ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Red privada virtual y la minería de criptomonedas
en el hardware de la nube pública, 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información

AUTOR:

Bueno Torres, Carlos Alberto (orcid.org/0000-0002-2274-6298)

ASESORES:

Mg. Poletti Gaitan, Eduardo (orcid.org/0000-0002-2143-4444)

Dr. Pereyra Acosta, Manuel Antonio (orcid.org/0000-0002-2593-5772)

LÍNEA DE INVESTIGACIÓN:
Infraestructura y Servicios de Redes y Comunicaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA — PERÚ

2023

Dedicatoria

Esta investigación es dedicada a mi amada esposa y mis 3 hijas, quienes fueron las que me apoyaron a continuar progresando y lograr culminar la maestría, por cada una de sus palabras y buenos ánimos en que lograre titularme en el 2024

Agradecimiento

Mi gratitud en primer lugar es a Dios, quien me ha bendecido este tiempo con muchas oportunidades para lograr terminar la maestría, a cada uno de mis maestros, los que lograron abrir mi mente hacia nuevos horizontes de conocimientos a través de su vasta experiencia, a mi asesor quien me ha guiado en todo este camino de preparación y a mi familia quienes son la razón y el pilar del porque busque la meta de titularme como magister en el 2024.

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Autenticidad del Asesor

Yo, POLETTI GAITAN EDUARDO HUMBERTO, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Red privada virtual y la minería de criptomonedas en el hardware de la nube pública, 2023", cuyo autor es BUENO TORRES CARLOS ALBERTO, constato que la investigación tiene un índice de similitud de 17.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 04 de Enero del 2024

Apellidos y Nombres del Asesor:	**Firma**
EDUARDO HUMBERTO POLETTI GAITAN **DNI:** 18073124 **ORCID:** 0000-0002-2143-4444	Firmado electrónicamente por: EPOLETTIG el 07-01-2024 17:23:52

Código documento Trilce: TRI - 0719706

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Originalidad del Autor

Yo, BUENO TORRES CARLOS ALBERTO estudiante de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Red privada virtual y la minería de criptomonedas en el hardware de la nube pública, 2023", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

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

Nombres y Apellidos	**Firma**
CARLOS ALBERTO BUENO TORRES **DNI:** 45883622 **ORCID:** 0000-0002-2274-6298	Firmado electrónicamente por: CBUENOT el 07-01-2024 23:23:25

Código documento Trilce: TRI - 0724282

INVESTIGA UCV

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

El propósito de realizar esta investigación fue lograr determinar la relación de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, 2023. Teniendo como unidad de análisis al Hardware. Se tomaron en cuenta 7 indicadores: Frame Length, Payload, Tasa de Hashrate local, Tasa de Hashrate efectivo, Tiempo de conexión, Tasa de Consumo de CPU y Tasa de Consumo de RAM, los cuales fueron evaluados en un Pre - Test y en un Post - Test, a 6 instancias de máquina ubicadas en la nube pública, obteniendo 180 observaciones. En la primera parte fue antes de utilizar la red privada virtual y la segunda etapa después durante 15 días, se utilizó una ficha de registro validada por expertos, se recolectaron datos que mostraron un 100,37% de mejora en la evaluación del Pre- Test y el Post- Test respecto al indicador de Tasa de hashrate local, adicionalmente para el indicador de tasa de hashrate efectivo tuvo 317,11%, además, para el indicador de Tiempo de conexión permaneció activo durante 60 minutos para el Post - Test, mientras que para el indicador consumo de CPU mostró 1,61% de incremento, además para el indicador consumo de RAM tuvo 10,29% de aumento y la variable independiente, para los indicadores frame length y payload, tuvo una reducción del 100%, de forma significativa mostrando un P_Value<0,05, en todos los indicadores, que son 7. Así mismo se determinó la relación de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, 2023.

.

Palabras clave: Red Privada Virtual, Nube Pública, Hardware, Minería de Criptomonedas.

Abstract

The purpose of conducting this research was to determine the relationship between the virtual private network and cryptocurrency mining on public cloud hardware, 2023. Working as a Hardware analysis unit. 7 indicators are taken into account: Frame length, Payload, Local hashrate rate, Effective hashrate rate, Connection time, CPU consumption rate and RAM consumption rate, which were evaluated in a Pre-Test and in a Post - Test, in 6 machine instances. located in the public cloud, obtaining 180 observations. In the first part, before using the virtual private network and in the second stage, after 15 days, a registration form validated by experts was used, data was collected that showed an improvement of 100.37% in the evaluation of the Pre -Test and the Post-Test. As for the local hashrate rate indicator, in addition to the effective hashrate rate indicator of 317.11%, in addition, the Connection Time indicator remained active for 60 minutes for the Post - Test, while for the consumption indicator of CPU showed an increase of 1.61%, in addition to the RAM consumption indicator there was an increase of 10.29% and the independent variable, for the frame length and payload indicators, there was a 100% reduction, significantly showing a P_Value<0.05, in all indicators, which is 7. This is how the relationship between the virtual private network and cryptocurrency mining on public cloud hardware, 2023, was determined.

Keywords: Virtual Private Network, Public Cloud, Hardware, Cryptocurrency Mining.

I. INTRODUCCIÓN

Según los especialistas de CISCO(2018), afirmaron que 2/3 de los habitantes del mundo contará con acceso a Internet. Para 2023 con 5,300Mill. de usuarios totales (66,00 % de habitantes a nivel mundial) y 29’300Mill. equipos con conexion para 2023, las conexiones M2M representarán la mitad de los dispositivos y conexiones globales, con las aplicaciones para el hogar conectadas y las aplicaciones para automóviles conectados creciendo más rápido.

Sin embargo, este avance de la tecnología no se detiene y el mundo financiero ha presenciado un cambio radical con la llegada de las criptomonedas. Según Almukaynizi et al.(2018) señalaron que las criptomonedas están definidas con la terminología de monedas digitales que operan sobre la blockchain.

Asimismo Poongodi et al.(2022) definieron esta blockchain como una tecnología encargada de registrar las transacciones de forma distribuida y segura sin ningún poder centralizado otorgado a un tercero.

Además, Sugieren Aggarwal et al. (2021) que estas blockchain protegen la identidad del usuario siendo más seguro ejecutar las transacciones de forma anónima, teniendo al bitcoin como una de las primeras monedas digitales en aplicar esta tecnología.

Sin embargo, muchos aspectos de las criptomonedas, en particular la minería de criptomonedas, permanecen esquivas para la mayoría. Por ejemplo Lasla et al.(2022) indicaron que cada vez que se ajusta la dificultad de la minería del bitcoin, ello conlleva a la red de mineros a adquirir plataformas aún más eficientes y poderosas para así poder competir con los demás mineros de la red.

