like the article (Sha, y otros, 2018) according to the article, IoT-based systems face a major security problem for which

they are not prepared compared to other systems, so the article offers layered solutions for IoT architecture. Like the article (Lee, 2019) The following work is based on studies on the enterprise IoT presenting an ecosystem and an architecture for implementation and how these could increase security in their companies.

(Qureshi, y otros, 2021) The following article aims to present solutions based on IoT to improve security in an educational environment by giving users a secure mechanism between school and home. Like the article (Belenguer, y otros, 2022) According to the articles, security systems have evolved into intelligent systems, causing the infeasibility of IoT devices, for which an approach is being used to mitigate these problems, working as a shared model of collaboration between different agents. As well as the article (Mosemann, 2022) The study focuses on seeing the security risks that exist in the IoT and which go unnoticed, so it concludes that IoT devices need to have more security, as well as computers to servers to maintain data confidentiality. Like the article (Pal, y otros, 2022) the book is an analysis of future technologies with a unitary approach, but adopting them to work together with others helping to make systems safer, it also points out the capabilities of intelligent systems at the time of making decisions together with contributions from countless experts in security, IoT and intelligent systems.

(Nižetić, y otros, 2020) With the aim of simplifying work and improving efficiency, we are presented with a new approach to IoT focused on technology, health and the environment, resulting in guides that help understand the areas of application in IoT. Like the article (Hong, y otros, 2018) the era of the IoT allows us to be interconnected, but it also generates a large number of insecurities. However, to solve these mishaps, a large number of projects have been implemented that help to solve this lack of security in IoT technologies.

(Babar, y otros, 2020) The following article proposes a secure management engine based on IoT that controls intrusions to the smart grid based on intelligent agents, as results it was obtained that the engine is less vulnerable and efficient to reduce the use of smart energy.

(Singh, y otros, 2020) the COVID-19 pandemic brought endless difficulties, for which an IoT-based monitoring system was implemented, helping to increase patient satisfaction and reduce costs for the patient, concluding that it is useful to identify symptoms of COVID-19 both for patients and doctors. Like the article (Sengupta, y

otros, 2020) in order to provide a guide to address the security vulnerabilities that IoT systems have, the article also analyzes real cases to identify the merits and drawbacks of using IoT technology and proposes using cloud-centric applications to improve security.

(Singh, y otros, 2020) According to the article, proposes to relate what is relevant to the physical with computing facilities based on IoT technology based on a secure environment where Blockchain provides a distributed environment by establishing protocols in the data network. Finally, the proposed infrastructure is evaluated, security methods are compared and the results are shown. Like the article (Mashkoor, y otros, 2020) a study on the protection of security systems is presented, which provides an overview of this field, proposing and answering important research questions, as well as identifying the preference of the places of publication. Así como el artículo de (Suárez, y otros, 2019) que analiza diferentes métodos de seguridad en base a IoT tomando en cuenta sus características de funcionalidad, buenas prácticas, los cuales generen estrategias de seguridad de última generación. Al igual que el artículo de (Vinicio, y otros, 2020) utilizando una metodología teórica y empírica, se realizó un estudio a 36 empresas referente al uso de los sistemas de seguridad, destacando elementos como cámaras, videovigilancia y accesos el cual la investigación determino que un 91.67% de empresas les gustaría aplicar este sistema por mejoraría su seguridad física.

(Bravo, y otros, 2018) El propósito de este trabajo es analizar la aceptación pública de las tecnologías que reconocen el rostro como una de las medidas de seguridad. Mostrando que tuvo 50% de aceptación el reconocimiento facial como medida de seguridad. Al igual que el artículo de (Vega, y otros, 2019) La finalidad fue diseñar un software de monitoreo para puertas y ventanas por medio de la asociación IoT que se muestre en línea a través de una interfaz de usuario, enviando alertas al móvil.

(Pastas, y otros, 2022) con un mapeo sistemático en cuanto a la seguridad de tipos de ataque redes informáticas se determinaron que el phishing afecta en un 11,90%, la inyección con un 37,29% y la denegación de servicios con un 28,57%. Además, las actualizaciones de software representan el 14,29% de la atracción del proyecto. Por último, se recomienda usar procedimientos como: Blockchain, Cloud Computing, Machine Learning, para prevenir posibles ataques.

(Leyva, 2018) que tienen como objetivo controlar los accesos de seguridad por medio de IoT el cual tuvo como resultado una mejora en el tiempo de accesos de un 98.38%, además de reducir la vulnerabilidad en un 43.75%, el cual demuestra que la investigación cumplió con su objetivo. Al igual que el artículo de (Santos, y otros, 2021) la investigación tiene como propósito optimizar la seguridad de los establecimientos en Trujillo en base a con un diseño experimental de grado preexperimental teniendo como resultados una mejoría del 75% en frustraciones de actos delictivos lo cual indica que con un sistema de seguridad en base a IoT si se mejoró la seguridad en los establecimientos.

(Huaranga, y otros, 2019) quienes en su investigación de tipo aplicada y usaron IoT para realizar un aplicativo que detecte los estacionamientos vacíos en el centro comercial real plaza. Arrojando como resultado una mejoría en la búsqueda y detección obteniendo una disminución de un 99%, al tener un margen de error del 0,22277% después de la implantación del aplicativo. Así como el artículo de (Mendoza, 2021) este expositivo arroja a la luz diversos riesgos a los que se afrontan los usuarios al usar elementos que están conectados a IoT. Se estima que al 2021 los hogares inteligentes en EE.UU. alcancen un 28% y al 2025 estiman que habrá 41 millones de dispositivos conectados generando 80 Zettabits de datos. Afectando la solidez, entereza y confidencialidad de los clientes que usan IoT. Trabajar en ello debe ser una precedencia para avalar la garantía para las personas y recuperar la confianza en el uso de los dispositivos.

Asimismo, en la revisión bibliográfica se determinó los siguientes indicadores:

Tiempo. – es la representación de una conexión que un equipo de trabajo implanta entre dos o más actividades, de los que tomamos uno en específico para poder referenciar o tomar como medidas para los otros (Norbert, 2021).

Seguridad. -se relata como el reconocimiento y observación de las diferentes vulneraciones que pueden llegar a enfrentar hogares, materiales y procesos con el objetivo de desarrollar estrategias además de diseñar sistemas que prevengan, dificulten o limiten los efectos de las amenazas más comunes que enfrenta la seguridad de los individuos (Figueroa, y otros, 2018).

Satisfacción. -representa lo que impulsa a un grupo humano a cómo proceder y causar un tipo de actitud que genera una impresión directa relacionada con el

trabajo en el que se desempeña cada persona de manera colectiva e individual (Paredes, y otros, 2022).

Tiempo de envió de alertas de incidencias. – el tiempo de envió de alertas es la cantidad de segundos en lo que se demora el sistema de seguridad en enviar una alerta de incidencia por medio de una aplicación móvil (Beltrán, 2018).

Tiempo de comprobación de acceso de seguridad. – se refiere al tiempo que demora en la comprobación de los datos y credenciales de la persona que va a ingresar a la empresa (Gómez, 2022).

Tiempo empleado para habilitar los dispositivos de seguridad. -se refiere al tiempo en que demora en activarse un dispositivo de seguridad como una alarma, una cámara de seguridad o cualquier otro dispositivo en la empresa (Montoya, y otros, 2018).

Cantidad de ataques por día. – se refiere a la cantidad de ataques que se registra en el log file (archivo lógico) del sistema de seguridad (Zuña, y otros, 2019).

Nivel de satisfacción del usuario con el sistema. – se refiere al bienestar que tienen los usuarios de la empresa en cuantos al sistema de seguridad (Febres, y otros, 2020).

Ley de modernización (LEY N.º 27658) El desarrollo de la gestión del Estado busca como propósito principal la obtener un mayor nivel de eficacia del dispositivo gubernamental, de varias maneras en las que pueda mejorar el cuidado de la población, anteponiendo y perfeccionando la utilización de bienes del sector público. Creando y condicionando para estimular el capital propio en el departamento de las TIC, generando evidencia jurídica y facilitando la demostración de las infraestructuras de mayores costos, de forma que se enfoque la inversión en poder enlazar a Internet a las poblaciones más vulnerables y que no tienen los suficientes medios, además de las áreas según el (Decreto Supremo que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030)

Ley de seguridad (Ley N° 30336) es una prestación que el estado brinda, la cual garantiza la entereza de la mayor parte de las personas y sus riquezas. La seguridad pública comprende que las personas puedan establecerse en paz, cada individuo conviviendo con respeto de los derechos individuales de cada uno según el (Decreto Supremo que aprueba la Política Nacional Multisectorial de Seguridad Ciudadana al 2030)

ISO/IEC 27000 es un grupo de modelos de nivel internacional que comprende la Seguridad de la Información. El Grupo de normas ISO 27000 tienen agrupaciones de normas para la instalación, acondicionamiento, conservación y que generen una mejoría en los Sistemas de Gestión de la Seguridad de la Información según las (Guías de referencia útiles para la implantación, mantenimiento, auditoría y certificación de los Sistemas de Gestión de la Seguridad de la Información serie 27000)

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

Tipo de Investigación

De acuerdo con la investigación podemos decir que fue de tipo aplicada, orientada al enfoque cuantitativo porque se tiene una hipótesis y se efectúa la recolección de información para después ser examinados estadísticamente según (Deroncele, 2022).

Diseño de Investigación

El diseño que vamos a usar en la investigación pertenece al diseño experimental, puntualmente a la sub clasificación pre experimental según (Manterola, y otros, 2019) porque admite cuantificar e identificar los orígenes dentro del estudio y la manipulación de variables. Además, se enfoca en comparar un antes y un después de la inserción del sistema basado en internet of thinks para mejorar la seguridad en la empresa Dr. PC.

De acuerdo al artículo de los autores (Mendoza, y otros, 2021). Nos dice que el diseño experimental consta de diseñar y realizar experimentos con el objetivo de iniciar antecedentes que, al ser estudiados estadísticamente, brinden pruebas reales que logren contestar las preguntas realizadas por el experimentador de un determinado tema, y de esta manera separar o dividir los aspectos inciertos de una determinada actividad, la cual logre resolver problemas.

Además, se empleó el diseño experimental de preprueba y posprueba.

Figura N°1: Diseño pre-experimental

$$O_1 – X – O_2$$

O_1: Seguridad sin el sistema basado en internet of thinks.

X: Se establece para la incorporación que vendría a ser el uso del Sistema basado en internet of thinks.

O_2: Seguridad con el sistema basado en internet of thinks.

3.2 Variables y operacionalización

Variable Independiente:

Sistema basado en internet of thinks, Constituyen un concepto que hace referencia a la conectividad entre objetos físicos, la suficiencia de estos para transportar información por medio de redes y que esta sea de forma autómata (Quichimbo, 2022).

Variable Dependiente:

Seguridad Física, la palabra seguridad física se utiliza siempre para relacionarse con las normas de prevención para exteriores. Las cuales se implantan por medio de mecanismos eléctricos, electrónicos, etc. Según (Montilla, 2020) (Anexo N°1: Operacionalización de variables).

3.3 Población, muestra y muestreo

3.3.1 Población

La investigación cuenta con una unidad de análisis que son las personas que interactúan con el sistema de seguridad basado en Internet of Thinks lo cual se está fijando en la tabla N°1.

Tabla 1

Población

POBLACION	MUESTRA
USUARIOS	1 gerente 1 jefe de seguridad 10 trabajadores
	12 usuarios

Fuente: Elaboración Propia

3.3.2 Muestra

Para el desenvolvimiento de la investigación, contemplando las particularidades en la población, se ha escogido un muestreo no probabilístico por conveniencia fijando la población de usuarios seleccionados en 12. Además, se consideró a trabajadores específicos en el departamento de seguridad en la empresa Dr. PC como el gerente, jefe de seguridad y los trabajadores.

3.4 Técnicas e instrumentos de recolección de datos

Se utilizaron técnicas como la observación y encuesta, estableciendo guías de observación y un cuestionario como medio para recolectar datos de los indicadores establecidos tal como se observa en la tabla N°2.

Tabla 2

Técnicas e instrumentos

Indicadores	Técnica	Instrumento	Fuente	Informantes
Tiempo de activación de dispositivos de seguridad	Observación	Guías de observación	Área de seguridad	Gerente Jefe de seguridad Trabajadores
Tiempo de comprobación de acceso de seguridad				
Tiempo de envió de alertas de incidencias				
Cantidad de ataques por día				
Nivel de satisfacción del usuario con el sistema	Encuesta	Cuestionario	Usuarios	

Fuente: Elaboración Propia

Validez

Para validar los instrumentos se llevó a cabo por medio de un juicio de expertos estuvo a cargo de tres profesionales en ingeniería de sistemas expertos en seguridad los cuales revisaron todas las expresiones del cuestionario.

Tabla 3

Validez a través de juicio de expertos

Experto	Especialidad	Comentario
Henry Maldonado Flores	Ingeniería de sistemas	Buen instrumento
Johon Jenry Huancas Huamán	Ingeniería de sistemas	Bien elaborado
Roland Kennet Echevarría Ibazeta	Ingeniería de sistemas	Buen instrumento

Fuente Elaboración Propia

Confiabilidad

Para la tesis de empleo el coeficiente de Alfa de Cronbach para decidir el nivel de la consistencia de los instrumentos desarrollados. Se efectuó una demostración piloto de 12 colaboradores para su adaptación y resolución de los coeficientes hallados en los instrumentos.

Tabla 4

Nivel de Confiabilidad de Instrumentos

Instrumento	Alfa de Cronbach	Nivel de Consistencia	
Cuestionario	0.967	**Estadísticas de fiabilidad**	
		Alfa de Cronbach	N de elementos
		,967	11

Fuente: Elaboración Propia

3.5 Procedimientos

Tras entender la situación real de la empresa Dr. PC en la ciudad de Tarapoto, Se ha hecho la coordinación institucional (Anexo N°5: Carta de aceptación) donde se han definido unidades analíticas y variables, en las despliegan determinadas dimensiones e indicadores con sus respectivas herramientas.

Se planteó un sistema basado en internet of thinks para mejorar la seguridad física; Donde se miden las variables estudiadas con un Pre test, gracias a las guías de observación.

Con la inserción del Sistema basado en internet of thinks, se miden las variables comprometidas igual que en el Pre Test, para así comparar y dar validez o declinar la hipótesis de la investigación establecida. Para lo cual tendremos la ayuda de un software estadístico SPSS y Exel 2021 que nos ayudara a extraer información de acuerdo a las pautas planteadas para la tesis.

3.6 Método de análisis de datos

Utilizamos un enfoque estadístico, es decir, recopilaremos información para la investigación a través de las herramientas planteadas anteriormente (guías de observación y cuestionario). Una vez aplicadas, son procesadas y analizadas mediante gráficos de barras y porcentajes para identificar y comparar los cambios

ocurridos a lo largo del pre-test y el post-test. Además de estar soportado por el software SPSS Y Excel 2021.

3.7 Aspectos éticos

La tesis considero principios exactos y comportamientos admisibles en la tesis, estando apoyados y empleando nomas ISO 690 para las citas teniendo en cuenta al autor y el año que no sea mayor a 5 años de antigüedad la investigación, tanto en la realidad problemática, antecedentes y marco teórico. Asimismo, se consideró la normativa de las guías vigentes de la Universidad César Vallejo y en definitiva se establece que la información proporcionada por la empresa Dr. PC están sujetos específicamente en el uso de este proyecto de investigación, brindando la confiabilidad de su información en su totalidad.

IV. RESULTADOS

Del objetivo Especifico N°1: Mejorar el tiempo de activación de dispositivos de seguridad (puertas de acceso y alarmas) en la empresa Dr. PC.

Indicador N°1: Tiempo de activación de dispositivos de seguridad.

Análisis Descriptivo

Tabla 5

Análisis de estadísticos descriptivos del Tiempo de activación de dispositivos de seguridad

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
Pre_Test	30	35	60	48,87	6,766
Post_Test	30	1	5	2,87	1,167
N válido (por lista)	30				

Fuente: Indicador N°1
Elaboración: SPSS V-25

En este indicador tiempo de activación de dispositivos de seguridad, para el pre-test se obtuvo un valor en la media de 48.87 segundos y para el post-test mostró un valor de 2.87 segundos en el tiempo de activación, esto indica que hay una reducción de 46.00 segundos, después de la implementación del sistema basado en IoT. De la misma forma el valor mínimo obtenido del Tiempo de activación de dispositivos de seguridad fue de 35 segundos y el máximo 60 segundos antes de la implementación del sistema basado en IoT y posteriormente a la implementación del sistema basado en IoT se obtuvo un valor mínimo de 1 segundo y un máximo de 5 segundos. De igual manera en la desviación estándar, en el pre-test se mostró un valor de 6.766 segundos, y en el post-test se mostró una variabilidad de 1.167 segundos.

Del objetivo Especifico N°2: Mejorar el tiempo de comprobación de acceso de seguridad en la empresa Dr. PC.

Indicador N°2: Tiempo de comprobación de accesos de seguridad.

Tabla 6

Análisis de estadísticos descriptivos del Tiempo de comprobación de accesos de seguridad

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
Pre_Test	30	50	80	62,97	8,088
Post_Test	30	1	4	2,47	1,074
N válido (por lista)	30				

Fuente: Indicador N°2
Elaboración: SPSS V-25

En este indicador tiempo de comprobación de accesos de seguridad, para el pre-test obtuvo un valor en la media de 62.97 segundos y para el post-test mostró un valor de 2.47 segundos, esto indica que hay una reducción de 60.05 segundos, después de la implementación del sistema basado en IoT. De la misma forma el valor mínimo obtenido del Tiempo de activación de dispositivos de seguridad fue de 50 segundos y el máximo 80 segundos antes de la implementación del sistema basado en IoT y posteriormente a la implementación del sistema basado en IoT se obtuvo un valor mínimo de 1 segundos y un máximo de 4 segundos. De igual manera en la desviación estándar, en el pre-test se mostró un valor de 8.088 segundos, y en el post-test se mostró una variabilidad de 1.074 segundos.

Del objetivo Especifico N°3: Mejorar el tiempo de envió de alertas de incidencias en la empresa Dr. PC.

Indicador N°3: Tiempo de envió de alertas de incidencias.

Tabla 7

Análisis de estadísticos descriptivos del Tiempo de envió de alertas de incidencias.

