FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE INFORMACION

TESIS

"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE REGISTRO DE ACCESOS UTILIZANDO IoT PARA MEJORAR LA SEGURIDAD FÍSICA EN EL DATACENTER DEL DEPARTAMENTO DE INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LAS AMAZONAS - 2021"

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS DE INFORMACION

AUTORES:

Bach. CESAR EDU LANDAETA ARCENTALES

Bach. PIERO FABIAN SOBERON HERNANDEZ

ASESOR: Ing. ANGEL ALBERTO MARTHANS RUIZ, MG.

REGIÓN LORETO, PERÚ

2021

Dedicatoria

El presente trabajo está dedicado principalmente a mis padres Fabian Soberon Diaz y Rosa Isabel Hernandez Vela quiénes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir uno de tantos objetivos anhelados, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no tener miedo a las adversidades porque Dios siempre está conmigo.

Bach. Piero Fabian Soberon Hernandez

Esto va dedicado a mi madre y abuelita Marly Rosario Arcentales Pezo y Rosario Arcentales Pezo, que a pesar de las adversidades siempre supieron cómo sacarme adelante, formarme, como profesional y persona, esto no sería posible sin el sacrificio de ellas, en siempre velar que su muchacho salga adelante y logre cumplir sus sueños.

Esta va por ustedes mamitas.

Bach. Cesar Edu Landaeta Arcentales

Agradecimiento

Doy gracias a cada persona que ha influenciado en mi vida de manera positiva y negativa, ya que gracias a ellos aprendí cosas que sirvieron de experiencia para formarme, gracias a mis amigos y amigas que no dudaron en extenderme su mano en los momentos que más los necesitaba.

Finalmente a mis queridos grupos los power rangers y los sadboys que siempre me sacan una sonrisa en buenos o malos tiempos.

Bach. Piero Fabian Soberon Hernandez

Estoy agrecido con todos, durante todo este proceso conocí muchas personas que me brindaron su apoyo, muchas de ellas no están aquí, algunos en otra ciudad otras en el cielo, pero solo espero que donde se encuentren se sientan orgullosos de verme cumplir mis sueños.

Gracias amigos, profesores, maestros, compañeros, familia, colegas, compañeros del judo, compañeros de barrio, compañero de tesis, etc.

Muchas Gracias ❤

Bach. Cesar Edu Landaeta Arcentales

CONSTANCIA DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN

DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP

El presidente del Comité de Ética de la Universidad Científica del Perú - UCP

Hace constar que:

La Tesis titulada:

"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE REGISTRO DE ACCESOS UTILIZANDO IoT PARA MEJORAR LA SEGURIDAD FÍSICA EN EL DATACENTER DEL DEPARTAMENTO DE INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LAS AMAZONAS - 2021"

De los alumnos: **LANDAETA ARCENTALES CESAR EDU Y SOBERON HERNANDEZ PIERO FABIAN,** de la Facultad de Ciencias e Ingeniería, pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **2% de plagio**.

Se expide la presente, a solicitud de la parte interesada para los fines que estime conveniente.

San Juan, 26 de Julio del 2022.

Dr. César J. Ramal Asayag
Presidente del Comité de Ética – UCP

CJRA/ri-a
339-2022

Ouriginal by Turnitin

Document Information

Analyzed document	UCP_INGENIERIA_2021_TESIS_EduLandaeta_PieroSoberon_V1.docx (D133873665)
Submitted	4/18/2022 5:55:00 PM
Submitted by	Comisión Antiplagio
Submitter email	revision.antiplagio@ucp.edu.pe
Similarity	2%
Analysis address	revision.antiplagio.ucp@analysis.urkund.com

Sources included in the report

W	URL: https://repositorioacademico.upc.edu.pe/bitstream/10757/625949/6/DeLaCruzA_A.pdf.txt Fetched: 12/31/2020 12:17:59 PM	1
SA	**1595117884_918__telematica3.docx** Document 1595117884_918__telematica3.docx (D77073840)	2
SA	**Ejercicios preparacion Prueba 1 SPSS Paloma Sánchez García.docx** Document Ejercicios preparacion Prueba 1 SPSS Paloma Sánchez García.docx (D66900161)	1
SA	**Prueba_1_SPSS_Hoja de Respuestas_2017.doc** Document Prueba_1_SPSS_Hoja de Respuestas_2017.doc (D26928103)	1

Entire Document

FACULTAD DE CIENCIAS E INGENIERÍA PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE INFORMACION
TESIS
“DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE REGISTRO DE ACCESOS UTILIZANDO IoT PARA MEJORAR LA SEGURIDAD FÍSICA EN EL DATACENTER DEL DEPARTAMENTO DE INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LAS AMAZONAS - 2021”
PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS DE INFORMACION
AUTORES: Bach. CESAR EDU LANDAETA ARCENTALES Bach. PIERO FABIAN SOBERÓN HERNÁNDEZ
ASESOR: Ing. ANGEL ALBERTO MARTHANS RUIZ, MG.
REGIÓN LORETO, PERÚ
2021
Dedicatoria
Agradecimiento
TESIS DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE REGISTRO DE ACCESOS UTILIZANDO IoT PARA MEJORAR LA SEGURIDAD FÍSICA EN EL DATACENTER DEL DEPARTAMENTO DE INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LAS AMAZONAS – 2021
Bach. CESAR EDU LANDAETA ARCENTALES Bach. PIERO FABIAN SOBERÓN HERNÁNDEZ
FACULTAD DE CIENCIAS E INGENIERÍA
MIEMBROS DEL JURADO
_____ Ing. Presidente
_____ Ing. Miembro

"Año del Fortalecimiento de la Soberanía Nacional"

ACTA DE SUSTENTACIÓN DE TESIS

FACULTAD DE CIENCIAS E INGENIERÍA

Con Resolución Decanal N° 791-2022-UCP-FCEI del 19 de noviembre del 2021, la FACULTAD DE CIENCIAS E INGENIERÍA DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP designa como Jurado Evaluador de la sustentación de tesis a los señores:

- Ing. Jimmy Max Ramírez Villacorta, Mgr. — Presidente
- Ing. Isaac Duhamel Castillo Chalco. — Miembro
- Lic. Carlos Enrique Marthans Ruiz, Mgr. — Miembro

Como Asesor: al **Ing. Angel Alberto Marthans Ruiz, Mgr**

En la ciudad de Iquitos, siendo las 8:30:00 horas del día 05 de agosto del 2022, a través de la plataforma ZOOM supervisado en línea por el Secretario Académico del programa Académico de Ingeniería de Sistemas de Información de la Facultad de Ciencias e Ingeniería de la Universidad Científica del Perú., se constituyó el Jurado para escuchar la sustentación y defensa de la Tesis: **"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE REGISTRO DE ACCESOS UTILIZANDO IoT PARA MEJORAR LA SEGURIDAD FÍSICA EN EL DATACENTER DEL DEPARTAMENTO DE INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LAS AMAZONAS - 2021".**

Presentado por los sustentantes: **CESAR EDU LANDAETA ARCENTALES Y PIERO FABIAN SOBERON HERNANDEZ**

Como requisito para optar el título profesional de**: INGENIERO DE SISTEMAS DE INFORMACIÓN**

Luego de escuchar la sustentación y formuladas las preguntas las que fueron: **ABSUELTAS**

El Jurado después de la deliberación en privado llegó a la siguiente conclusión:

La sustentación es: **APROBADA POR UNANIMIDAD**

En fe de lo cual los miembros del Jurado firman el acta.

_____

Ing. Jimmy Max Ramírez Villacorta, Mgr
Presidente

_____

Ing. Isaac Duhamel Castillo Chalco.
Miembro

_____

Lic. Carlos Enrique Marthans Ruiz, Mgr
Miembro

Índice de contenido

Índice de cuadros o tablas

Índice de gráficos o figuras

RESUMEN

El presente trabajo de investigación, que lleva como título: “DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE REGISTRO DE ACCESOS UTILIZANDO IoT, PARA MEJORAR LA SEGURIDAD FÍSICA EN EL DATACENTER DEL DEPARTAMENTO DE INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LAS AMAZONAS - 2021”, tuvo como objetivo general diseñar e implementar un sistema de registro de accesos datacenter del departamento de informática de la municipalidad distrital de las amazonas, de la ciudad de Iquitos.

Para el desarrollo de la investigación, se utilizó un enfoque descriptivo, realizándose un análisis estadístico descriptivo, a través de la recolección de datos, que sirvieron para comprobar la hipótesis y proponer una solución. El tipo de investigación fue aplicada, para establecer la relación entre las variables *Sistema de registro de accesos utilizando IoT* y *Seguridad Física.* El diseño de la investigación, fue pre experimental y se aplicaron encuestas en dos momentos de la investigación (pre y post test). La población fue de 10 trabajadores del Departamento de Informática de la municipalidad distrital de las amazonas - Iquitos, correspondiendo la muestra del estudio, a la totalidad de la población. Se aplicó la técnica de la encuesta, a través de un cuestionario de 12 preguntas, para cuyo análisis e interpretación, se utilizó la escala de Likert.

Esta investigación y su respectivo análisis de datos, demuestran que la implementación de un sistema integral de registro de accesos, utilizando IoT, mejoran la seguridad del datacenter del Departamento de informática de la municipalidad distrital de las amazonas – Iquitos; repercutiendo, asimismo, en la prevención de riesgos informáticos y uso óptimo de los recursos de la institución.

PALABRAS CLAVE: Internet de las cosas**,** Hardware, Seguridad, Eficiencia.

ABSTRACT

The present research work, entitled: "DESIGN AND IMPLEMENTATION OF AN ACCESS LOGGING SYSTEM USING IoT, TO IMPROVE PHYSICAL SECURITY IN THE DATACENTER OF THE COMPUTING DEPARTMENT OF DISTRICT MUNICIPALITY OF AMAZONAS 2021", had as general objective to design and implement an access logging system using IoT, to improve the security of the datacenter of the computing department of district municipality of amazonas 2021, in the city of Iquitos.

For the development of the research, a descriptive approach was used, performing a descriptive statistical analysis, through data collection, which served to test the hypothesis and propose a solution. The type of research was applied, to establish the relationship between the variables *Access Logging System using IoT* and *Physical Security*. The research design was pre-experimental and surveys were applied in two moments of the research (pre- and post-test). The population consisted of 10 employees of the computing department of disctric municipality of amazonas 2021 - Iquitos, corresponding to the entire population of the study sample. The survey technique was applied through a 12-question questionnaire, for whose analysis and interpretation, the Likert scale was used.

This research and its respective data analysis show that the implementation of a comprehensive access log system, using IoT, improve the security of the datacenter of the computing department of distric municipality of amazonas 2021 - Iquitos; also having an impact on the prevention of computer risks and optimal use of the resources of the institution.

KEY WORDS: Internet of Things, Hardware, Security, Efficiency.

INTRODUCCIÓN

Todos los cambios que experimentan nuestras sociedades, repercuten en cada aspecto de nuestras vidas. Muchos de estos cambios, se producen para facilitar la vida de las personas. En los últimos años, la gran transformación se ha realizado en el campo de la tecnología, revolucionando el funcionamiento de empresas y organizaciones de todo tipo.

Esta revolución, permite a las organizaciones a funcionar de manera cada vez más eficiente y a usar las innovaciones tecnológicas, para resguardar sus instalaciones, proteger sus sistemas, teniendo entornos seguros, que les permitan minimizar riesgos y disminuir pérdidas. Está comprobado que, al tener entornos seguros, las organizaciones consiguen maximizar el uso de sus recursos e impulsar la productividad laboral.

Para lograr esta seguridad, las organizaciones recurren a la tecnología del Internet de las cosas (en inglés, *Internet of Things - IoT*), buscando métodos más eficientes y de bajo costo. Esta tecnología cuenta con un crecimiento y potencial impresionante, pues nos encontramos viviendo un mundo hiperconectado, donde se estima que hay alrededor de 50 mil millones de dispositivos a internet, facilitando el desarrollo funcional de organizaciones y personas.

Los dispositivos inteligentes basados en IoT, para el caso de organizaciones del rubro educativo, ofrecen grandes oportunidades para elevar su nivel competitivo y académico, permitiendo automatizar y mejorar sus procesos y tareas cotidianas. En el ámbito de la seguridad física, permite tener un registro minucioso y en tiempo real, de las personas que ingresan y salen de sus instalaciones y sistemas.

En esta investigación, resolveremos un asunto preocupante para la seguridad y funcionalidad del Departamento de Informática de la municipalidad distrital de las amazonas, ubicado en la ciudad de Iquitos.

CAPÍTULO I

MARCO TEÓRICO

1.1. ANTECEDENTES DEL ESTUDIO

1.1.1 Antecedentes Internacionales

Según (Córdova Toro, 2017), en su investigación titulada “Elaboración de prácticas de aprendizaje de programación con software libre aplicado a la plataforma Raspberry Pi 3, orientado a estudiantes de bachillerato”, concluye que se pudo observar que los estudiantes asimilan con gran facilidad, los contenidos de programación, ya que se comprobó que el centro de cómputo de la unidad educativa, está bien equipado y resulta fácil adaptar la tarjeta Raspberry Pi 3, para que los estudiantes puedan hacer uso de esta y desarrollar sus conocimientos sobre las TICS.

Según (Zapata Romero, y otros, 2016) en su investigación titulada “Sistema de detección de movimiento para uso residencial, con notificación a móviles, utilizando el microcomputador Raspberry Pi”, concluyen que, con el uso de estos equipos de bajo costo, se pueden construir sistemas de seguridad eficientes, así como lograr solventar tareas básicas domésticas de manera automatizada.

1.1.2 Antecedentes nacionales

Según (Quintana Olarte, 2018) en su tesis titulada: “Desarrollo de un sistema de geolocalización de alerta de recojo de residuos sólidos en el distrito de San Jerónimo, 2018”, en Andahuaylas – Perú, concluye que los sistemas de geolocalización aplicados con tecnología Raspberry Pi, sí solucionaron la ubicación geográfica de los camiones recolectores, para así fomentar una participación más activa del ciudadano, en la tarea de disminuir la contaminación ambiental.

Según (Huivín Suárez, 2017) en su tesis titulada: “Implementación de un sistema informático para el control de riego de cultivos, empleando IoT con Raspberry Pi, en el vivero de la Municipalidad Provincial de San Martín, 2017”, tuvo como población y muestra 4 trabajadores del vivero de la Municipalidad Provincial de San Martín. Concluye que el sistema informático, influye significativamente en el Control de Riego de Cultivos, empleando IoT con Raspberry Pi, en el Vivero de la Municipalidad Provincial de San Martín.

1.1.3 Antecedentes locales

Según (Bardales Cabanillas, 2020) en su tesis titulada: “Evaluación del potencial del empleo de aplicativos Android, en los experimentos del laboratorio del curso de Física General. Iquitos 2020”, tuvo como población y muestra a 7 docentes del curso de física general, teniendo como técnica a la encuesta y como instrumento el cuestionario. Concluye que los sistemas basados en IoT, facilitan la recolección de datos, aseguran la calidad de resultados y facilitan el procesamiento y visualización de los resultados.

Según (López Gonzales, 2018) en su tesis “Aplicación de un sistema de control mediante cámaras de vigilancia, para mejorar el control de paneles publicitarios electrónicos en la ciudad de Iquitos 2018”, tuvo como población y muestra 48 personas, la técnica para la recolección de datos empleada fue la encuesta y el instrumento el cuestionario. La aplicación de un sistema de control mediante cámaras de vigilancia, para mejorar el control de paneles publicitarios electrónicos en la ciudad de Iquitos 2018, utilizando la norma ISO 9001:2015, tendrá un impacto positivo en las empresas y usuarios.

1.2 BASES TEÓRICAS

1.2.1. Internet de las cosas

El Internet de las cosas o *Internet of Things* (IoT), hace referencia a la tendencia constante de conectar todo tipo de objetos físicos al Internet. Cualquier tipo de elemento, puede ser factible de interconectar a internet. Objetos domésticos, como los refrigeradores y televisores; recursos empresariales, como las tabletas y los dispositivos médicos; elementos portátiles, dispositivos inteligentes e incluso ciudades inteligentes, existen gracias al IoT. (RedHat, 2020)

El término IoT, se refiere a los dispositivos físicos que tienen la capacidad de recibir y enviar datos a través de redes inalámbricas, sin necesidad de la intervención humana. Esto es posible, gracias a la integración de dispositivos informáticos simples que utilizan sensores.

Podríamos, también, definir IoT como una agrupación e interconexión de dispositivos y objetos a través de internet, donde existe interacción entre dichos dispositivos y objetos, sin importar su tipo, ya que podrían ser sensores, dispositivos mecánicos, objetos cotidianos domésticos, objetos que se llevan puestos, tales como ropa, calzado o accesorios; en fin, cualquier cosa imaginable, podría estar conectada a internet e interactuar sin necesidad de intervención humana. El objetivo es lograr una interacción entre máquinas, o lo que se conoce como M2M (Machine to Machine) o máquina a máquina.

La veloz evolución de internet, ha permitido que IoT, no solo sea una visión de futuro, sino, mas bien, una realidad. Las posibilidades de aplicación que proporciona esta tecnología para mejorar la vida cotidiana de las personas, como también los entornos empresariales e industriales, son esenciales.

Existen términos relacionados con IoT, tales como "*Smart Cities*", "*Smart Buildings*", incluso "*Smart People*", donde se utilizan dichos dispositivos IoT, para mejorar el control del tránsito vehicular, el control de los recursos

sustentables en edificios, control de transporte público e, incluso, monitoreo de signos vitales.

Una característica importante de los dispositivos IoT, es la capacidad de extensión por medio de los sensores, los cuales permiten la recopilación de datos de su entorno, a través de la telemetría.

Un sistema de IoT convencional, envía, recibe y analiza datos de forma permanente, en un ciclo de repetitivo de retroalimentación.

Desde el punto de vista de las tecnologías de información empresarial, las soluciones de IoT, dan la oportunidad de que las organizaciones mejoren sus sistemas, generando nuevos desafíos para las TI.

La seguridad del IoT es un aspecto fundamental que debe ser considerado al momento de decidir qué tan abierta o restringida deberá ser una plataforma de IoT.

La conectividad a través de IoT, para enviar y recibir datos, da como resultado muchas ventajas que podemos utilizar de manera eficiente, para construir entornos más seguros, cómodos, productivos e inteligentes.

Los recursos de IoT ya desempeñan un rol importante en el proceso de transformación digital de las organizaciones. Al combinar datos provenientes de la IoT con analítica avanzada e inteligencia artificial, se abre un mundo de oportunidades y posibilidades. (SaS Institute Inc., 2020)

La inteligencia artificial, multiplica el valor que aporta IoT utilizando los datos de dispositivos inteligentes conectados, con el fin de promover el aprendizaje y el conocimiento colectivos. Algunas de las técnicas que emplea la inteligencia artificial, son el *Machine Learning*[1], el *Deep*

[1] Machine Learning en una disciplina científica del ámbito de la inteligencia artificial que crea sistemas que aprenden automáticamente.

Learning[2], el procesamiento del lenguaje natural y la visión por computadora.

1.2.2 Plataformas IoT

Usualmente, un ecosistema o plataforma de IoT, se encuentra compuesto por 4 elementos fundamentales:

1. **Hardware:** Son los sensores y dispositivos que recopilan datos del entorno; por ejemplo, sensores de humedad y temperatura. El hardware también se encarga de realizar acciones específicas previamente establecidas, en función de los datos recolectados.
2. **Conectividad:** El hardware requiere transmitir los datos recopilados, por lo general, a plataformas en la nube. Algunos sistemas IoT, utilizan componentes intermedios entre el hardware y la nube, como pasarelas o enrutadores.
3. **Software:** Por lo general, el software está en la nube, dada su cercanía con los datos enviados por los dispositivos de hardware conectados y transmitiendo. El software tiene la función de analizar los datos recibidos y generar acciones concretas en función de estos datos.
4. **Interfaz de usuario:** Los sistemas IoT necesitan alguna interfaz a través de la cual, los usuarios puedan interactuar con el sistema IoT. Esta podría ser una aplicación para teléfonos inteligentes, basada en la web con un tablero de control, que muestre las diversas opciones disponibles.