Esta tesis se propone descifrar el misterio y explorar cómo la minería de criptomonedas puede optimizarse y hacerse más accesible a través de un enfoque innovador.

Por un lado a nivel internacional Según Aye et al. (2023) describieron como el uso de las criptomonedas, con el pasar de los años, han obtenido en los países en desarrollo, una importancia cada vez mayor como en África y Asia, teniendo al bitcoin como uno de los mayores activos que provoca el incremento de la actividad de minería liderado por China, Rusia y Estados Unidos.

Por otro lado López Miranda (2019) afirmó que hasta marzo del 2019 se tenía más de 50 empresas de las cuales 30 estaban en Lima y el resto en otras ciudades que aceptaban el intercambio de criptomonedas. Sin embargo en noticias de la web de RPP(2021) describieron que se ha incrementó el interés por minar criptomonedas, utilizando programas gratuitos de fuentes desconocidas, los cuales están siendo aprovechado por los hackers, que vienen infectando con malware todas las computadoras de casa a través de métodos de criptohacking, confirmado por Tekiner et al. (2021), quienes mencionaron los daños causados a servicios alojados en la nube publica, como youtube-Google Cloud, zoom y tesla en AWS, kubernets en AZURE, entre otros servicios y aplicaciones.

Esto es confirmado por Vries (2023) indicó que cualquier persona es capaz de unirse con cualquier hardware de una computadora y realizar minería de criptomonedas.

Sin embargo para Taylor (2017) enfatizó que la minería de criptomonedas es un proceso que demanda intensivamente recursos computacionales, lo que requiere un poder de cómputo significativo si se desea obtener mejores ganancias, recomendado la nube como una mejor opción. Esto apoyado por Sibande et al.(2023) describieron que los mineros de criptomonedas suelen enfrentar costos significativos, tanto en términos de hardware como de consumo energético a través de sus granjas de servidores.

Así mismo Reedy (2023) realizó pruebas para leer el tráfico de la transmisión de los bitcoin a nivel IP, atacando una red en la nube de almacenamiento diseñada en blockchain demostrando que aquellas redes ponen en riesgo la seguridad y el anonimato de la información luego de ser almacenados. Sin embargo, no solo son atacados los usuarios comunes, según Chauhan et al. (2023) afirmaron que los delincuentes informáticos atacan la infraestructura en la nube para adueñarse de todos los servicios, realizando entre varias cosas la minería de bitcoin ocasionando perdidas para las organizaciones.

En cuanto a la Justificación, de tipo social, esta investigación buscó la utilización de tecnologías de red privada virtual para proteger el tráfico que fluye por internet, tal como lo indican para Seraj et al. (2023) describieron que las redes privadas virtuales fueron inicialmente diseñadas para que las personas pudieran acceder a la red del trabajo desde sus hogares o mientras estén viajando,

otorgando privacidad y seguridad, así como para ocultar el tráfico de Internet, evitar la censura o acceder a contenido bloqueado geográficamente.

Como justificación tecnológica, es en este contexto dentro de la investigación que se planteó aplicar la Red privada virtual y la minería de criptomonedas en el hardware de la nube pública, 2023. Al utilizar una red privada virtual según Safaei Pour et al.(2023) afirmaron que habría una conexión directa entre el usuario y un servidor sin importar la ubicación geográfica dando como resultado el anonimato y la privacidad de la información permitiendo conectarse a un proveedor de nube pública. Así mismo Karmakar et al.(2020) indicaron que la seguridad mediante la autenticación es confiable y segura en este tipo de red privada virtual, manteniendo todo el tráfico de datos protegido.

A pesar de estas justificaciones tecnológicas y sociales de la utilización de la red privada virtual, hay una serie de realidades problemáticas que deben abordarse. Según Heinonen et al.(2022) señalaron que estas incluyen cuestiones de seguridad, siendo la minería de criptomonedas el objetivo principal para los piratas informáticos convirtiendo a las criptomonedas en su medio de pago principal. Además, según un informe periodístico de Peru21(2021) escribieron que las criptomonedas no están regulada actualmente en muchas jurisdicciones, lo que puede generar incertidumbre y riesgo para los mineros.

No obstante, Chen et al. (2022) propusieron que la red privada virtual tiene como objetivo mejorar la seguridad al permitir conexiones seguras ocultando todo el tráfico de datos minimizando así el riesgo de ataques de piratas informáticos.

En resumen, una red privada virtual puede optimizar el rendimiento de la minería de criptomonedas en la nube pública. A través de una evaluación detallada de los aspectos prácticos, teóricos y técnicos, en este enfoque, se espera proporcionar una contribución significativa a la comprensión y la práctica de la minería de criptomonedas.

Tras haber presentado la problemática, como situación existente, se propone el siguiente problema general: ¿Existe una relación de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, 2023?,

de igual manera se presentan los problemas específicos, ¿Existe una relación de la confidencialidad impacta en la eficiencia de hashrate en el hardware de la nube pública, 2023?, ¿Existe una relación de la confidencialidad en la Conexión en el hardware de la nube pública, 2023?, ¿Existe una relación de la confidencialidad en el rendimiento en el hardware de la nube pública, 2023?.

De acuerdo con lo mencionado, el objetivo general pretende determinar la relación de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, 2023. Así mismo, se mencionan en orden, los tres objetivos específicos, tal como, determinar la relación de la confidencialidad en la eficiencia de hashrate en el hardware de la nube pública, 2023. Así mismo tenemos, determinar la relación de la confidencialidad en la Conexión en el hardware de la nube pública, 2023. Por último, determinar la relación de la confidencialidad en el rendimiento en el hardware de la nube pública, 2023.

Después de determinar los problemas y objetivos de la investigación, se plantea una hipótesis general que sugiere que, existe una relación significativa de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, 2023. A continuación, se plantea las tres hipótesis específicas, tal como, existe una relación significativa de la confidencialidad en la eficiencia de hashrate en el hardware de la nube pública, 2023. Además, existe una relación significativa de la confidencialidad en la Conexión en el hardware de la nube pública, 2023. Por último, existe relación significativa de la confidencialidad en el rendimiento en el hardware de la nube pública, 2023. Esta investigación proporcionará información valiosa sobre la relación que existe en una red privada virtual y la minería de criptomonedas en el hardware de la nube pública, 2023. Los resultados de la investigación serán de interés para los mineros de criptomonedas, los proveedores de la nube y los encargados de formular nuevas políticas que mejoren la seguridad de la información.

II. MARCO TEÓRICO

Durante el desarrollo de este documento, se logró recolectar diversos precedentes, tanto a nivel internacional como nacional. Se brindará un listado detallado de estos precedentes.