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación
Pre_Test	30	180	600	364,67	141,098
Post_Test	30	1	4	2,60	1,070
N válido (por lista)	30				

Fuente: Indicador N°3
Elaboración: SPSS V-25

En este indicador Tiempo de envió de alertas de incidencias, para el pre-test obtuvo un valor en la media de 364.67 segundos y para el post-test mostró un valor de 2.60 segundos, esto indica que hay una reducción de 362.07 segundos, después de la implementación del sistema basado en IoT. De la misma forma el valor mínimo obtenido del Tiempo de envió de alertas de incidencias fue de 180 segundos y el máximo 600 segundos antes de la implementación del sistema basado en IoT y posteriormente a la implementación del sistema basado en IoT se obtuvo un valor mínimo de 1 segundo y un máximo de 4 segundos. De igual manera en la desviación estándar, en el pre-test se mostró un valor de 141.098 segundos, y en el post-test se mostró una variabilidad de 1.070 segundos.

Del objetivo Especifico N°4: Reducir la vulnerabilidad de los accesos de seguridad en la empresa Dr. PC.

Indicador N°4: Cantidad de ataques por día.

Tabla 8

Análisis de estadísticos descriptivos para la Cantidad de ataques por día.

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación
Pre_Test	30	1	8	4,97	1,884
Post_Test	30	0	2	,83	,791
N válido (por lista)	30				

Fuente: Indicador N°4

Elaboración: SPSS V-25

En este indicador cantidad de ataques por día, para el pre-test obtuvo un valor en la media de 4.97 ataques y para el post-test mostró un valor de 0.83 ataques, esto indica que hay una reducción de 4.14 ataques, después de la implementación del sistema basado en IoT. De la misma forma el valor mínimo obtenido para la cantidad de ataques por día fue de 1 ataque y el máximo 8 ataques antes de la implementación del sistema basado en IoT y posteriormente a la implementación del sistema basado en IoT se obtuvo un valor mínimo de 0 ataques y un máximo de 2 ataques. De igual manera en la desviación estándar, en el pre-test se mostró un valor de 1.884 ataques, y en el post-test se mostró una variabilidad de 0.791 ataques.

Del objetivo Especifico N°5: Mejorar el nivel de satisfacción del usuario (directivos y responsables de seguridad) en la empresa Dr. PC.

Indicador N°5: Grado de satisfacción del usuario.

Tabla 9

Análisis de estadísticos descriptivos para el grado de satisfacción del usuario.

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
Pre_Test	12	13	32	22,00	7,640
Post_Test	12	35	55	47,75	6,210
N válido (por lista)	12				

Fuente: Indicador N°5
Elaboración: SPSS V-25

En este indicador grado de satisfacción del usuario, para el pre-test obtuvo un valor en la media de 22.00 y para el post-test mostró un valor de 47.75 esto indica que hay un aumento de 25,75 después de la implementación del sistema basado en IoT. De la misma forma el valor mínimo obtenido para el grado de satisfacción del usuario fue de 13 y el máximo 32 antes de la implementación del sistema basado en IoT y posteriormente a la implementación del sistema basado en IoT se obtuvo un valor mínimo de 35 y un máximo de 55. De igual manera en la desviación estándar, en el pre-test se mostró un valor de 7.640 y en el post-test se mostró una variabilidad de 6.210.

Prueba de Normalidad

Tabla 10

Test de Normalidad para el Tiempo de activación de dispositivos de seguridad

Pruebas de normalidad			
	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pre_Test	,966	30	,438
Post_Test	,918	30	,024
Diferencia	,966	30	,434

Fuente: Indicador N°1
Elaboración: SPSS V-25

Los valores obtenidos en la tabla N°10 indican que el valor de (sig.) del tiempo de activación de dispositivos de seguridad en el pre-test fue de 0.438 (> a 0.05), y en el post-test indica que el valor de (sig.) fue de 0.024 (> a 0.05) y la diferencia indica que el valor de (sig.) fue de 0.434 (> a 0.05) que la de esta manera se comprobó que el tiempo de activación de dispositivos de seguridad cumple con la distribución normal por lo tanto usaremos una prueba paramétrica t student.

Tabla 11

Test de Normalidad para el Tiempo de comprobación de accesos de seguridad

Pruebas de normalidad			
	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pre_Test	,972	30	,607
Post_Test	,873	30	,002
Diferencia	,982	30	,865

Fuente: Indicador N°2
Elaboración: SPSS V-25

Los valores obtenidos en la tabla N°11 indican que el valor de (sig.) del tiempo de comprobación de accesos de seguridad. en el pre-test fue de 0.607 (> a 0.05), y en el post-test indica que el el valor de (sig.) fue de 0.002 (< a 0.05) y la diferencia indica que el valor de (sig.) fue de 0.865 (> a 0.05) que la de esta manera se comprobó que el tiempo de comprobación de accesos de seguridad cumple con la distribución normal por lo tanto usaremos una prueba paramétrica t student.

Tabla 12

Test de Normalidad para Tiempo de envió de alertas de incidencias.

Pruebas de normalidad			
	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pre_Test	,902	30	,009
Post_Test	,870	30	,002
Diferencia	,904	30	,010

Fuente: Indicador N°3
Elaboración: SPSS V-25

Los valores obtenidos en la tabla N°12 indican que el valor de (sig.) del tiempo de envió de alertas de incidencias en el pre-test fue de 0.009 (< a 0.05), y en el post-test indica que el el valor de (sig.) fue de 0.002 (< a 0.05) y la diferencia indica que el valor de (sig.) fue de 0.010 (< a 0.05) de esta manera se comprobó que el tiempo de envió de alertas de incidencias no cumple con la distribución no normal.

Tabla 13

Test de Normalidad para la Cantidad de ataques por día.

Pruebas de normalidad

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pre_Test	,938	30	,082
Post_Test	,794	30	,000
Diferencia	,935	30	,066

Fuente: Indicador N°4
Elaboración: SPSS V-25

Los valores obtenidos en la tabla N°13 indican que el valor de (sig.) de la cantidad de ataques por día en el pre-test fue de 0.082 (> a 0.05), y en el post-test indica que el el valor de (sig.) fue de 0.000 (< a 0.05) y la diferencia indica que el valor de (sig.) fue de 0.066 (< a 0.05) de esta manera se comprobó que la cantidad de ataques por día cumple con la distribución normal.

Tabla 14

Test de Normalidad para el grado de satisfacción del usuario.

Pruebas de normalidad

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pre_Test	,850	12	,036
Post_Test	,908	12	,200

Fuente: Indicador N°5
Elaboración: SPSS V-25

Los valores obtenidos en la tabla N°14 indican que el valor de (sig.) del grado de satisfacción del usuario en el pre-test fue de 0.036 (< a 0.05), y en el post-test indica que el valor de (sig.) fue de 0.200 (> a 0.05) de esta manera se comprobó que el tiempo de activación de dispositivos de seguridad cumple con la distribución normal.

Prueba de Hipótesis

Tabla 15

Prueba T-Student para el Tiempo de activación de dispositivos de seguridad

Prueba de muestras emparejadas

		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	Pre_Test - Post_Test	46,000	6,502	1,187	43,572	48,428	38,750	29	,000

Fuente: Indicador N°1
Elaboración: SPSS V-25

H0: Con un sistema basado en internet of thinks no se mejora el tiempo de activación de dispositivos de seguridad en la empresa Dr. PC Tarapoto, San Martin 2022.

H1: Con un sistema basado en internet of thinks si se mejora el tiempo de activación de dispositivos de seguridad en la empresa Dr. PC Tarapoto, San Martin 2022.

Como el nivel de significancia (0.000) es menor que 0.05 se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alternativa (H_1), además, con el sistema basado en IoT el tiempo de activación de dispositivos de seguridad disminuye de 48.87 segundos a 2.87 segundos; lo que representa una mejora porcentual de 94.13% al tiempo de la activación sin el sistema basado en IoT.

Tabla 16

Prueba T-Student para el Tiempo de comprobación de accesos de seguridad

Prueba de muestras emparejadas

		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	Pre_Test - Post_Test	60,500	8,216	1,500	57,432	63,568	40,333	29	,000

Fuente: Indicador N°2
Elaboración: SPSS V-25

H_0: Con un sistema basado en internet of thinks no se mejora el tiempo de comprobación de acceso de seguridad en la empresa Dr. PC Tarapoto, San Martin 2022.

H_1: Con un sistema basado en internet of thinks si se mejora el tiempo de comprobación de acceso de seguridad en la empresa Dr. PC Tarapoto, San Martin 2022.

Como el nivel de significancia (0.000) es menor que 0.05 se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alternativa (H_1), además, con el sistema basado en IoT el tiempo de comprobación de accesos de seguridad disminuye de 62.97 segundos a 2.47 segundos; lo que representa una mejora porcentual de 96.08% al tiempo de la comprobación sin el sistema basado en IoT.

Tabla 17

Prueba de Wilcoxon para el Tiempo de envió de alertas de incidencias.

Estadísticos de prueba[a]	
	Post_Test - Pre_Test
Z	-4,784[b]
Sig. asintótica(bilateral)	,000

Fuente: Indicador N°3
Elaboración: SPSS V-25

H_0: Con un sistema basado en internet of thinks no se mejora el tiempo de envió de alertas incidencias en la empresa Dr. PC Tarapoto, San Martin 2022.

H_1: Con un sistema basado en internet of thinks si se mejora el tiempo de envió de alertas incidencias en la empresa Dr. PC Tarapoto, San Martin 2022.

Como el nivel de significancia (0.000) es menor que 0.05 se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alternativa (H_1), además, con el sistema basado en IoT el tiempo de envió de alertas de incidencias disminuye de 364.67 segundos a 2.60 segundos; lo que representa una mejora porcentual de 99.29% al tiempo del envió sin el sistema basado en IoT.

Tabla 18

Test de Normalidad para la Cantidad de ataques por día.

Prueba de muestras emparejadas

		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	Pre_Test - Post_Test	4,133	2,080	,380	3,357	4,910	10,884	29	,000

Fuente: Indicador N°4
Elaboración: SPSS V-25

H_0: "Con un sistema basado en internet of thinks no se disminuyen las vulnerabilidades de los accesos de seguridad en la empresa Dr. PC Tarapoto, San Martin 2022.

H_1: "Con un sistema basado en internet of thinks si se disminuyen las vulnerabilidades de los accesos de seguridad en la empresa Dr. PC Tarapoto, San Martin 2022.

Como el nivel de significancia (0.000) es menor que 0.05 se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alternativa (H_1), además, con el sistema basado en IoT la cantidad de ataques por día disminuye de 4.967 ataques a 0.83 ataques; lo que representa una mejora porcentual de 83.30% a la Cantidad de ataques por día sin el sistema basado en IoT.

Tabla 19

Prueba T-Student para el grado de satisfacción del usuario.

Prueba de muestras emparejadas

		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	Pre_Test - Post_Test	-25,750	4,615	1,332	-28,682	-22,818	-19,330	11	,000

Fuente: Indicador N°5
Elaboración: SPSS V-25

H_0: Con un sistema basado en internet of thinks no se mejora el nivel de satisfacción del usuario en la empresa Dr. PC Tarapoto, San Martin 2022.

H_1: Con un sistema basado en internet of thinks si se mejora el nivel de satisfacción del usuario en la empresa Dr. PC Tarapoto, San Martin 2022.

Como el nivel de significancia (0.000) es menor que 0.05 se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alternativa (H_1), además según el gráfico N°5, con el sistema basado en IoT el grado de Satisfacción del usuario aumenta de 22.00 a 47.75; lo que representa una mejora porcentual de 53.93% con la implementación del sistema basado en IoT.

V. DISCUSIÓN

En relación al primer objetivo específico Tiempo de activación de dispositivos de seguridad nuestra investigación arrojo como resultado que con el sistema basado en internet of thinks el tiempo de activación de dispositivos de seguridad disminuye; lo que representa una mejora. De acuerdo con el artículo de (Zambrano, y otros, 2019) nos dicen que gracias a la implementación de una cantidad de sensores y su sincronización y coordinación en tiempo real en el sistema basada en IoT se obtuvieron óptimos resultados detallados en los acontecimientos estudiados, se puede observar que el 60% fueron solucionados por el sistema. Además, la participación comunitaria agrega un 37%, de valor agregado en la recuperación de personas desaparecidas. Según la experimentación que se realizó para el presente artículo de investigación se descubrió que el recorrido promedio para recuperar una persona perdida es de 24,5 km, lo que significa que gracias a los métodos planteados se pudo resolver el problema en la misma ciudad. Al igual que el artículo de (Agudelo, y otros, 2019) nos dice que, en la actualidad, es evidente que las instituciones de educación tienen problemas de seguridad física, debido a la falta de barreras para reducir los riesgos. Este artículo presenta su principal contribución como una propuesta de arquitectura IoT enfocada en la seguridad, pretendiendo reunir todas herramientas necesarias para su acondicionamiento, con el objetivo de comparar y distinguir los distintos tiempos de respuesta y procesamiento. De esta manera se comprueba que este componente de la arquitectura utiliza por parte del procesador una memoria entre el 15 y 23 % de su uso, y la línea de distribución también determina que estos datos se mantienen estables, por lo cual se concluye que la propuesta arquitectónica utiliza un bajo uso de recursos de memoria, dado que no sobrepasa el 50 % de ésta, según los valores obtenidos. También se determinó el porcentaje de memoria RAM empleado para la función evaluada determinando que existen unos picos altos de hasta 93.5% y otros muy bajos de 5%. Lo anterior permite evidenciar que el consumo de memoria RAM no permanece estable durante el procesamiento de la identificación de imágenes bajo el tiempo que duró la prueba.

Con respecto al segundo objetivo específico Tiempo de comprobación de acceso de seguridad nuestra investigación arrojo como resultado que con el sistema basado en internet of thinks el tiempo de comprobación de accesos disminuye; lo que representa una mejora, De acuerdo con el artículo de (Mbarek, y otros, 2020) dicen que su principal problema es la vulneración de la autenticación de accesos, por lo que para solucionar el problema se propuso un esquema de autenticación de claves auto adaptativa y mutua. Dando como resultados un porcentaje de fallas de autenticación entre los enfoques SAM (módulo de acceso seguro) y TAP (Punto de acceso a la terminal). En particular, muestra que el porcentaje de falla de autenticación es menor con SAM, especialmente cuando el número de ataques de interferencia es alto, es decir, superior a 10. Por ejemplo, con TAP, podemos detectar alrededor del 80% de los paquetes falsificados mientras que solo 60 % fallan con SAM porque utiliza dos formas de autenticación que son claves actuales y anteriores. Lo que da como conclusión una reducción de tiempos en la comprobación de accesos y una mejora en la seguridad. Así como también el artículo de (Qureshi, y otros, 2021) que presenta un sistema de seguridad para monitorear y enviar alertas, el sistema propuesto se basa en 5G, en la nube y en servicios avanzados de análisis de datos. El sistema propuesto es una solución completa para que los padres rastreen la ubicación, el movimiento, la presencia, la asistencia a la escuela de sus hijos y tomen decisiones rápidas en caso de emergencia el cual da como resultado que proporciona un mecanismo de alerta más seguro y facilita el tiempo de comprobación de accesos ya que evalúa los términos de entrega de datos, tiempo y parámetros de alerta de respuesta. Así como el artículo de (Koohang, y otros, 2022) que propone un modelo de cinco constructos que fue evaluado con el coeficiente de determinación la medida de redundancia con validación cruzada basada en el vendaje y los coeficientes de ruta. Los valores miden la varianza explicada en cada uno de los constructos predictores fueron privacidad = 59 %, seguridad = 66 %, confianza = 14 % e intención = 0,60 %, lo que sugiere valores colectivos de moderados a altos, esta investigación ha contribuido a construir una mejor comprensión de cómo la conciencia de IoT desempeña un rol fundamental en la rama de seguridad y privacidad de IoT que, a su vez, afecta la confianza de IoT y, en consecuencia, conduce al uso continuo de IoT.

Con respecto al tercer objetivo específico Tiempo de envió de alertas de incidencias nuestra investigación arrojo como resultado que con el sistema basado en internet of thinks el tiempo de envió de alertas disminuye; lo que representa una mejora, De acuerdo con el artículo de (Vega, y otros, 2019) que tuvieron como objetivo diseñar un aplicativo para monitoreo de accesos por medio de la infraestructura IoT que se muestre en línea a través de una interfaz de usuario, en el momento que un acceso está abierto por un cierto tiempo manda una alerta al móvil. Dando como resultado un sistema de monitorización el cual redujo el tiempo de envió de alertas además de proporcionar servicios eficientes y confiables para un almacenamiento de información y así poder enviar los textos de alerta a un teléfono celular logrando que el alcance de la transmisión wifi sea 47 metros con línea de vista. Así como también el artículo de (Fayez, y otros, 2020) que diseñó un esquema de monitoreo basado en la confianza empleando middleware y agentes inteligentes. Los resultados demuestran que se logró de menores tiempos de respuesta y mayor tasa de detección. Al igual que el artículo de (Toledo, y otros, 2019) que plantean un sistema de vigilancia que cumple con las expectativas de la comunidad, generando las alertas predeterminadas en tiempos convenientes siendo capaces de informar a los responsables de la seguridad sobre la activación de la alerta, asimismo generando satisfacción en la población debido a que ahora se cuenta con un sistema que pueda tolerar y guardar su consistencia física y particularidades necesarias que dan como resultados que el 46.3% de los moradores está de acuerdo con que la autoridad llega de manera inmediata además de tener la conformidad y credibilidad de la comunidad, ya que, los datos almacenados por los teléfonos celulares son de gran ayuda para avisar a la población de cualquiera de los tipos de incidencias riesgosas; originando una ética situacional colectiva, que pueda permitir tomar decisiones correctas. Al igual que el artículo de (Balla, y otros, 2018) que tiene como objetivo establecer una alerta para los visitantes del hogar y proporcionar información a través de una aplicación telefónica. Dando como resultado una mayor eficiencia en cuanto al tiempo de envió de alertas y además ofrece una gran ventaja que es la facilidad de uso. Así como también en artículo de (Cuervo, y otros, 2018) que plantea un sistema de monitoreo de alarmas que busca mejorar el tiempo que tarde un sistema en responder y monitorear un sector de 750

metros, nos da como respuesta que tarda 2,09 minutos con una velocidad de 8 m/s, y la revisión con capturas de imagen tarda 7,09 minutos. Los resultados externos capturados en imágenes y videos ante cualquier caso de robo generando resultados que se lograron cuantificar los tiempos de respuesta y supervisión, de un modo favorable en el monitoreo.