Existen diversos tipos de entornos o plataformas IoT; por lo general, se encargan del software y de la interacción con el usuario, simplificando la implementación de dichos entornos o plataformas IoT y facilitando la

[2] Deep Learning es un tipo de Machine Learning que entrena a una computadora para que realice tareas como el reconocimiento del habla, identificación de imágenes o hacer predicciones; tal como las hacemos los seres humanos.

comunicación, el flujo de datos, la administración de dispositivos y la funcionalidad de las aplicaciones. (America Digital News, 2020).

Los entornos o plataformas de IoT permiten:

- Conectar hardware, dispositivos tales como sensores y otros.
- Manejar y gestionar diferentes protocolos de comunicación.
- Proveer métodos de seguridad para dispositivos y usuarios.
- Procesar, visualizar y analizar los datos que los sensores y dispositivos recopilan.
- Integrar sus funcionalidades con otras plataformas SaaS[3].

1.2.3 Hardware IoT

Implementar un sistema de IoT, requiere componentes de hardware fuertemente integrados en entornos físicos, capaces de interactuar y transmitir información. De la misma forma. requiere un componente de software adecuado, para gestionar la información generada y actuar en consecuencia sobre el hardware anteriormente mencionado. (Equipo ALTRAN, 2016)

Las placas de desarrollo de hardware y software, surgieron hace unos pocos años con un objetivo académico, para fomentar y facilitar el aprendizaje de lenguajes de programación.

Sin embargo, fuera de este propósito inicial, los desarrolladores emplean esta tecnología para diseñar sistemas interactivos y de alta calidad. Principalmente, por la simpleza de su instalación, así como su buen potencial, capacidad y eficiencia. Dichas características, junto a un precio relativamente bajo y accesible, los convierten en dispositivos ideales para crear ambientes digitalizados.

[3] SaaS, del inglés “Software as a Service”; es un modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de una empresa de tecnologías de información, a los que se accede vía internet desde un cliente.

Asimismo, estos sistemas necesitan componentes que logren procesar los datos que reciben, transformándolos en información útil.

En ocasiones, no necesitaremos un sistema con especificaciones técnicas muy atractivas o complejas, como las que posee Raspberry Pi. En ese sentido, Arduino sería una solución ideal para instalar un medidor de temperatura o de humedad y transmitir esta información, hacia una plataforma de IoT. Sin embargo, sería deficiente si llegáramos a necesitar mayor capacidad de procesamiento para interactuar con otros dispositivos o con el medio ambiente.

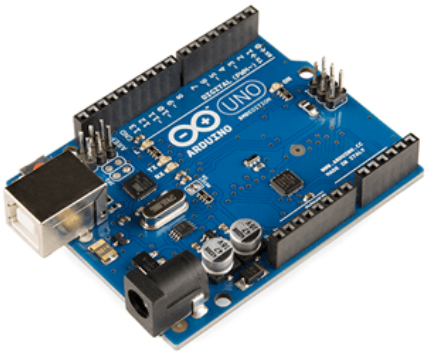
Raspberry Pi sería la opción ideal si necesitáramos diseñar e instalar un entorno domótico en casa, gestionando información de distintos sensores e interactuando con elementos de la vivienda.

Estos sensores estarían conectados directamente en la Raspberry Pi o a alguna placa auxiliar que hiciera de intermediario, por ejemplo, una placa Arduino o XBee, por citar algunas opciones.

1.2.4. Arduino

Arduino está basado en una placa electrónica de hardware libre, que incorpora un microcontrolador programable y una serie de pines, los cuales permiten establecer conexiones entre el microcontrolador y los diferentes sensores de una manera muy sencilla e intuitiva. (Arduino.cl, 2018)

Gráfico A. Placa Arduino UNO



Fuente: (Arduino.cl, 2018)

Las placas electrónicas o PCB (“*Printed Circuit Board*”, “Placa de Circuito Impreso”), son superficies planas fabricadas en un material no conductor y tiene distintas capas de material conductor. Una PCB es la forma más compacta y estable de construir un circuito electrónico. Por lo tanto, la placa Arduino, es una PCB que implementa un determinado diseño de circuitos internos. De esta forma, el usuario final no se debe preocupar por las conexiones eléctricas que necesita el microcontrolador para funcionar y puede empezar directamente a desarrollar las diferentes aplicaciones electrónicas que necesite.

Cuando se habla de Arduino, es necesario indicar el modelo específico, ya que existen diferentes modelos de placas Arduino oficiales, cada una obedece a un propósito diferente y características variadas, tales como el tamaño, número de pines de E/S, modelo del microcontrolador, entre otras. A pesar de la variedad de placas existente, todas pertenecen a la misma familia de microcontroladores marca Atmel; esto quiere decir que comparten muchas de sus características de software, tales como arquitectura, las librerías y la documentación.

El ecosistema Arduino es muy variado y bastante versátil, está catalogado en productos de nivel inicial, productos con características avanzadas, productos IoT, productos orientados a la educación, e incluso productos ya obsoletos y que han sido retirados de su producción pero que aún mantienen su documentación y soporte. En suma, más de 80 productos Arduino diferentes para cubrir las necesidades y demanda del mercado de las placas de desarrollo.

Arduino es libre y escalable; así cualquiera que desee ampliar y mejorar el diseño de hardware de las placas como el entorno de desarrollo, podrá hacerlo sin mayores problemas o contratiempos. Esto permite la existencia de un gran ecosistema de placas electrónicas no oficiales para distintos propósitos y también, librerías de software de terceros, que pueden adaptarse mejor a las necesidades del mercado.

Arduino tiene una gran comunidad aportando al crecimiento y mejoras de esta plataforma. Así se genera una documentación extensa, la cual abarca casi cualquier necesidad.

Su entorno de programación es multiplataforma y su lenguaje de programación basado en C++ es de fácil compresión.

La placa Arduino estándar (Arduino UNO), tiene un valor aproximado de US$ 35 (dólares americanos), aunque existen también las placas alternativas de menor costo.

Arduino es reutilizable, ya que, una vez terminado el proyecto, es muy sencillo desmontar los componentes externos a la placa y empezar con un nuevo proyecto. De igual manera todos los pines del microcontrolador están accesibles a través de conectores hembra y esto permite sacar partido de todas las bondades del microcontrolador, con un riesgo muy bajo de realizar alguna conexión errónea.

1.2.5. Raspberry Pi

La Raspberry Pi es una microcomputadora de bajo costo y con un tamaño compacto, del tamaño similar al de una tarjeta de crédito, puede ser conectada a un monitor de computadora o un televisor y usarse con un mouse y teclado estándar. Es un microcomputador que funciona con un sistema operativo Linux, capaz de permitirle a las personas interesadas, adentrarse en la computación y aprender a programar en lenguajes como Python. Es capaz de hacer la mayoría de las tareas comunes de un computador de escritorio, como navegar en internet, reproducir videos en alta resolución, manipular documentos, y hasta reproducir juegos. (RaspberryPi.cl, 2018)

Raspberry Pi, busca poner el poder de la computación y el desarrollo de la tecnología digital, en manos de las personas alrededor del mundo, para el trabajo, la resolución de problemas y el desarrollo de la creatividad.

Además, la Raspberry Pi tiene la capacidad de interactuar con el mundo exterior a través de interfaces de conexión a redes, puede ser usada en una amplia variedad de proyectos digitales, desde reproductores de música y video, detectores, estaciones meteorológicas y hasta con cámaras infrarrojas.

Gráfico B. Placa Raspberry Pi

Fuente: (RaspberryPi.cl, 2018)

Gran parte de su popularidad es gracias a su bajo costo, su versatilidad y la facilidad que brinda para modificar y adaptarse a diferentes proyectos; y también a la capacidad de ejecutar el sistema operativo Linux.

En lo relacionado el sistema operativo, Raspberry Pi, a través de su sitio web oficial, ofrece la opción llamada Raspberry Pi OS, conocido antes como Raspbian, la cual era una distribución de Linux basada en Debian; se puede obtener usando una utilidad conocida como Raspberry Pi Imager, la cual permite de manera fácil la instalación de Raspberry Pi OS u otro sistema operativo soportado directamente a una memoria micro SD.

La Raspberry Pi 3 B+ cuenta con un GPIO[4] de 40 pines, que permite el contacto con el mundo exterior mediante sensores y otros dispositivos de conectividad. Además, cuenta con conexiones tradicionales encontradas también en las computadoras de escritorio, como son puertos USB, conector de red Ethernet, Jack de 3.5mm, puerto HDMI, puerto para memoria microSD y un conector micro USB para la alimentación eléctrica.

Asimismo, podemos destacar, también, a los puertos de conexión especiales para la cámara y la pantalla.

El modelo más reciente y disponible en el mercado, es la Raspberry Pi 4 Model B, la cual posee hasta 8GB de RAM DDR4, conexión USB tipo C, 2 puertos micro HDMI, puertos USB versión 2 y 3, conexión Gigabit ethernet, 802.11ac, Bluetooth 5.0, y un procesador Quad core Cortex-A72 de 64 bits a 1.5GHz.

1.2.6. Comparativa entre placas de desarrollo

Arduino y Raspberry Pi, ambos dispositivos son placas de desarrollo y, como tales, muchas personas tienen tendencia a compararlos y querer saber cuál de ellos es mejor.

Sin embargo, son dos plataformas muy diferentes y no son comparables, ya que han sido diseñadas para propósitos distintos. (Hard Zone, 2020)

Raspberry Pi es una placa de desarrollo, pero que realmente es todo un computador.

Posee la potencia suficiente como para realizar tareas básicas, aplicaciones de multimedia, soporta entornos de programación y puede compilar programas que se ejecuten en él.

Por su parte, Arduino es una plataforma de creación de código abierto basada en hardware y software libre que ofrece su plataforma Arduino IDE,

[4] GPIO, del inglés “General Purpose Input/Output”, es un pin genérico en un chip cuyo comportamiento se puede programar por el usuario en tiempo de ejecución.

el cual es un entorno de desarrollo integrado, un sistema de programación para crear rutinas específicas para las placas Arduino.

Tabla A. Especificaciones de hardware Raspberry Pi - Arduino

Especificación	Raspberry Pi 3 Model B	Arduino UNO R3
Chip (SoC)	BCM2837	ATmega328
CPU	Quad Cortex A54 @ 1.2Ghz	16Mhz
Set de Instrucciones	ARMv8-A	Arduino IDE
GPU	VideoCore IV 400Mhz	ATmega328
RAM	1GB SDRAM	2KB
Almacenamiento	MicroSD	EEPROM 1KB
Ethernet	10/100	NO
Wireless	802.11n/Bluetooth 4.0	NO
Salidas de video	HDMI/RCA	NO
Salidas de audio	HDMI/Stereo	NO

Fuente: (Hard Zone, 2020)

En términos de hardware, la principal diferencia entre ambas placas radica en que Arduino solo ejecuta un programa a la vez de forma continua y repetitiva, mientras que con Raspberry Pi podremos hacer casi lo mismo que en una PC en términos de metodología. En resumen, Raspberry Pi es una microcomputadora mientras que Arduino es una microcontroladora.

Tabla B. Comparativa de plataformas Raspberry Pi - Arduino

Raspberry Pi	Arduino
Es una microcomputadora con capacidad multitarea y multiproceso.	Es un microcontrolador, con capacidad monotarea y mono proceso.
Requiere alimentación eléctrica continua.	Está pensado para funcionar con batería.
Requiere realizar tareas más complejas como la instalación librerías y software adicional para interactuar con sensores y otros componentes.	Sus componentes y sensores funcionan de manera integrada y embebida.
Es más caro que Arduino.	Es más barato que las demás placas similares.
Posee capacidad de conexión ethernet y 802.11	Requiere hardware externo para conectarse a Internet y hay que programar su conectividad.
No tiene almacenamiento interno, pero se puede usar su ranura micro SD.	Puede venir con almacenamiento limitado integrado.
Tiene 4 puertos USB para conectar distintos dispositivos.	Solo tiene un puerto USB para conectarlo a una PC.
Utiliza procesadores ARM.	Utiliza un procesador de familia AVR.
Debemos apagarlo correctamente para que no haya riesgo de corrupción de archivos.	Es un dispositivo plug and play.
Soporta lenguajes de programación como Python, C, C++ y Ruby.	Solo utiliza Arduino y C/C++.

Fuente: (Hard Zone, 2020)

Como podemos observar en la tabla anterior, las diferencias son más que evidentes y es que, de hecho, no son comparables, porque a pesar que físicamente parecen ser componentes similares, poco tienen que ver el uno con el otro en su funcionamiento.

Las posibilidades de aplicaciones que da una Raspberry Pi, son enormes en comparación con Arduino. Es toda una microcomputadora, y con tan solo instalarle un sistema operativo en una micro SD, podremos utilizarlo como estación multimedia, para reproducir contenidos en una TV, para programar utilizando una distribución de Linux, como servidor de archivos, como controlador de dominio, entre otras configuraciones posibles.

Por su parte, con Arduino solo podremos ejecutar programas individuales. Podríamos utilizar Arduino para programar las acciones de un robot autómata, para crear una estación meteorológica, una gestión de iluminación con sensores de movimiento, las posibilidades también son muy amplias, pero deben ser con un propósito único y, en todos los casos, se requiere hardware adicional.

Ambas placas de desarrollo, obligan al usuario a aprender y mejorar sus habilidades en programación.

1.2.7. Seguridad de la información

La Organización Internacional de Estandarización (ISO), a través de las normas recogidas en ISO/IEC 27000, establece una implementación efectiva de la seguridad de la información empresarial desarrolladas en las normas ISO 27001/ISO 27002.

Los requisitos de la Norma ISO 27001, aportan un Sistema de Gestión de la Seguridad de la Información (SGSI), el cual consiste en una serie de medidas orientadas a proteger la información, contra cualquier amenaza, de manera que se pueda garantizar en todo momento la continuidad de las actividades de la organización. (Normas ISO, 2019)

Los objetivos del SGSI son:

- Asegurar y preservar la confidencialidad.
- Asegurar y preservar la integridad.
- Asegurar y preservar la disponibilidad de la Información.

Antes de implementar un SGSI, según la norma ISO 27001, es necesario considerar la Evaluación de Riesgos. En primer lugar, elegir una metodología de evaluación del riesgo apropiada, para los requerimientos del negocio.

Fases de la metodología:

1. Identificar los activos de información y sus responsables, se entiende por activo todo aquello que genera valor para la organización.
2. Identificar las vulnerabilidades de cada activo, aquellas debilidades propias del activo que lo hacen susceptible de sufrir ataques o daños.
3. Identificar las amenazas, aquellas cosas que puedan suceder y dañar el activo de la información, tales como desastres naturales, incendios o ataques de virus, entre otros.
4. Identificar los requisitos legales y contractuales que la organización está obligada a cumplir con sus clientes, socios o proveedores.
5. Identificar los riesgos, definir para cada activo, la probabilidad de que las amenazas o las vulnerabilidades propias del activo puedan causar un daño total o parcial al activo de la información, en relación a su disponibilidad, confidencialidad e integridad del mismo.
6. Cálculo del riesgo, el cual se realiza a partir de la probabilidad de ocurrencia del riesgo y el impacto que este tiene sobre la organización.
7. Plan de tratamiento del riesgo, se debe definir la política de tratamiento de los riesgos en función de los puntos anteriores y de la política definida por la dirección estratégica.

Seleccionaremos los controles adecuados para cada riesgo, orientados a:

- Asumir el riesgo
- Reducir el riesgo
- Eliminar el riesgo
- Transferir el riesgo

El Anexo A de la Norma ISO 27001, provee una herramienta esencial para la gestión de la seguridad, una lista de los controles o medidas de seguridad que pueden ser usados para mejorar la seguridad de la información. (Advisera, 2019)

Hay 114 controles listados en ISO 27001 dentro de cada una de las 14 secciones del Anexo A, a saber:

- ✓ **(5) Políticas de seguridad de la información** – Define controles acerca de cómo deben ser escritas y revisadas las políticas de seguridad de la información.
- ✓ **(6) Organización de la seguridad de la información** – Define controles acerca de cómo se asignan las responsabilidades en materia de seguridad de la información; también incluye los controles para los dispositivos móviles y el teletrabajo.
- ✓ **(7) Seguridad de los recursos humanos** – Define controles antes, durante y después de emplear personal idóneo para cada rol o función dentro de la organización.
- ✓ **(8) Gestión de recursos** – Define controles acerca de lo relacionado con el inventario de recursos y su uso aceptable, también la clasificación de la información y la gestión de los medios de almacenamiento alineados a las políticas de seguridad de la información.
- ✓ **(9) Control de acceso** – Define controles para las políticas de control de acceso a la información, gestión de acceso de los usuarios, control de acceso para el sistema y las aplicaciones, y responsabilidades del usuario.
- ✓ **(10) Criptografía** – Define controles relacionados con la gestión de encriptación y claves, para usuarios y para los sistemas de información.
- ✓ **(11) Seguridad física y del entorno** – Define controles que establecen áreas seguras, controles de entrada, protección contra amenazas, seguridad de equipos, descarte seguro, políticas de escritorio, alineados al resguardo de la información y de los activos físicos que las contienen.
- ✓ **(12) Seguridad operacional** – Establecen muchos de los controles relacionados con la gestión de la producción en tecnologías de información: gestión de cambios, gestión de capacidad, malware, respaldo, bitácoras,

espejos, instalación, vulnerabilidades, entre otros controles de seguridad de la información.

- ✓ **(13) Seguridad de las comunicaciones** – Define controles relacionados con la seguridad de redes, segregación, servicios de redes, transferencia de información, mensajería, entre otros controles de seguridad de la información.
- ✓ **(14) Adquisición, desarrollo y mantenimiento de sistemas** – Define controles que establecen los requerimientos de seguridad y la seguridad en los procesos de desarrollo y soporte alineados al resguardo de la información.
- ✓ **(15) Relaciones con los proveedores** – Define controles acerca de qué incluir en los contratos, y cómo hacer el seguimiento a los proveedores para salvaguardar la integridad de la información involucrada.
- ✓ **(16) Gestión de incidentes en seguridad de la información** – Define controles para reportar los eventos y debilidades, definir responsabilidades, procedimientos de respuesta, y recolección de evidencias en cuanto a salvaguardar la integridad de la información.
- ✓ **(17) Aspectos de seguridad de la información de la gestión de la continuidad del negocio** – Define controles que requieren la planificación de la continuidad del negocio, procedimientos, verificación y revisión, y redundancia de tecnologías de información.
- ✓ **(18) Cumplimiento** – Define controles que requieren la identificación de las leyes y regulaciones aplicables, protección de la propiedad intelectual, protección de datos personales, y revisiones de la seguridad de la información.

Sección A11 – Seguridad física y del entorno

Este anexo se centra en la necesidad de identificar y establecer medidas de control físicas para proteger adecuadamente los activos de información para evitar incidentes que afecten a la integridad física de la información o interferencias no deseadas. (Normas ISO 27001, 2019)

Objetivo 1 - Áreas seguras: Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de información y la información de la organización.

Objetivo 2 - Equipamiento: Prevenir pérdidas, daños, hurtos o comprometer los activos, así como la interrupción de las actividades de la organización.

La seguridad física y del entorno de un sistema informático, consiste en aplicar restricciones físicas y procedimientos para controlar las amenazas físicas hacia el hardware. Este nivel de seguridad, se enfoca en cubrir las amenazas ocasionadas por las personas y también amenazas ocasionadas por desastres naturales, que afectan al entorno y medio físico en donde se encuentra ubicado el sistema informático.