En la India, Shuaib et al.(2022), en su investigación titulado: “Una nueva optimización para la minería de GPU utilizando overclocking y undervolting.”la cual es de tipo aplicada, el estudio presenta una nueva estrategia para optimizar la minería con unidades de procesamiento gráfico (GPU) utilizando métodos de sobrecalentamiento y subcalentamiento. Los autores enfatizan la economía y eficiencia de la minería con GPU, destacando la capacidad de estas unidades para realizar cálculos matemáticos complejos. Además, destacan que la combinación de sobrecalentamiento y sobrecalentamiento permite a los mineros optimizar sus equipos de minería, al reducir la energía consumida y mantener las temperaturas de las GPU. Además, el estudio trata sobre la minería de criptomonedas y su sostenibilidad, sugiriendo la utilización de fuentes de energía renovable para reducir los efectos y costos ambientales. Los autores argumentan que la minería de criptomonedas a través de fuentes de energía renovable ofrece la oportunidad de superar las barreras financieras y tecnológicas, transformando los desechos en recursos económicos. Debido al consumo elevado de energía y sobrecalentamiento los autores observaron un aumento de la eficiencia de hashrate de 60MH/s hacia los 73,91MH/s. Concluyeron que este método innovador debe alentar a los mineros a considerar el uso de energías renovables de tal forma que se mejore la eficiencia a través de nuevas técnicas de minería sostenible.

En la India, Gundaboina et al.(2022), en su investigación "Seguridad basada en la minería de criptomonedas utilizando energía renovable como fuente", de tipo experimental aplicada, analizaron el uso de energía renovable para la minería de criptomonedas. Se trata de un estudio cuantitativo cuyo objetivo es maximizar el impacto y la rentabilidad ambiental de la minería de criptomonedas utilizando fuentes de energía sostenibles. Mencionaron que, para disminuir el consumo de energía, utilizaron técnicas de optimización de hardware como el sobrecalentamiento y el subcalentamiento de las unidades de procesamiento gráfico (GPU). Como resultados lograron obtener como mínimo 26 MH/s y hasta un

máximo de 121 MH/s en el hardware utilizado, señalaron que los resultados numéricos muestran que la optimización de hardware y el uso de energía renovable pueden reducir significativamente el impacto en el medio ambiente ocasionado por la minería de criptomonedas al mismo tiempo que aumentan las ganancias para los mineros. Además, destacaron que la utilización de energía renovable no solo beneficia a los mineros en términos de rentabilidad, sino que también tiene un impacto significativo en el medio ambiente al reducir la huella de carbono de la minería de criptomonedas y la generación de desechos electrónicos. Como conclusión, el estudio sugiere que la minería de criptomonedas con energía renovable puede contribuir al desarrollo sostenible y beneficiar tanto a la industria como al público en general.

En Taiwán, Wu et al.(2022), en su investigación titulada “MinerGuard: una solución para detectar aplicaciones basadas en navegador Minería de criptomonedas mediante aprendizaje automático”, de tipo aplicada, con un diseño experimental, presentaron los efectos perjudiciales del uso excesivo de la CPU al acceder a páginas web con scripts de minería incrustados, utilizaron MinerGuard enfocando principalmente en la implementación de aprendizaje automático a través de un modelo de Red Neuronal Artificial (ANN), para identificar y bloquear actividades de minería maliciosas. El experimento realizado para validar MinerGuard se centró en analizar los datos de uso de recursos de páginas web. El modelo de aprendizaje automático fue entrenado utilizando 140 sitios sin scripts de minería y 75 sitios con scripts de minería ocultos. Posteriormente, se utilizaron un conjunto de 800 sitios web para evaluar la eficacia del sistema. Entre los hallazgos se encontró que el cryptohacking produce un consumo del 100% de CPU de un hardware, además dentro de los resultados de los experimentos muestran que MinerGuard es más preciso que el mecanismo de lista negra y no requiere actualizaciones manuales frecuentes, además la tasa de detección precisa de MinerGuard, según los autores, demuestra su capacidad para identificar y evitar script de minería, por último concluyeron que MinerGuard reduce la carga de mantenimiento humano y protege a los usuarios contra scripts de minería, incluidos los de día cero, indicando que los resultados ofrecen un enfoque proactivo para contrarrestar la amenaza de la minería de criptomonedas basada en el navegador y sus implicaciones para la seguridad cibernética y la privacidad en línea.

Mientras que en México, Cruz et al.(2022) en su investigación “Rendimiento Del Hardware De Un Equipo Personal En La Minería De Criptomoneda”, de tipo aplicada, trabajo un enfoque cuantitativo en la recolección de los datos, tuvo como objetivo comparar la diferencia existente en la eficiencia de Hashrate obtenidos al minar hardware de CPU versus hardware de GPU. Utilizando una computadora con el aplicativo XMRig 6.7.2 y un hardware de CPU AMD Ryzen 7, una memoria RAM de 16GB, con un ssd de 120GB y una Tarjeta de video GTX1050-TI de marca GygaByte. Obteniendo como resultados de la minería de criptomonedas solo con CPU se produce un máximo de 1968.1 H/s contra los 12 MH/s alcanzado los cuales fueron generados por el uso de la GPU, teniendo una disponibilidad de 6 Horas de minado.

En china, Sun et al.(2022), en su investigación titulada “Un método de extracción de características convolucionales en etapa temprana que se utiliza para la detección de tráfico minero”, de tipo aplicada, presentaron una nueva estrategia para detectar comportamientos de minería de criptomonedas utilizando tráfico de red y técnicas de aprendizaje automático, utilizaron una función convolucional con una ventana deslizante para extraer características de los primeros paquetes de flujos fue el enfoque sugerido. El método que los autores utilizaron logró distinguir con gran precisión entre los flujos de minería y los flujos normales al mapear los flujos en un espacio de características con tráfico de datos. Para respaldar esta propuesta, los autores recopilaron un conjunto de trazas de tráfico de minería que incluían ocho tipos distintos de comportamientos de minería de criptomonedas en una red real y se llevaron a cabo estudios utilizando este conjunto de datos. Los resultados demostraron que el método propuesto cumplió con los requisitos establecidos para detectar el tráfico de minería real. Según el estudio, los autores mencionaron que se necesitaba un tamaño de payload mínimo de 20 byte para identificar el tráfico de minería. Como respuesta a esta necesidad, se creó un programa de software que funciona como una plataforma en línea para identificar el tráfico de minería. Señalaron que el mínimo de frame length requerido para detectar el tráfico de minería varió según el tipo de criptomoneda, pero el valor medio de paquete fue de 46 a 566 byte. El estudio también comparó el método sugerido con otros existentes y destacó que funciona mejor en términos de eficiencia y precisión. Concluyeron que el estudio demostró que el aprendizaje

automático y la identificación de tráfico de red funcionaron bien para identificar hábitos de minería de criptomonedas, destacaron los usos potenciales de la detección de tráfico de minería, que incluyen la identificación de otros eventos de seguridad de red y destacaron la necesidad de desarrollar nuevos métodos para detectar y abordar comportamientos de minería debido al gran consumo de energía y los efectos ambientales que tiene esta práctica.