Con respecto al cuarto objetivo específico Reducir la vulnerabilidad de los accesos de seguridad nuestra investigación arrojo como resultado que con el sistema basado en internet of thinks se reduce la vulnerabilidad de los accesos de seguridad; lo que representa una mejora, De acuerdo con el artículo de (Miloslavskaya, y otros, 2019) que tuvo como objetivo desarrollar una taxonomía la cual identifique la vulnerabilidad y los posibles riesgos en seguridad de equipos IoT para lo que se propuso un enfoque de inteligencia de seguridad el cual tuvo como resultado que se reduce la vulnerabilidad en los accesos de seguridad específicamente en tecnología IoT. Así como también el artículo de (Balakrishnan, y otros, 2021) que gracias a la tecnología basada en IoT busca garantizar a los usuarios un entorno seguro para lo que surgen algoritmos y protocolos de seguridad para lo que el artículo propone una hibridación algorítmica de IDS (sistema de detección de intrusiones) el cual sea capaz de reducir las vulnerabilidades teniendo como resultado que la recopilación de datos capacita al sistema y además hace que obtenga resultados más prometedores. Al igual que el artículo de (Lata, y otros, 2022) que presenta un sinnúmero de modelos para la seguridad IoT asimismo se siguen buscando modelos con estándares mundiales que resistan amenazas malévolas de vulneración de seguridad. Además del artículo de (Memos, y otros, 2022) que presentan nuevos estándares en tecnología generando nuevas ventajas y nuevas vulnerabilidades en seguridad para lo cual se propone un nuevo modelo de red obteniendo los siguientes resultados experimentales que demuestran que tuvo una mejora en reducir las vulnerabilidades contra ataques de bots conocidos y desconocidos. Al igual que el artículo de (Castaño, y otros, 2021) que nos dice que los sistemas de seguridad física son menos afectados en cuanto a vulneraciones por terceros gracias a al avance en la tecnología y al IoT, con el objetivo de identificar elementos usados para los sistemas de seguridad física y IoT que sean capaces de destacar las ventajas y limitaciones en un sistema de

seguridad basado en Iot. Además del artículo de (Deebak, y otros, 2020) que se enfoca en proporcionar una seguridad flexible con un protocolo de autentificación y cifrado para resistir la vulnerabilidad de los ataques. El resultado muestra que resistente a múltiples adversarios móviles; y, por lo tanto, garantiza la entrega de múltiples rutas y la seguridad. Así como también el artículo de (Sani, y otros, 2019) que nos plantea que frente a las vulnerabilidades plantean un marco de seguridad cibernética capaz de proporcionar seguridad y privacidad adecuadas utilizando mecanismos de seguridad basados en la identidad, teniendo como resultados que nuestro marco propuesto proporciona mejoras de seguridad y privacidad basada en IoT, es resistente contra muchos ataques de seguridad y es superior a los esquemas relacionados existentes. Al igual que el artículo de (Chu, y otros, 2021) que nos habla de la nueva era de la tecnología y hace referencia al uso de IoT por parte de las empresas para su desarrollo al igual que las amenazas que encontramos por lo que el artículo plantea una premisa por la necesidad de los sistemas de seguridad usados para, evaluar riesgos y prevenir virus de manera oportuna. Por lo que la gestión debe fortalecerse desde los aspectos técnicos hasta los legales. Así como el artículo de (Díaz, 2019) nos dice que la sociedad es cada vez más dependiente de las tecnologías. Es común en las ciudades el monitoreo por cámaras o dispositivos y sensores. Este artículo señala los riesgos que tiene las tecnologías IoT, cuyo crecimiento va de la mano con las vulnerabilidades, por el aumento de ataques a los sistemas de seguridad denegando un servicio distribuido y otras vulnerabilidades que se relaciona con IoT. Así como el artículo de (eshta, 2022) quienes plantean que la tecnología y el objeto en la nube está recibiendo atención en las instituciones. El objetivo de esta tesis se basa en el estudio de los esenciales inconvenientes de seguridad y privacidad IoT impulsada por IA (inteligencia artificial) y sugerir cómo abordar adecuadamente estos problemas. Para el estudio se recopiló información de diversas fuentes. Mostrando crecimiento de IoT impulsado por IA, creando inseguridad entre los usuarios. El estudio recomienda tener un estándar arquitectónico bien definido que garantice la privacidad. Así como el artículo de (Guerra, y otros, 2021) Que tienen como objetivo insertar un sistema que gestione la información y cree un precedente en metodologías capaces de identificar y analizar el riesgo que se da en el transcurso de sucesos bibliotecarios. Los resultados obtenidos del cálculo de riesgos

intrínsecos y efectivos demuestran la presencia de medidas de protección y evalúan los impactos. concluyendo que la combinación de lo propuesto para desplegar el control y evaluación de índices en la calidad, optimiza el sistema de gestión de seguridad de la información (SGSI).

En relación al quinto objetivo específico Mejorar el nivel de satisfacción del usuario con el sistema nuestra investigación arrojo como resultado que con el sistema basado en internet of thinks se mejora la satisfacción del usuario; De acuerdo con el artículo de (Bravo, y otros, 2018) que tuvo como propósito analizar la aceptación pública a las tecnologías que reconocen rostros basada en IoT como medida de seguridad. Mostrando que tuvo un 50% de aceptación como medida de seguridad. Al igual que el artículo de (Singh, y otros, 2020) que con la inserción de un sistema de vigilancia basado en IoT, ayuda a mejorar la satisfacción del doliente y mitigar el costo, concluyendo que la implementación adecuada de esta tecnología, ayuda y da soporte a investigadores, médicos y gobiernos que pueden crear un mejor ambiente para luchar contra esta enfermedad COVID-19. Así como el artículo de (Jaigirdar, y otros, 2021) nos dice que para una aplicación basada en IoT sea exitosa depende de la precisión y la recopilación de numerosas fuentes de información. Sin embargo, la naturaleza altamente dinámica de la red IoT impide el establecimiento de perímetros de seguridad claros y dificulta la comprensión de los aspectos de seguridad. En este documento, discutimos la importancia de agregar metadatos de seguridad en un gráfico de procedencia de datos. Proponemos un nuevo modelo de procedencia de IoT, Prov-IoT (modelo de procedencia IoT), que documenta el historial de los registros de datos teniendo en cuenta el procesamiento y la agregación de datos junto con los metadatos de seguridad para permitir una base para la confianza en los datos. Dando como resultados que es beneficioso para descubrir fallas o intrusiones en el sistema lo cual mejora la satisfacción del usuario con el sistema de seguridad.

VI. CONCLUSIONES

6.1 Se logro mejorar significativamente la seguridad física en la empresa Dr. PC con la inserción de un sistema que se basa en IoT con respecto a al tiempo, seguridad y satisfacción del usuario.

6.2 Se logro mejorar el tiempo de activación de dispositivos de seguridad (puertas de acceso y alarmas de la empresa) en la empresa Dr. PC en un 94.13% posterior a la implementación del sistema basado en internet of thinks, con p valor de (0.000) menor al nivel de significancia (0.05).

6.3 Se logro mejorar el tiempo de comprobación de acceso de seguridad en la empresa Dr. PC en un 96.08% posterior a la implementación del sistema basado en internet of thinks, demostrado con p valor (0.000) menor al nivel de significancia (0.05).

6.4 Se logro mejorar él envió de alertas de incidencias en la empresa Dr. PC reduciendo el tiempo en un 98.84% utilizando el sistema basado en IoT posterior a la implementación del sistema basado en internet of thinks, con p valor de (0.000) menor al nivel de significancia (0.05).

6.5 Se logró reducir la vulnerabilidad de los accesos de seguridad en la empresa Dr. PC en un 83.30%, lo cual se logró utilizando el sistema basado en IoT posterior a la implementación del sistema basado en internet of thinks, con un p valor de (0.000) menor al nivel de significancia (0.05).

6.6 Se logro mejorar el nivel de satisfacción del usuario (directivos y responsables de seguridad) en la empresa Dr. PC en un 53.93% posterior a la implementación del sistema basado en internet of thinks, demostrado con un p valor de (0.000) menor al nivel de significancia (0.05).

VII. RECOMENDACIONES

7.1 Se recomienda a la empresa Dr. PC gestionar sistemas de seguridad de información para reforzar la integridad de datos dentro de la empresa complementando a la seguridad física existente y así ayudar a mejorar los procesos en la empresa.

7.2 Se recomienda usar dispositivos de calidad que garanticen el buen funcionamiento en seguridad para así no tener inconvenientes en la empresa sabemos que en el mercado hay una gran gama de productos por lo que siempre se debe hacer una investigación comparativa para ver los mejores y así aplicarlos en la empresa.

7.3 Se recomienda que para la comprobación de accesos también se puedan incluir indicadores que detecten el rostro de las personas e incluso el sistema pueda conectar a una base de datos de la RENIEC y así el sistema sea capaz de identificar el nombre de la persona que realice una intrusión en el sistema de seguridad.

7.4 Se recomienda usar herramientas que ofrezcan múltiples rutas para poder enviar las alertas de incidencias garantizando así él envió de la información a los responsables de seguridad dentro de la compañía.

7.5 Se recomienda utilizar claves para los clientes con un alto nivel de complejidad además de incluir protocolos de autenticación de datos que ayuden a reducir las vulneraciones en la seguridad física al igual que implementar más protocolos con respecto a la seguridad técnica y administrativa en todo el entorno de la empresa.

7.6 Se recomienda establecer estrategias para poder identificar los requerimientos o necesidades de los usuarios mediante metodologías agiles para establecer soluciones que garanticen la seguridad dentro del entorno de trabajo. Además de capacitar a los trabajadores para tomar mejores decisiones de manera que mejore las estrategias que tiene la empresa para las diferentes áreas de trabajo.

REFERENCIAS

Agudelo, Darly Mildred Delgado, y otros. 2019. ProQuest. [En línea] Enero de 2019. https://www.proquest.com/docview/2195126457.

Al, Turjman Fadi y Deebak, B.D. 2020. SciencieDirect. [En línea] febreo de 2020. https://www.sciencedirect.com/science/article/pii/S1570870519305050?via%3Dihub.

Alqahtani, Fayez, y otros. 2020. ScienceDirect. [En línea] 15 de enero de 2020. https://www.sciencedirect.com/science/article/pii/S0140366419312459?via%3Dihub.

Angulo, Guiza Leonardo y Pabón, Jaimes Carlos Daniel. 2019. repositorio institucional Universidad Autónoma de Bucaramanga. [En línea] 31 de mayo de 2019. http://hdl.handle.net/20.500.12749/7035.

Babar, Muhammad, Tariq, Muhammad Usman y Jan, Mian Ahmad. 2020. SciencieDirect. [En línea] noviembre de 2020. https://www.sciencedirect.com/science/article/pii/S2210670720305904?via%3Dihub.

Balakrishnan, Nagaraj, y otros. 2021. ScienceDirect. [En línea] junio de 2021. https://www.sciencedirect.com/science/article/pii/S2542660519301957?via%3Dihub.

—. 2021. ScienceDirect. [En línea] junio de 2021. https://www.sciencedirect.com/science/article/pii/S2542660519301957?via%3Dihub.

Balla, Prashanth Balraj y Jadhao, K. T. 2018. IEEE Xplore. [En línea] 19 de Noviembre de 2018. https://ieeexplore.ieee.org/document/8537344.

Belenguer, Aitor, Navaridas, Javier y Pascual, Jose A. 2022. arXiv. [En línea] 26 de abril de 2022. https://arxiv.org/abs/2204.12443.

Beltrán, Canessa Pedro Oswaldo. 2018. Repositorio Digital de la Universidad Cesar Vallejo. [En línea] 2018. https://hdl.handle.net/20.500.12692/33677.

Botero, Ochoa Luis Carlos. 2019. Repositorio de la Universidad Nacional Abierta y a Distancia UNAD. [En línea] 17 de 07 de 2019. https://repository.unad.edu.co/handle/10596/27409.

Bravo, Cristián J. y Ramírez, Patricio E. 2018. Scielo. [En línea] Marzo de 2018. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642018000200115&lng=en&nrm=iso&tlng=en.

—. 2018. Scielo. [En línea] Marzo de 2018. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642018000200115&lng=en&nrm=iso&tlng=en.

Carreras, Alma Brenda Leyva, Blanco, Joel Enrique Espejel y Arroyo, Judith Cavazos. 2020. REvistas UNAL. *Revista de la universidad nacional de Colombia.* [En línea] 07 de abril de 2020. https://revistas.unal.edu.co/index.php/innovar/article/view/85192.

Castaño, Gómez M, López, Echeverr A M y Villa, Sánchez PA. 2021. ingenieria y competitvidad revista cientifica y tecnologica. [En línea] 30 de octubre de 2021. [Citado el: 27 de abril de 2022.] https://revistaingenieria.univalle.edu.co/index.php/ingenieria_y_competitividad/article/view/11034.

Castaño, Gómez Mauricio,, López Echeverry, AM, y PA., Villa Sánchez. 2021. ingenieria y competitvidad revista cientifica y tecnologica. [En línea] 30 de octubre de 2021. [Citado el: 27 de abril de 2022.] https://revistaingenieria.univalle.edu.co/index.php/ingenieria_y_competitividad/article/view/11034.

Chu, Mingde y Song, Yufei. 2021. IEEE Xplore. [En línea] 13 de Noviembre de 2021. https://ieeexplore.ieee.org/document/9590786.

Cuervo, Maycol Alexander Segura y Lara, Jairo Alonso Mesa. 2018. INGENIERÍA SOLIDARIA. [En línea] Enero de 2018. https://revistas.ucc.edu.co/index.php/in/article/view/2160.

Decreto Supremo que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030. El Peruano. [En línea] https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-la-politica-nacional-de-moderniz-decreto-supremo-n-103-2022-pcm-2097747-1/.

Decreto Supremo que aprueba la Política Nacional Multisectorial de Seguridad Ciudadana al 2030. El Peruano. [En línea] https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-la-politica-nacional-multisector-decreto-supremo-n-006-2022-in-2079733-

1/#:~:text=N%C2%BA%20006%2D2022%2DIN&text=Apru%C3%A9base%20la%20Pol%C3%ADtica%20Nacional%20Multisectorial,segur.

Deebak, B.D. y Turjman, Fadi Al. 2020. SciencieDirect. [En línea] febreo de 2020. https://www.sciencedirect.com/science/article/pii/S1570870519305050?via%3Dihub.

Deroncele, Acosta Angel. 2022. SciELO. [En línea] 10 de Febrero de 2022. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202022000100102&lng=es&nrm=iso.

Díaz, Jairo Márquez. 2019. SciELO. [En línea] 01 de Octubre de 2019. https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872019000200006&lng=es&nrm=iso.

eshta, IsmailK. 2022. ScienceDirect. [En línea] 2022. https://www.sciencedirect.com/science/article/pii/S2352914822000545.

Estrada, Bolívar Luis Bernardo. 2021. Repositorio Institucional de la Universidad de Antioquia. [En línea] 2021. https://hdl.handle.net/10495/21530.

Fayez, Alqahtani, y otros. 2020. ScienceDirect. [En línea] 15 de enero de 2020. https://www.sciencedirect.com/science/article/pii/S0140366419312459?via%3Dihub.

Febres, Ramos Richard J. y Mercado, Rey Miguel R. 2020. Scielo. [En línea] 2020. http://www.scielo.org.pe/scielo.php?pid=S2308-05312020000300397&script=sci_arttext.

Figueroa, Suárez Juan A., y otros. 2018. Polo del conocimiento. [En línea] 2018. https://polodelconocimiento.com/ojs/index.php/es/article/view/420.

García, Herrera José Yon Frans. 2018. repositorio institucional Universidad Autónoma de Bucaramanga. [En línea] noviembre de 2018. http://hdl.handle.net/20.500.12749/3545.

Gómez, Vieites Álvaro. 2022. *Auditoría de seguridad informática.* Bogotá : s.n., 2022.

Guerra, Erick, y otros. 2021. SciELO. [En línea] Octubre de 2021. https://scielo.conicyt.cl/scielo.php?pid=S0718-07642021000500145&script=sci_arttext.

Guías de referencia útiles para la implantación, mantenimiento, auditoría y certificación de los Sistemas de Gestión de la Seguridad de la Información serie 27000. ISO27000.ES. [En línea] https://www.iso27000.es/iso27000.html.

Hernández, Mendoza Cristian Camilo y Layton, Díaz Cristian Camilo. 2021. Repositorio Institucional Universidad Católica de Colombia - RIUCaC. [En línea] 17 de Mayo de 2021. https://hdl.handle.net/10983/26663.

Hong, Seungwan, y otros. 2018. SciencieDirect. [En línea] mayo de 2018. https://www.sciencedirect.com/science/article/abs/pii/S0167739X17308567?via%3Dihub.

Huaranga, Heredia Delly Heidy y Ojeda, Buendía Walter Miguel. 2019. Repositorio de la Universidad César Vallejo. [En línea] 2019. https://hdl.handle.net/20.500.12692/52117.

Instituto Nacional de Estadistica e Informatica. 2022. INEI. [En línea] 29 de Marzo de 2022. https://www.inei.gob.pe/biblioteca-virtual/boletines/estadisticas-de-seguridad-ciudadana/1/.

Jaigirdar, Fariha Tasmin, Rudolph, Carsten y Bain, Chris. 2021. IEEE Xplore. [En línea] 09 de febrero de 2021. https://ieeexplore.ieee.org/document/9343199.

Koohang, Alex, y otros. 2022. ScienceDirect. [En línea] febrero de 2022. https://www.sciencedirect.com/science/article/pii/S0268401221001353#sec0070.

Lata, Navdeep y Kumar, Dr. Raman. 2022. Mathematical Statistician and Engineering Applications. [En línea] 11 de marzo de 2022. http://philstat.org.ph/index.php/MSEA/article/view/68.

—. 2022. MATHEMATICAL STATISTICIAN AND ENGINEERING APPLICATIONS. [En línea] 11 de marzo de 2022. http://philstat.org.ph/index.php/MSEA/article/view/68.

Lee, In. 2019. ScienceDirect. [En línea] septiembre de 2019. https://www.sciencedirect.com/science/article/pii/S2542660519301386?via%3Dihub.

Leyva, Díaz Erick Martin. 2018. Repositorio de la Universidad César Vallejo. [En línea] 2018. https://hdl.handle.net/20.500.12692/34015.

Limahuaya, Paco y Nhewspkki, Jhovy. 2019. Repositorio de Tesis Universidad Peruana Union. [En línea] 02 de diciembre de 2019. http://hdl.handle.net/20.500.12840/2745.

Luna, José Ignacio Vega, Rangel, Francisco Javier Sánchez y Aceves, José Francisco Cosme. 2019. Revista de Ciencia y Tecnología Ingenius. [En línea] diciembre de 2019. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-860X2019000200072.

Manjia, Tahsien Syeda, Hadis, Karimipour y Petros, Spachos. 2020. ScienceDirect. [En línea] julio de 2020. https://www.sciencedirect.com/science/article/pii/S1084804520301041?via%3Dihub.

Manterola, Carlos, y otros. 2019. Revista Médica Clínica Las Condes. [En línea] febrero de 2019. https://www.clinicalkey.es/#!/content/playContent/1-s2.0-S0716864019300057?returnurl=https:%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS0716864019300057%3Fshowall%3Dtrue&referrer=.

Mashkoor, Atif, Egyed, Alexander y Wille, Robert. 2020. arXiv. [En línea] 17 de abril de 2020. https://arxiv.org/abs/2004.08471.