La base para integrar la seguridad como función primordial, es la evaluación y control permanente de la misma. Tener el entorno y el acceso físico controlados, permitirá disminuir la oportunidad de siniestros y permitirá obtener los medios para hacer frente a los accidentes e incidentes.

1.3 DEFINICIÓN DE TÉRMINOS BÁSICOS

- **Datacenter:** Es una infraestructura física o virtual utilizada para alojar sistemas informáticos que puedan procesar, servir o almacenar datos. Hoy en día es común la implementación y despliegue de centros de datos en la nube o también virtualizados, lo cual es una ventaja para las organizaciones que pueden ahorrar en la compra de equipos físicos y también obtener una ventaja competitiva tecnológica.
- **Hardware:** Es el conjunto de elementos físicos o dispositivos que conforman un sistema informático. Es todo dispositivo electrónico que forma parte de un sistema más complejo y que tiene funciones y características específicas compatibles para asegurar el funcionamiento en conjunto.
- **Software:** Es el conjunto de elementos lógicos o programas que permiten a un sistema informático, realizar determinadas tareas. Es un conjunto de rutinas o instrucciones programadas en un lenguaje en particular

destinadas a resolver una problemática específica. En el caso de los sistemas operativos, el software se encarga de gestionar los recursos de hardware que tiene disponibles de una manera eficiente.

- **Transformación digital:** Se dice que es la reinvención o cambio de cultura organizacional a través de la adopción de tecnologías de información para mejorar su desempeño. Hoy en día las organizaciones tienen la misión de reinventarse cada cierto tiempo, ir moldeando su cultura organizacional según los cambios de su entorno donde se desarrollan sus actividades, la adopción de nuevas tecnologías no es una opción, transformase digitalmente es un requisito fundamental para lograr la ventaja competitiva tecnológica.
- **Seguridad de la información:** Es la adopción de un conjunto de medidas preventivas y reactivas, previamente normadas, que permiten el resguardo y protección la información; son todas las regulaciones, políticas y medidas que afectan al tratamiento de los datos que se producen y utilizan en una organización. Desde el punto de vista de los activos organizacionales, la información es el activo más importante y valioso que tienen las organizaciones, por esto es que se deben plantear estrategias que incluyan el establecimiento de normas para la seguridad de la información.
- **Información:** Es un conjunto de datos procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto determinado. Los datos dispersos por si solos no representan un significado de valor para las organizaciones; una vez catalogados, analizados, y transformados en información se vuelven herramientas fundamentales para la toma de decisiones.
- **Riesgos:** Es la probabilidad de que una amenaza se convierta en un desastre. Las vulnerabilidades o las amenazas, no representan peligro por sí solas; pero, en conjunto, se convierten en un riesgo, es decir, en la probabilidad de que ocurra un desastre. Los riesgos pueden reducirse o mitigarse. La gestión de proyectos define todo un capítulo a la gestión de riegos, esto no solo para resaltar su importancia sino también para aceptar su existencia y trabajar en el peligro que representan para las organizaciones.

CAPÍTULO II

PLANTEAMIENTO DEL PROBLEMA

2.1. DESCRIPCIÓN DEL PROBLEMA

El Departamento De Informática De La Municipalidad Distrital De Las Amazonas, tiene por objetivo desarrollar, administrar y dar soporte a las redes, sistemas, equipos de cómputo y servidores del Departamento De Informática De La Municipalidad Distrital De Las Amazonas.

Sus funciones son:

1. Dar mantenimiento y administrar las redes, para apoyar las actividades de todas las áreas y departamentos administrativos de la Municipalidad distrital de las amazonas.
2. Desarrollar, actualizar y dar mantenimiento a los sistemas de información y, también, a los equipos de cómputo.
3. Dar soporte a los usuarios en asuntos relacionados a las diversas plataformas de software, tanto académicas como administrativas.
4. Supervisar los proyectos informáticos que se contraten con terceros y brindar asesoría técnica para los equipos utilizados por contratos de nivel de servicio, asegurando la calidad de los servicios adquiridos.
5. Generar propuestas que faciliten el acceso y uso de la tecnología, por parte de la comunidad.
6. Velar por la integridad y seguridad de la información almacenada en los servidores de propiedad de la municipalidad distrital de las amazonas, elaborar, revisar y ejecutar los planes de contingencia necesarios en caso de pérdida de información.
7. Desarrollar, diseñar y dar mantenimiento a la página web institucional de la municipalidad distrital de las amazonas.
8. Investigar, desarrollar, implementar y/o adaptar nuevas tecnologías, para la mejora de la gestión interna de la municipalidad distrital de las amazonas.

9. Velar por la seguridad de la red LAN, a través de una adecuada administración de los equipos de seguridad perimetral, analizando y detectando posibles vulnerabilidades y/o intrusiones.
10. Velar por la seguridad física de los equipos informáticos que dan el soporte a toda la infraestructura tecnológica de la municipalidad distrital de las amazonas, aplicando y adaptando las normas de seguridad de la información.

La seguridad es un aspecto fundamental a considerar por parte de las instituciones de educación superior. Aunque se han establecido medidas, como el sistema de cámaras de vigilancia CCTV[5] y alarmas, esto no ha sido suficiente, debido a que sus tiempos de operación son variables. Tampoco ha sido efectivo, ni adecuado para el caso particular de limitar el acceso a zonas restringidas, dentro de los ambientes de la Departamento De Informática De La Municipalidad Distrital De Las Amazonas.

Dentro de las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas, se encuentra el centro de datos o datacenter, el cual provee la infraestructura tecnológica (hardware, software, almacenamiento y redes), para todos los sistemas de información utilizados en la municipalidad distrital de las amazonas. El datacenter, debe ser operado sólo por personal autorizado perteneciente al Departamento de Informática.

El acceso a la oficina es de libre tránsito para administrativos, personal de limpieza, e incluso, personas externas a la municipalidad, tales como mensajeros, entre otros. No existe un control de seguridad, para limitar o restringir el acceso físico al datacenter, el cual está ubicado dentro de las instalaciones del Departamento de Informática.

[5] CCTV son siglas de Circuito Cerrado de Televisión, y hace referencias a un circuito de cámaras de acceso privado comúnmente utilizado para seguridad perimetral y vigilancia.

No hay un personal de vigilancia designado para el área en cuestión, ni existe algún sistema contra intrusiones, que se haya implementado para asegurar y restringir el acceso físico al datacenter.

No existe algún sistema de registro y control de acceso físico al datacenter, que se pueda usar como bitácora o registro de sucesos e incidencias.

Existe un riesgo de acceso físico no autorizado al datacenter, que puede ocasionar pérdidas tales como sustracción no autorizada de equipos, sustracción, pérdida o modificación no autorizada de información, uso malintencionado, intrusiones, virus informáticos, entre otros.

Las pérdidas podrían ser económicas, ya que los equipos informáticos que se encuentran instalados y funcionando en el datacenter, son costosos por su naturaleza y funcionalidad específica. Algunos de ellos, pertenecen al activo contable de la municipalidad distrital de las amazonas, como los servidores, equipos de redes y equipos de suministro eléctrico. Otros equipos, pertenecen al proveedor de servicios de internet, siendo la municipalidad distrital de las amazonas la responsable de su custodia y cuidado.

El valor total estimado de los equipos instalados en el datacenter, sobrepasa los US$ 20,000.00, según los registros de inventario que se manejan en el Departamento de Informática de la municipalidad distrital de las amazonas.

Por otro lado, podríamos estar hablando de sustracción, pérdida y/o modificación indebida de información sensible de estudiantes (como la información de notas, pagos, datos personales), de los docentes (como honorarios, cursos asignados) y de los trabajadores administrativos y operativos (como sueldos, cargos), entre otros.

Existe también el riesgo de virus informáticos y otro tipo de software malicioso, que pone en riesgo inminente a la información almacenada en

los servidores, debido a intrusiones o acceso físico de personas no autorizadas al datacenter.

2.2. FORMULACIÓN DEL PROBLEMA

2.2.1. Problema general

¿Cómo se podría mejorar la seguridad y evitar que personas no autorizadas puedan ingresar al datacenter?

2.2.2 Problemas Específicos

- ¿Qué tecnología existente en la actualidad se puede usar para mejorar la seguridad de un datacenter?
- ¿Cómo guardar un registro visual de todas las personas que ingresan al datacenter?
- ¿Cómo emitir alertas o notificaciones silenciosas cada vez que alguien ingrese al datacenter?

2.3. OBJETIVOS

2.3.1. Objetivo general

Diseñar e implementar un sistema de registro de accesos utilizando IoT.

2.3.2. Objetivos específicos

- Mejorar la seguridad del datacenter, registrando a las personas que ingresan, mediante un sistema de seguridad basado en IoT.
- Programar un dispositivo IoT, para capturar imágenes y registrar los datos del acceso físico al datacenter.
- Programar un dispositivo IoT, para enviar notificaciones por email al personal encargado del Departamento de Informática

2.4 JUSTIFICACIÓN DE LA INVESTIGACIÓN

La realización de este proyecto de investigación, tuvo la intención de proporcionar una alternativa versátil, flexible y de bajo costo, para la implementación de un sistema capaz de registrar el acceso físico de las personas al datacenter de la municipalidad distrital de las amazonas, por medio del uso de sensores de movimiento y de una cámara conectados a una plataforma de hardware IoT, la cual permite el envío de notificaciones vía correo electrónico al personal designado del Departamento de Informática y, a la vez, guarda un registro en una memoria extraíble, todo esto al momento de detectar movimiento en el rango de detección de los sensores.

Se utilizó *Hardware Open Source*[6], por su bajo costo de implementación y por su facilidad para introducir cambios y mejoras en un futuro cercano, automatizando diferentes tareas con el fin de crear un sistema de seguridad robusto, eficiente y confiable.

En lo económico, la implementación del prototipo aporta al cuidado de los activos tecnológicos de la municipalidad distrital de las amazonas, al utilizar como herramientas, software libre y hardware libre, con lo que se reducen los costos por pérdidas.

En lo social, el prototipo puede ser implementado y utilizado en los hogares y se podrían agregar más funcionalidades de domótica[7], debido a la naturaleza flexible y versátil de la plataforma de hardware IoT.

En lo tecnológico, es importante el uso y desarrollo de tecnologías emergentes basados en la continua evolución de los dispositivos

[6] El término Hardware Open Source, se refiere al hardware cuyo diseño se hace públicamente disponible para que cualquier persona pueda estudiarlo, modificarlo y distribuirlo, además de poder producir y vender hardware basado en ese diseño.

[7] Se llama Domótica a los sistemas capaces de automatizar una vivienda o edificación de cualquier tipo, aportando servicios de gestión energética, seguridad, bienestar y comunicación.

inteligentes, lo cual ofrece grandes oportunidades para elevar el nivel competitivo y académico. El uso y aplicación de diversas herramientas tecnológicas basadas en IoT, permite automatizar y mejorar los procesos y tareas cotidianas, en el ámbito institucional.

2.5 HIPÓTESIS

2.5.1 Hipótesis General

El diseño e implementación de un sistema de registro de accesos utilizando IoT, mejorará la seguridad física en el datacenter del Departamento de Informática de la municipalidad distrital de las amazonas.

2.6. VARIABLES

2.6.1. Identificación de las variables

- ✓ **Independiente (X):** Sistema de registro de accesos utilizando IoT.
- ✓ **Dependiente (Y):** Seguridad física.

2.6.2. Definición de las variables

La variable independiente (X): Sistema de registro de accesos utilizando IoT, se define como el prototipo que utiliza sensores y tiene una funcionalidad programada.

La variable dependiente (Y): Seguridad física, se define como el conjunto de mecanismos y acciones que buscan la detección y prevención de riesgos con el fin de proteger algún recurso o bien material.

2.6.3. Operacionalización de las variables

Tabla 01: Operacionalización de variables

Variables	Dimensión	Indicadores	Índices
Independiente (X): Sistema de registro de accesos utilizando IoT.	**Simplificación de los procesos**	• Nivel de confiabilidad. • Nivel de usabilidad. • Nivel de Funcionalidad.	Bueno, Regular, Malo.
Dependiente (Y): Seguridad física	**Seguridad física y del entorno**	• Nivel de implementación de áreas seguras. • Nivel de implementación de controles de entrada. • Nivel de protección contra amenazas.	Bueno, Regular, Malo.

Fuente: Elaboración propia.

CAPÍTULO III
METODOLOGÍA

3.1 TIPO Y DISEÑO DE INVESTIGACIÓN

3.1.1. Tipo de investigación

En el presente proyecto se utilizará el tipo de investigación aplicada, puesto que se hará uso de tecnologías de información, y se adaptarán conocimientos existentes y adquiridos en la solución práctica de un problema conocido, tal como se ha descrito en la problemática

3.1.2. Diseño de investigación

La investigación tendrá un diseño pre experimental, con pre test y post test, ya que se realizarán pruebas antes y después de la implementación de la solución propuesta.

$$\mathbf{G: O_1 X O_2}$$

Donde:

G: Grupo experimental

O_1: Pre Test

O_2: Post Test

3.2. POBLACIÓN Y MUESTRA

3.2.1. Población

La población tomada en cuenta para esta investigación, estuvo conformada por todas las personas que laboran en el Departamento de Informática de la municipalidad distrital de las amazonas, que en total son 10 individuos.

3.2.2. Muestra

La muestra fue de tipo no aleatoria intencional y estuvo conformada por la totalidad de la población, que son 10 individuos.

3.3. TÉCNICAS, INSTRUMENTOS Y PROCEDIMIENTOS DE RECOLECCIÓN DE DATOS

3.3.1. Técnica de recolección de datos

- **Encuesta**: es una técnica que se lleva a cabo mediante la aplicación de un cuestionario a una muestra de personas; esto proporciona información sobre las opiniones, actitudes y comportamiento de las personas participantes. Se aplica ante la necesidad de probar una hipótesis o descubrir una solución a un problema.

3.3.2. Instrumento de recolección de datos

El instrumento utilizado fue el cuestionario y estuvo dirigido a todos los sujetos de muestra. Las preguntas contenidas fueron las mismas para el Pre y Post Test.

3.3.3. Procedimiento de recolección de datos

El procedimiento para la recolección de datos, se planteó de la siguiente manera:

- Solicitar al jefe del Departamento de Informática, el permiso correspondiente para realizar el estudio.
- Elaborar el instrumento de recolección de datos.
- Realizar pruebas de validez y confiabilidad al instrumento de recolección de datos.
- Aplicar la encuesta Pre Test a la muestra seleccionada.
- Realizar el procesamiento y análisis de los datos obtenidos.
- Realizar la implementación de la solución propuesta.
- Aplicar la encuesta Post Test a la muestra seleccionada.
- Realizar el procesamiento y análisis de los datos obtenidos.
- Interpretar los datos.
- Elaborar la discusión e informe final.
- Sustentar los resultados del informe final.

3.4. PROCESAMIENTO Y ANÁLISIS DE DATOS

3.4.1. Procesamiento de los datos

El procesamiento de los datos se realizó a través de la estadística descriptiva, aplicando tablas, cuadros, gráficos y figuras. Los datos se analizaron utilizando un software estadístico especializado.

3.4.2. Análisis de los datos

Para la realización de la inferencia estadística se aplicó prueba de normalidad. De acuerdo a los resultados, se optó por la utilización de los estadísticos de prueba Z de Wilcoxon, debido a que la distribución de los datos, no es normal, indicativo de que deben usarse pruebas no paramétricas.

CAPÍTULO IV
RESULTADOS

4.1 RESULTADOS

4.1.1 Pruebas de Normalidad

Tabla 02. Resumen de procesamiento de casos

RESUMEN DE PROCESAMIENTO DE CASOS						
	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Pre Test	120	100,0%	0	0,0%	120	100,0%
Post Test	120	100,0%	0	0,0%	120	100,0%

Fuente: Elaboración propia.

Tabla 03. Pruebas de Normalidad

PRUEBAS DE NORMALIDAD						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Pre Test	,370	120	,000	,631	120	,000
Post Test	,405	120	,000	,613	120	,000
a. Corrección de significación de Lilliefors						

Fuente: Elaboración propia.

En la presente tabla se observa que los resultados obtenidos con esta prueba de normalidad, demuestran que la significancia (Sig.) es menor a 0.05, por lo que los datos tienen una distribución no normal, en consecuencia, el estadístico a utilizar es la prueba Z de Wilcoxon.

4.1.2 Contrastación de la hipótesis

Planteamiento de las hipótesis:

H1: El diseño e implementación de un sistema de registro de accesos utilizando IoT, mejora la seguridad física en el datacenter del departamento de informática de la municipalidad distrital de las amazonas.

H0: El diseño e implementación de un sistema de registro de accesos utilizando IoT, no mejora la seguridad física en el datacenter del departamento de informática de la municipalidad distrital de las amazonas.

En análisis del nivel de significancia de la hipótesis, se trabajó a través de la prueba de Z de Wilcoxon, por lo que se acepta la hipótesis alterna.

Tabla 04. Pruebas No Paramétricas – Prueba de rangos con signo de Wilcoxon

Rangos[a]				
		N	Rango promedio	Suma de rangos
Post Test (Categorizado) - Pre Test (Categorizado)	Rangos negativos	0[b]	,00	,00
	Rangos positivos	106[c]	53,50	5671,00
	Empates	14[d]		
	Total	120		

a. Grupo de Estudio = Control *Fuente: Elaboración propia.*

b. Post Test (Categorizado) < Pre Test (Categorizado)

c. Post Test (Categorizado) > Pre Test (Categorizado)

d. Post Test (Categorizado) = Pre Test (Categorizado)

Tabla 05. Estadísticos de Prueba

Estadísticos de prueba[a,b]	
	Post Test (Categorizado) - Pre Test (Categorizado)
Z	-9,553[c]
Sig. asintótica(bilateral)	,000

a. Grupo de Estudio = Control

b. Prueba de rangos con signo de Wilcoxon

c. Se basa en rangos negativos.

La significancia (Sig.) igual a 0.000 es menor a 0.05, lo que nos indica que existe relación significativa entre la variable independiente y la dependiente.

4.1.3 Estadísticos Descriptivos Kolmogorov-Smirnov

Tabla 06. Pruebas No Paramétricas

	N	Media	Desv. Desviación	Mínimo	Máximo
Pre Test	120	1,56	,499	1	2
Post Test	120	2,62	,486	2	3

Fuente: Elaboración propia.

Tabla 07. Prueba de Kolmogorov-Smirnov para una muestra

		Pre Test	Post Test
N		120	120
Parámetros normales[a,b]	Media	1,56	2,63
	Desv. Desviación	,499	,486
Máximas diferencias extremas	Absoluto	,370	,405
	Positivo	,310	,276
	Negativo	-,370	-,405
Estadístico de prueba		,370	,405
Sig. asintótica(bilateral)		,000[c]	,000[c]

a. La distribución de prueba es normal.

b. Se calcula a partir de datos.

c. Corrección de significación de Lilliefors.

Fuente: Elaboración propia.