En Japon, Duong Le et al. (2021)en su investigación titulada "MRSA: Un acelerador de Scrypt de múltiples ROMix de alta eficiencia para la minería de criptomonedas y la seguridad de datos", la cual es de tipo aplicada, mencionaron la utilización y el desarrollo de hardware de bajo consumo y alta eficiencia para la minería de criptomonedas y los riesgos de seguridad relacionados con el uso ASIC se presenta un acelerador de Scrypt de múltiples ROMix de alta eficiencia para la minería de criptomonedas y la seguridad de datos". La investigación describe cómo los mineros utilizan su poder de cómputo para encontrar la prueba necesaria para agregar un bloque candidato a la red blockchain, así como el Pow (mecanismo de consenso de prueba de trabajo) siendo utilizado por criptomonedas en su mayoría. Mencionan que los ASIC también son necesarios para evitar la centralización del poder de minería y los riesgos de seguridad asociados. El estudio trata sobre la implementación y diseño de un MRSA, un acelerador de Scrypt de múltiples ROMix de alta eficiencia para la seguridad de datos y la minería de criptomonedas. Teniendo como resultado un incremento de 4,56KH/s hacía los 297,76KH/s, mostrando un alto consumo de memoria RAM.

En Rusia, Sukharev (2020) en su investigación “Overclocking De Hardware Para Mejorar La Eficiencia De La Minería De Criptomonedas Ethereum”, el cual fue de tipo experimental, trabajo un enfoque cuantitativo, aplicando ficha de registros, tuvo como objetivo realizar minería de criptomonedas en un hardware de computadora, manipulando algunos parámetros como la velocidad de MHz del CPU, la velocidad de la memoria RAM y la velocidad del GPU durante un tiempo específico. Utilizando un programa de minería de código abierto, como resultado logro incrementar la eficiencia de Hashrate en un 77% y la disponibilidad de la minería durante 10 minutos sin daños en el hardware del equipo, produciendo mayor cantidad de Hashrate, demostrando que se puede minar cualquier hardware

y obtener recompensas reflejadas en criptomonedas al manipular algunas variables.

En Qatar, Alkaeed et al.(2020)en su investigación titulada “Destacando la minería de criptomonedas con CPU y GPU y sus beneficios basados en sus características”. La cual es de tipo aplicada, mencionaron una visión detallada de la minería de criptomonedas utilizando CPU y GPU, destacando la mejora de la velocidad de transferencia de información y el número de cálculos simultáneos. Contrastaron también las diferencias entre la arquitectura de CPU y las GPU, enfatizando la capacidad de las GPU para realizar operaciones en paralelo en múltiples conjuntos de datos. Presentaron comparaciones detalladas entre las CPU de Intel y las GPU de AMD, incluido el ancho de banda de memoria, la frecuencia, el número de núcleos. Además, el artículo analiza el desarrollo y la evolución de las arquitecturas de sistemas CPU-GPU, así como el uso de la herramienta de programación de GPU NVIDIA CUDA. Como resultado realizaron una comparación de algunos pools de minería, obteniendo para Sulsh 4,8 KH/s, mientras que para XMRPool 750,9KH/s Además, mencionaron las aplicaciones de la tecnología blockchain en redes eléctricas inteligentes y proporcionaron un marco para analizar los beneficios de utilizar CPUs y GPUs en la minería de criptomonedas.

En Portugal, Gomes et al.(2020)en su investigación titulada “Detección de Cryptojacking con métricas de uso de CPU” de tipo aplicada, realizaron un estudio sobre la detección de malware de minería de criptomonedas utilizando el análisis del uso de la CPU. La investigación, llevada a cabo de manera experimental sobre un hardware de la nube pública, se basa en métricas de uso de CPU recopiladas durante un intervalo de 60 segundos para evaluar la presencia de scripts de minería en páginas web. Los resultados mostraron una alta precisión en la detección de malware con una tasa de falsos positivos cercana al 0%, utilizaron un método de análisis que se concentró en observar el comportamiento de la CPU en ciertas páginas web, lo que permitió encontrar patrones distintivos relacionados con la ejecución de scripts de minería. Concluyeron que la utilización de métricas de CPU que provocan que la CPU tenga 50% de consumo hasta 100% permite detectar malware de minería y que para lograr una detección más precisa, también destacaron la importancia de considerar el comportamiento de múltiples núcleos de

CPU estableciendo una base sólida para investigaciones futuras sobre la ciberseguridad y la detección de malware.

En Reino Unido, Jayasinghe et al.(2020) en su investigación titulado “Una encuesta de casos de ataque dirigidos a Cryptohacking en la infraestructura de la nube”, estudiaron cómo la minería de criptomonedas impacta sobre el consumo de CPU en la nube pública. Destacaron la estrategia de los atacantes para evitar levantar sospechas y controlar el porcentaje de uso de la CPU que alcanza el 100% de uso con minería de criptomonedas en un hardware de la nube pública, señalaron como las herramientas de minería como XMRig son utilizadas para usar un número específico de núcleos y establecer límites y prioridades en el uso de la CPU, permitiendo minar criptomonedas de manera discreta y evitar la detección de los sistemas de seguridad. En el estudio los autores indicaron la importancia de monitorear el consumo de memoria RAM como un indicador adicional para detectar actividades maliciosas relacionadas con la minería de criptomonedas en entornos de infraestructura en la nube pública. Mencionaron que incluso si los atacantes utilizan técnicas de evasión complejas, es necesario desarrollar sistemas de detección capaces de detectar patrones de consumo de CPU y RAM relacionados con la minería de criptomonedas. Concluyeron en el estudio la importancia de comprender y monitorear el consumo de recursos, como la CPU y la RAM, para detectar actividades de minería de criptomonedas ilegales en entornos de nube pública. Además, enfatizaron la importancia de desarrollar técnicas de detección que puedan detectar patrones de comportamiento relacionados con la minería de criptomonedas, incluso cuando los atacantes utilizan técnicas de evasión para ocultar sus actividades.

En Reino Unido, Runchao et al.(2019)en su investigación titulada “Desmitificando la criptominería: Análisis y optimizaciones de algoritmos PoW con memoria dura”, de tipo aplicada, analizaron y optimizaron los algoritmos de prueba de trabajo (PoW) de memoria utilizados en la minería. Indicaron que depende de la tecnología blockchain y sus protocolos de consenso, mencionaron que mientras que los algoritmos PoW se utilizan para resolver problemas de consenso mediante la competencia basada en funciones criptográficas. Sin embargo, destacan que la proliferación de hardware específico para aplicaciones ha llevado a un aumento en los costos de energía y a la centralización del proceso de minería. Los autores con

100 ejecuciones y cada una de 60 segundos, encontraron que los algoritmos PoW se han vuelto más intensivos en memoria, lo que ha aumentado la cantidad de memoria y energía requerida. Este estudio examina los algoritmos Ethash, CryptoNight y Scrypt en las GPU de Nvidia, así como las optimizaciones de datos y el software de pipelining para aumentar la eficiencia energética y los hashrate. Teniendo como resultado al cambiar de algoritmo, los resultados muestran una mejora de 0,79KH/s hacia 926,61KH/s, concluyeron que el algoritmo Ethash optimizado supera a Claymore, el software comercial de Ethash más rápido.