Mbarek, Bacem, Ge, Mouzhi y Pitner, Tomáš. 2020. ScienceDirect. [En línea] marzo de 2020. https://www.sciencedirect.com/science/article/pii/S2542660520300032?via%3Dihub.

—. 2020. ScienceDirect. [En línea] marzo de 2020. https://www.sciencedirect.com/science/article/pii/S2542660520300032?via%3Dihub.

Memos, Vasileios A., Psannis, Kostas y Lv, Zhihan. 2022. IEEE Transactions on Industrial Informatics. [En línea] 29 de Marzo de 2022. https://ieeexplore.ieee.org/document/9744453.

—. 2022. IEEE Transactions on Industrial Informatics. [En línea] 29 de Marzo de 2022. https://ieeexplore.ieee.org/document/9744453.

Mendoza, Domínguez Esly Lorena. 2021. Repositorio Universidad Abierta y a Distancia. [En línea] 12 de Octubre de 2021. [Citado el: 29 de Abril de 2022.] https://repository.unad.edu.co/handle/10596/47752.

Mendoza, Gallardo Judith, Rodríguez, Picón Luis Alberto y Méndez, González Luis Carlos. 2021. Cultura Científica Y Tecnológica. [En línea] agosto de 2021. https://erevistas.uacj.mx/ojs/index.php/culcyt/article/view/3983.

Miloslavskaya, Natalia y Tolstoy, Alexander. 2019. springer link. [En línea] 15 de marzo de 2019. https://link.springer.com/article/10.1007/s10586-018-2823-6.

—. 2019. Springer Link. [En línea] 15 de marzo de 2019. https://link.springer.com/article/10.1007/s10586-018-2823-6.

Montilla, Malaver Leonardo. 2020. Repositorio de la Universidad Nacional Abierta y a Distancia. [En línea] 04 de Junio de 2020. https://repository.unad.edu.co/handle/10596/34638.

Montoya, Correa Tatiana y Molano, Luján Andrés. 2018. Repositorio Institucional ITM. [En línea] 2018. https://repositorio.itm.edu.co/handle/20.500.12622/433.

Mosemann, Faith. 2022. the institucional repository Liberty University. [En línea] abril de 2022. https://digitalcommons.liberty.edu/honors/1182.

Nižetić, Sandro, y otros. 2020. scienceDirect. [En línea] 20 de Noviembre de 2020. https://www.sciencedirect.com/science/article/pii/S095965262032922X?via%3Dihub.

Noor, Mardiana binti Mohamad y Hassan, Wan Haslina. 2019. ScienceDirect. [En línea] 15 de enero de 2019. https://www.sciencedirect.com/science/article/pii/S1389128618307035?via%3Dihub.

Norbert, Elias. 2021. *Sobre el tiempo.* 2021.

Pal, Souvik, De, Debashis y Buyya, Rajkumar. 2022. SpringerLink. [En línea] 2022. https://link.springer.com/book/10.1007/978-3-030-87059-1.

Paredes, Floril Priscilla Rossana y Santos, Ortiz Edgar Daniel. 2022. Revista Angolana de Ciencias RAC. [En línea] 22 de 06 de 2022. http://publicacoes.scientia.co.ao/ojs2/index.php/rac/article/view/244.

Pastas, Pastaz Jonathan Sebastian y Pujos, Tualombo Jonathan Fernando. 2022. Repositorio Institucional de la Universidad Politécnica Salesiana-Ecuador. [En línea] marzo de 2022. http://dspace.ups.edu.ec/handle/123456789/22245.

Quichimbo, Angamarca Edwin Fernando. 2022. Repositorio Digital Universidad Catolica de Santiago de Guayaquil. [En línea] 11 de marzo de 2022. http://repositorio.ucsg.edu.ec/handle/3317/17874.

Qureshi, Kashif Naseer, y otros. 2021. ScienceDirect. [En línea] julio de 2021. https://www.sciencedirect.com/science/article/pii/S0045790621002585?via%3Dihub.

—. 2021. ScienceDirect. [En línea] julio de 2021. https://www.sciencedirect.com/science/article/pii/S0045790621002585?via%3Dihub.

Rasim, Alguliyev, Yadigar, Imamverdiyev y Lyudmila, Sukhostat. 2018. ScienceDirect. [En línea] septiembre de 2018. https://www.sciencedirect.com/science/article/pii/S0166361517304244?via%3Dihub.

Sani, Abubakar Sadiq, y otros. 2019. ScienceDirect. [En línea] Abril de 2019. https://www.sciencedirect.com/science/article/abs/pii/S0167739X1730660X?via%3Dihub.

Sani, bubakar Sadiq, y otros. 2019. ScienceDirect. [En línea] abril de 2019. https://www.sciencedirect.com/science/article/abs/pii/S0167739X1730660X?via%3Dihub.

Santos, Chorres Farias Deyvis y Kleyber, Sánchez Carrión Hardy. 2021. Repositorio de la Universidad César Vallejo. [En línea] 2021. https://hdl.handle.net/20.500.12692/62192.

Sarker, Iqbal H., y otros. 2022. Springer Link. [En línea] 14 de March de 2022. https://link.springer.com/article/10.1007/s11036-022-01937-3.

Sebastián, Rodríguez Rengifo Juan y Cristina, Quintero Sepulveda Isabel. 2022. *Universidad Nacional de Colombia.* [En línea] 31 de diciembre de 2022. https://revistas.unlp.edu.ar/CADM/article/view/10337.

Sengupta, Jayasree, Ruj, Sushmita y Bit, Sipra Das. 2020. SciencieDirect. [En línea] 01 de enero de 2020. https://www.sciencedirect.com/science/article/pii/S1084804519303418?via%3Dihub.

Sha, Kewei, y otros. 2018. ScienceDirect. [En línea] junio de 2018. https://www.sciencedirect.com/science/article/abs/pii/S0167739X17324883?via%3Dihub.

Singh, Ravi Pratap, y otros. 2020. SciencieDirect. [En línea] julio-agosto de 2020. https://www.sciencedirect.com/science/article/pii/S1871402120301065?via%3Dihub.

—. 2020. SciencieDirect. [En línea] julio-agosto de 2020. https://www.sciencedirect.com/science/article/pii/S1871402120301065?via%3Dihub.

Singh, Sushil Kumar, Jeong, Young Sik y Park, Jong Hyuk. 2020. SciencieDirect. [En línea] septiembre de 2020. https://www.sciencedirect.com/science/article/pii/S221067072030473X?via%3Dihub.

Smith, Rueda Rueda Johan. 2018. repositorio institucional Universidad Autónoma de Bucaramanga- Colombia. [En línea] mayo de 2018. http://hdl.handle.net/20.500.12749/3552.

Suárez, Andrés Camilo Morales, Ávila, Shayther Stewar Díaz y Páez, Miguel Ángel Leguizamón. 2019. Revista Vinculos. [En línea] 19 de 12 de 2019. https://revistas.udistrital.edu.co/index.php/vinculos/article/view/15758.

Toledo, Manuel Rogelio Nevárez, Ortiz, Verónica Yánez y Vélez, Walter Francisco Mecía. 2019. ProQuest. [En línea] 2019. https://www.proquest.com/docview/2305092013.

—. 2019. ProQuest. [En línea] 2019. https://www.proquest.com/docview/2305092013.

Vega, Luna José Ignacio, Sánchez, Rangel Francisco Javier y Cosme, Aceves José Francisco. 2019. Scielo. [En línea] diciembre de 2019. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-860X2019000200072.

Vinicio, Mejía Vayas Carlos y Maribel, Guapisaca Guamán Jissenia. 2020. Repositorio Universidad Técnica de Ambato. [En línea] febrero de 2020. https://repositorio.uta.edu.ec/jspui/handle/123456789/31145.

Yang, Xing, y otros. 2022. IEEE Transactions on Industrial Informatics. [En línea] 07 de January de 2022. https://ieeexplore.ieee.org/document/9674793.

Zambrano, Ana, y otros. 2019. ProQuest. [En línea] Abril de 2019. https://www.proquest.com/docview/2260411368.

Zuña, Macancela Edgar René, y otros. 2019. Scielo. [En línea] 2019. http://scielo.sld.cu/scielo.php?pid=S2218-36202019000400487&script=sci_arttext&tlng=en.

ANEXOS

Anexo N°1: Operacionalización de variables

Tabla N°

Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición
Variable independiente Sistema basado en internet of thinks	Constituyen un concepto que hace referencia a la conectividad entre objetos físicos, la capacidad de estos para transferir datos a través de una red y que sea de forma autómata (Quichimbo, 2022).	Sistema de dispositivos de computación interrelacionados, máquinas mecánicas y digitales y objetos, que tienen identificadores únicos y la capacidad de transferir datos a través de una red, sin requerir de interacciones humano a humano (Estrada, 2021). Mediante el sistema basado en IoT se evalúa la funcionalidad respecto a un algoritmo de caja negra.	Funcionalidad	Prueba de caja negra	De razón
Variable dependiente Seguridad física	El término seguridad física se emplea frecuentemente para referirse a las medidas de protección externas. Las cuales se implementan mediante dispositivos eléctricos, electrónicos, etc. (Montilla, 2020).	La seguridad física se refiere a la identificación y análisis de las amenazas y riesgos que enfrentan o pueden llegar a enfrentar instalaciones, bienes y procesos a fin de implementar planes y sistemas tendientes a prevenir, dificultar o limitar los resultados de las posibles acciones dañinas contra la seguridad física (Botero, 2019). La variable se medirá de acuerdo a la dimensión tiempo,	Tiempo	Tiempo de activación de dispositivos de seguridad. P4	De razón
				Tiempo de comprobación de acceso de seguridad. P2, P3, P5	
				Tiempo de envió de alertas de incidencias. P6	
			Seguridad	Cantidad de ataques por día. P1, P7, P9, P10, P11	
			Satisfacción	Nivel de satisfacción del	Ordinal

		seguridad y satisfacción, mediante las guías de observación y la encuesta a los colaboradores de la empresa Dr. PC.		usuario con el sistema. P8	

Anexo N°2: Guías de observación

Guía de Observación para Medir el Tiempo de activación de dispositivos Pre-Test

Dia	Fecha/hora Inicio	Fecha/hora Fin	Tiempo medido	observaciones
1	8:00 a.m.	8:10 a.m.	60	
2	8:10 a.m.	8:20 a.m.	50	
3	8:30 a.m.	8:40 a.m.	55	
4	9:00 a.m.	9:10 a.m.	48	
5	9:20 a.m.	9:30 a.m.	55	
6	10:30 a.m.	10:40 a.m.	60	
7	10:00 a.m.	10:15 a.m.	56	
8	11:05 a.m.	11:20 a.m.	53	
9	8:25 a.m.	8:40 a.m.	60	
10	9:10 a.m.	9:23 a.m.	45	
11	10:15 a.m.	10:30 a.m.	50	
12	11:05 a.m.	11:15 a.m.	52	
13	11:45 a.m.	12:00 p.m.	49	
14	2:05 p.m.	2:20 p.m.	40	
15	2:10 p.m.	2:23 p.m.	38	
16	3:30 p.m.	3:42 p.m.	40	
17	5:10 p.m.	5:25 p.m.	39	
18	6:05 p.m.	6:17 p.m.	47	
19	5:02 p.m.	5:12 p.m.	46	
20	4:00 p.m.	4:15 p.m.	51	
21	7:30 a.m.	7:40 a.m.	50	
22	8:00 p.m.	8:13 p.m.	45	
23	3:45 p.m.	4:00 p.m.	48	
24	5:05 p.m.	5:20 p.m.	58	
25	7:03 p.m.	7:13 p.m.	53	
26	8:10 a.m.	8:23 a.m.	49	
27	9:02 a.m.	9:13 a.m.	47	
28	10:50 a.m.	11:00 a.m.	35	
29	6:43 p.m.	7:00 p.m.	47	
30	8:19 a.m.	8:29 a.m.	40	

Guía de Observación para Medir el Tiempo de activación de dispositivos Post-Test

Dia	Fecha/hora Inicio	Fecha/hora Fin	Tiempo medido	observaciones
1	8:00 a.m.	8:10 a.m.	3	
2	8:10 a.m.	8:20 a.m.	4	
3	8:30 a.m.	8:40 a.m.	2	
4	9:00 a.m.	9:10 a.m.	3	
5	9:20 a.m.	9:30 a.m.	4	
6	10:30 a.m.	10:40 a.m.	5	
7	10:00 a.m.	10:15 a.m.	3	
8	11:05 a.m.	11:20 a.m.	1	
9	8:25 a.m.	8:40 a.m.	3	
10	9:10 a.m.	9:23 a.m.	4	
11	10:15 a.m.	10:30 a.m.	5	
12	11:05 a.m.	11:15 a.m.	2	
13	11:45 a.m.	12:00 p.m.	5	
14	2:05 p.m.	2:20 p.m.	3	
15	2:10 p.m.	2:23 p.m.	3	
16	3:30 p.m.	3:42 p.m.	2	
17	5:10 p.m.	5:25 p.m.	1	
18	6:05 p.m.	6:17 p.m.	2	
19	5:02 p.m.	5:12 p.m.	1	
20	4:00 p.m.	4:15 p.m.	4	
21	7:30 a.m.	7:40 a.m.	2	
22	8:00 p.m.	8:13 p.m.	3	
23	3:45 p.m.	4:00 p.m.	3	
24	5:05 p.m.	5:20 p.m.	4	
25	7:03 p.m.	7:13 p.m.	2	
26	8:10 a.m.	8:23 a.m.	3	
27	9:02 a.m.	9:13 a.m.	1	
28	10:50 a.m.	11:00 a.m.	2	
29	6:43 p.m.	7:00 p.m.	3	
30	8:19 a.m.	8:29 a.m.	3	

Guía de Observación para Medir el Tiempo de comprobación de acceso de seguridad Pre-Test

Dia	Fecha/hora Inicio	Fecha/hora Fin	Tiempo medido	observaciones
1	9:10 a.m.	9:23 a.m.	70	
2	10:15 a.m.	10:30 a.m.	60	
3	11:05 a.m.	11:15 a.m.	50	
4	11:45 a.m.	12:00 p.m.	56	
5	2:05 p.m.	2:20 p.m.	65	
6	2:10 p.m.	2:23 p.m.	80	
7	3:30 p.m.	3:42 p.m.	71	
8	5:10 p.m.	5:25 p.m.	68	
9	6:05 p.m.	6:17 p.m.	63	
10	5:02 p.m.	5:12 p.m.	59	
11	4:00 p.m.	4:15 p.m.	58	
12	7:30 a.m.	7:40 a.m.	60	
13	8:00 p.m.	8:13 p.m.	74	
14	3:45 p.m.	4:00 p.m.	62	
15	8:00 a.m.	8:10 a.m.	51	
16	8:10 a.m.	8:20 a.m.	63	
17	8:30 a.m.	8:40 a.m.	56	
18	9:00 a.m.	9:10 a.m.	71	
19	9:20 a.m.	9:30 a.m.	65	
20	10:30 a.m.	10:40 a.m.	56	
21	10:00 a.m.	10:15 a.m.	72	
22	11:05 a.m.	11:20 a.m.	68	
23	8:25 a.m.	8:40 a.m.	52	
24	5:05 p.m.	5:20 p.m.	61	
25	7:03 p.m.	7:13 p.m.	75	
26	8:10 a.m.	8:23 a.m.	73	
27	9:02 a.m.	9:13 a.m.	59	
28	10:50 a.m.	11:00 a.m.	50	
29	6:43 p.m.	7:00 p.m.	54	
30	10:30 a.m.	10:35 a.m.	67	

Guía de Observación para Medir el Tiempo de comprobación de acceso de seguridad Post-Test

Dia	Fecha/hora Inicio	Fecha/hora Fin	Tiempo medido	observaciones
1	9:10 a.m.	9:23 a.m.	2	
2	10:15 a.m.	10:30 a.m.	4	
3	11:05 a.m.	11:15 a.m.	4	
4	11:45 a.m.	12:00 p.m.	3	
5	2:05 p.m.	2:20 p.m.	3	
6	2:10 p.m.	2:23 p.m.	1	
7	3:30 p.m.	3:42 p.m.	2	
8	5:10 p.m.	5:25 p.m.	4	
9	6:05 p.m.	6:17 p.m.	3	
10	5:02 p.m.	5:12 p.m.	2	
11	4:00 p.m.	4:15 p.m.	4	
12	7:30 a.m.	7:40 a.m.	1	
13	8:00 p.m.	8:13 p.m.	3	
14	3:45 p.m.	4:00 p.m.	3	
15	8:00 a.m.	8:10 a.m.	1	
16	8:10 a.m.	8:20 a.m.	2	
17	8:30 a.m.	8:40 a.m.	4	
18	9:00 a.m.	9:10 a.m.	3	
19	9:20 a.m.	9:30 a.m.	1	
20	10:30 a.m.	10:40 a.m.	1	
21	10:00 a.m.	10:15 a.m.	2	
22	11:05 a.m.	11:20 a.m.	4	
23	8:25 a.m.	8:40 a.m.	3	
24	5:05 p.m.	5:20 p.m.	1	
25	7:03 p.m.	7:13 p.m.	2	
26	8:10 a.m.	8:23 a.m.	3	
27	9:02 a.m.	9:13 a.m.	3	
28	10:50 a.m.	11:00 a.m.	2	
29	6:43 p.m.	7:00 p.m.	1	
30	10:30 a.m.	10:35 a.m.	2	

Guía de Observación para Medir el Tiempo de envió de alertas de incidencias Pre-Test

Dia	Fecha/hora Inicio	Fecha/hora Fin	Tiempo medido	observaciones
1	3:45 p.m.	4:00 p.m.	300	
2	8:00 a.m.	8:10 a.m.	240	
3	8:10 a.m.	8:20 a.m.	280	
4	8:30 a.m.	8:40 a.m.	600	
5	9:00 a.m.	9:10 a.m.	600	
6	9:20 a.m.	9:30 a.m.	480	
7	10:30 a.m.	10:40 a.m.	540	
8	10:00 a.m.	10:15 a.m.	300	
9	11:05 a.m.	11:20 a.m.	360	
10	8:25 a.m.	8:40 a.m.	180	
11	5:05 p.m.	5:20 p.m.	360	
12	7:03 p.m.	7:13 p.m.	240	
13	8:10 a.m.	8:23 a.m.	480	
14	9:02 a.m.	9:13 a.m.	180	
15	10:50 a.m.	11:00 a.m.	300	
16	6:43 p.m.	7:00 p.m.	280	
17	6:05 p.m.	6:17 p.m.	360	
18	5:02 p.m.	5:12 p.m.	600	
19	4:00 p.m.	4:15 p.m.	180	
20	7:30 a.m.	7:40 a.m.	600	
21	8:00 p.m.	8:13 p.m.	300	
22	9:10 a.m.	9:23 a.m.	480	
23	10:15 a.m.	10:30 a.m.	540	
24	11:05 a.m.	11:15 a.m.	300	
25	11:45 a.m.	12:00 p.m.	180	
26	2:05 p.m.	2:20 p.m.	480	
27	2:10 p.m.	2:23 p.m.	360	
28	3:30 p.m.	3:42 p.m.	300	
29	5:10 p.m.	5:25 p.m.	360	
30	6:20 p.m.	6:40 p.m.	180	