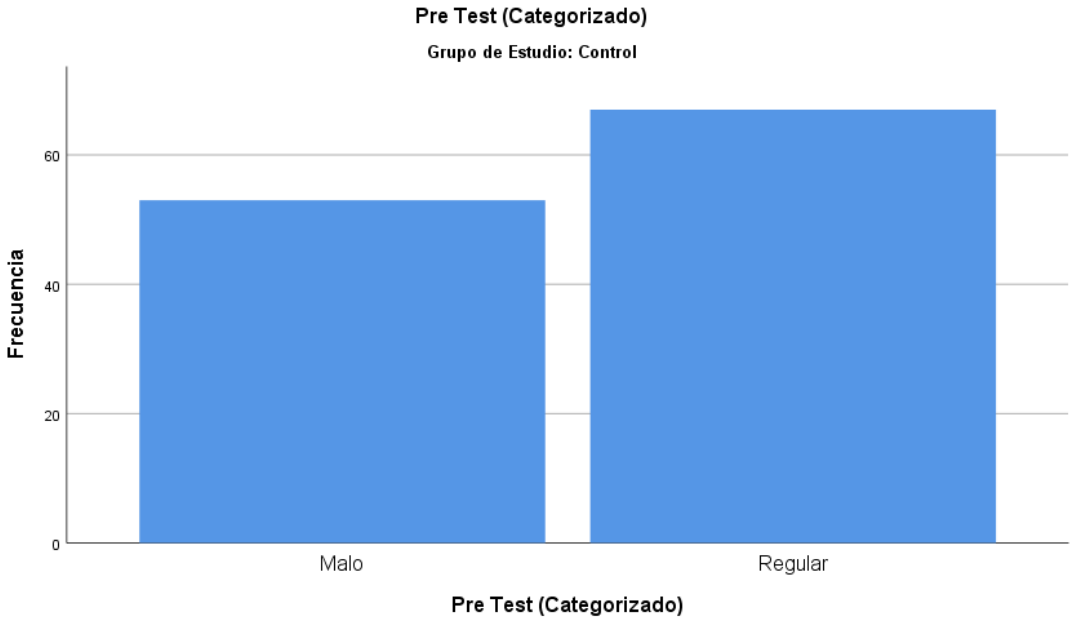
4.1.4 Estadísticos descriptivos – Frecuencias Pre Test

Tabla 08. Pre Test (Categorizado)

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	53	44,2	44,2	44,2
	Regular	67	55,8	55,8	100,0
	Total	120	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 01. Pre Test (Categorizado)



Fuente: Elaboración propia.

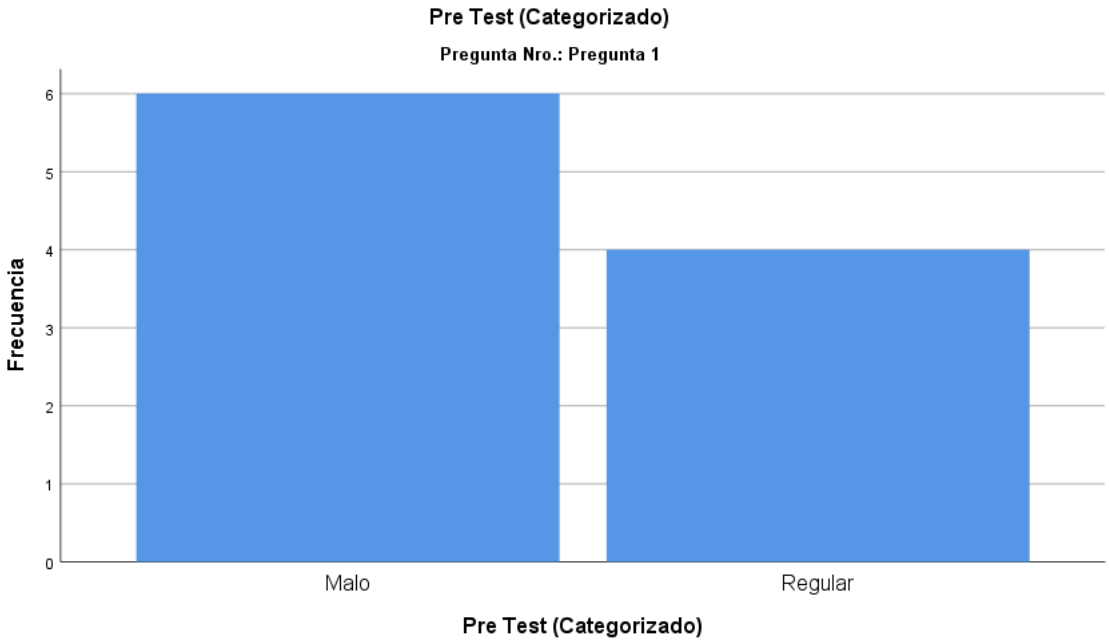
4.1.5 Estadísticos Descriptivos – Frecuencias Pre Test por Pregunta (Categorizado)

Tabla 09: Pre Test (Categorizado) – Pregunta 1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	60,0	60,0	60,0
	Regular	4	40,0	40,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 02. Pre Test (Categorizado) – Pregunta 1



Fuente: Elaboración propia.

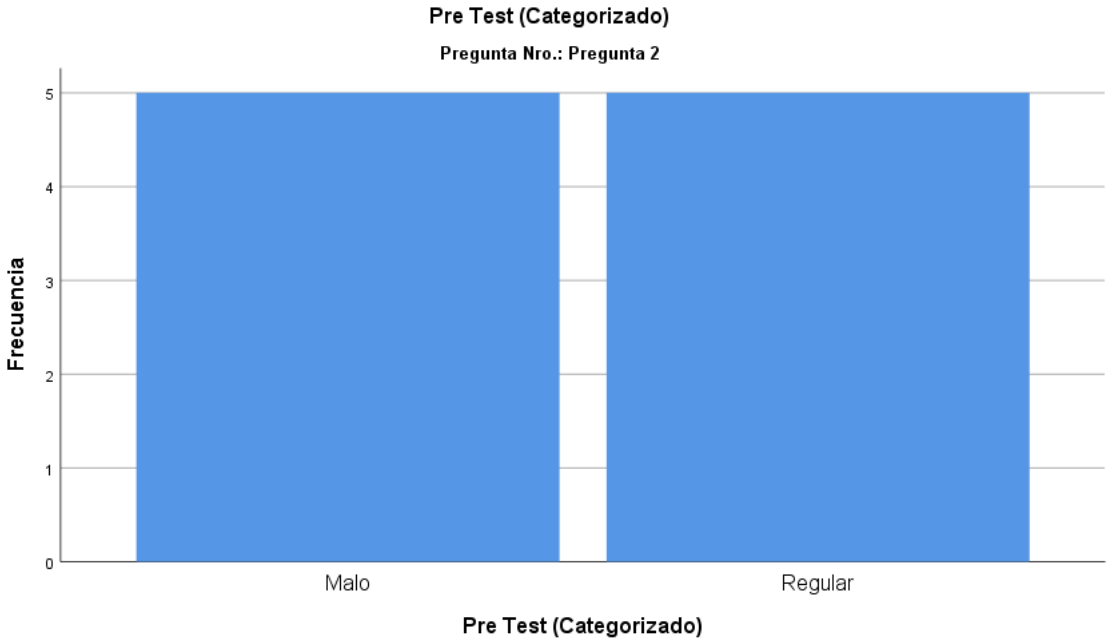
En cuanto al nivel de confianza del sistema de registro de accesos al datacenter investigado, los encuestados indicaron un 60% como Malo y 40% Regular; lo que muestra un alto grado de desconfianza en su seguridad, tal como lo muestra la Tabla 09 y Gráfico02.

Tabla 10: Pre Test (Categorizado) – Pregunta 2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	5	50,0	50,0	50,0
	Regular	5	50,0	50,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 03. Pre Test (Categorizado) – Pregunta 2



Fuente: Elaboración propia.

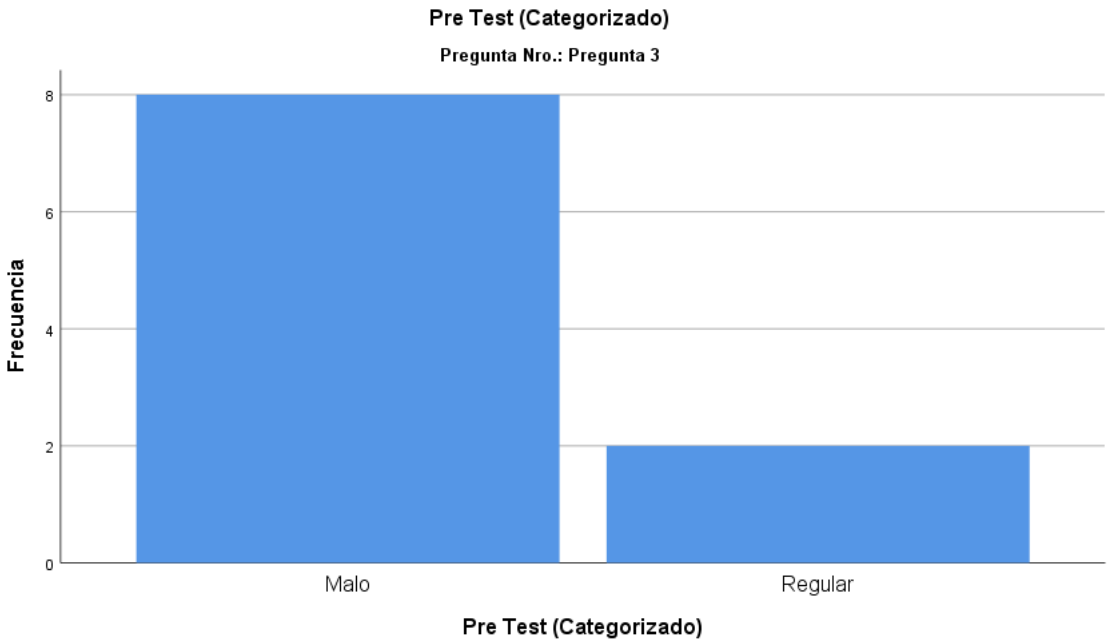
En la Tabla 10 y Gráfico 03, se muestra que la confianza de la que se habla en el punto anterior, no ha mejorado en los últimos tiempos. El índice Malo y Regular, alcanzan cada uno, el 50%.

Tabla 11: Pre Test (Categorizado) – Pregunta 3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	8	80,0	80,0	80,0
	Regular	2	20,0	20,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 04. Pre Test (Categorizado) – Pregunta 3



Fuente: Elaboración propia.

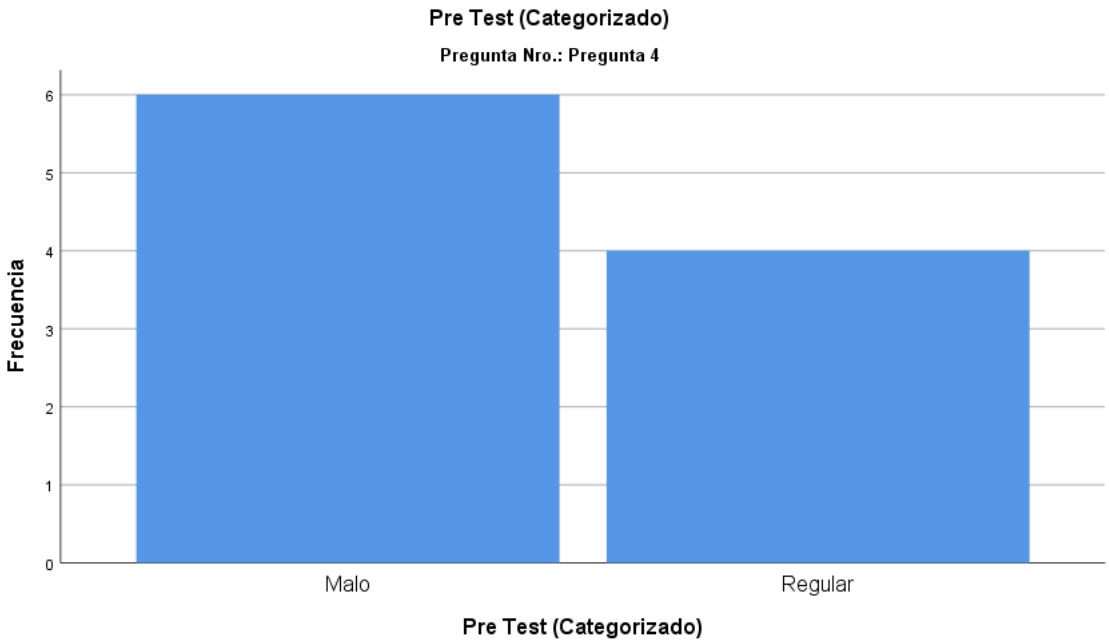
En la Tabla 11 y Gráfico 04, observamos que el 80% de los encuestados, calificó como Malo el nivel de usabilidad, del sistema de registro de accesos, en el datacenter del Departamento de Informática de la municipalidad distrital de las amazonas. Sólo un 20%, lo califica como Regular.

Tabla 12. Pre Test (Categorizado) – Pregunta 4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	60,0	60,0	60,0
	Regular	4	40,0	40,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 05. Pre Test (Categorizado) – Pregunta 4



Fuente: Elaboración propia.

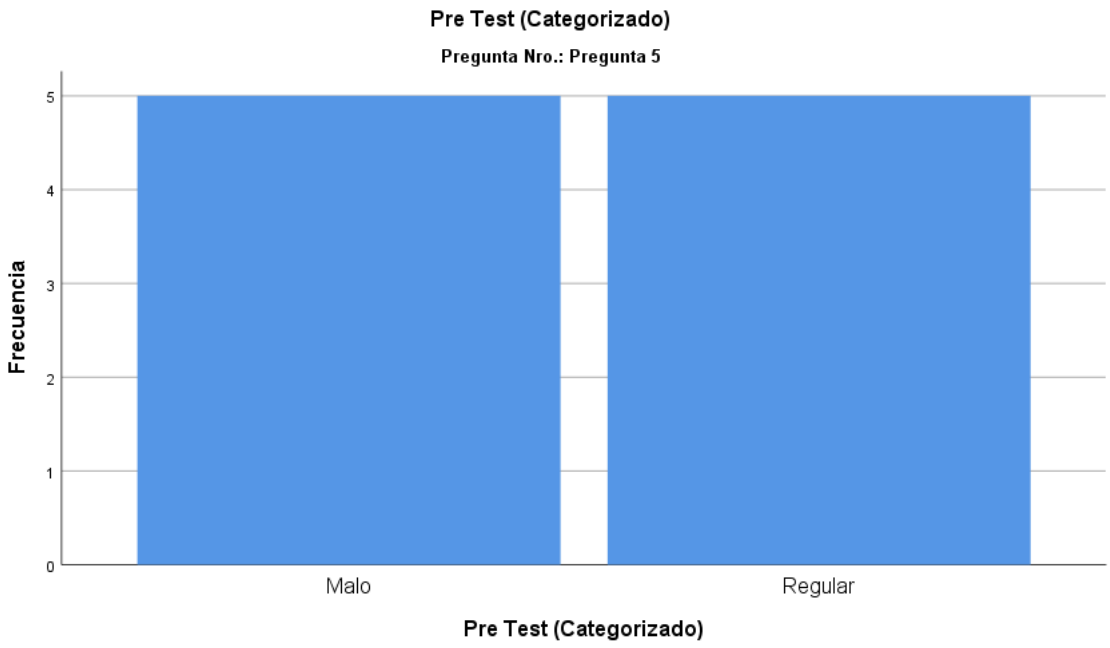
En relación con el punto anterior, el 60% de los encuestados indican que, en los últimos tiempos, el nivel de mejora en la usabilidad del sistema en cuestión, es Malo. El 40% restante, cree que es Regular.

Tabla 13. Pre Test (Categorizado) – Pregunta 5

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	5	50,0	50,0	50,0
	Regular	5	50,0	50,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 06. Pre Test (Categorizado) – Pregunta 5



Fuente: Elaboración propia.

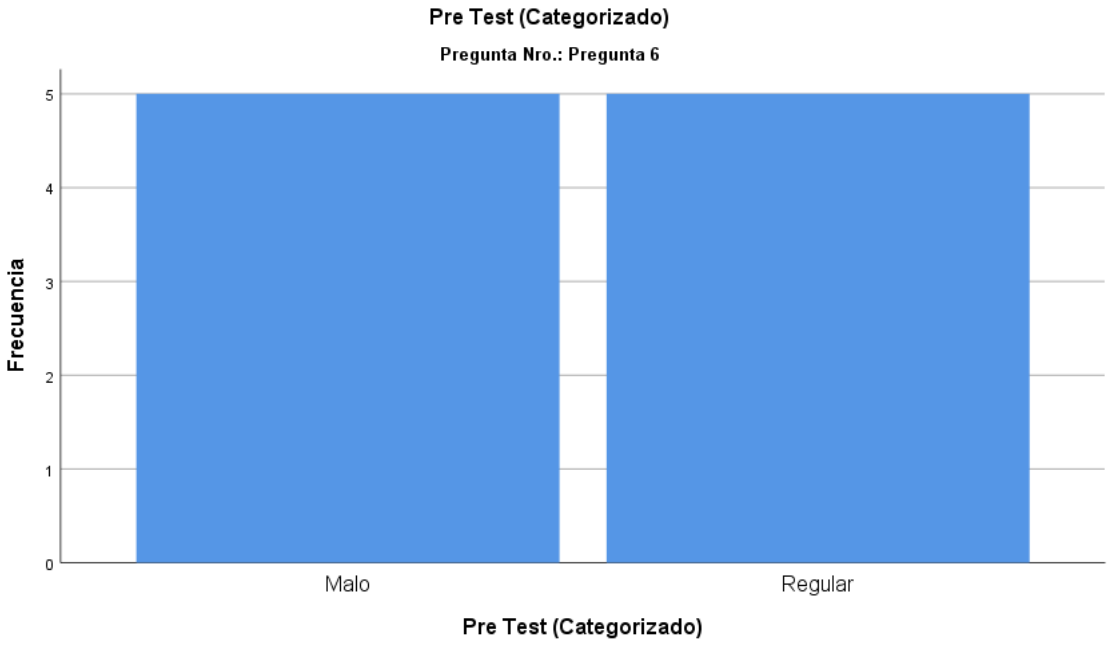
Cuando se pide a los encuestados, calificar el nivel de funcionalidad del sistema de registro de accesos al datacenter del Departamento de Informática de la municipalidad distrital de las amazonas, un 50% lo califica como Malo y el 50% como Regular, lo que demuestra su poca eficiencia.

Tabla 14. Pre Test (Categorizado) – Pregunta 6

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	5	50,0	50,0	50,0
	Regular	5	50,0	50,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 07. Pre Test (Categorizado) – Pregunta 6



Fuente: Elaboración propia.

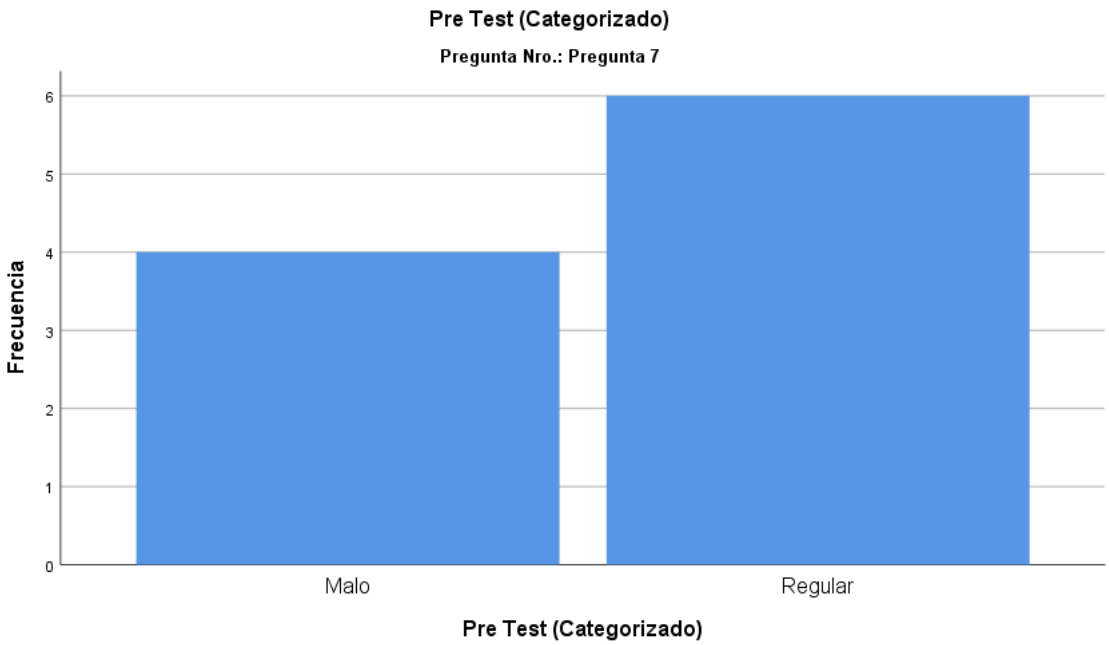
En relación al punto anterior, se muestran los mismos resultados cuando se consulta en cuánto ha mejorado la funcionalidad del sistema en cuestión: 50% Malo y 50% Regular.