En Rusia, Sukharev et al.(2018), en su investigación titulada “Minería Asincrónica de la Criptomoneda Ethereum”, de tipo experimental, cuasi experimental, propusieron un nuevo método asincrónico para mejorar el rendimiento del algoritmo de minería de la criptomoneda Ethereum. Para abordar un problema específico en el contexto de la minería de Ethereum, este trabajo se enmarca en la investigación aplicada. Mencionaron que el enfoque utilizado consistió en cambiar el código del software de minería para resolver el problema. Luego realizaron experimentos para evaluar el rendimiento del nuevo algoritmo. Utilizaron dos mineros con diferentes hardware durante las pruebas de 10 minutos para medir el número de hashes por segundo (H/s). Los resultados indicaron que la implementación del nuevo algoritmo de minería asincrónica resultó en un aumento del rendimiento de hashrate (H/s) del 1,3 % para un hardware y del 1,2 % para otro hardware. Demostraron que la implementación de un algoritmo de minería asincrónica puede mejorar el rendimiento de la minería de Ethereum, destacando la importancia de optimizar el código del software de minería para lograr mejoras significativas.

En, India, Iyer et al.(2018) en su investigación titulada “Minería acelerada por GPU y CPU de Criptomonedas y su análisis financiero”, de tipo aplicada, con una metodología experimental, enfocaron su estudio en la minería de criptomonedas con GPU y CPU. El objetivo principal de la investigación fue llevar a cabo un análisis financiero detallado y optimizar el rendimiento de la minería. Para recopilar datos, esta investigación utiliza un experimento controlado. Para cada una de las criptomonedas evaluadas durante el estudio, se llevó a cabo la minería de criptomonedas durante un período de 24 horas. La aplicación del método de

overclocking en las GPU con "EVGA PrecisionX" para maximizar el rendimiento fue una parte importante de la metodología. Los resultados mostraron un aumento significativo en los hashrates (H/S) después de aplicar el overclocking; en promedio, aumentaron un 20% en comparación con los valores iniciales. Además, se analizó el uso de energía del hardware utilizado, y se descubrió que la NVIDIA GTX 1060 requería 120 vatios, mientras que la NVIDIA GTX 1050 Ti requería 75 vatios. Las conclusiones destacan la relevancia del overclocking para optimizar el rendimiento en la minería de criptomonedas. Asimismo, se subraya la importancia de considerar el consumo de energía en relación con el hashrate al evaluar la rentabilidad de las operaciones mineras.

Por Indonesia, para Surantha et al. (2018) durante su investigación respecto a “Red privada virtual portátil segura con Algoritmo Rabbit Stream Cipher”, de tipo experimental, analizo el rendimiento de la aplicación OpenVpn y cambiando el algoritmo de cifrado con Rabbit, utilizando el software Wireshark lograron capturar el tráfico de datos en la red, teniendo como resultado una encapsulación del tráfico de los datos, donde no se podía interpretar los parámetros que aparecían en wireshark. A través del estudio se logró conseguir que todos los datos viajan por la red privada virtual totalmente cifrados.

Por ultimo en Irak, según Salman (2017) en su investigación sobre “Implementación de túnel IPsec-VPN usando GNS3”, de tipo experimental, se basó en el uso de la red privada virtual mediante una simulación de 2 clientes en diferentes sitios, configurando la red de tal forma que solicite a cada usuario sus accesos de autenticación, cifrando todo el tráfico de la red, se utilizó wireshark para capturar los paquetes de datos del tráfico en la red, como resultado se tiene que la red privada virtual otorgo anonimato de las comunicaciones haciendo que todo el tráfico de la red sea privado, teniendo éxito en los escenarios otorgando un elevado nivel de seguridad.

Dentro del ámbito de esta investigación, se toman en consideración las siguientes bases teóricas, las cuales sustentan el estudio en cuestión:

Para Crawshaw(2021), la red privada virtual asegura y encripta las comunicaciones de tal forma que funciona como redes de cable virtuales creados

para conectar terminales que querían compartir recursos y pasar a formar parte de una misma red.

Para Peters(2019), los hackers son personas que realizan actos delictivos teniendo como ejemplo al rasomware.

Existen diversas tecnologías de red privada virtual disponibles, Según Parthasarathy et al. (2022)como IPSec, SSL, MPLS, L2F, PPTP, L2TP y GRE. Sin embargo, IPSec ha ganado popularidad como solución de seguridad para una red privada virtual.

Entre sus características más notorias según Abbas et al.(2023) mencionan que la red privada virtual debe garantizar la confidencialidad y el anonimato en la comunicación. Sin embargo, presentan desafíos en términos de seguridad por una mala configuración al ser implementada, dificultando a los usuarios aprovechar al máximo esta tecnología innovadora.

Existen 2 tipos de VPN, según Lackorzynski et al. (2019) señalan la de tipo VPN de hardware, que por lo general, ofrecen un rendimiento y eficiencia superiores las VPN de tipo software.

Aunque las soluciones para redes privadas virtuales ofrecidas por los proveedores son fácilmente accesibles, para Chua et al. (2022) mencionan que implementar soluciones de software de código abierto, debe considerar a los más raqueados: OpenConnect, Wireguard y OpenVPN.

Para Coonjah et al. (2018) definen a OpenVPN como una solución de código abierto y multiplataforma que ofrece seguridad y alta configurabilidad, compatible con los modos de comunicación TCP y UDP, siendo especialmente útil en industrias donde el ancho de banda es crucial, como las comunicaciones por satélite, se utiliza comúnmente como opción predeterminada para las redes privadas virtuales.

Con ello se define red privada virtual de sitio a sitio, según Hauser et al.(2020) describe su uso como un túnel donde se establece entre dos conmutadores este modo para conectar dos redes internas.

Para ello Li et al. (2023) conceptualizaron a UDP(User Datagram Protocol) como protocolo de capa de transporte que se destaca por su eficiencia y rapidez en la transmisión de datos. Es ampliamente utilizado en sistemas de comunicación que requieren una transmisión en tiempo real, como los sistemas de comunicación multimedia.

Por otro lado TCP, según Steenkiste (2023) lo define como un protocolo de control de transmisión de capa de transporte ampliamente utilizado en Internet cuya principal función es asegurar una transmisión de datos confiable mediante la división de los datos en paquetes y el manejo de la congestión de la red.