Guía de Observación para Medir el Tiempo de envió de alertas de incidencias Post-Test

Dia	Fecha/hora Inicio	Fecha/hora Fin	Tiempo medido	observaciones
1	3:45 p.m.	4:00 p.m.	4	
2	8:00 a.m.	8:10 a.m.	5	
3	8:10 a.m.	8:20 a.m.	4	
4	8:30 a.m.	8:40 a.m.	5	
5	9:00 a.m.	9:10 a.m.	4	
6	9:20 a.m.	9:30 a.m.	2	
7	10:30 a.m.	10:40 a.m.	3	
8	10:00 a.m.	10:15 a.m.	5	
9	11:05 a.m.	11:20 a.m.	4	
10	8:25 a.m.	8:40 a.m.	3	
11	5:05 p.m.	5:20 p.m.	4	
12	7:03 p.m.	7:13 p.m.	5	
13	8:10 a.m.	8:23 a.m.	2	
14	9:02 a.m.	9:13 a.m.	4	
15	10:50 a.m.	11:00 a.m.	5	
16	6:43 p.m.	7:00 p.m.	3	
17	6:05 p.m.	6:17 p.m.	3	
18	5:02 p.m.	5:12 p.m.	5	
19	4:00 p.m.	4:15 p.m.	2	
20	7:30 a.m.	7:40 a.m.	5	
21	8:00 p.m.	8:13 p.m.	3	
22	9:10 a.m.	9:23 a.m.	4	
23	10:15 a.m.	10:30 a.m.	3	
24	11:05 a.m.	11:15 a.m.	5	
25	11:45 a.m.	12:00 p.m.	3	
26	2:05 p.m.	2:20 p.m.	3	
27	2:10 p.m.	2:23 p.m.	4	
28	3:30 p.m.	3:42 p.m.	3	
29	5:10 p.m.	5:25 p.m.	5	
30	6:20 p.m.	6:40 p.m.	2	

Guía de Observación para Medir la Cantidad de Ataques por Día Pre-Test

Dia	Fecha/hora Inicio	Fecha/hora Fin	Cantidad de Ataques	observaciones
1	11:05 a.m.	11:10 a.m.	2	
2	11:55 a.m.	12:00 p.m.	5	
3	2:05 p.m.	2:12 p.m.	7	
4	2:10 p.m.	2:23 p.m.	8	
5	3:30 p.m.	3:35 p.m.	5	
6	5:10 p.m.	5:15 p.m.	5	
7	3:50 p.m.	4:00 p.m.	8	
8	8:00 a.m.	8:10 a.m.	3	
9	8:10 a.m.	8:20 a.m.	4	
10	8:30 a.m.	8:40 a.m.	6	
11	9:00 a.m.	9:10 a.m.	1	
12	9:20 a.m.	9:30 a.m.	5	
13	10:30 a.m.	10:40 a.m.	6	
14	10:00 a.m.	10:15 a.m.	4	
15	11:05 a.m.	11:20 a.m.	7	
16	8:25 a.m.	8:35 a.m.	3	
17	5:05 p.m.	5:15 p.m.	5	
18	7:03 p.m.	7:13 p.m.	2	
19	8:10 a.m.	8:15 a.m.	5	
20	9:02 a.m.	9:07 a.m.	5	
21	10:50 a.m.	11:00 a.m.	7	
22	6:55 p.m.	7:00 p.m.	5	
23	6:05 p.m.	6:10 p.m.	5	
24	5:02 p.m.	5:12 p.m.	8	
25	4:00 p.m.	4:05 p.m.	3	
26	7:30 a.m.	7:40 a.m.	6	
27	8:00 p.m.	8:07 p.m.	7	
28	9:10 a.m.	9:15 a.m.	5	
29	10:15 a.m.	10:20 a.m.	5	
30	11:05 a.m.	11:15 a.m.	2	

Guía de Observación para Medir la Cantidad de Ataques por Día Post-Test

Dia	Fecha/hora Inicio	Fecha/hora Fin	Cantidad de Ataques	observaciones
1	11:05 a.m.	11:10 a.m.	1	
2	11:55 a.m.	12:00 p.m.	2	
3	2:05 p.m.	2:12 p.m.	1	
4	2:10 p.m.	2:23 p.m.	1	
5	3:30 p.m.	3:35 p.m.	1	
6	5:10 p.m.	5:15 p.m.	0	
7	3:50 p.m.	4:00 p.m.	1	
8	8:00 a.m.	8:10 a.m.	0	
9	8:10 a.m.	8:20 a.m.	0	
10	8:30 a.m.	8:40 a.m.	2	
11	9:00 a.m.	9:10 a.m.	1	
12	9:20 a.m.	9:30 a.m.	0	
13	10:30 a.m.	10:40 a.m.	0	
14	10:00 a.m.	10:15 a.m.	1	
15	11:05 a.m.	11:20 a.m.	0	
16	8:25 a.m.	8:35 a.m.	1	
17	5:05 p.m.	5:15 p.m.	2	
18	7:03 p.m.	7:13 p.m.	1	
19	8:10 a.m.	8:15 a.m.	0	
20	9:02 a.m.	9:07 a.m.	2	
21	10:50 a.m.	11:00 a.m.	0	
22	6:55 p.m.	7:00 p.m.	2	
23	6:05 p.m.	6:10 p.m.	1	
24	5:02 p.m.	5:12 p.m.	2	
25	4:00 p.m.	4:05 p.m.	0	
26	7:30 a.m.	7:40 a.m.	0	
27	8:00 p.m.	8:07 p.m.	0	
28	9:10 a.m.	9:15 a.m.	1	
29	10:15 a.m.	10:20 a.m.	0	
30	11:05 a.m.	11:15 a.m.	2	

Anexo N°3: Cuestionario

CUESTIONARIO N°01

CUESTIONARIO PARA CONOCER EL NIVEL DE SATISFACCIÓN DEL USUARIO CON EL SISTEMA DE SEGURIDAD

Somos estudiantes de la universidad cesar vallejo-Tarapoto y estamos ejecutando un trabajo de investigación titulado “Sistema Basado en Internet of Thinks para Mejorar la Seguridad Física en la Empresa Dr. PC Tarapoto, San Martin 2022”, integrados por: Cigüeñas Piña Edwin Alcides, Coronel Dávila Luis Humberto, para tal efecto necesitamos que usted responda lo más veraz posible la siguiente encuesta:

Instrucciones:

Estimados usuarios, el propósito de esta encuesta es saber qué tan satisfecho está con el sistema de seguridad de la empresa Dr. PC, responda a cada pregunta marcando del 1 al 5, siendo 1 el nivel más bajo y 5 el nivel más alto según considere correspondiente a las siguientes preguntas:

Edad _____ Sexo _____(M/F)	1 Muy Bajo	2 Bajo	3 Regular	4 Alto	5 Muy Alto
1.- ¿cómo calificaría usted la seguridad en la empresa?					
2.- ¿Como calificaría usted los equipos instalados para el sistema de seguridad?					
3.- ¿cómo calificaría usted las políticas de seguridad en la empresa?					
4.- ¿cómo calificaría usted el tiempo de activación de dispositivos de seguridad en la empresa?					
5.- ¿cómo calificaría usted el tiempo de comprobación de acceso de seguridad en la empresa?					
6.- ¿cómo calificaría usted el tiempo de envió de alertas de incidencias en la empresa?					
7.- ¿cómo calificaría usted la capacitación de los empleados para prevenir errores de seguridad?					
8.- ¿Cuál es su nivel de satisfacción con el sistema de seguridad en la empresa?					
9.- ¿cómo calificaría usted la inversión de la empresa en seguridad física?					
10.- ¿cómo calificaría usted el conocimiento que tienes sobre los dispositivos de seguridad con los que cuenta la empresa?					
11.- ¿cómo calificarías la seguridad de los usuarios empresariales?					

Anexo N°4: Fichas de validación de juicio de expertos

EXPERTO N°01

VALIDACIÓN DE CONTENIDO DEL CUESTIONARIO PARA CONOCER EL NIVEL DE SATISFACCIÓN DEL USUARIO

INSTRUCCIÓN: A continuación, se le hace llegar el instrumento de recolección de datos (Cuestionario) que permitirá recoger la información en la presente investigación: "Sistema Basado en Internet of Thinks para Mejorar la Seguridad Física en la Empresa Dr. PC Tarapoto, San Martin 2022". Por lo que se le solicita que tenga a bien evaluar el instrumento, haciendo, de ser caso, las sugerencias para realizar las correcciones pertinentes. Los criterios de validación de contenido son:

Criterios	Detalle	Calificación
Suficiencia	El ítem pertenece a la dimensión y basta para obtener la medición de esta	1: de acuerdo 0: en desacuerdo
Claridad	El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1: de acuerdo 0: en desacuerdo
Coherencia	El ítem tiene relación lógica con el indicador que está midiendo	1: de acuerdo 0: en desacuerdo
Relevancia	El ítem es esencial o importante, es decir, debe ser incluido	1: de acuerdo 0: en desacuerdo

Nota. Criterios adaptados de la propuesta de Escobar y Cuervo (2008).

MATRIZ DE VALIDACIÓN DEL CUESTIONARIO DE LA VARIABLE DEPENDIENTE

Definición de la variable: Seguridad Física

Dimensión	Indicador	Ítem	Suficiencia	Claridad	Coherencia	Relevancia	Observación
Tiempo	Tiempo de activación de dispositivos	¿cómo calificaría usted el tiempo de activación de dispositivos de acceso en la empresa?	1	1	1	1	1
	Tiempo de comprobación de acceso de seguridad	¿Como calificaría usted los equipos instalados para el sistema de seguridad?	1	1	1	1	1
		¿cómo calificaría usted las políticas de seguridad en la empresa?	1	1	1	1	1
		¿cómo calificaría usted el tiempo de comprobación de acceso de seguridad en la empresa?	1	1	1	1	1
	Tiempo de envió de alertas de incidencias	cómo calificaría usted el tiempo de envió de alertas de incidencias en la empresa?	1	1	1	1	1
Satisfacción	Reducir la vulnerabilidad de los accesos de seguridad.	¿cómo calificaría usted la capacitación de los empleados para prevenir errores de seguridad?	1	1	1	1	1
		¿cómo calificaría usted la inversión de la empresa en seguridad física?	1	1	1	1	1

		¿cómo calificaría usted el conocimiento que tienes sobre los dispositivos de seguridad con los que cuenta la empresa?	1	1	1	1	1
		¿cómo calificarías la seguridad de los usuarios empresariales?	1	1	1	1	1
	Nivel de satisfacción del usuario con el sistema	¿cómo calificaría usted la seguridad en la empresa?	1	1	1	1	1
		¿Cuál es su nivel de satisfacción con el sistema de seguridad en la empresa?	1	1	1	1	1

Cuestionario para la variable dependiente

CUESTIONARIO PARA CONOCER EL NIVEL DE SATISFACCIÓN DEL USUARIO

Somos estudiantes de la universidad cesar vallejo-Tarapoto y estamos ejecutando un trabajo d investigación titulado "Sistema Basado en Internet of Thinks para Mejorar la Seguridad Física en l Empresa Dr. PC Tarapoto, San Martin 2022", integrados por: Cigüeñas Piña Edwin Alcides, Corone Dávila Luis Humberto, para tal efecto necesitamos que usted responda lo más veraz posible l siguiente encuesta:

Instrucciones:

Estimados usuarios, el propósito de esta encuesta es saber qué tan satisfecho está con el sistem de seguridad de la empresa Dr. PC, responda a cada pregunta marcando del 1 al 5, siendo 1 e nivel más bajo y 5 el nivel más alto según considere correspondiente a las siguientes preguntas:

Edad _____ Sexo _____(M/F)	1	2	3	4	5
1.- ¿cómo calificaría usted la seguridad en la empresa?					
2.- ¿Como calificaría usted los equipos instalados para el sistema de seguridad?					
3.- ¿cómo calificaría usted las políticas de seguridad en la empresa?					
4.- ¿cómo calificaría usted el tiempo de activación de dispositivos de acceso en la empresa?					
5.- ¿cómo calificaría usted el tiempo de comprobación de acceso de seguridad en la empresa?					
6.- cómo calificaría usted el tiempo de envió de alertas de incidencias en la empresa?					
7.- ¿cómo calificaría usted la capacitación de los empleados para prevenir errores de seguridad?					

8.- ¿Cuál es su nivel de satisfacción con el sistema de seguridad en la empresa?					
9.- ¿cómo calificaría usted la inversión de la empresa en seguridad física?					
10.- ¿cómo calificaría usted el conocimiento que tienes sobre los dispositivos de seguridad con los que cuenta la empresa?					
11.- ¿cómo calificarías la seguridad de los usuarios empresariales?					

¡Muchas gracias por su participación!

FICHA DE VALIDACIÓN DE JUICIO DE EXPERTO

Nombre del instrumento	Cuestionario
Objetivo del instrumento	conocer el nivel de satisfacción del usuario con el sistema de seguridad
Nombres y apellidos del experto	Henry Maldonado Flores
Documento de identidad	40705180
Años de experiencia en el área	8 años
Máximo Grado Académico	Ingeniero de Sistemas.
Nacionalidad	Peruano
Institución	Dr. PC SAC
Cargo	Jefe de seguridad
Número telefónico	942457310
Firma	
Fecha	06/07/22

EXPERTO N°02

VALIDACIÓN DE CONTENIDO DEL CUESTIONARIO PARA CONOCER EL NIVEL DE SATISFACCIÓN DEL USUARIO

INSTRUCCIÓN: A continuación, se le hace llegar el instrumento de recolección de datos (Cuestionario) que permitirá recoger la información en la presente investigación: "Sistema Basado en Internet of Thinks para Mejorar la Seguridad Física en la Empresa Dr. PC Tarapoto, San Martin 2022". Por lo que se le solicita que tenga a bien evaluar el instrumento, haciendo, de ser caso, las sugerencias para realizar las correcciones pertinentes. Los criterios de validación de contenido son:

Criterios	Detalle	Calificación
Suficiencia	El ítem pertenece a la dimensión y basta para obtener la medición de esta	1: de acuerdo 0: en desacuerdo
Claridad	El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1: de acuerdo 0: en desacuerdo
Coherencia	El ítem tiene relación lógica con el indicador que está midiendo	1: de acuerdo 0: en desacuerdo
Relevancia	El ítem es esencial o importante, es decir, debe ser incluido	1: de acuerdo 0: en desacuerdo

Nota. Criterios adaptados de la propuesta de Escobar y Cuervo (2008).

MATRIZ DE VALIDACIÓN DEL CUESTIONARIO DE LA VARIABLE DEPENDIENTE

Definición de la variable: Seguridad Física

Dimensión	Indicador	Ítem	Suficiencia	Claridad	Coherencia	Relevancia	Observación
Tiempo	Tiempo de activación de dispositivos	¿cómo calificaría usted el tiempo de activación de dispositivos de acceso en la empresa?	1	1	1	1	1
	Tiempo de comprobación de acceso de seguridad	¿Como calificaría usted los equipos instalados para el sistema de seguridad?	1	1	1	1	1
		¿cómo calificaría usted las políticas de seguridad en la empresa?	1	1	1	1	1
		¿cómo calificaría usted el tiempo de comprobación de acceso de seguridad en la empresa?	1	1	1	1	1
	Tiempo de envió de alertas de incidencias	cómo calificaría usted el tiempo de envió de alertas de incidencias en la empresa?	1	1	1	1	1
Satisfacción	Reducir la vulnerabilidad de los accesos de seguridad.	¿cómo calificaría usted la capacitación de los empleados para prevenir errores de seguridad?	1	1	1	1	1
		¿cómo calificaría usted la inversión de la empresa en seguridad física?	1	1	1	1	1

		¿cómo calificaría usted el conocimiento que tienes sobre los dispositivos de seguridad con los que cuenta la empresa?	1	1	1	1	1
		¿cómo calificarías la seguridad de los usuarios empresariales?	1	1	1	1	1
	Nivel de satisfacción del usuario con el sistema	¿cómo calificaría usted la seguridad en la empresa?	1	1	1	1	1
		¿Cuál es su nivel de satisfacción con el sistema de seguridad en la empresa?	1	1	1	1	1

Cuestionario para la variable dependiente

CUESTIONARIO PARA CONOCER EL NIVEL DE SATISFACCIÓN DEL USUARIO

Somos estudiantes de la universidad cesar vallejo-Tarapoto y estamos ejecutando un trabajo de investigación titulado "Sistema Basado en Internet of Thinks para Mejorar la Seguridad Física en la Empresa Dr. PC Tarapoto, San Martin 2022", integrados por: Cigüeñas Piña Edwin Alcides, Coronel Dávila Luis Humberto, para tal efecto necesitamos que usted responda lo más veraz posible la siguiente encuesta:

Instrucciones:

Estimados usuarios, el propósito de esta encuesta es saber qué tan satisfecho está con el sistema de seguridad de la empresa Dr. PC, responda a cada pregunta marcando del 1 al 5, siendo 1 el nivel más bajo y 5 el nivel más alto según considere correspondiente a las siguientes preguntas:

Edad _____ Sexo _____(M/F)	1	2	3	4	5
1.- ¿cómo calificaría usted la seguridad en la empresa?					
2.- ¿Como calificaría usted los equipos instalados para el sistema de seguridad?					
3.- ¿cómo calificaría usted las políticas de seguridad en la empresa?					
4.- ¿cómo calificaría usted el tiempo de activación de dispositivos de acceso en la empresa?					
5.- ¿cómo calificaría usted el tiempo de comprobación de acceso de seguridad en la empresa?					
6.- cómo calificaría usted el tiempo de envió de alertas de incidencias en la empresa?					
7.- ¿cómo calificaría usted la capacitación de los empleados para prevenir errores de seguridad?					

8.- ¿Cuál es su nivel de satisfacción con el sistema de seguridad en la empresa?					
9.- ¿cómo calificaría usted la inversión de la empresa en seguridad física?					
10.- ¿cómo calificaría usted el conocimiento que tienes sobre los dispositivos de seguridad con los que cuenta la empresa?					
11.- ¿cómo calificarías la seguridad de los usuarios empresariales?					

¡Muchas gracias por su participación!