Tabla 15. Pre Test (Categorizado) – Pregunta 7

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	4	40,0	40,0	40,0
	Regular	6	60,0	60,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 08. Pre Test (Categorizado) – Pregunta 7



Fuente: Elaboración propia.

La Tabla 15 y Gráfico 08, correspondiente al análisis del nivel de seguridad en el acceso físico al datacenter, muestra un 40% en el índice Malo y un 60% en el índice Regular, lo que indica una baja percepción de seguridad que tiene el personal, que labora en el Departamento de Informática de la municipalidad distrital de las amazonas – Iquitos, en su propio sistema.

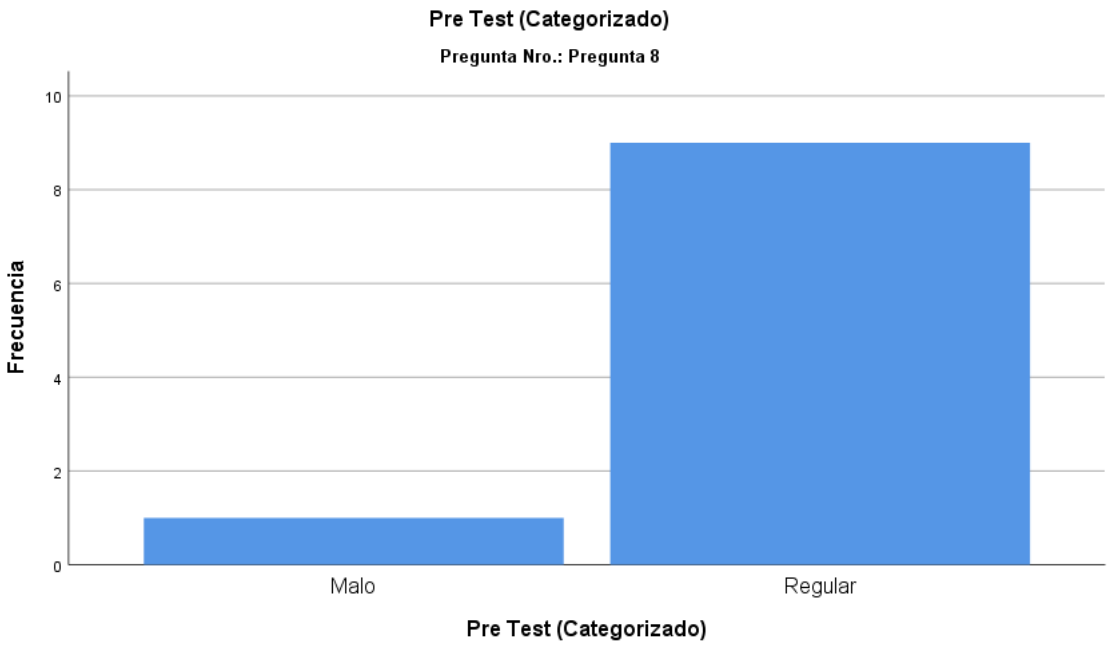
Tabla 16. Pre Test (Categorizado) – Pregunta 8

Pre Test (Categorizado)[a]

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	1	10,0	10,0	10,0
	Regular	9	90,0	90,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 09. Pre Test (Categorizado) – Pregunta 8



Fuente: Elaboración propia.

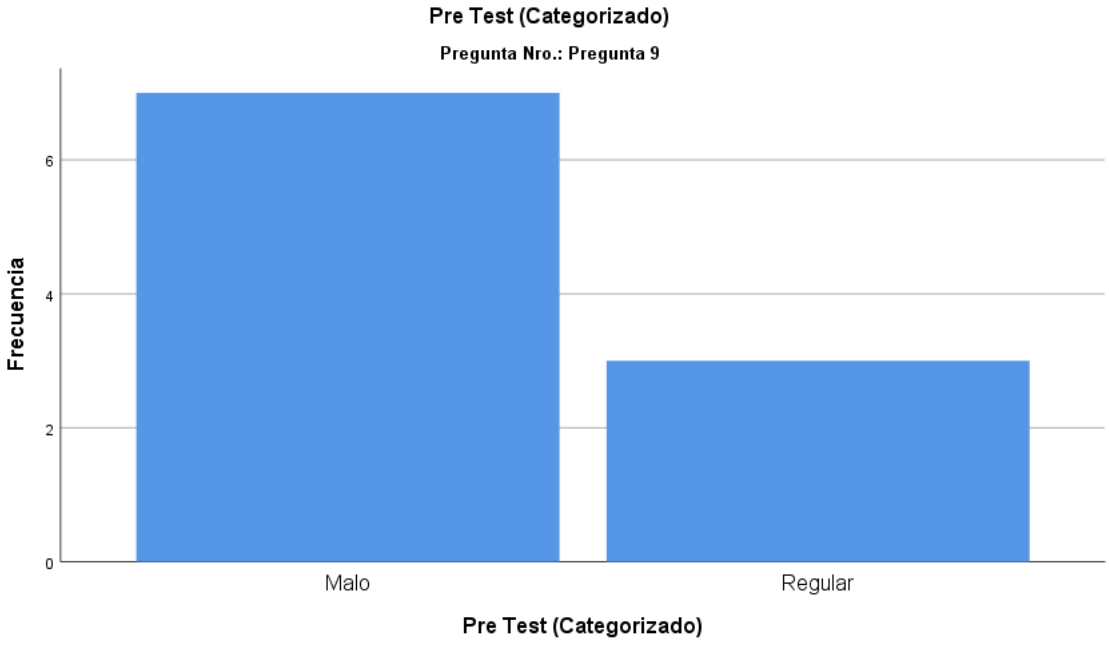
En la Tabla 16 y Gráfico 10, los encuestados indican un 90% como Regular el nivel de implementación de áreas seguras en las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas, mientras que un 10%, lo señala como Malo.

Tabla 17. Pre Test (Categorizado) – Pregunta 9

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	70,0	70,0	70,0
	Regular	3	30,0	30,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 10. Pre Test (Categorizado) – Pregunta 9



Fuente: Elaboración propia.

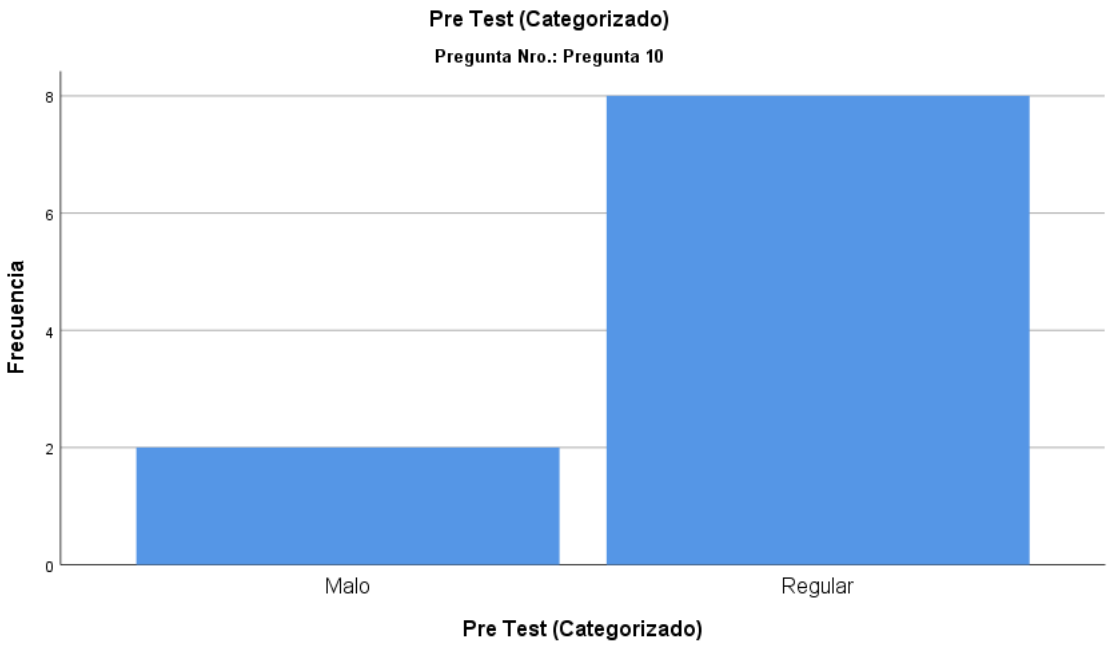
En cuanto al nivel de implementación de controles de entrada en las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas, en la Tabla 17 y Gráfico 10, los encuestados indican un 70% como Malo y 30%, regular.

Tabla 18. Pre Test (Categorizado) – Pregunta 10

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	2	20,0	20,0	20,0
	Regular	8	80,0	80,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico11. Pre Test (Categorizado) – Pregunta 10



Fuente: Elaboración propia.

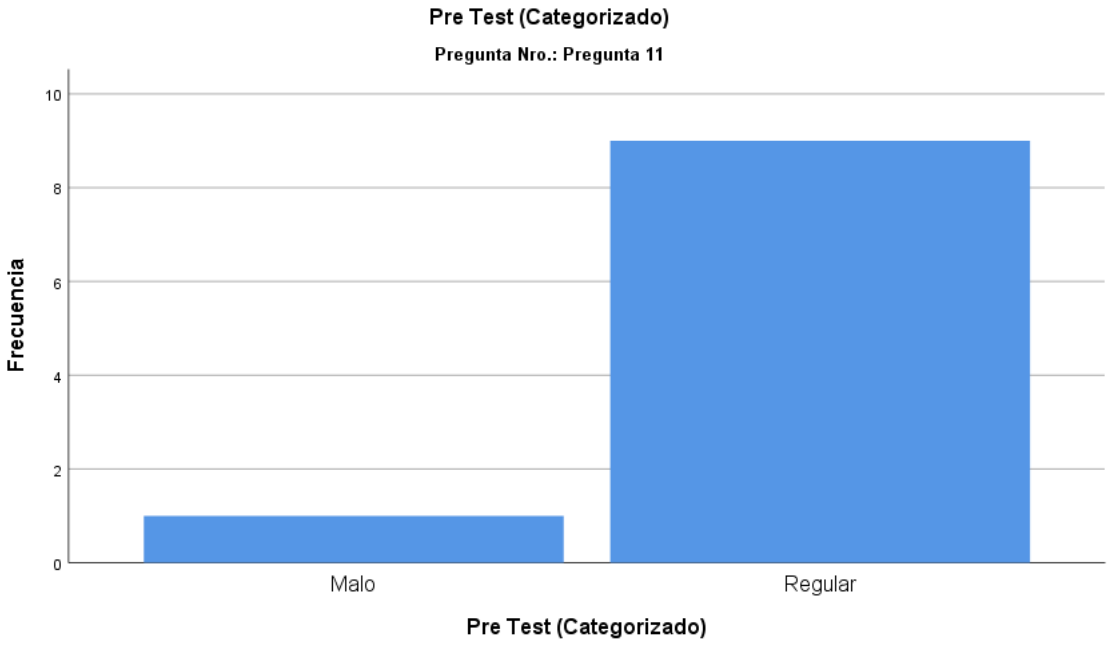
En cuanto al nivel de monitoreo en la implementación de controles de entrada en las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas, el 80% de los encuestados indicaron que se encuentra en un nivel Regular, mientras que el 20% restante, indicó un nivel Malo.

Tabla 19. Pre Test (Categorizado) – Pregunta 11

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	1	10,0	10,0	10,0
	Regular	9	90,0	90,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 12. Pre Test (Categorizado) – Pregunta 11



Fuente: Elaboración propia.

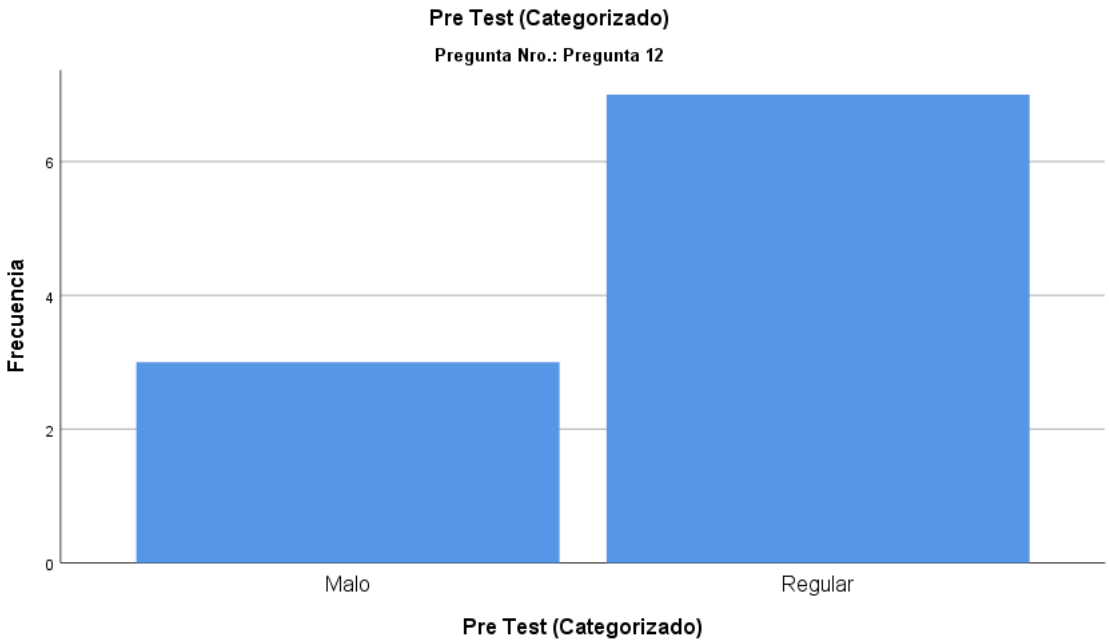
Al evaluar el nivel de protección contra amenazas en las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas, en la Tabla 19 y Gráfico 12, un 90% de los encuestados lo indican como Regular y un 10% como malo.

Tabla 20. Pre Test (Categorizado) – Pregunta 12

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	3	30,0	30,0	30,0
	Regular	7	70,0	70,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 13. Pre Test (Categorizado) – Pregunta 12



Fuente: Elaboración propia.

Ante la pregunta: ¿En qué forma considera usted que se monitorea el nivel de protección contra amenazas en las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas?, el 70% lo considera Regular y el 30% como malo. No existen respuestas positivas en este punto, tal como lo expresa la Tabla 20 y Gráfico 13.

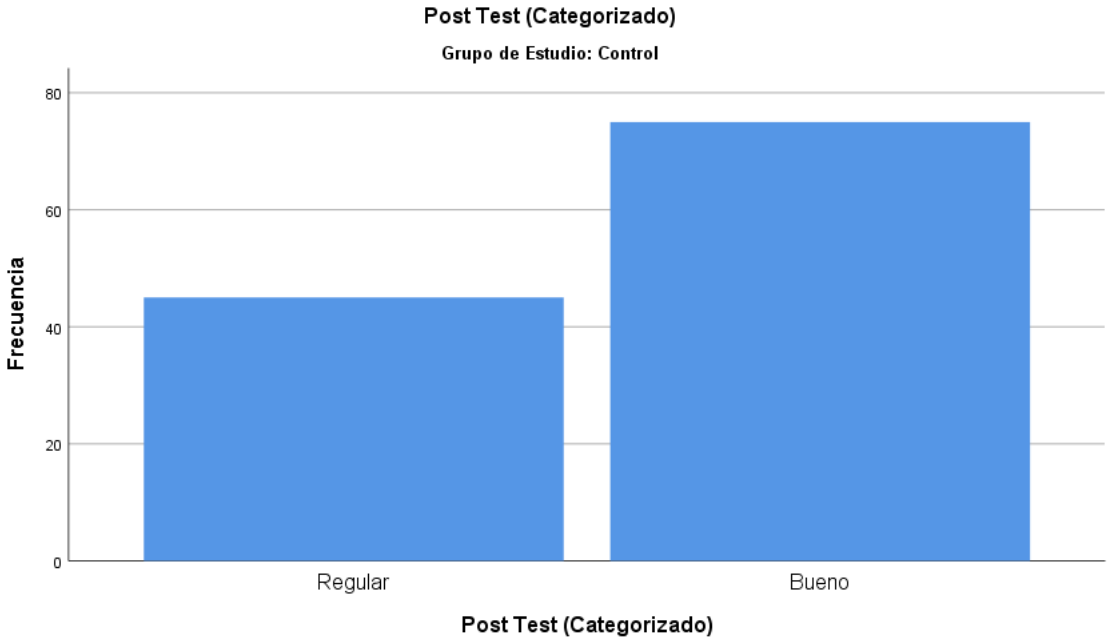
4.1.6 Estadísticos descriptivos – Frecuencias Post Test

Tabla 21. Post Test (Categorizado)

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	45	37,5	37,5	37,5
	Bueno	75	62,5	62,5	100,0
	Total	120	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 14. Post Test (Categorizado)



Fuente: Elaboración propia.

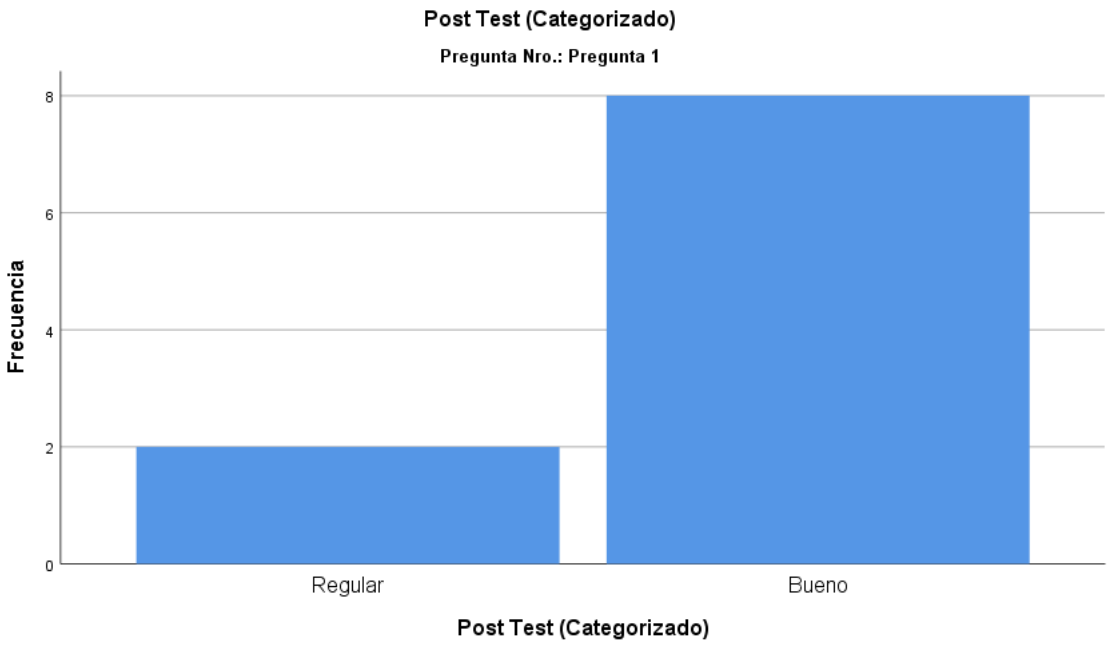
4.1.7 Estadísticos Descriptivos – Frecuencias Post Test por Pregunta (Categorizado)

Tabla 22. Post Test (Categorizado) – Pregunta 1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	2	20,0	20,0	20,0
	Bueno	8	80,0	80,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 15. Post Test (Categorizado) – Pregunta 1



Fuente: Elaboración propia.