Una forma de tecnología VPN según Shaikh et al. (2018) es el protocolo, llamado SSL, responsable de asegurar y mantener la conexión cifrada entre un cliente con el servidor a través de Internet. Las VPN SSL utilizan certificados SSL para verificar la identidad del servidor y encriptar la transmisión de datos.

Un tipo de protocolo es TLS, según Turner(2014) define a este protocolo como un estándar ampliamente utilizado para proteger las comunicaciones entre clientes y servidores permitiendo evitar escuchas, modificaciones y falsificación de mensajes.

Para Kheirkhah et al.(2020) definen a IP como el Protocolo de Internet utilizado para la comunicación entre dispositivos en la red de Internet formando parte de las capas de red y transporte, siendo IPv4 ampliamente utilizado, teniendo a IPv6 como una alternativa con múltiples aplicaciones en el dominio del Internet de las Cosas.

Para CLOUDFLARE(2023) define un puerto como el punto virtual en el que las conexiones de red comienzan y terminan, para ello el sistema operativo de una computadora gestiona los puertos a través de software, con ello cada puerto está conectado a un proceso o servicio, haciendo que los puertos puedan distinguir fácilmente entre los diversos tipos de tráfico: los correos electrónicos van a un puerto diferente al de las páginas web, aunque ambos lleguen a una computadora a través de la misma conexión a Internet.

El frame length, según CISCO(2019) es el tamaño de un paquete capturado en byte, desde los 0 byte hasta los 1500byte, bajo el estándar IEEE 802.3, confirmado por WHIRESHARK(2020) quien a través de su aplicación, pueden capturar datos del usuario que transitan por una red de comunicaciones.

El payload, para WIRESHARK(2021) definieron que son datos que se transmiten entre los socios de comunicación, excluyendo los encabezados/metadatos. Sin embargo, depende del punto de vista de la capa de protocolo, siendo en caso del payload del protocolo que son visibles proviene de los datos de las capas de protocolo superpuestas, tal como al observar una trama

Ethernet que transporta una solicitud teniendo según García et al.(2017) indicaron que se puede extraer hasta 256 byte de caracteres.

Para Zhou et al.(2018) definieron a wireshark como una herramienta que utiliza rastreadores para llevar a cabo la recopilación de datos de la red a través de una gestión centralizada, estos rastreadores de paquetes son una de las herramientas de captura de paquetes más conocidas.

El termino byte según KINGSTON(2023) mencionaron que es una unidad de medida utilizada para almacenar datos, como un carácter de texto, además de que 1 byte es igual a 8bit, siendo los bit la medida de datos más básica, que se representa con un cero o un uno.

Por otro lado, una criptomoneda para Dudani et al. (2023), afirman que es un tipo de dinero digital que eliminará la necesidad de utilizar instituciones financieras para realizar transacciones, nació con el bitcoin en 2009 y actualmente existen varias criptomonedas entre las cuales se tiene a Ethereum, dogecoin, Monero, etc.

Sin embargo, Dogecoin para Nani(2022) es un tipo de moneda digital que no tiene límite en la cantidad de DOGE que se puede producir, teniendo muchas otras criptomonedas las cuales tienen una cantidad limitada, como el Bitcoin, la se dejara de producir una vez que se hayan generado 21 mil millones de bitcoins.

Además la minería de criptomonedas según Tovanich et al.(2021) definieron esta actividad como un método para extraer nuevos tipos de monedas digitales y garantizar que las transacciones sean confiables, consumiendo mucho hardware de computación, para ello al aumento del valor de una criptomoneda puede incentivar a los mineros a mejorar sus inversiones y atraer nuevos mineros al aumentar los ingresos esperados de la minería.

También respecto a Oracle Cloud, según Jakóbczyk(2020) indicó que es parte de la nueva generación de nube de Oracle, ofrece capacidades de infraestructura como capacidades de servicio (IaaS) (computo, almacenamiento, redes), servicios de borde (DNS, firewall de aplicaciones web) y capacidades de plataforma como capacidades de servicio (PaaS) (como la base de datos autónoma de Oracle, que admite cargas de trabajo tanto transaccionales como analíticas, Oracle Kubernetes Enginer, certificado así como administrado y otros.

Dentro de las cuales podemos ejecutar una instancia de máquina, según Laszewski et al.(2012) señalaron que es denominadas VM, esta virtualización se da en la computación en la nube, la cual suele implicar la implementación de múltiples imágenes de sistema operativo en un solo servidor que comparte los recursos de RAM Y CPU disponibles. Además, la capacidad de implementar múltiples máquinas virtuales permite a los usuarios pagar solo por los recursos utilizados en lugar de pagar por toda la capacidad instalada en los servidores, facilitando el monitoreo del consumo de recursos de las máquinas virtuales individuales.

Con todo lo presentado, se procederá a realizar el análisis correspondiente a cada terminología, identificando cada proceso y la aplicación que se utilizará para definir la red privada virtual y la minería de criptomonedas en el hardware de la nube pública, 2023. Después de haber sido establecido, la propuesta de ingeniería se determinó cuál de los aplicativos ayudará a conseguir cada objetivo en la investigación, así mismo se formulará los parámetros de investigación.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

La presente investigación se define como aplicada, según Vargas (2009) señala la utilización de conocimientos prácticos para beneficiar a grupos y a la sociedad mediante la generación de nuevos conocimientos. Teniendo como objetivo de estudio el descubrir dónde ocurrieron los eventos o fenómenos y determinar las condiciones que explican la relación entre dos o más variables.

Aunque implica construir la red privada virtual y la minería de criptomonedas en el hardware de la nube pública. El enfoque metodológico es cuantitativo, para ello Hernández et al. (2014) afirman que sigue una secuencia ordenada y se basa en pruebas. Cada paso debe seguirse en un orden estricto, aunque algunos pasos pueden ser redefinidos. Comienza con ideas limitadas y luego se determinan las preguntas y objetivos. La información se revisa para luego pasar bajo un marco establecido de teorías u opiniones. Las hipótesis se establecerán a partir de las preguntas e identificarán cada variable. Posterior a ello se tiene la intención de probar una variable que ha sido medida en una situación específica, obteniendo una serie de resultados que se derivan del análisis estadístico de las medidas obtenidas.

Se empleó un enfoque cuantitativo para probar la teoría de las variables como la Red Privada Virtual y la minería de criptomonedas. Se utilizaron datos estadísticos y resultados numéricos. Según Hernández et al. (2018) afirma que el diseño experimental se utiliza para evaluar el impacto potencial de lo que se está manipulando, pero también se reduce el nivel de control.