FICHA DE VALIDACIÓN DE JUICIO DE EXPERTO

Nombre del instrumento	Cuestionario
Objetivo del instrumento	conocer el nivel de satisfacción del usuario
Nombres y apellidos del experto	Johon Jenry Huancas Huamán
Documento de identidad	42745321
Años de experiencia en el área	3 años y 10 meses
Máximo Grado Académico	Maestro en Gestión Pública
Nacionalidad	Peruana
Institución	Oficina de Tecnologías de Información – OTI
Cargo	Responsable de OTI – DIRESA
Número telefónico	971145992
Firma	San Martín GOBIERNO REGIONAL DIRECCIÓN REGIONAL DE SALUD SAN MARTÍN Mg. Johon Jenry Huancas Huamán Ingeniero de Sistemas CIP N° 224623
Fecha	18/10/2022

EXPERTO N°03

VALIDACIÓN DE CONTENIDO DEL CUESTIONARIO PARA CONOCER EL NIVEL DE SATISFACCIÓN DEL USUARIO

INSTRUCCIÓN: A continuación, se le hace llegar el instrumento de recolección de datos (Cuestionario) que permitirá recoger la información en la presente investigación: "Sistema Basado en Internet of Thinks para Mejorar la Seguridad Física en la Empresa Dr. PC Tarapoto, San Martin 2022". Por lo que se le solicita que tenga a bien evaluar el instrumento, haciendo, de ser caso, las sugerencias para realizar las correcciones pertinentes. Los criterios de validación de contenido son:

Criterios	Detalle	Calificación
Suficiencia	El ítem pertenece a la dimensión y basta para obtener la medición de esta	1: de acuerdo 0: en desacuerdo
Claridad	El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1: de acuerdo 0: en desacuerdo
Coherencia	El ítem tiene relación lógica con el indicador que está midiendo	1: de acuerdo 0: en desacuerdo
Relevancia	El ítem es esencial o importante, es decir, debe ser incluido	1: de acuerdo 0: en desacuerdo

Nota. Criterios adaptados de la propuesta de Escobar y Cuervo (2008).

MATRIZ DE VALIDACIÓN DEL CUESTIONARIO DE LA VARIABLE DEPENDIENTE

Definición de la variable: Seguridad Física

Dimensión	Indicador	Ítem	Suficiencia	Claridad	Coherencia	Relevancia	Observación
Tiempo	Tiempo de activación de dispositivos	¿cómo calificaría usted el tiempo de activación de dispositivos de acceso en la empresa?	1	1	1	1	1
	Tiempo de comprobación de acceso de seguridad	¿Como calificaría usted los equipos instalados para el sistema de seguridad?	1	1	1	1	1
		¿cómo calificaría usted las políticas de seguridad en la empresa?	1	1	1	1	1
		¿cómo calificaría usted el tiempo de comprobación de acceso de seguridad en la empresa?	1	1	1	1	1
	Tiempo de envió de alertas de incidencias	cómo calificaría usted el tiempo de envió de alertas de incidencias en la empresa?	1	1	1	1	1
Satisfacción	Reducir la vulnerabilidad de los accesos de seguridad.	¿cómo calificaría usted la capacitación de los empleados para prevenir errores de seguridad?	1	1	1	1	1
		¿cómo calificaría usted la inversión de la empresa en seguridad física?	1	1	1	1	1

		¿cómo calificaría usted el conocimiento que tienes sobre los dispositivos de seguridad con los que cuenta la empresa?	1	1	1	1	1
		¿cómo calificarías la seguridad de los usuarios empresariales?	1	1	1	1	1
	Nivel de satisfacción del usuario con el sistema	¿cómo calificaría usted la seguridad en la empresa?	1	1	1	1	1
		¿Cuál es su nivel de satisfacción con el sistema de seguridad en la empresa?	1	1	1	1	1

Cuestionario para la variable dependiente

CUESTIONARIO PARA CONOCER EL NIVEL DE SATISFACCIÓN DEL USUARIO

Somos estudiantes de la universidad cesar vallejo-Tarapoto y estamos ejecutando un trabajo de investigación titulado "Sistema Basado en Internet of Thinks para Mejorar la Seguridad Física en la Empresa Dr. PC Tarapoto, San Martin 2022", integrados por: Cigüeñas Piña Edwin Alcides, Coronel Dávila Luis Humberto, para tal efecto necesitamos que usted responda lo más veraz posible la siguiente encuesta:

Instrucciones:

Estimados usuarios, el propósito de esta encuesta es saber qué tan satisfecho está con el sistema de seguridad de la empresa Dr. PC, responda a cada pregunta marcando del 1 al 5, siendo 1 el nivel más bajo y 5 el nivel más alto según considere correspondiente a las siguientes preguntas:

Edad _____ Sexo _____(M/F)	1	2	3	4	5
1.- ¿cómo calificaría usted la seguridad en la empresa?					
2.- ¿Como calificaría usted los equipos instalados para el sistema de seguridad?					
3.- ¿cómo calificaría usted las políticas de seguridad en la empresa?					
4.- ¿cómo calificaría usted el tiempo de activación de dispositivos de acceso en la empresa?					
5.- ¿cómo calificaría usted el tiempo de comprobación de acceso de seguridad en la empresa?					
6.- cómo calificaría usted el tiempo de envió de alertas de incidencias en la empresa?					
7.- ¿cómo calificaría usted la capacitación de los empleados para prevenir errores de seguridad?					

8.- ¿Cuál es su nivel de satisfacción con el sistema de seguridad en la empresa?					
9.- ¿cómo calificaría usted la inversión de la empresa en seguridad física?					
10.- ¿cómo calificaría usted el conocimiento que tienes sobre los dispositivos de seguridad con los que cuenta la empresa?					
11.- ¿cómo calificarías la seguridad de los usuarios empresariales?					

¡Muchas gracias por su participación!

FICHA DE VALIDACIÓN DE JUICIO DE EXPERTO

Nombre del instrumento	Cuestionario
Objetivo del instrumento	conocer el nivel de satisfacción del usuario con el sistema de seguridad
Nombres y apellidos del experto	ROLAND KENNET ECHEVERRIA IBAZETA
Documento de identidad	45479217
Años de experiencia en el área	3 AÑOS
Máximo Grado Académico	MAGISTER
Nacionalidad	PERUANO
Institución	MUNICIPALIDAD DISTRITAL DE TABALOSOS
Cargo	JEFE DE LA UNIDAD INFORMATICA Y ESTADISTICA
Número telefónico	963546603
Firma	MUNICIPALIDAD DISTRITAL DE TABALOSOS Mg. Ing. ROLAND K. ECHEVERRIA IBAZETA JEFE DE LA UNIDAD INFORMÁTICA Y ESTADÍSTICA
Fecha	06/07/2022

Anexo N°5: Prueba de confiabilidad de Alfa de Cronbach

Tabla N°20: *Prueba de confiabilidad de Alfa de Cronbach*

Alfa de Cronbach	Nivel de Consistencia	
0.967	**Estadísticas de fiabilidad**	
	Alfa de Cronbach	N de elementos
	,967	11

Fuente: Elaboración Propia
Elaboración: SPSS V-25

Anexo N°6: Carta de Aceptación

"AÑO DEL FORTALECIMIENTO DE LA SOBERANIA NACIONAL"

Tarapoto, **06** de Julio del 2022

Presente,

ASUNTO: ACEPTACION PARA REALIZAR PROYECTO DE INVESTIGACION

Tengo el agrado de hacer de su conocimiento que los **Señores, Cigüeñas Piña Edwin Alcides y Coronel Dávila Luis Humberto,** Identificados con **DNI 70587639** y **DNI 72040840** estudiante de la Escuela de INGENIERIA DE SISTEMAS, de la Institución Universitaria Cesar Vallejo, han sido admitidos para realizar su proyecto de investigación titulado "Sistema Basado en Internet of Thinks para Mejorar la Seguridad Física en la Empresa Dr. PC Tarapoto, San Martin 2022 en nuestra empresa Dr. PC S.A.C.

Atentamente,

DR. PC SAC
Carla Reategui Del Aguila
GERENTE GENERAL

Carla Reategui del Águila
Gerente General Dr. PC
S.A.C.-Tarapoto
DNI: 42653477

Anexo N°7: Carta autorización para el uso de la información

AUTORIZACIÓN DE USO DE INFORMACIÓN DE EMPRESA

Yo, Carla Reategui del Aguila, identificado con DNI 42653477, en mi calidad de Gerente General de la empresa Dr. PC S.A.C. con R.U.C N° 20450477096, ubicada en la ciudad de Tarapoto.

OTORGO LA AUTORIZACIÓN,

A los señores Cigüeñas Piña, Edwin Alcides, Identificado con DNI N°70587639 y Coronel Dávila, Luis Humberto, Identificado con DNI N°72040840 de la Carrera profesional de Ingeniería de Sistemas, para que utilice la siguiente información brindada por la empresa con la finalidad de que pueda desarrollar su Proyecto de Investigación.

Indicar si el Representante que autoriza la información de la empresa, solicita mantener el nombre o cualquier distintivo de la empresa en reserva, marcando con una "X" la opción seleccionada.

( ) Mantener en Reserva el nombre o cualquier distintivo de la empresa; o
( ) Mencionar el nombre de la empresa.

Carla Reategui del Aguila
Gerente General
DNI: 42653477

El Estudiante declara que los datos emitidos en esta carta y en el Proyecto de Investigación, son auténticos. En caso de comprobarse la falsedad de datos, el Estudiante será sometido al inicio del procedimiento disciplinario correspondiente; asimismo, asumirá toda la responsabilidad ante posibles acciones legales que la empresa, otorgante de información, pueda ejecutar.

Cigüeñas Piña, Edwin Alcides
DNI: 70587639

Coronel Dávila, Luis Humberto
DNI: 72040840

Anexo N°8: Consentimiento informado para encuestas

Protocolo de consentimiento informado para encuestas

El propósito de este protocolo es informarle sobre el proyecto de investigación y solicitarle su consentimiento. De aceptar, el investigador se quedará con una copia firmada de este documento, mientras usted poseerá otra copia también firmada.

La presente investigación se titula "Sistema Basado en Internet of Thinks para Mejorar la Seguridad Física en la Empresa Dr. PC Tarapoto, San Martin 2022" y está elaborada por los investigadores "Cigüeñas Piña, Edwin Alcides" y "Coronel Dávila, Luis Humberto" de la carrera profesional de Ingeniería de Sistemas en el centro universitario Cesar Vallejo sede Tarapoto. El propósito de la investigación es conocer su satisfacción en cuanto al sistema de seguridad física.

Para ello, se le solicita participar en una encuesta que le tomará 5 minutos de su tiempo. Su participación en la investigación es completamente voluntaria y usted puede decidir interrumpirla en cualquier momento, sin que ello le genere ningún perjuicio. Asimismo, participar en esta encuesta no le generará ningún perjuicio académico. Si tuviera alguna consulta sobre la investigación, puede formularla cuando lo estime conveniente.

Su identidad será tratada de manera anónima, es decir, el investigador no conocerá la identidad de quién completó la encuesta. Asimismo, su información será analizada de manera conjunta con la respuesta de sus compañeros y servirá para la elaboración de artículos y presentaciones académicas. Además esta será conservada por cinco años, contados desde la publicación de los resultados, en la computadora personal del investigador responsable, a la cual podrá también acceder su grupo de investigación.

Si está de acuerdo con los puntos anteriores, complete sus datos a continuación

Nombre	Fecha	Firma	Firma (encuestador)
Carla Ratheza del Aguila.	06/07/22		
Rod Saavedra Pinedo	06/07/22		
Ronni Fasabi Topullima	06/07/22		
Daniela Vásquez Vásquez	06/07/22		
Ghia Torres Paredes	06/07/22		
ALFREDO Jose Urbina Fernandez	06/07/22		
Shonzat an Laureano Flores	06/07/22		
Gronel Paul Canoza Isuiza	06/07/22		
Segundo Teodoro Shupingahua Ishuiza	06/07/22		
Tony Rodriguez Paredes	06/07/22		
Romy clarense Padilla Diaz	06/07/22		
Erika Merlith Fasabi Tuanama	06/07/22		

Anexo N°9: Documentación de desarrollo de encuestas y guías de observación

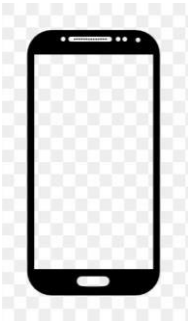
Anexo N°10: Diseño y desarrollo del sistema

Requerimientos de dispositivos para el sistema

FASE DE PRE ESTUDIO			
Entregable:		Requerimiento	
Para la construcción y/o adaptación del sistema basado en internet of thinks se utilizó			
Objetivo	Reconocer los dispositivos que se necesitan para el sistema		
Alcance	Todos los elementos que se utilizan para el funcionamiento del sistema basado en internet of thinks.		
Nombre	**Descripción**	**Imagen**	**Costo**
control de acceso biométrico DS-PS1-R DS-K1T343EWX de reconocimiento facial HIKVISION	Terminal WiFi / Touch de Reconocimiento Facial Ultra Rápido para ASISTENCIA y Control de ACCESO/ 1500 Rostros, 3000 huellas dactilares y 3,000 tarjetas / Lee códigos QR / Videoportero / Detección de Cubrebocas		S/.380.00

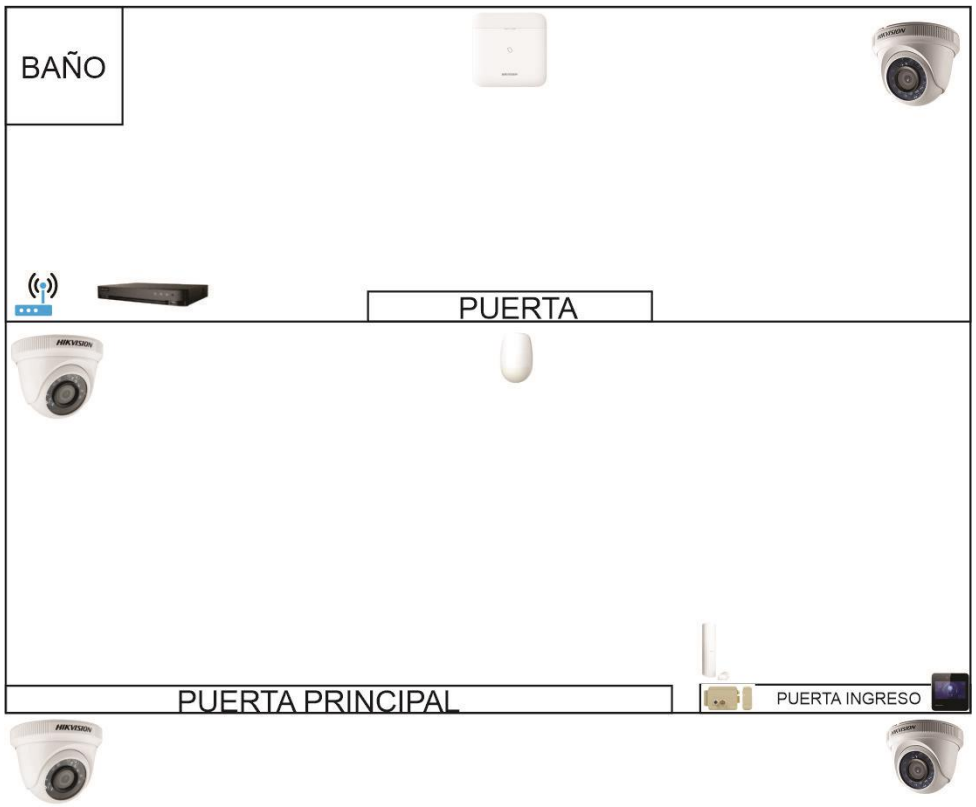
kit de alarma wifi 64 zonas HK-DS-PWA64-KIT-WB (panel, pir, imagen y pulsador)	Protocolo TCP/IP, red wifi, Protocolo inalámbrico de nueva generación: Tri-X/Cam-X, Larga distancia de transmisión de RF, Comunicación bidireccional con encriptación AES-128, Admite hasta 16 usuarios de red, incluidos 1 instalador, 1 administrador y 14 usuarios normales, mensaje de voz, Configuración a través de cliente web, cliente móvil y Convergence Cloud, La configuración de Hik-Connect y Hik-ProConnect depende del nivel de acceso del usuario, Ve videos en vivo de Hik-Connect, Videoclips de alarma a través de correos electrónicos y APP, Admite indicador LED para indicar el estado del sistema, Batería de respaldo de litio de 4520 mAh, Protocolo SIA-DC09 y admite formato de datos Contact ID y SIA, Admite Hik-IP Receiver y Hik-IP Receiver Pro para comunicación ARC		S/.590.00 (kit completo)