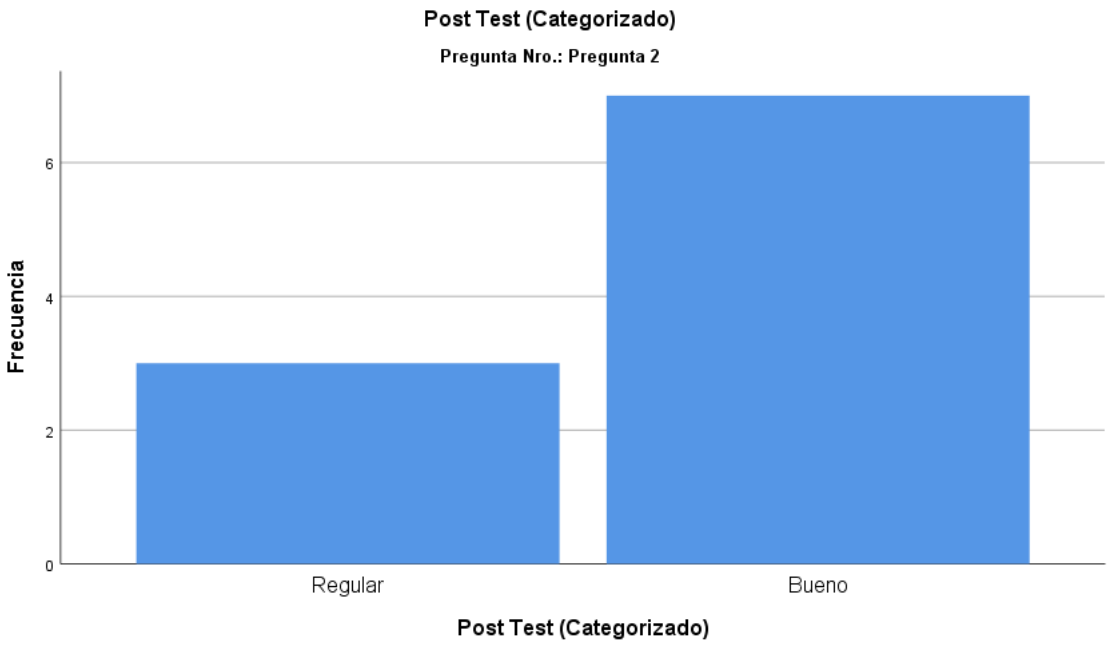
Luego de implementado el sistema de seguridad, el nivel de confianza del sistema de registro de accesos al datacenter del Departamento de Informática de la municipalidad distrital de las amazonas, sube considerablemente, alcanzando una calificación de 80% bueno y sólo un 20% como regular.

Tabla 23. Post Test (Categorizado) – Pregunta 2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	3	30,0	30,0	30,0
	Bueno	7	70,0	70,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 16. Post Test (Categorizado) – Pregunta 2



Fuente: Elaboración propia.

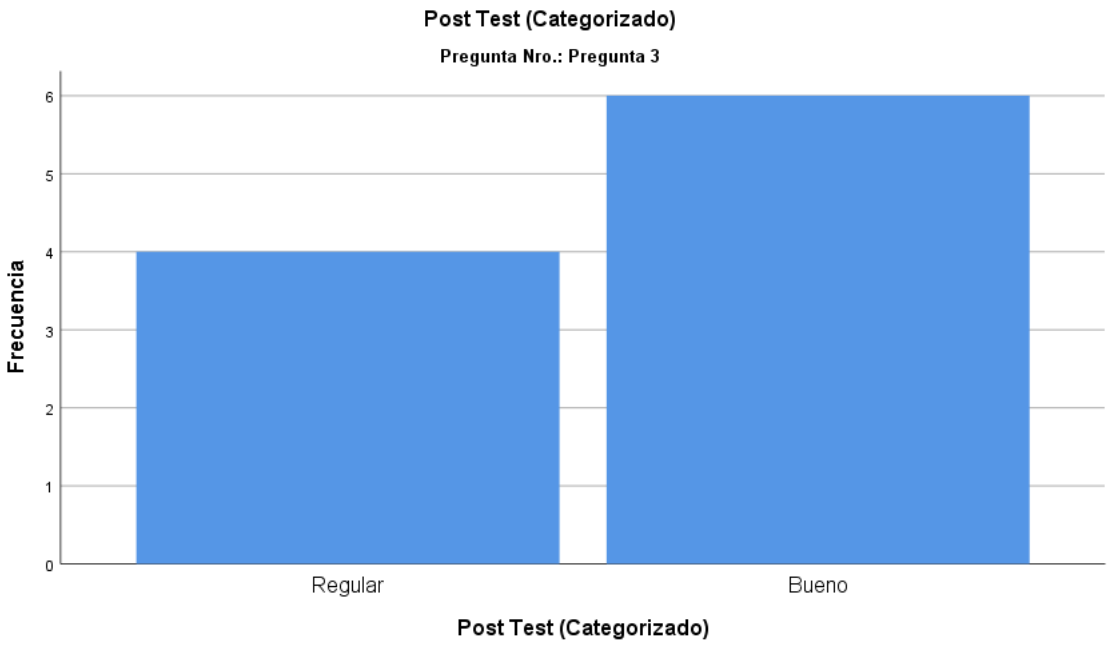
La Tabla 23 y Gráfico 16, correspondiente a la percepción de confianza en el sistema de registro de accesos al datacenter, los encuestados lo encuentran como un 70% Bueno y 30% regular, luego de implementadas las mejoras de seguridad.

Tabla 24. Post Test (Categorizado) – Pregunta 3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	4	40,0	40,0	40,0
	Bueno	6	60,0	60,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 17. Post Test (Categorizado) – Pregunta 3



Fuente: Elaboración propia.

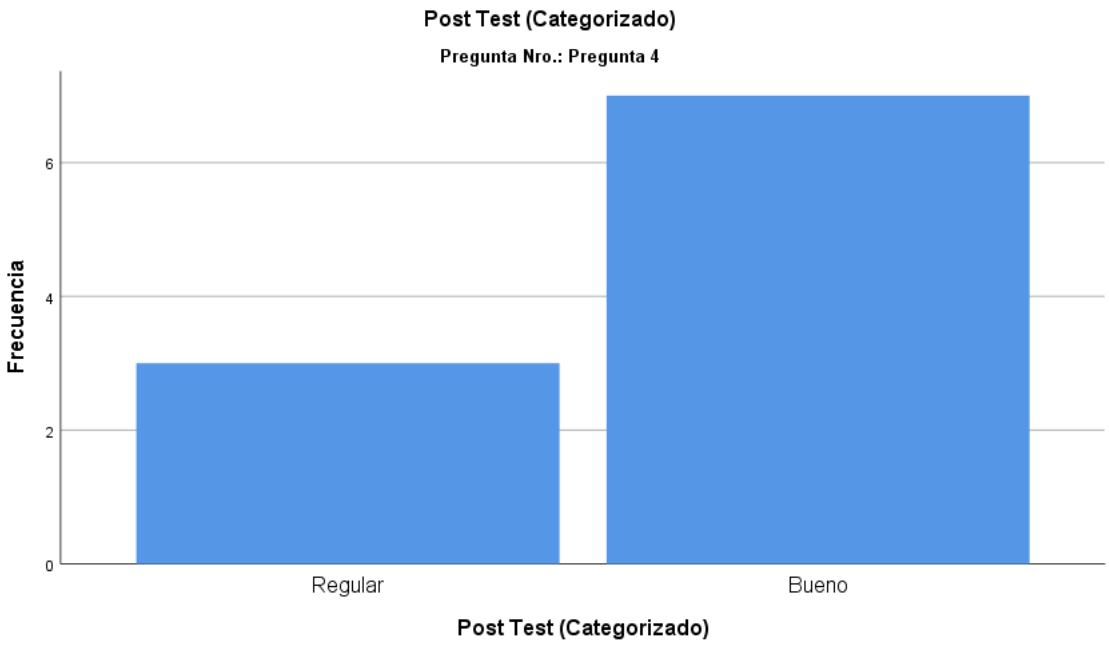
En cuanto a la sencillez en el uso del sistema de registro de accesos al datacenter del Departamento de Informática de la municipalidad distrital de las amazonas, la Tabla 24 y Gráfico 17, muestra que los encuestados lo califican como 60% Bueno y 40% Regular.

Tabla 25. Post Test (Categorizado) – Pregunta 4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	3	30,0	30,0	30,0
	Bueno	7	70,0	70,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 18. Post Test (Categorizado) – Pregunta 4



Fuente: Elaboración propia.

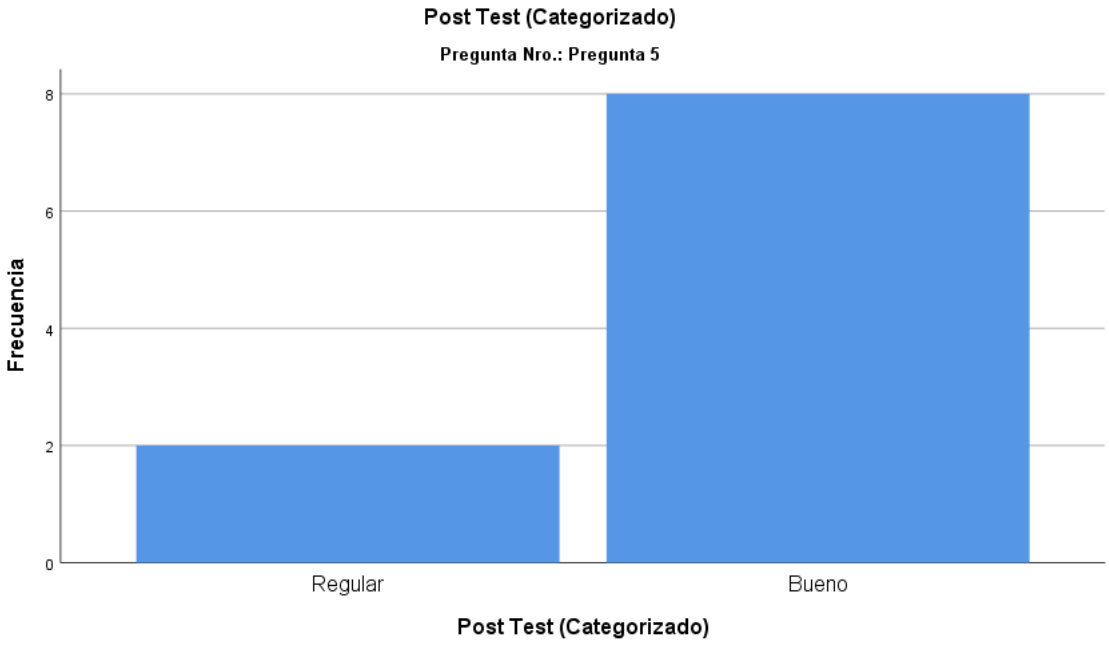
En relación con el punto anterior, luego de implementadas las medidas de seguridad, un 70% de los encuestados consideran que las mejoras en el nivel de usabilidad del sistema de registro de accesos al datacenter investigado, es Bueno. Por otro lado, un 30% lo consideran Regular.

Tabla 26. Post Test (Categorizado) – Pregunta 5

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	2	20,0	20,0	20,0
	Bueno	8	80,0	80,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 19. Post Test (Categorizado) – Pregunta 5



Fuente: Elaboración propia.

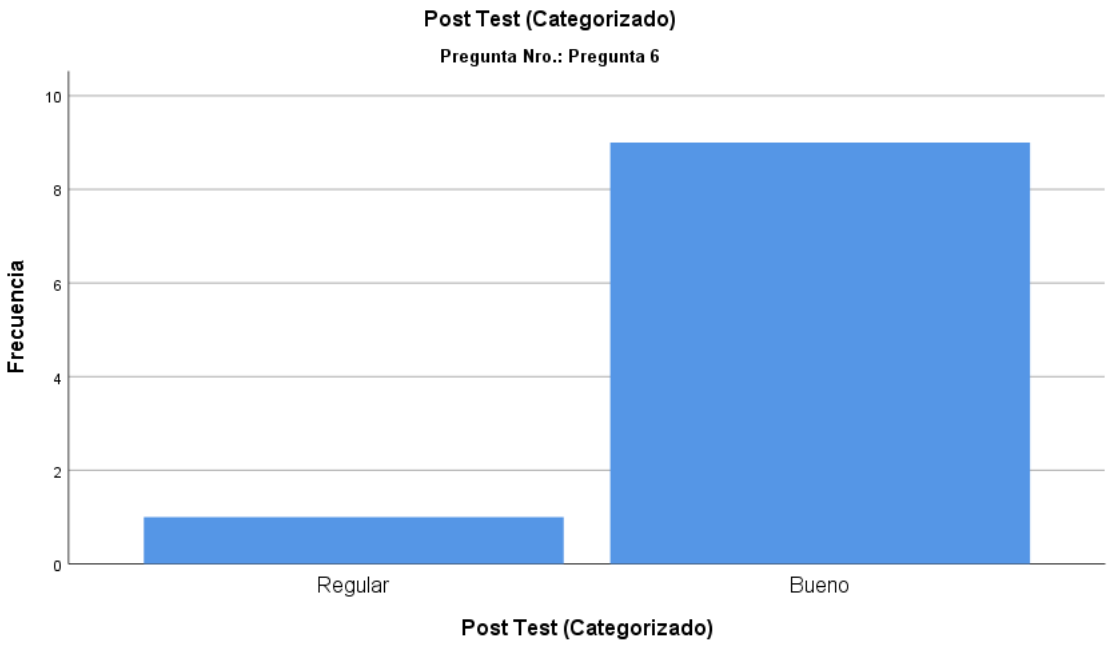
En cuanto a las características que hacen que el sistema de seguridad, sea práctico y utilitario, es decir, el nivel de funcionalidad, los encuestados lo califican como 80% Bueno y 20% regular, tal como lo muestra la Tabla 26 y Gráfico 19. Es preciso indicar, que, en la encuesta post test, no encontramos respuestas negativas (índice Malo).

Tabla 27. Post Test (Categorizado) – Pregunta 6

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	1	10,0	10,0	10,0
	Bueno	9	90,0	90,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 20. Post Test (Categorizado) – Pregunta 6



Fuente: Elaboración propia.

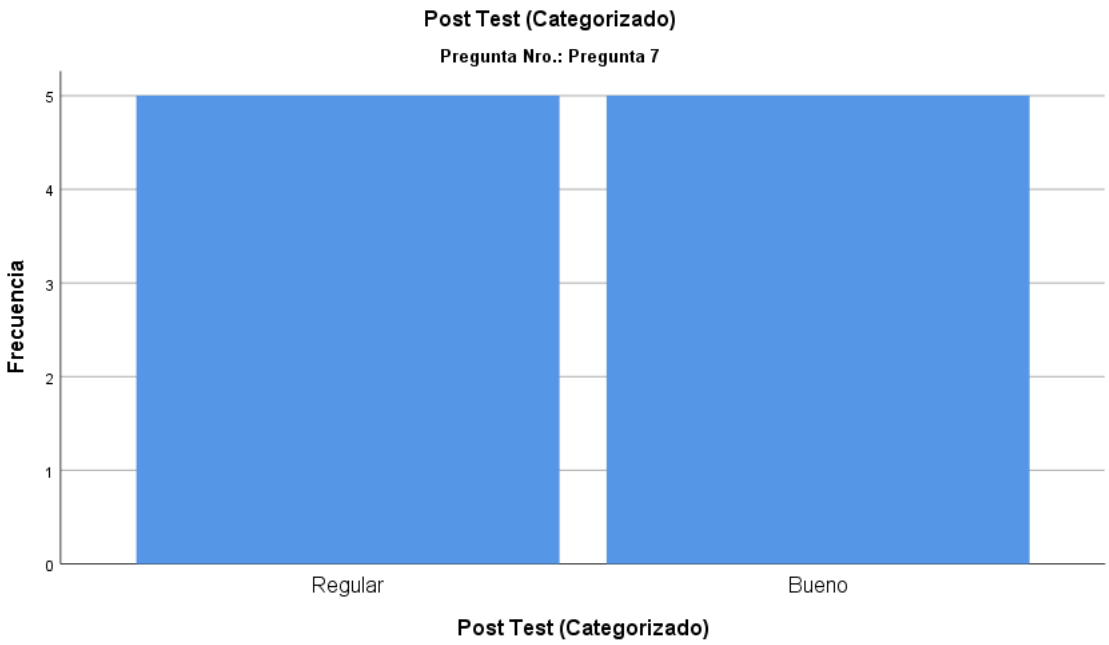
En línea como los resultados del punto anterior, los encuestados consideran que las mejoras en la funcionalidad del sistema de registro de accesos al datacenter del Departamento de Informática de la municipalidad distrital de las amazonas – Iquitos, se encuentran en un 90% Bueno y sólo 10% lo considera Regular, siendo un resultado óptimo para la investigación.

Tabla 28. Post Test (Categorizado) – Pregunta 7

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	5	50,0	50,0	50,0
	Bueno	5	50,0	50,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 21. Post Test (Categorizado) – Pregunta 7



Fuente: Elaboración propia.

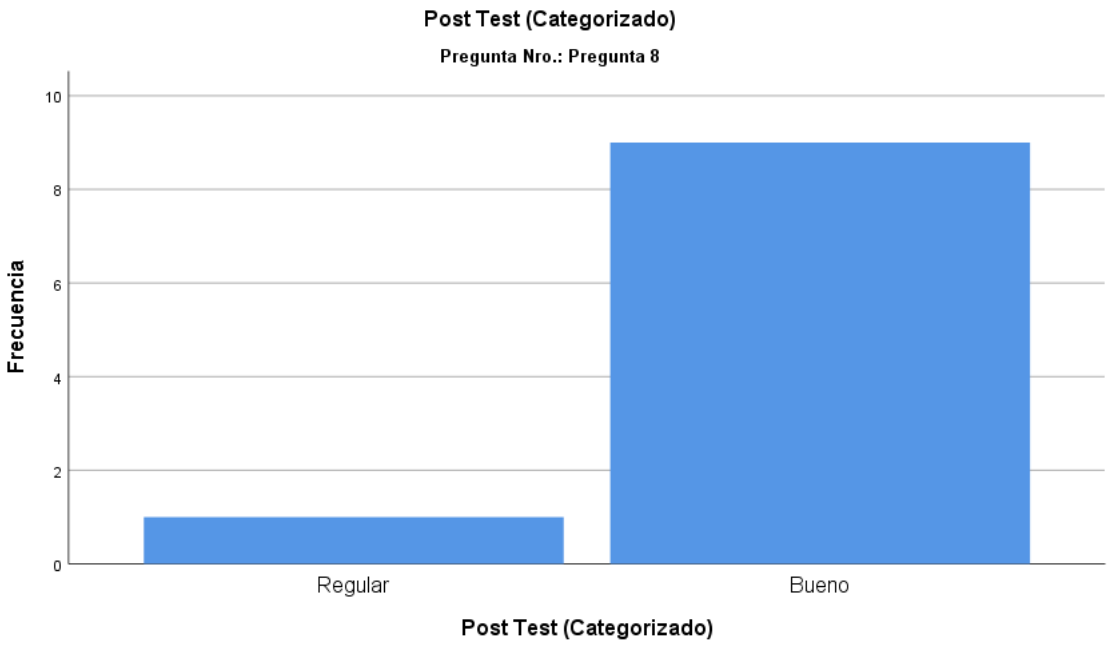
En cuanto a la calificación del nivel de seguridad en el acceso físico al datacenter en cuestión, un 50% de los encuestados lo consideran Bueno y el otro 50%, Regular. Pese a estos resultados, la percepción de los encuestados, ha mejorado, puesto que antes de la implementación de las medidas de seguridad, un 40% lo calificaba como Malo y un 60%, como Regular (tal como se muestra en la Tabla 15 y Gráfico 08).