El diseño del presente estudio se estableció de tipo experimental, específicamente cuasi experimental, de tal forma que se pueda controlar la variable independiente. La estructura de diseño incluye un pre- test además del pos- test cuyo propósito es ver la relación que existe entre la variable dependiente y la independiente, visible en la Tabla 1.

Tabla 1. *Diseño Cuasi-experimental*

MUESTRA	PRE- TEST	EJECUCIÓN	POS- TEST
G.E.	O-1	D	O-2

Elaborado por Propia

G.E.=Instancia de Máquinas Virtuales en la nube Publica

O-1=Uso de cada instrumento por cada indicador de la utilización de la red privada virtual (pre-test).

D= Red Privada Virtual.

O-2: Uso de cada instrumento según cada indicador de la utilización de la red privada virtual (post-test).

3.2 Variables y operacionalización

Se tomaron en cuenta las siguientes variables, revisar Anexo 3.

VI: Red Privada Virtual.

VD: Minería de criptomonedas.

Variable dependiente: Minería de criptomonedas.

Como definición conceptual, la minería de criptomonedas implica utilizar hardware para resolver problemas computacionales, su objetivo es que las ganancias comienzan a llegar, para ello la tasa de hashrate debe superar los 0 H/s (Alsindi & Lotti, 2021).

Como definición Operacional, al medir cada indicador a través de las propias aplicaciones donde se ejecuta la minería se procederá a anotar en una ficha de registros, bajo las escalas validadas por expertos, se obtendrá a través del uso de instrumentos elaborado por el investigador.

Indicadores según dimensiones:

D1: Eficiencia de Hashrate, los indicadores son: Tasa de hashrate local y tasas de hashrate efectivo.

D2: Conexión, el indicador es el Tiempo de conexión.

D3: Rendimiento, el indicador es tasa de consumo de CPU y Tasa de consumo de RAM.

Por consiguiente, la escala que se utilizara como medición es de tipo Razón.

Variable Independiente: Red Privada Virtual

Como definición conceptual, La red privada virtual permite una conexión directa entre el usuario y un servidor sin importar la ubicación geográfica dando

como resultado el anonimato y la privacidad de la información permitiendo conectarse a un proveedor de nube pública (Safaei Pour et al.2023).

Como definición operacional, mediante la red privada virtual, se desea establecer una conexión segura entre terminales de dispositivos, lo que permitirá la minería de criptomonedas en hardware de la nube pública. Se pretende encontrar la relación que existe de la red privada virtual y la minería de criptomonedas en la nube publica, propuesto mediante una ficha de recolección de datos validada por expertos. Revisar Anexo 2.

Indicadores

D1: Confidencialidad, tenemos al Frame Length y al Payload.

Se tiene como matriz de consistencia dentro del Anexo 3. Además, se tiene como matriz de la operacionalización de la variable independiente, la cual se muestra en el Anexo 2.

3.3 Población, muestra y muestreo

3.3.1 Población. Para Sampieri(2018) Es necesario situar a la población de manera precisa en función de sus características de contenido, lugar y tiempo, así como de su accesibilidad, así mismo, si no tiene acceso a los casos o unidades de interés, plantear un estudio no tiene sentido.

En el caso de la población, para la presente tesis que es de diseño cuasiexperimental, se tomó en consideración 6 máquinas virtuales N1- us-central1-a, de las cuales se generará 180 observaciones, con ello se puede utilizar el post – Test y el pre- test.

3.3.2 Muestra: Con ello, Hernández et al. (2014) define la muestra debe cumplir con criterios establecidos para la recolección de datos por parte de los investigadores, Primero, debe determinar la unidad de análisis, si se trata de personas, organizaciones, periodos, comunidades, situaciones, piezas producidas, eventos, etc. Sin embargo, por ser de diseño cuasiexperimental, no se presenta muestras.

3.3.2 Muestreo: No se considera, dentro de la investigación, el muestreo, puesto que es de diseño cuasiexperimental.

3.3.4 Unidad de análisis: Teniendo como unidad de análisis al Hardware.

3.4 Técnicas e instrumentos de recolección de datos

Para Pineda et al.(2019) la ficha de registro se utiliza para obtener información sobre las características propias, lo cual es importante para comprender la situación actual del contexto y realizar un diagnóstico real. Además, permite evaluar las dimensiones en el pre- test así como en el post- test.

Dentro del presente estudio, se utilizaron las fichas de registro, tanto para la variable independiente, así como la variable dependiente. Estas evaluaciones se realizaron antes y después de la utilización de la red privada virtual.

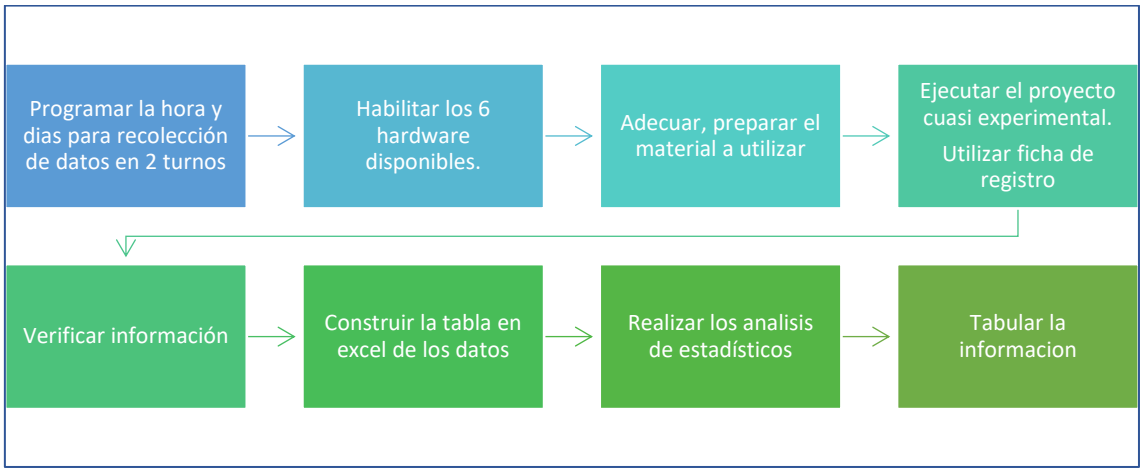
3.5 Procedimientos

El proyecto se ejecutó con la aprobación del asesor, lo cual se confirma con la autorización para llevar a cabo la investigación y su implementación, así como para difundir los resultados. Esto permitió la utilización de la red privada virtual y la minería de criptomonedas en el hardware de la nube pública y la aplicación de los instrumentos rigurosamente validados por los expertos (ver anexo 4 y anexo 5).

Siendo la ejecución del proyecto, el cual se llevó a cabo en coordinación con el asesor, quien ha establecido que se realizará del 26 de octubre al 9 de noviembre, en 2 turnos del día, estos instrumentos validados por los expertos son visibles en los anexos 4 y 5.