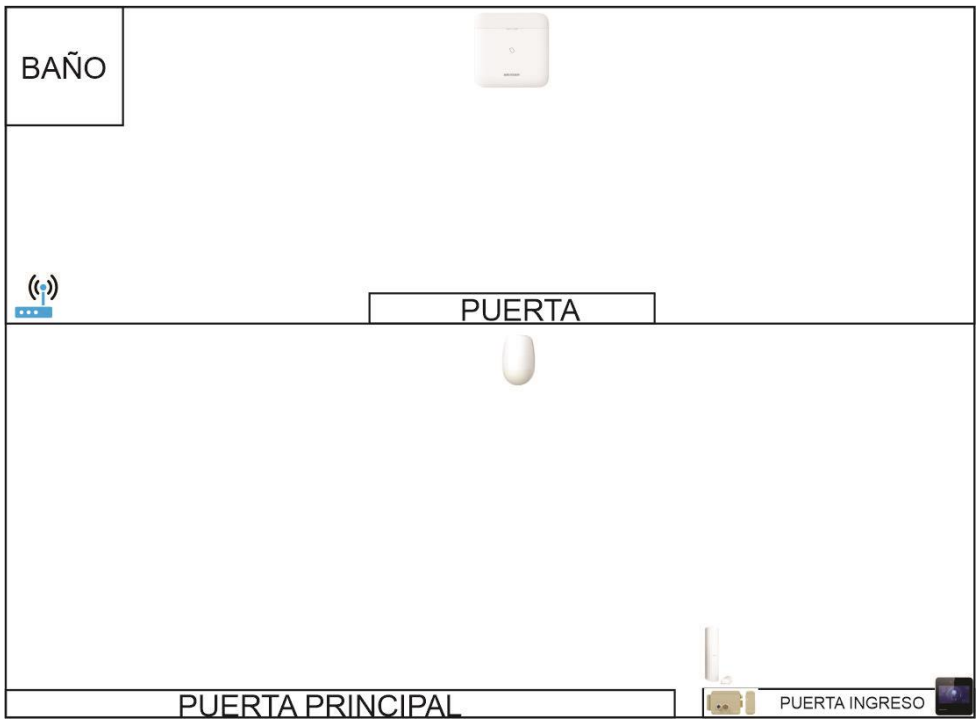
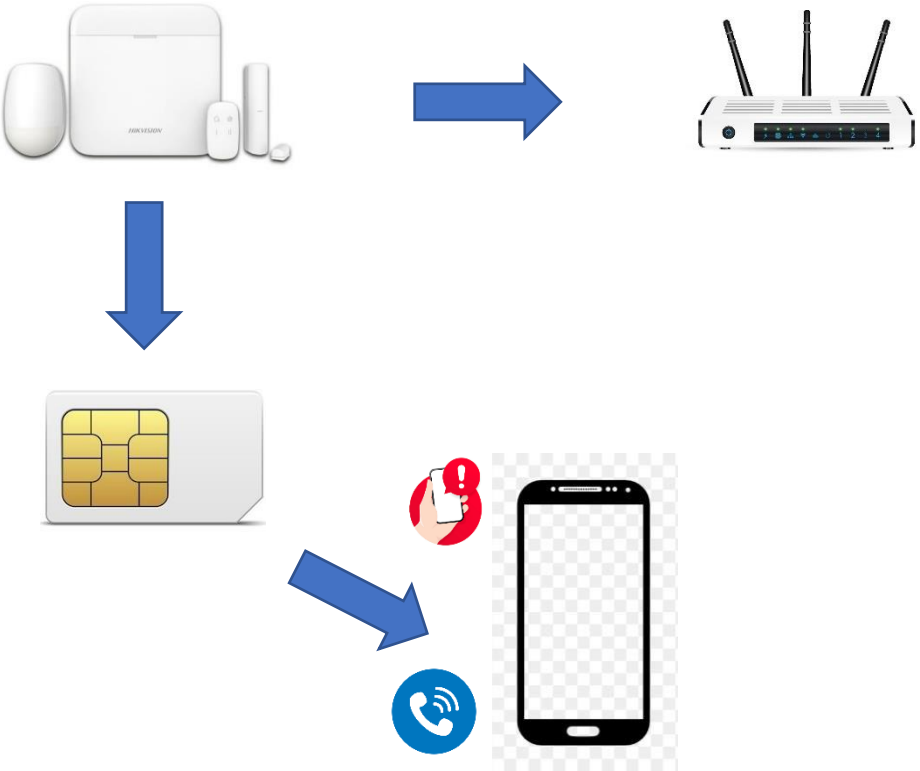
DVR HIKVISION HK-IDS7204HQHI-M1/FA 4CH ACUSENSE 1080P 1HDD	Tiene 4 canales y 1 HDD 1U AcuSense DVR, Admite reconocimiento facial o reducción de falsas alarmas basado en un algoritmo de aprendizaje profundo, Admite la comparación de imágenes faciales y la búsqueda de imágenes faciales, Hasta 16 bibliotecas de imágenes de rostros, con hasta 500 imágenes de rostros en total, Eficiente tecnología de compresión H.265 pro+, Capacidad de codificación de hasta 1080p a 15 fps, Entrada de 5 señales adaptable (HDTVI/AHD/CVI/CVBS/IP), Se pueden conectar hasta 6 cámaras de red		S/.280.00
4 kits de cámaras de seguridad domo HIKVISION FULLHD 1080p	Ideal para interiores y exteriores, Resolución FULLHD 1080p 2mp, Luz infrarroja, Resistente a altas y bajas temperaturas, Lente de 2.8 mm, Ángulo de visión de 90°, Ahorro de energía		S/.300.00
Cable De Corriente 2 Pines	Dimensión: 2x0.75 mm2, Rango de Tensión: Nominal de 110/220 Voltios.		S/.15.00

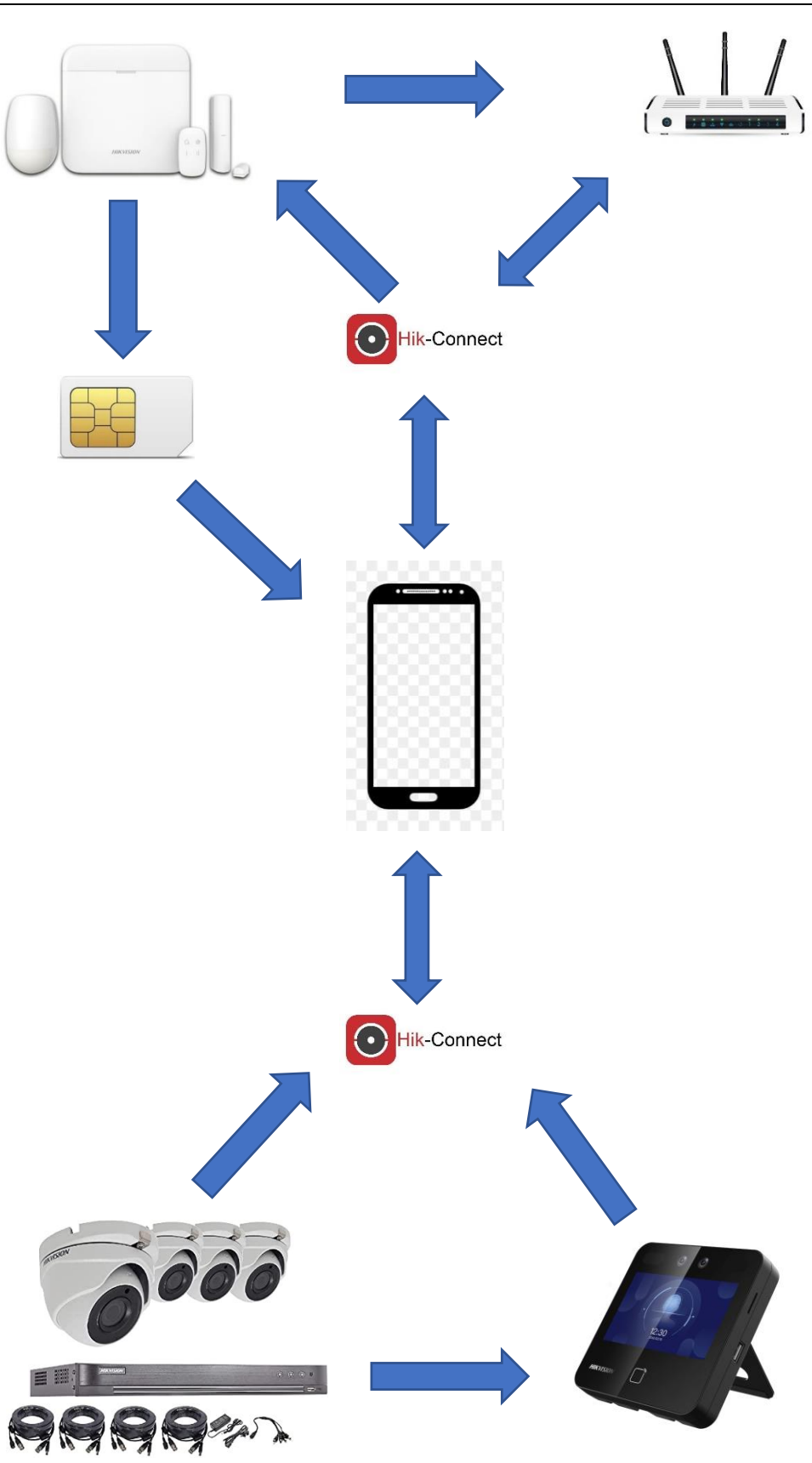
Cerradura de llanta eléctrica antirrobo para puerta de Metal	Cerradura de Control eléctrico. Se puede abrir con dispositivos eléctricos, pulsando el botón (Interior) o la tecla (exterior). Adecuado para puertas abiertas derecha e izquierda (puede elegirlo usted mismo). Está altamente asegurado y anti-theft.It también puede evitar que alguien abra La cerradura con otras herramientas.		S/.250.00
Smartphone	Smartphone con sistema operativo Android que deberá estar conectado a la red Wifi del servidor Web.		S/.480.00
CHIP SIM	CHIP SIM que será el mediador para el envío de mensajes de textos con las alertas.		S/5.00

Documento de relación de elemento y aplicaciones.

FASE DE DEFINICIÓN	
Entregable:	Documento de relación
A continuación, la definición y relación que tienen cada componente del sistema.	
Objetivo	Relacionar los componentes para el funcionamiento del sistema
Alcance	Todos los elementos que se utilizan para el funcionamiento del sistema basado en internet of thinks.

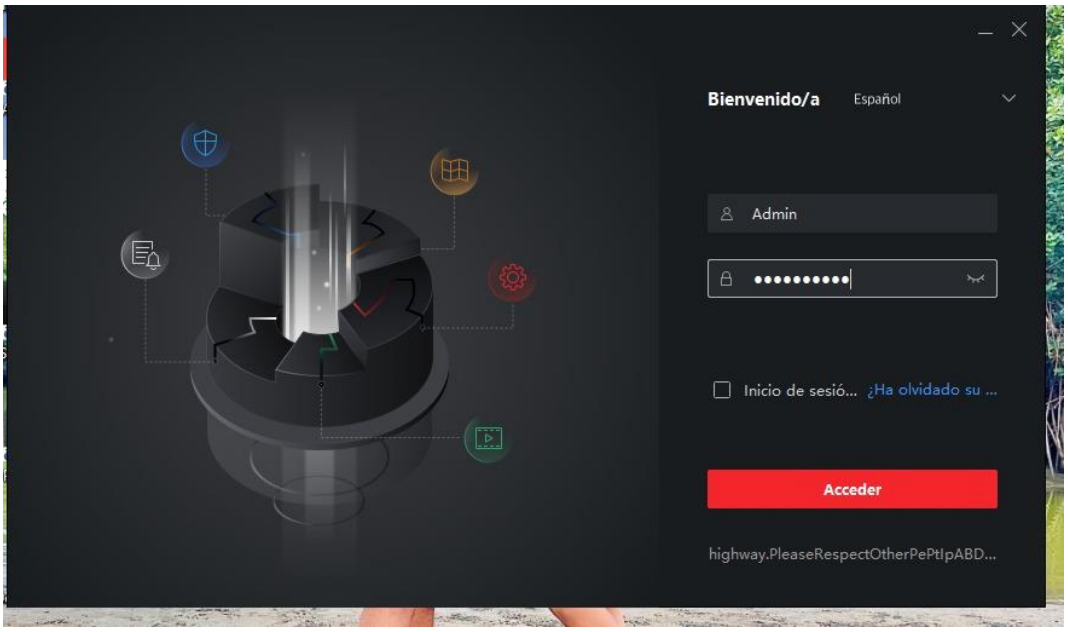
Descripción	Imagen
Definición y Relación del sistema basado en internet of thinks	

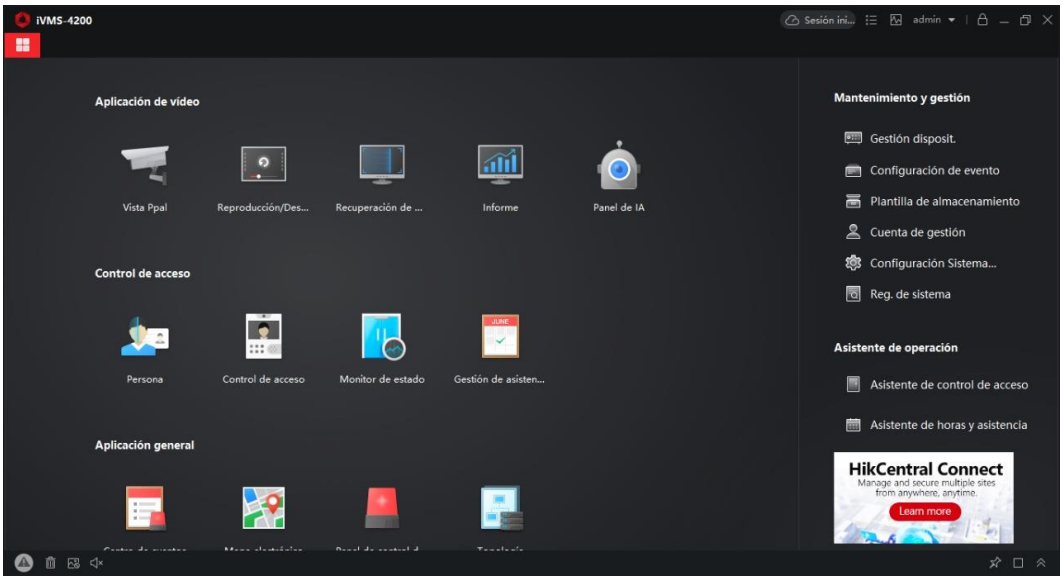
Definición y relación de sensor de puerta y ventana	
Relación de funcionalidad entre el kit de alarmas y los sensores	

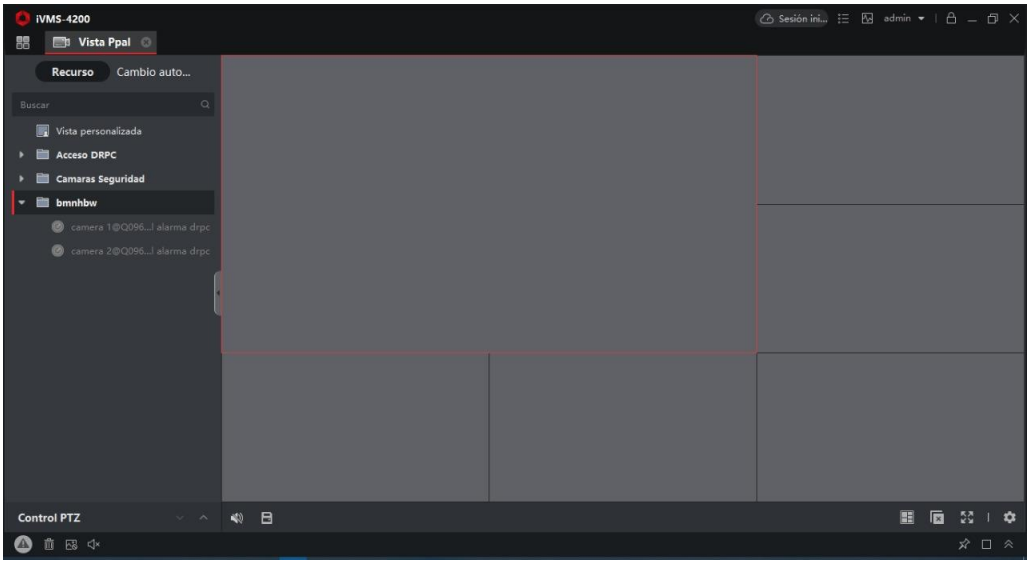
Relación de todos los elementos que conforman el sistema de seguridad.	

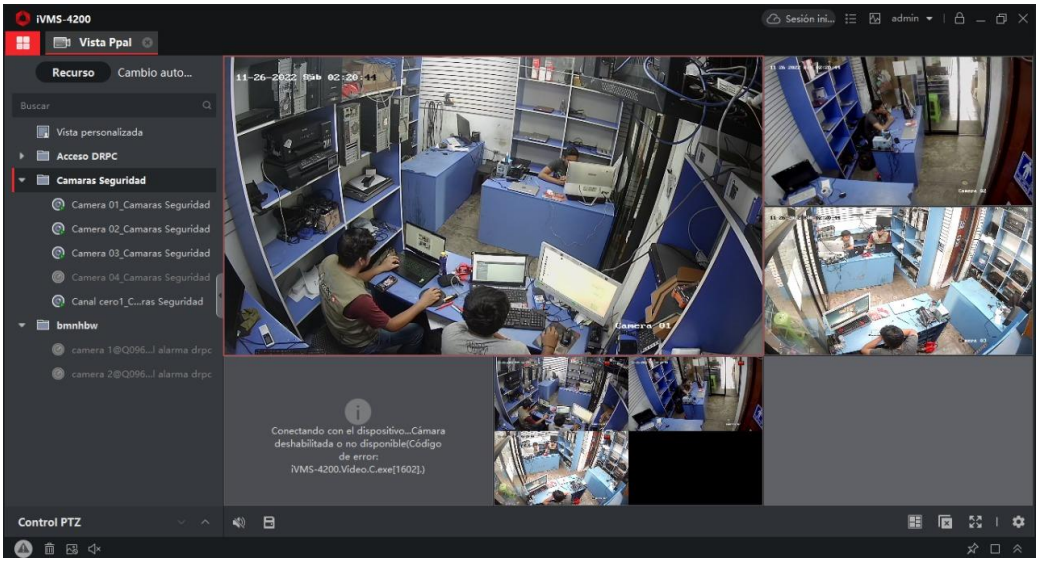
FASE DE IMPLEMENTACIÓN	
Entregable	Sistema basado en internet of thinks
Objetivo:	Correcto funcionamiento de sistema basado en internet of thinks
Alcance:	Este entregable de implementación muestra al sistema funcionamiento en los escenarios pertinentes

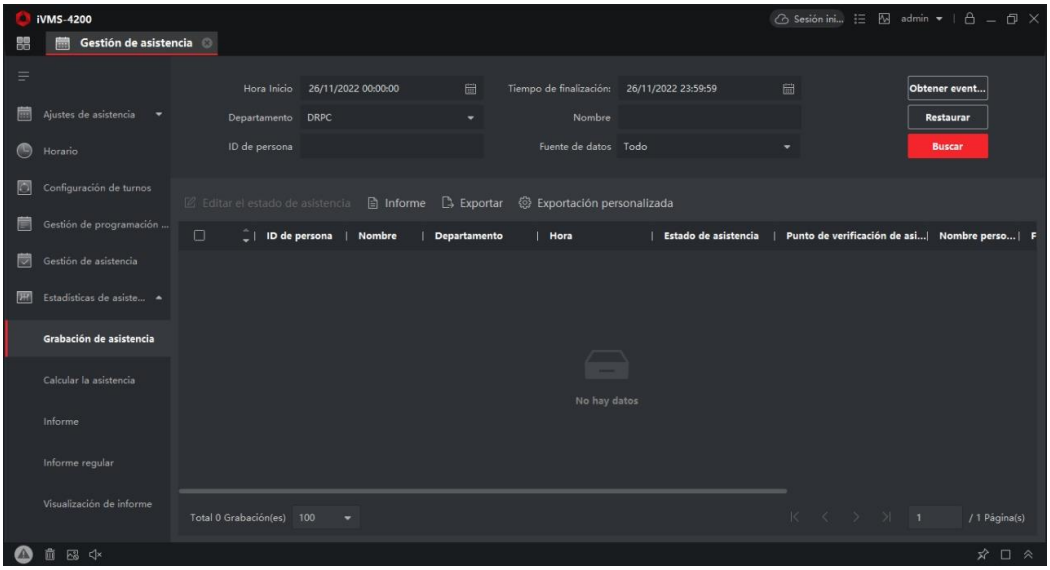
Prototipo de Sistema basado of thinks en funcionamiento.