Tabla 29. Post Test (Categorizado) – Pregunta 8

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	1	10,0	10,0	10,0
	Bueno	9	90,0	90,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 22. Post Test (Categorizado) – Pregunta 8



Fuente: Elaboración propia.

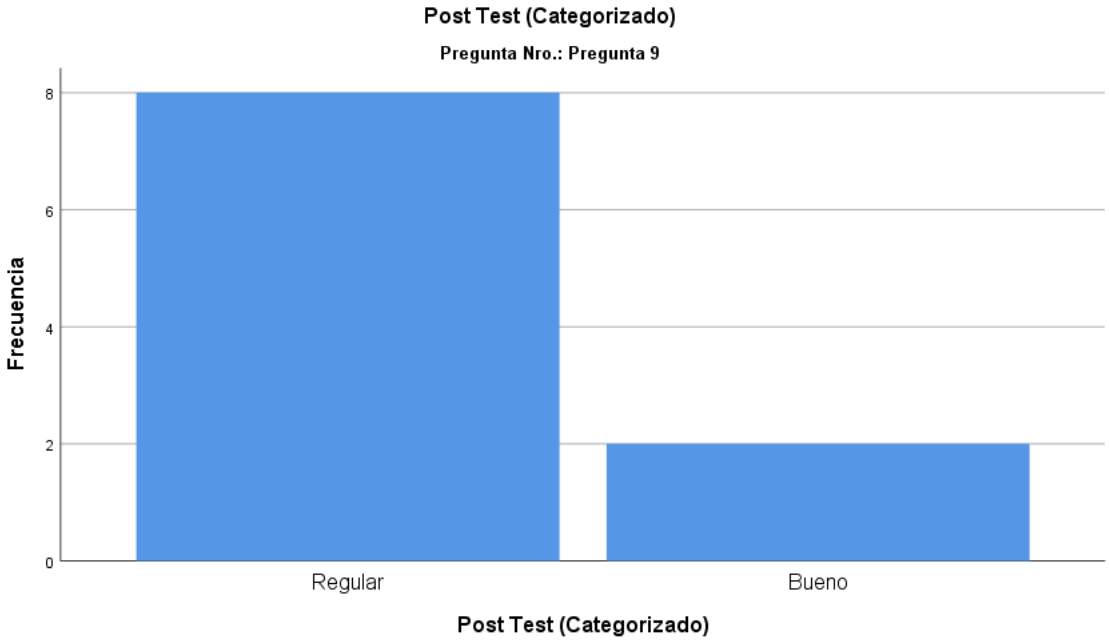
En la Tabla 29 y Gráfico 22, se muestra que un 90% de los encuestados, califican al nivel de implementación de áreas seguras en las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas, como Bueno y sólo un 10% como Regular. Estos resultados son alentadores para la investigación realizada.

Tabla 30. Post Test (Categorizado) – Pregunta 9

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	8	80,0	80,0	80,0
	Bueno	2	20,0	20,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 23. Post Test (Categorizado) – Pregunta 9



Fuente: Elaboración propia.

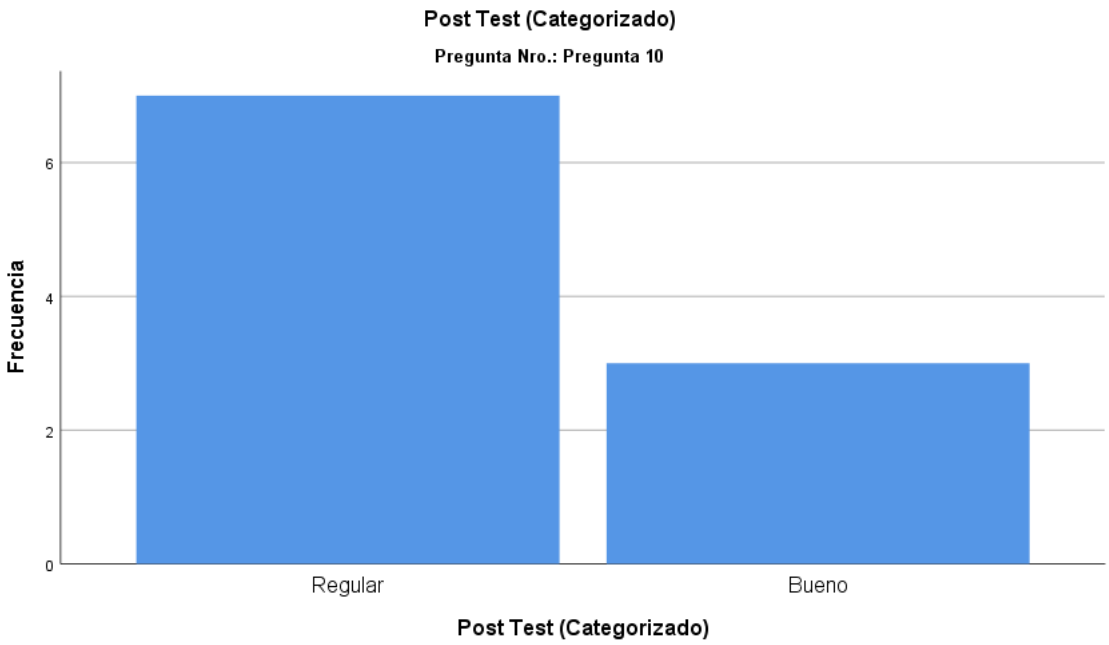
En cuanto al nivel de implementación de controles de entrada en las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas, un 80% de encuestados lo califica como Regular y un 20%, como Bueno. A pesar de estos datos, resulta positivo si lo comparamos con los resultados del pre test, donde un 70% lo calificaba como Malo y un 30%, Regular.

Tabla 31. Post Test (Categorizado) – Pregunta 10

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	7	70,0	70,0	70,0
	Bueno	3	30,0	30,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 24. Post Test (Categorizado) – Pregunta 10



Fuente: Elaboración propia.

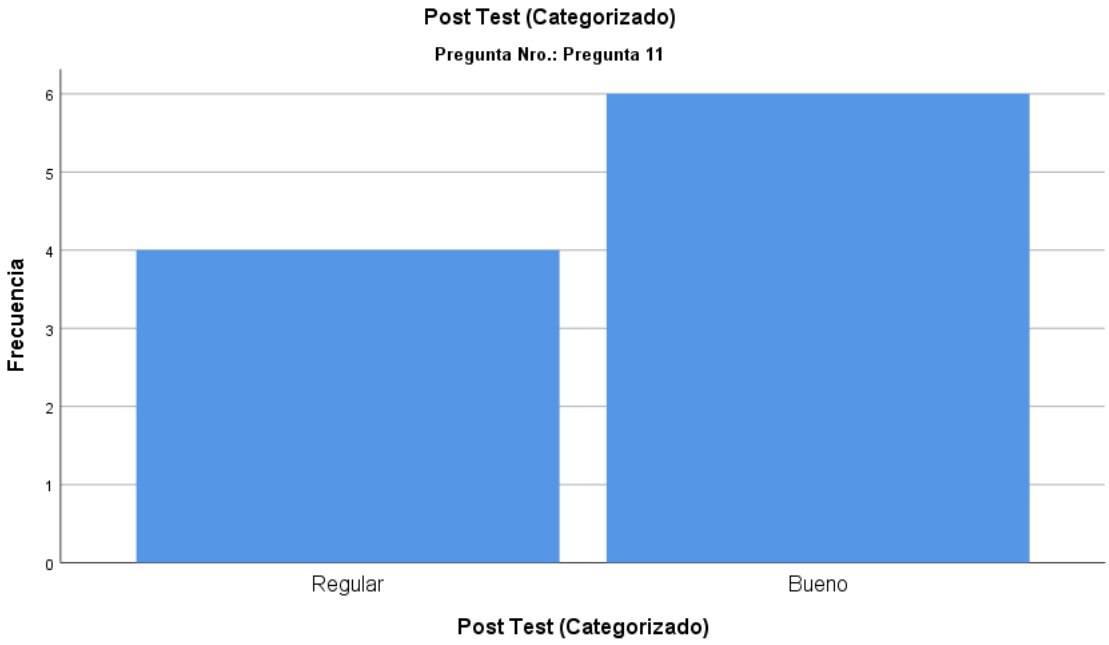
Ante la pregunta: ¿En qué forma considera usted que se monitorea el nivel de implementación de controles de entrada en las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas?, en la Tabla 31 y Gráfico 24, un 70% de los encuestados lo califica como Regular y un 30% como Bueno.

Tabla 32. Post Test (Categorizado) – Pregunta 11

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	4	40,0	40,0	40,0
	Bueno	6	60,0	60,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 25. Post Test (Categorizado) – Pregunta 11



Fuente: Elaboración propia.

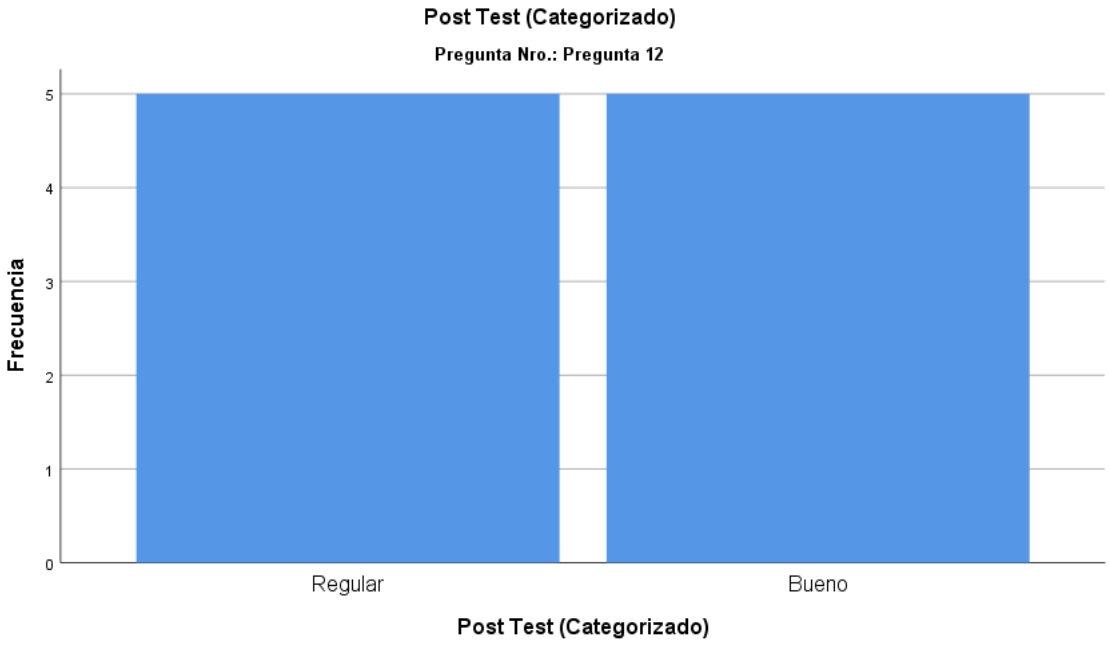
En la Tabla 32 y Gráfico 25, que corresponde al nivel de protección contra amenazas en las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas, los encuestados lo consideran un 60% Bueno y un 40% Regular. Contrasta con el 90% Regular y 10% Malo, que indicaron los encuestados en la evaluación pre test.

Tabla 33. Post Test (Categorizado) – Pregunta 12

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	5	50,0	50,0	50,0
	Bueno	5	50,0	50,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico 26. Post Test (Categorizado) – Pregunta 12



Fuente: Elaboración propia.

Finalmente, en cuanto al monitoreo del nivel de protección contra amenazas en las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas, un 50% de los encuestados lo califica como Bueno y el 50% restante, como Regular.

4.1.8 Resumen de procesamiento de casos (Pre y Post test)

Tabla 34. Resumen Pregunta 1

		Pre Test (Categorizado)	Post Test (Categorizado)
1		Malo	Bueno
2		Malo	Bueno
3		Regular	Bueno
4		Regular	Bueno
5		Malo	Regular
6		Regular	Bueno
7		Regular	Bueno
8		Malo	Regular
9		Malo	Bueno
10		Malo	Bueno
Total	N	10	10
	Media	1,40	2,80
	Mediana	1,00	3,00
	Suma	14	28
	Mínimo	Malo	Regular
	Máximo	Regular	Bueno
	Desv. Desviación	,516	,422
	Varianza	,267	,178
	Curtosis	-2,277	1,406
	Media armónica	1,25	2,73
	Media geométrica	1,32	2,77
	Error estándar de asimetría	,687	,687
	Asimetría	,484	-1,779

Fuente: Elaboración propia.

Tabla 35. Resumen Pregunta 2

		Pre Test (Categorizado)	Post Test (Categorizado)
1		Malo	Regular
2		Malo	Regular
3		Malo	Bueno
4		Malo	Bueno
5		Regular	Bueno
6		Regular	Bueno
7		Regular	Bueno
8		Malo	Regular
9		Regular	Bueno
10		Regular	Bueno
Total	N	10	10
	Media	1,50	2,70
	Mediana	1,50	3,00
	Suma	15	27
	Mínimo	Malo	Regular
	Máximo	Regular	Bueno
	Desv. Desviación	,527	,483
	Varianza	,278	,233
	Curtosis	-2,571	-1,224
	Media armónica	1,33	2,61
	Media geométrica	1,41	2,66
	Error estándar de asimetría	,687	,687
	Asimetría	,000	-1,035

Fuente: Elaboración propia.

Tabla 36. Resumen Pregunta 3

		Pre Test (Categorizado)	Post Test (Categorizado)
1		Malo	Bueno
2		Malo	Bueno
3		Malo	Bueno
4		Malo	Regular
5		Malo	Bueno
6		Malo	Bueno
7		Regular	Regular
8		Regular	Bueno
9		Malo	Regular
10		Malo	Regular
Total	N	10	10
	Media	1,20	2,60
	Mediana	1,00	3,00
	Suma	12	26
	Mínimo	Malo	Regular
	Máximo	Regular	Bueno
	Desv. Desviación	,422	,516
	Varianza	,178	,267
	Curtosis	1,406	-2,277
	Media armónica	1,11	2,50
	Media geométrica	1,15	2,55
	Error estándar de asimetría	,687	,687
	Asimetría	1,779	-,484

Fuente: Elaboración propia.

Tabla 37. Resumen Pregunta 4

		Pre Test (Categorizado)	Post Test (Categorizado)
1		Malo	Bueno
2		Malo	Regular
3		Malo	Bueno
4		Regular	Bueno
5		Regular	Bueno
6		Regular	Bueno
7		Regular	Bueno
8		Malo	Regular
9		Malo	Bueno
10		Malo	Regular
Total	N	10	10
	Media	1,40	2,70
	Mediana	1,00	3,00
	Suma	14	27
	Mínimo	Malo	Regular
	Máximo	Regular	Bueno
	Desv. Desviación	,516	,483
	Varianza	,267	,233
	Curtosis	-2,277	-1,224
	Media armónica	1,25	2,61
	Media geométrica	1,32	2,66
	Error estándar de asimetría	,687	,687
	Asimetría	,484	-1,035

Fuente: Elaboración propia.

Tabla 38. Resumen Pregunta 5

		Pre Test (Categorizado)	Post Test (Categorizado)
1		Malo	Bueno
2		Malo	Bueno
3		Malo	Bueno
4		Malo	Regular
5		Regular	Bueno
6		Regular	Bueno
7		Regular	Bueno
8		Regular	Bueno
9		Regular	Bueno
10		Malo	Regular
Total	N	10	10
	Media	1,50	2,80
	Mediana	1,50	3,00
	Suma	15	28
	Mínimo	Malo	Regular
	Máximo	Regular	Bueno
	Desv. Desviación	,527	,422
	Varianza	,278	,178
	Curtosis	-2,571	1,406
	Media armónica	1,33	2,73
	Media geométrica	1,41	2,77
	Error estándar de asimetría	,687	,687
	Asimetría	,000	-1,779

Fuente: Elaboración propia.

Tabla 39. Resumen Pregunta 6

		Pre Test (Categorizado)	Post Test (Categorizado)
1		Malo	Regular
2		Malo	Bueno
3		Malo	Bueno
4		Malo	Bueno
5		Malo	Bueno
6		Regular	Bueno
7		Regular	Bueno
8		Regular	Bueno
9		Regular	Bueno
10		Regular	Bueno
Total	N	10	10
	Media	1,50	2,90
	Mediana	1,50	3,00
	Suma	15	29
	Mínimo	Malo	Regular
	Máximo	Regular	Bueno
	Desv. Desviación	,527	,316
	Varianza	,278	,100
	Curtosis	-2,571	10,000
	Media armónica	1,33	2,86
	Media geométrica	1,41	2,88
	Error estándar de asimetría	,687	,687
	Asimetría	,000	-3,162

Fuente: Elaboración propia.

Tabla 40. Resumen Pregunta 7

		Pre Test (Categorizado)	Post Test (Categorizado)
1		Malo	Bueno
2		Malo	Regular
3		Malo	Regular
4		Regular	Bueno
5		Regular	Bueno
6		Regular	Bueno
7		Regular	Bueno
8		Regular	Regular
9		Regular	Regular
10		Malo	Regular
Total	N	10	10
	Media	1,60	2,50
	Mediana	2,00	2,50
	Suma	16	25
	Mínimo	Malo	Regular
	Máximo	Regular	Bueno
	Desv. Desviación	,516	,527
	Varianza	,267	,278
	Curtosis	-2,277	-2,571
	Media armónica	1,43	2,40
	Media geométrica	1,52	2,45
	Error estándar de asimetría	,687	,687
	Asimetría	-,484	,000

Fuente: Elaboración propia.

Tabla 41. Resumen Pregunta 8

		Pre Test (Categorizado)	Post Test (Categorizado)
1		Malo	Regular
2		Regular	Bueno
3		Regular	Bueno
4		Regular	Bueno
5		Regular	Bueno
6		Regular	Bueno
7		Regular	Bueno
8		Regular	Bueno
9		Regular	Bueno
10		Regular	Bueno
Total	N	10	10
	Media	1,90	2,90
	Mediana	2,00	3,00
	Suma	19	29
	Mínimo	Malo	Regular
	Máximo	Regular	Bueno
	Desv. Desviación	,316	,316
	Varianza	,100	,100
	Curtosis	10,000	10,000
	Media armónica	1,82	2,86
	Media geométrica	1,87	2,88
	Error estándar de asimetría	,687	,687
	Asimetría	-3,162	-3,162

Fuente: Elaboración propia.

Tabla 42. Resumen Pregunta 9

		Pre Test (Categorizado)	Post Test (Categorizado)
1		Regular	Regular
2		Regular	Bueno
3		Regular	Bueno
4		Malo	Regular
5		Malo	Regular
6		Malo	Regular
7		Malo	Regular
8		Malo	Regular
9		Malo	Regular
10		Malo	Regular
Total	N	10	10
	Media	1,30	2,20
	Mediana	1,00	2,00
	Suma	13	22
	Mínimo	Malo	Regular
	Máximo	Regular	Bueno
	Desv. Desviación	,483	,422
	Varianza	,233	,178
	Curtosis	-1,224	1,406
	Media armónica	1,18	2,14
	Media geométrica	1,23	2,17
	Error estándar de asimetría	,687	,687
	Asimetría	1,035	1,779

Fuente: Elaboración propia.

Tabla 43. Resumen Pregunta 10

		Pre Test (Categorizado)	Post Test (Categorizado)
1		Malo	Regular
2		Malo	Regular
3		Regular	Bueno
4		Regular	Regular
5		Regular	Bueno
6		Regular	Regular
7		Regular	Regular
8		Regular	Bueno
9		Regular	Regular
10		Regular	Regular
Total	N	10	10
	Media	1,80	2,30
	Mediana	2,00	2,00
	Suma	18	23
	Mínimo	Malo	Regular
	Máximo	Regular	Bueno
	Desv. Desviación	,422	,483
	Varianza	,178	,233
	Curtosis	1,406	-1,224
	Media armónica	1,67	2,22
	Media geométrica	1,74	2,26
	Error estándar de asimetría	,687	,687
	Asimetría	-1,779	1,035

Fuente: Elaboración propia.

Tabla 44. Resumen Pregunta 11

		Pre Test (Categorizado)	Post Test (Categorizado)
1		Regular	Regular
2		Regular	Bueno
3		Regular	Bueno
4		Regular	Regular
5		Malo	Regular
6		Regular	Bueno
7		Regular	Regular
8		Regular	Bueno
9		Regular	Bueno
10		Regular	Bueno
Total	N	10	10
	Media	1,90	2,60
	Mediana	2,00	3,00
	Suma	19	26
	Mínimo	Malo	Regular
	Máximo	Regular	Bueno
	Desv. Desviación	,316	,516
	Varianza	,100	,267
	Curtosis	10,000	-2,277
	Media armónica	1,82	2,50
	Media geométrica	1,87	2,55
	Error estándar de asimetría	,687	,687
	Asimetría	-3,162	-,484

Fuente: Elaboración propia.

Tabla 45. Resumen Pregunta 12

		Pre Test (Categorizado)	Post Test (Categorizado)
1		Regular	Bueno
2		Malo	Regular
3		Malo	Regular
4		Regular	Bueno
5		Regular	Regular
6		Regular	Regular
7		Regular	Bueno
8		Regular	Bueno
9		Malo	Regular
10		Regular	Bueno
Total	N	10	10
	Media	1,70	2,50
	Mediana	2,00	2,50
	Suma	17	25
	Mínimo	Malo	Regular
	Máximo	Regular	Bueno
	Desv. Desviación	,483	,527
	Varianza	,233	,278
	Curtosis	-1,224	-2,571
	Media armónica	1,54	2,40
	Media geométrica	1,62	2,45
	Error estándar de asimetría	,687	,687
	Asimetría	-1,035	,000

Fuente: Elaboración propia.

CAPÍTULO V
DISCUSIÓN, CONCLUSIONES Y RECOMENDACIONES

5.1 DISCUSIÓN

Los recursos de IoT, ya desempeñan un rol importante en el proceso de transformación digital de las organizaciones, teniendo a la mano un mundo de oportunidades y herramientas. Estos recursos, contribuyen a mejorar sus procesos, en diferentes aspectos organizacionales.

En materia de seguridad, las organizaciones deben aplicar medidas orientadas a proteger sus instalaciones, así como la información que posean, ante cualquier amenaza, de manera que se pueda garantizar, en todo momento, la continuidad de las actividades de la organización.

Implementar innovación tecnológica basada en herramientas con IoT, resulta considerablemente positivo para la seguridad las organizaciones y, específicamente, del Departamento de Informática de la municipalidad distrital de las amazonas, así como de su datacenter, tal como lo muestran los resultados de la presente investigación.

La población tomada en cuenta para este análisis, representó al 100% de los trabajadores del Departamento de Informática de la municipalidad distrital de las amazonas - Iquitos (10 personas), ayudando a la obtención de resultados confiables.

En relación con la investigación de (Córdova Toro, 2017), que lleva como título “Elaboración de prácticas de aprendizaje de programación con software libre aplicado a la plataforma Raspberry Pi 3, orientado a estudiantes de bachillerato”, concluye que los estudiantes asimilan con gran facilidad, los contenidos de programación, ya que se comprobó que el centro de cómputo de la unidad educativa, está bien equipado y resulta fácil adaptar la tarjeta Raspberry Pi 3, para que los estudiantes puedan hacer uso de esta y desarrollar sus conocimientos sobre las TICS. Es decir, resulta bueno el nivel de usabilidad de los recursos de este centro de cómputo, lo que guarda

relación con lo expresado en la Tabla 24 y Gráfico 17, donde un 60% de encuestados califica como Bueno el nivel de usabilidad de las medidas de seguridad implementadas en el Departamento de Informática de la municipalidad distrital de las amazonas – Iquitos.

La investigación de (Zapata Romero, y otros, 2016), titulada “Sistema de detección de movimiento para uso residencial, con notificación a móviles, utilizando el microcomputador Raspberry Pi”, concluye que, con el uso de estos equipos de bajo costo, se pueden construir sistemas de seguridad eficientes, así como lograr solventar tareas básicas domésticas de manera automatizada. Este punto, guarda relación con lo expresado en la Tabla 28 y Gráfico 21, donde los encuestados de nuestra investigación, han visto un incremento en el nivel de seguridad en el acceso físico al datacenter del Departamento de Informática de la municipalidad distrital de las amazonas, gracias a uso de tecnología IoT.

Según (Huivín Suárez, 2017) en su tesis titulada: “Implementación de un sistema informático para el control de riego de cultivos, empleando IoT con Raspberry Pi, en el vivero de la Municipalidad Provincial de San Martín, 2017”, concluye que el sistema informático influye significativamente en el Control de Riego de Cultivos, empleando IoT con Raspberry Pi.
Es decir, el sistema informático con IoT, es funcional a los objetivos de la institución. Esta conclusión, se relaciona con lo expresado en la Tabla 26 y Gráfico 19, donde un 80% de los encuestados califica como Bueno, el nivel de funcionalidad del sistema de registro de accesos al datacenter del Departamento de Informática de la municipalidad distrital de las amazonas – Iquitos.

Según (Bardales Cabanillas, 2020) en su tesis titulada: “Evaluación del potencial del empleo de aplicativos Android, en los experimentos del laboratorio del curso de Física General. Iquitos 2020”, concluye que los sistemas basados en IoT, facilitan la recolección de datos, aseguran la

calidad de resultados y facilitan el procesamiento y visualización de los resultados. En relación a esta conclusión, la Tabla 27 y Gráfico 20, nos muestra una mejora sustancial, en la funcionalidad del sistema de accesos al datacenter del Departamento de Informática de la municipalidad distrital de las amazonas, confirmando la eficiencia de los sistemas basados en IoT.

En concordancia con la tesis de (López Gonzales, 2018), titulada “Aplicación de un sistema de control mediante cámaras de vigilancia, para mejorar el control de paneles publicitarios electrónicos en la ciudad de Iquitos 2018”, asegura que esta tendrá un impacto positivo en las empresas y usuarios de este servicio. Es decir, existe un alto grado de confianza en el sistema de control de paneles publicitarios, lo que guarda relación con lo expresado en la Tabla 23 y Gráfico 16, respecto a la mejora en el nivel de confianza de las medidas de seguridad implementadas en el Departamento de Informática de la municipalidad distrital de las amazonas.

5.2 CONCLUSIONES

Para salvaguardar los intereses de una organización o institución, esta debe invertir en su seguridad, en todos sus niveles. En este punto, podemos hablar de seguridad financiera, seguridad jurídica, seguridad informática o seguridad laboral. Todas ellas evitan riesgos y pérdidas, para garantizar una administración eficiente.

En lo que concierne a esta investigación, la seguridad informática y de acceso físico a las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas, requerían mejoras que garanticen un sistema de seguridad robusto, eficiente y confiable.

En línea con el desarrollo de esta investigación, hemos llegado a las siguientes conclusiones:

a. La implementación de un sistema de seguridad basado en IoT, para registrar a las personas que ingresan al datacenter, ha logrado mejorar sustancialmente la seguridad del mismo, evitando riesgos y reduciendo

pérdidas en el Departamento de Informática de la municipalidad distrital de las amazonas.

b. Se logró una mejora valiosa en la seguridad del datacenter, con la implementación del dispositivo de captura de imágenes y registro de datos, de las personas que acceden físicamente a él, restringiendo el acceso a personal no autorizado.
c. La seguridad expresada en las conclusiones anteriores, también se vio reforzada con la emisión de notificaciones por email, al personal encargado de la seguridad del Departamento de Informática de la municipalidad distrital de las amazonas.

El Departamento de Informática de la municipalidad distrital de las amazonas, cuenta ahora con un sistema de seguridad confiable, que, si bien requerirá mejoras graduales, es más funcional a los intereses de la institución.

5.3 RECOMENDACIONES

Del análisis de la investigación realizada, podemos proponer las siguientes recomendaciones:

- Garantizar el mantenimiento oportuno y adecuado, a través de planes de mantenimiento; así como la actualización del sistema y dispositivos utilizados en la seguridad, tanto del Departamento de Informática, como de su datacenter.
- Implementar un sistema de suministro eléctrico ininterrumpido, para garantizar el funcionamiento continuo del sistema de seguridad.
- Adecuar el sistema de seguridad, para expandir la capacidad de almacenamiento de las capturas y videos de los accesos autorizados y posibles intrusiones.
- Extender el alcance de las alertas emitidas por el sistema de seguridad, ante una intrusión fuera del horario laboral, no sólo al personal del Departamento de Informática, sino también al personal de Seguridad de la Departamento De Informática De La Municipalidad Distrital De Las Amazonas e, inclusive, a la Policía Nacional del Perú.
- Agregar un control biométrico, para reforzar la seguridad del acceso físico al datacenter, como complemento al sistema de seguridad ya instalado.

- Ampliar las funcionalidades del sistema de seguridad, implementando algún algoritmo de reconocimiento facial, para identificar a las personas autorizadas que ingresen al datacenter, evitando intrusiones a través de posibles suplantaciones.

REFERENCIAS BIBLIOGRÁFICAS

Advisera. 2019. Advisera.com. [En línea] 07 de 06 de 2019. [Citado el: 29 de 12 de 2020.] https://advisera.com/27001academy/es/knowledgebase/resumen-del-anexo-a-de-la-norma-iso-270012013/.

America Digital News. 2020. America Digital News. [En línea] 27 de 01 de 2020. [Citado el: 29 de 12 de 2020.] https://news.america-digital.com/iot-plataformas-implementacion-exitosa/.

Arduino.cl. 2018. Arduino.cl. [En línea] 28 de 05 de 2018. [Citado el: 29 de 12 de 2020.] https://arduino.cl/que-es-arduino/.

Bardales Cabanillas, Benny Bryan. 2020. *Evaluación del potencial del empleo de aplicativos Android en los experimentos del laboratorio del curso de Física General.* Iquitos : s.n., 2020.

Córdova Toro, Luis Adolfo. 2017. *Elaborqación de prácticas de aprendizaje de programación con software libre aplicado a la plataforma Raspberry Pi 3 orientado a estudiantes de bachillerato.* Guayaquil : s.n., 2017.

Equipo ALTRAN. 2016. Altran.es. [En línea] 03 de 03 de 2016. [Citado el: 29 de 12 de 2020.] https://equipo.altran.es/hardware-iot-internet-de-las-cosas/.

Hard Zone. 2020. HardZone.es. [En línea] 03 de 04 de 2020. [Citado el: 29 de 12 de 2020.] https://hardzone.es/reportajes/comparativas/raspberry-pi-vs-arduino/.

Huivín Suárez, Jonathan. 2017. *Implementación de un sistema informático para el control de riego de cultivos empleando IoT con Raspberry Pi en el vivero de la Municipalidad Provincial de San Martín.* Tarapoto : s.n., 2017.

López Gonzales, David. 2018. *Aplicación de un sistema de control mediante cámaras de vigilancia para mejorar el control de paneles publicitarios.* Iquitos : s.n., 2018.

Normas ISO 27001. 2019. NormasIso27001.es. [En línea] 19 de 10 de 2019. [Citado el: 29 de 12 de 2020.] https://normaiso27001.es/a11-seguridad-fisica-y-del-entorno/.

Normas ISO. 2019. NormasIso.com. [En línea] 21 de 02 de 2019. [Citado el: 29 de 12 de 2020.] https://www.normas-iso.com/iso-27001/.

Quintana Olarte, Elizabeth Alejandrina. 2018. *Desarrollo de un sistema de geolocalización de alerta de recojo de residuos sólidos en el distrito de San Jerónimo.* Andahuaylas : s.n., 2018.

RaspberryPi.cl. 2018. RaspberryPi.cl. [En línea] 10 de 10 de 2018. [Citado el: 29 de 12 de 2020.] https://raspberrypi.cl/que-es-raspberry/.

RedHat. 2020. RedHat.com. [En línea] 29 de 12 de 2020. [Citado el: 29 de 12 de 2020.] https://www.redhat.com/es/topics/internet-of-things/what-is-iot.

SaS Institute Inc. 2020. SaS.com. [En línea] 29 de 12 de 2020. [Citado el: 29 de 12 de 2020.] https://www.sas.com/es_pe/insights/big-data/internet-of-things.html.

Zapata Romero, Omar Octavio y Rivera Zeas, Darwin Raúl. 2016. *Sistema de detección de moviminto para uso residencial con notificación a móviles utilizando el microcomputador Raspberry Pi.* Managua : s.n., 2016.

ANEXOS

Anexo 01: Matriz de consistencia.

Anexo 02: Instrumento de recolección de datos.

Anexo 01: Matriz de consistencia

"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE REGISTRO DE ACCESOS, UTILIZANDO IoT PARA MEJORAR LA SEGURIDAD FÍSICA EN EL DATACENTER DEL DEPARTAMENTO DE INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LAS AMAZONAS - 2021"

Problema	Objetivo	Hipótesis	Variable	Dimensiones e Indicadores	Índices	Metodología
Problema general: • ¿Cómo se podría mejorar la seguridad y evitar que personas no autorizadas puedan ingresar al datacenter? **Problemas específicos:** • ¿Qué tecnología existente en la actualidad se puede usar para mejorar la seguridad de un datacenter? • ¿Cómo guardar un registro visual de todas las personas que ingresan al datacenter? • ¿Cómo emitir alertas o notificaciones silenciosas cada vez que alguien ingrese al datacenter?	**Objetivo general:** • Diseñar e implementar un sistema de registro de accesos utilizando IoT. **Objetivos específicos:** • Mejorar la seguridad del datacenter, registrando a las personas que ingresan, mediante un sistema de seguridad basado en IoT. • Programar un dispositivo IoT para capturar imágenes y registrar los datos del acceso físico al datacenter. • Programar un dispositivo IoT para enviar notificaciones por email al personal encargado del Departamento de Informática.	**Hipótesis general:** • El diseño e implementación de un sistema de registro de accesos utilizando IoT mejorará la seguridad física en el datacenter del Departamento de Informática de la municipalidad distrital de las amazonas.	**Independiente (X):** Sistema de registro de accesos utilizando IoT.	**Simplificación de los procesos:** - Nivel de confiabilidad - Nivel de usabilidad - Nivel de Funcionalidad.	Bueno, Regular, Malo.	**Tipo de investigación:** Aplicada. **Diseño de investigación:** Pre Experimental **G: O_1 X O_2** **Población:** todas las personas que laboran en el Departamento de Informática de la municipalidad distrital de las amazonas, que en total son 10 individuos. **Muestra:** de tipo no aleatoria intencional, y estará conformada por la totalidad de la población, que son 10 individuos.
			Dependiente (Y): Seguridad física.	**Seguridad física y del entorno:** - Nivel de implementación de áreas seguras. - Nivel de implementación de controles de entrada. - Nivel de protección contra amenazas.	Bueno, Regular, Malo.	

Anexo 02: Instrumento de recolección de datos

CUESTIONARIO (Pre y Post Test)

I. PRESENTACIÓN

El presente cuestionario forma parte del proyecto de investigación titulado: “DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE REGISTRO DE ACCESOS UTILIZANDO IoT PARA MEJORAR LA SEGURIDAD FÍSICA EN EL DATACENTER DEL DEPARTAMENTO DE INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LAS AMAZONAS - 2021”.

II. INSTRUCCIONES

Antes de proceder a responder las preguntas del cuestionario debe leer las siguientes instrucciones:

- ✓ Lea cada una de las preguntas y responda de acuerdo a lo que considere pertinente.
- ✓ Debe responder a todas las preguntas del cuestionario.
- ✓ Podrá solicitar aclaración cuando encuentre alguna dificultad en las preguntas.
- ✓ La información proporcionada será de carácter confidencial.
- ✓ No existen preguntas correctas ni incorrectas.
- ✓ Marque con un aspa (X) solamente una de las alternativas para cada pregunta.
- ✓ La duración aproximada para el llenado del cuestionario será de 10 minutos.

Dimensión: Simplificación de los procesos

Pregunta 01: ¿Cómo califica usted el nivel de confianza del sistema de registro de accesos al datacenter del Departamento de Informática de la municipalidad distrital de las amazonas?

☐ **Bueno** ☐ **Regular** ☐ **Malo**

Pregunta 02: ¿En qué nivel considera usted que ha mejorado la confianza en el sistema de registro de accesos al datacenter del Departamento de Informática de la municipalidad distrital de las amazonas?

☐ **Bueno** ☐ **Regular** ☐ **Malo**

Pregunta 03: ¿Cómo califica usted el nivel de usabilidad del sistema de registro de accesos al datacenter del Departamento de Informática de la municipalidad distrital de las amazonas?

☐ **Bueno** ☐ **Regular** ☐ **Malo**

Pregunta 04: ¿En qué nivel considera usted que ha mejorado la usabilidad del sistema de registro de accesos al datacenter del Departamento de Informática de la municipalidad distrital de las amazonas?

☐ **Bueno** ☐ **Regular** ☐ **Malo**

Pregunta 05: ¿Cómo califica usted el nivel de funcionalidad del sistema de registro de accesos al datacenter del Departamento de Informática de la municipalidad distrital de las amazonas?

☐ **Bueno** ☐ **Regular** ☐ **Malo**

Pregunta 06: ¿En qué nivel considera usted que ha mejorado la funcionalidad del sistema de registro de accesos al datacenter del Departamento de Informática de la municipalidad distrital de las amazonas?

☐ **Bueno** ☐ **Regular** ☐ **Malo**

Dimensión: Seguridad física y del entorno

Pregunta 07: ¿Cómo califica usted el nivel de seguridad en el acceso físico al datacenter del Departamento de Informática de la municipalidad distrital de las amazonas?

☐ **Bueno** ☐ **Regular** ☐ **Malo**

Pregunta 08: ¿Cómo califica usted el nivel de implementación de áreas seguras en las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas?

☐ **Bueno** ☐ **Regular** ☐ **Malo**

Pregunta 09: ¿Cómo califica usted el nivel de implementación de controles de entrada en las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas?

☐ **Bueno** ☐ **Regular** ☐ **Malo**

Pregunta 10: ¿En qué forma considera usted que se monitorea el nivel de implementación de controles de entrada en las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas?

☐ **Bueno** ☐ **Regular** ☐ **Malo**

Pregunta 11: ¿Cómo califica usted el nivel de protección contra amenazas en las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas?

☐ **Bueno** ☐ **Regular** ☐ **Malo**

Pregunta 12: ¿En qué forma considera usted que se monitorea el nivel de protección contra amenazas en las instalaciones del Departamento de Informática de la municipalidad distrital de las amazonas?

☐ **Bueno** ☐ **Regular** ☐ **Malo**