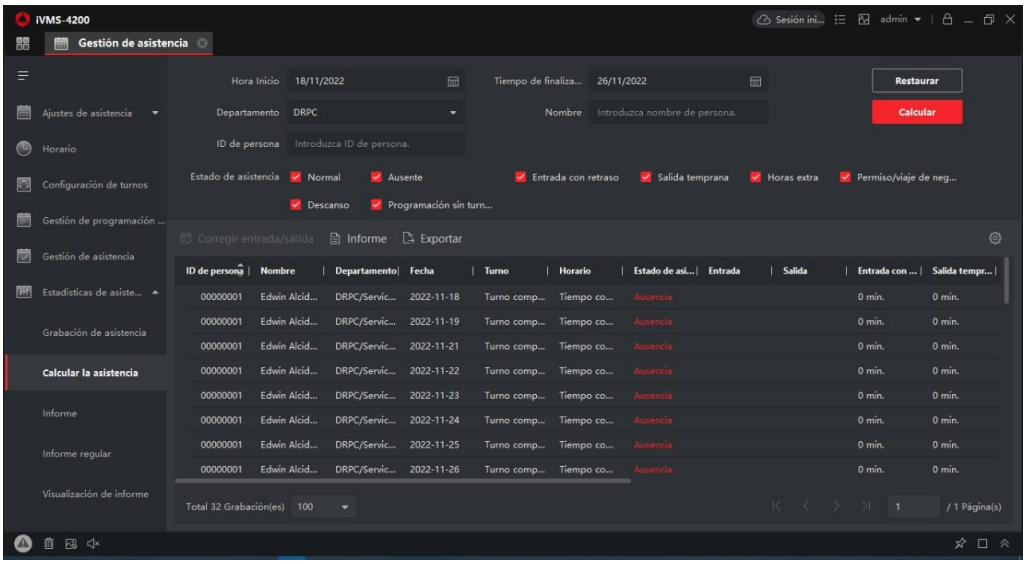




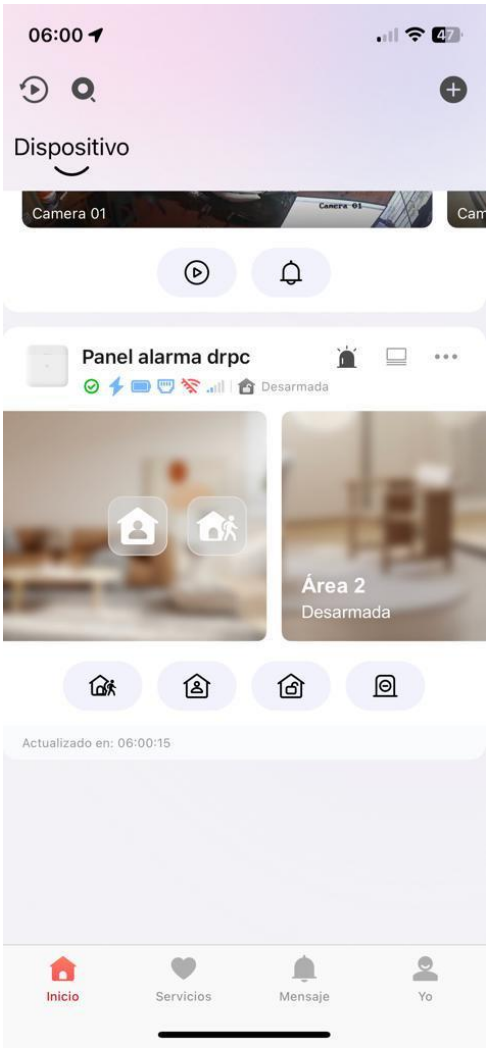

iVMS-4200
Vista Ppal
Recurso
Cambio auto...
Buscar
Vista personalizada
Acceso DRPC
Camaras Seguridad
bmnhbw
Control PTZ


iVMS-4200
Vista Ppal
Recurso
Cambio auto...
Buscar
Vista personalizada
Acceso DRPC
Camaras Seguridad
Camera 01_Camaras Seguridad
Camera 02_Camaras Seguridad
Camera 03_Camaras Seguridad
Camera 04_Camaras Seguridad
bmnhbw
Conectando con el dispositivo...Cámara deshabilitada o no disponible(Código de error: iVMS-4200.Video.C.exe[1602].)
Control PTZ

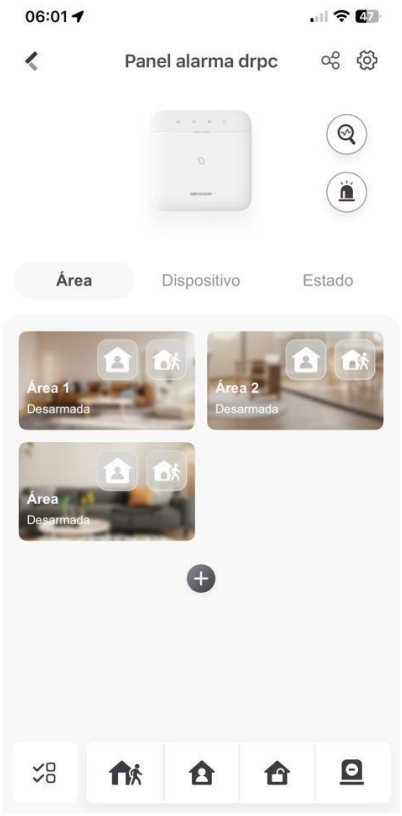

iVMS-4200
Gestión de asistencia
Hora Inicio
26/11/2022 00:00:00
Tiempo de finalización:
26/11/2022 23:59:59
Departamento
DRPC
Nombre
ID de persona
Fuente de datos
Todo
Obtener event...
Restaurar
Buscar
Ajustes de asistencia
Horario
Configuración de turnos
Gestión de programación ...
Gestión de asistencia
Estadísticas de asiste...
Grabación de asistencia
Calcular la asistencia
Informe
Informe regular
Visualización de informe
Editar el estado de asistencia
Informe
Exportar
Exportación personalizada
ID de persona
Nombre
Departamento
Hora
Estado de asistencia
Punto de verificación de asi...
Nombre perso...
No hay datos
Total 0 Grabación(es)
100
1
/ 1 Página(s)



INTERFAZ INICIO PANEL DE ALARMA



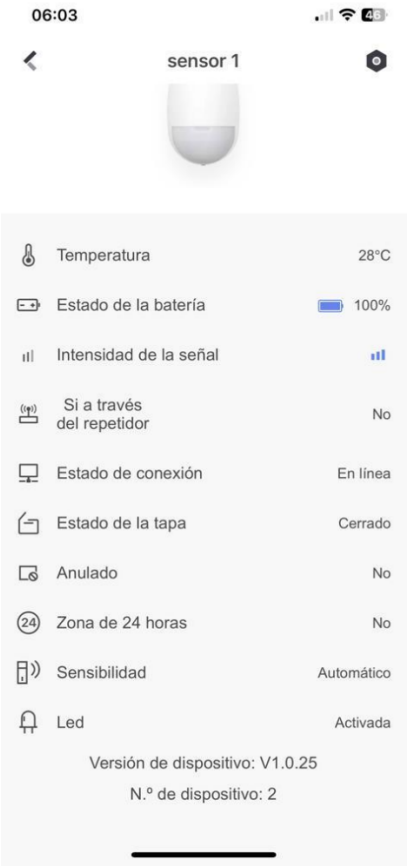
ÁREAS AGREGADAS HASTA 32 MAX



DISPOSITIVOS VINCULADOS AL ÁREA 1

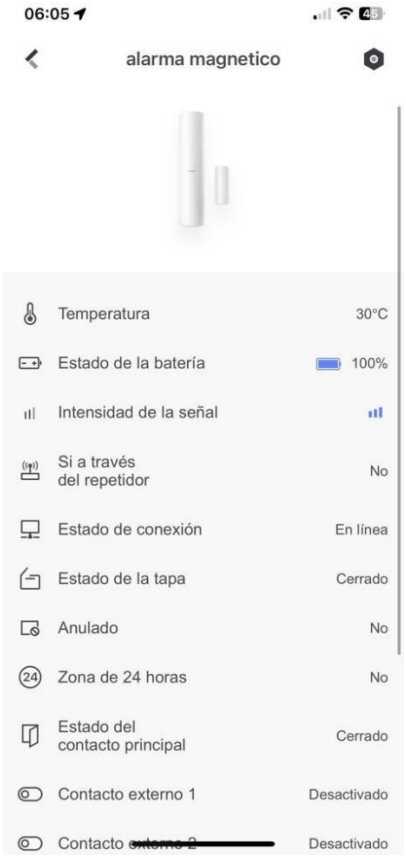
AJUSTES DEL SENSOR O PIR DE MOVIEMIENTO

AJUSTES RÁPIDOS DEL SENSOR

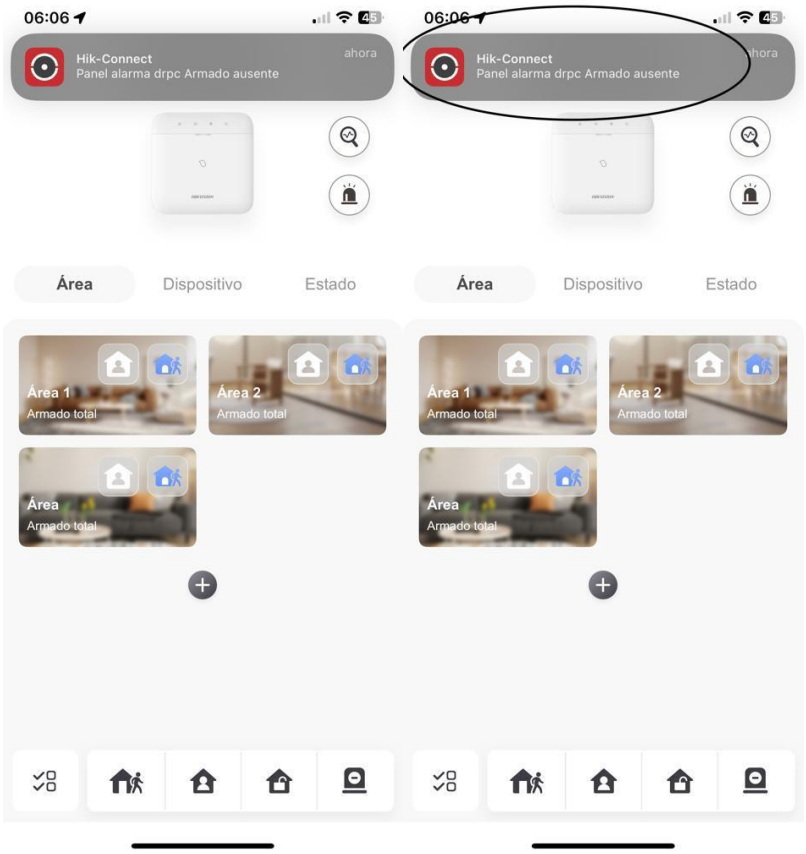


AJUSTES DEL ALARMA MAGNÉTICO

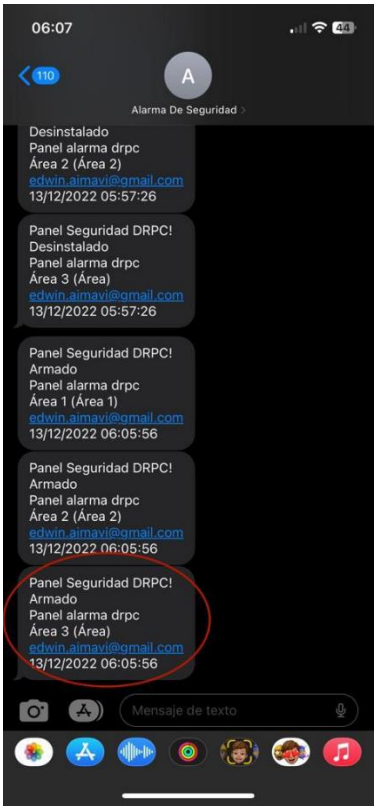
CARACTERÍSTICAS RÁPIDAS DEL ALARMARLA MAGNÉTICA



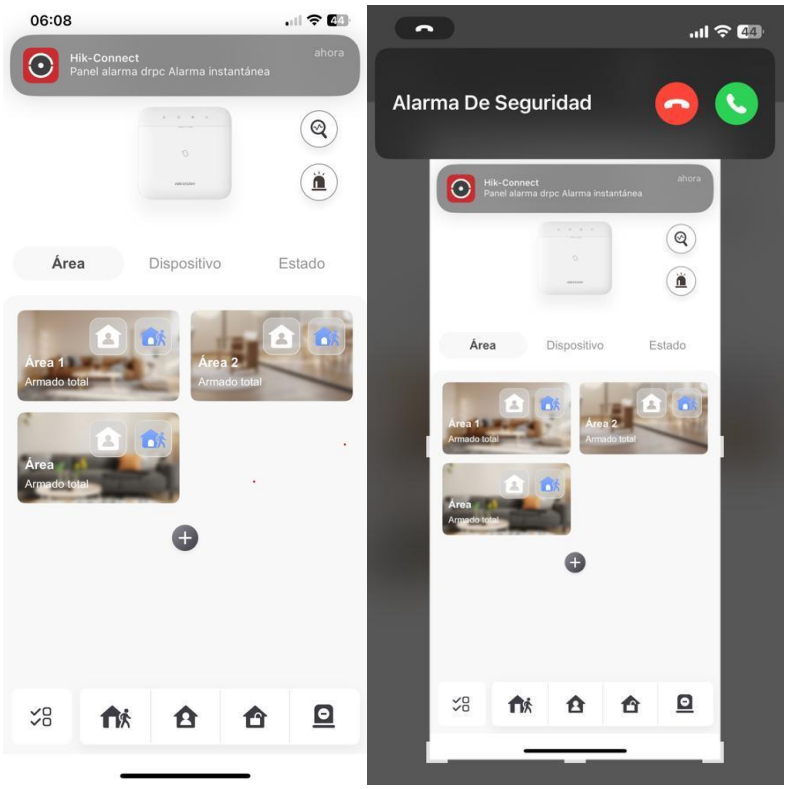
ARMADO DE SISTEMA



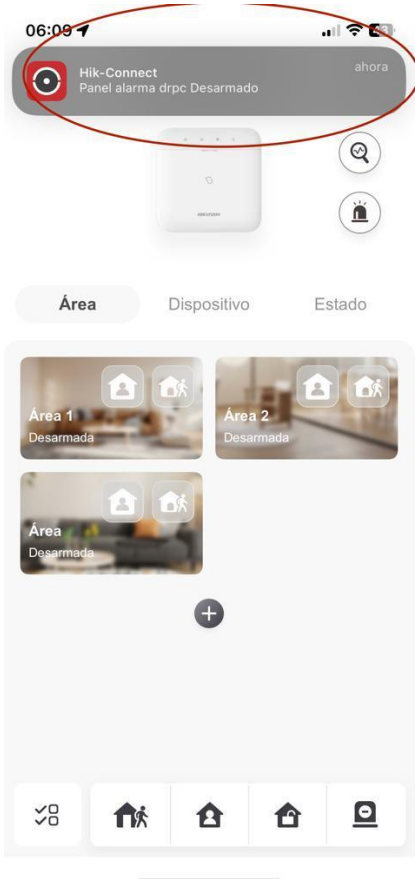
MENSAJE DE TEXTO DEL SISTEMA INDICANDO QUE EL PANEL ESTA ARMADO



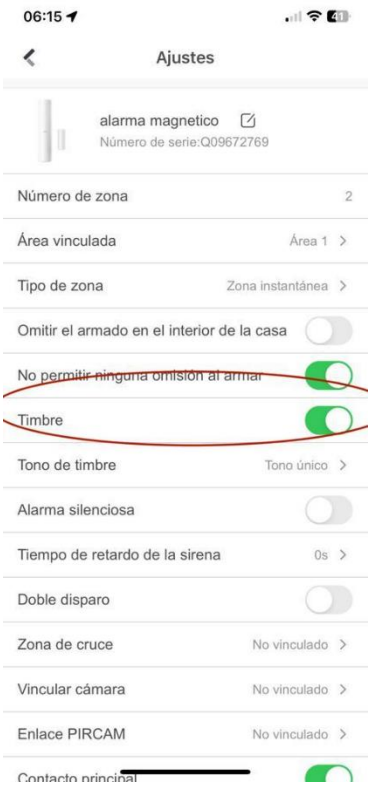
ALERTA INSTANTÁNEA DE INTRUSIÓN



SISTEMA DESCONECTADO



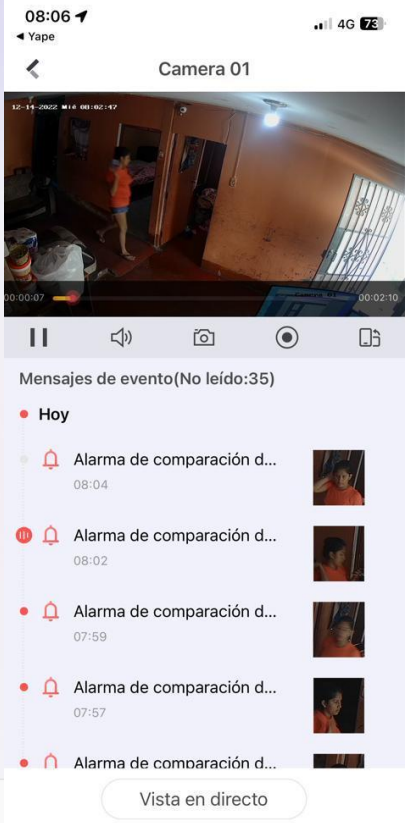
VINCULAMOS COMO TIMBRE DE PUERTA AL SENSOR MAGNÉTICO



VINCULAMOS UNA DE NUESTRAS CÁMARAS PARA EL ENVÍO DE ALERTAS

CÁMARA VINCULADA

ALERTA DE MOVIMIENTO Y COMPARACIÓN FACIAL



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, LIZETH ERLY MESCUA AMPUERO, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - TARAPOTO, asesor de Tesis titulada: "Sistema Basado en Internet of Thinks para Mejorar la Seguridad Física en la Empresa Dr. PC Tarapoto, San Martin 2022", cuyos autores son CORONEL DAVILA LUIS HUMBERTO, CIGÜEÑAS PIÑA EDWIN ALCIDES, constato que la investigación tiene un índice de similitud de 13.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

TARAPOTO, 26 de Noviembre del 2022

Apellidos y Nombres del Asesor:	**Firma**
LIZETH ERLY MESCUA AMPUERO **DNI:** 42694079 **ORCID:** 0000-0003-2748-479X	Firmado electrónicamente por: MAMPUEROL8 el 22-12-2022 10:51:21

Código documento Trilce: TRI - 0455559

INVESTIGA UCV