Posterior a ello, después de obtener la información del hardware a través de las fichas, se procedió a verificar la información y organizarlas en tablas, obteniendo una tabla de datos para ser procesados. Por último, se procedió a la verificación y revisión, para luego, hacer el análisis estadístico (ver Figura 1).

Figura 1. Procedimientos



Elaboración Propia

3.6 Método de análisis de datos

En el presente estudio, se planteó el uso de estadísticos comparativo y descriptivo. Esto se reflejará a través de tablas que contienen los estadísticos, que utiliza métricas de tendencia central, mediana, media, moda, máximo y mínimo. Estos procedimientos permitieron conocer la distribución de las medidas resultantes de la población que se está estudiando. Así mismo, después de verificar los supuestos de normalidad, se realizaron análisis estadísticos inferenciales no paramétricos. Dentro del cual, para muestras relacionadas, será la "Spearman". Se trabajó con el 5% de error o significancia, así como el nivel de confianza al 95%.

3.7 Aspectos éticos

Se respetaron los niveles de conocimiento de cada autor y se tuvieron en cuenta sus criterios. Teniendo dentro de la UCV, una biblioteca virtual, Se hizo referencia a varios autores de las bases de datos científicas disponibles. La tabla de propuestas de ingeniería técnica y recolección de datos incluye varias definiciones citadas, respetando las ideas y frases de los artículos. Se utilizarán tablas estadísticas y otros métodos de investigación para garantizar la veracidad de los hallazgos. La presente investigación se basa en la necesidad de verificar el nivel de seguridad de la nube pública para completar la investigación y establecer una referencia para futuros estudios. También se consideró respetar la

confidencialidad de los datos de las nubes públicas que se utilizarán. Según la declaración de autenticidad del asesor y autenticidad del autor, el investigador afirma que la información es precisa. También se utilizó la guía para certificar la originalidad de la investigación y se aprobó a través de Turnitin<20% dentro del porcentaje aprobado en la guía 062, cumpliendo con el porcentaje aceptable establecido por la UCV.

IV. RESULTADOS

4.1 Análisis descriptivo de los Resultados

4.1.1 Confiabilidad

En la presente investigación se aplicó el alfa de cronbach, Para ello Oviedo et al.(2005) señaló que es un índice utilizado para evaluar la confiabilidad del tipo consistencia interna de una escala, es decir, la magnitud en que los ítems de una escala están correlacionados entre sí.

Tabla 2.

Estadística de fiabilidad: Coeficiente de Cronbach

Alfa de Cronbach	N de elementos
,896	14

Elaboración propia

De la tabla 2, a continuación, se describe los resultados y su interpretación

1) Las estadísticas de fiabilidad del coeficiente alfa de Cronbach, proporciona información sobre la consistencia interna del cuestionario aplicado como recopilación de datos
2) Alfa de Cronbach: El coeficiente alfa de Cronbach es 0,896. Este valor está en el rango de 0 a 1, donde un valor más cercano a 1 indica una mayor consistencia interna entre los elementos del cuestionario. En este caso, un valor de 0,896 sugiere una buena consistencia interna, lo que implica que las preguntas están correlacionadas de manera positiva entre sí, y además que el instrumento usado tiene una fuerte confiabilidad, es decir que el instrumento de recopilación de datos ha permitido realzar mediciones estables y consistentes.

Número de elementos: Son los 7 indicadores del instrumento de recopilación de datos que se están evaluando para medir la consistencia interna; esto es, 5 indicadores de la variable dependiente y 2 indicador de la variable independiente.

4.1.2 Pruebas de normalidad

Tabla 3.

Pruebas de normalidad: Criterio de decisión para Ho y Ha, formulación de Hipótesis

Pruebas de Normalidad	Red privada virtual	Minería de criptomonedas
Distribución normal: Ho	Se tiene Ho, donde X es igual a N(μ, σ2)	Se tiene Ho, donde X es igual a N(μ, σ2)
Distribución no normal: Ha	Se tiene Ha, donde X es diferente de N (μ, σ2)	Se tiene Ha, donde X es diferente de N (μ, σ2)
α	95% (0,950)	95% (0,950)
α-error	5% (0,050)	5% (0,050)
Prueba de normalidad	Kolmogorov-Smirnov, aplica cuando 50<=n	Kolmogorov-Smirnov, aplica cuando 50<=n
	Shapiro-Wilk, donde 50>n	Shapiro-Wilk, donde 50>n
Criterio de decisión	Se tiene p-valor el cual es menor a 0,050 entonces aceptar Ha y declinar Ho	Se tiene p-valor el cual es menor a 0,050 entonces aceptar Ha y declinar Ho
	Se tiene p-valor el cual es mayor o igual a 0,050 entonces se declina Ha aceptar Ho	Se tiene p-valor el cual es mayor o igual a 0,050 entonces se declinar Ha aceptar Ho

Elaboración Propia

En la tabla 3 se tiene los criterios de decisión utilizados para las pruebas de normalidad para Ho y Ha, formulación de Hipótesis.

En la Tabla 4, se evidencia las pruebas de normalidad aplicadas.

Tabla 4.

Resultados de pruebas de normalidad

	Kolmogorov-Smirnov		
	Estadístico	**gl**	**Sig.**
VD: Minería de criptomonedas			
Tasa de Hashrate local	0,315	180	0
Tasa de Hashrate efectivo	0,332	180	0
Tiempo de conexión	0,341	180	0
Tasa de Consumo de CPU.	0,106	180	0
Tasa de Consumo DE RAM	0,227	180	0
VI: Red privada virtual			
Frame Length	0,341	180	0
Payload	0,341	180	0

Elaboración Propia

De acuerdo con la Tabla 4 Resultados de pruebas de Normalidad, se evidencia que los indicadores de las variables independientes Red privada virtual, además de los indicadores de la variable dependiente Minería de Criptomonedas; tienen un valor p-valor = 0; y contrastándolo con los criterios de decisión de la Tabla 3, Se tiene p-valor el cual es menor a 0,050 entonces se aprueba la Ha y se declina Ho.

4.1.3 Pruebas T para muestras independientes

Tabla 5.

Pruebas T: Estadísticas de grupo

Estadísticas de grupo

	Pre(0)_post(1)	N	Media	Desv. Desviación	Desv. Error promedio
Tasa de Hashrate Local	,00	90	52,4870	1,30059	,13709
	1,00	90	105,1670	1,30059	,13709
Tasa de Hashrate Efectivo	,00	90	10,4977	,26015	,02742
	1,00	90	43,7870	1,30059	,13709
Tiempo de Conexión	,00	90	5,9444	,48107	,05071
	1,00	90	60,0000	,00000	,00000
Tasas de Consumo CPU	,00	90	61,9444	,48107	,05071
	1,00	90	62,9444	,48107	,05071
Tasas de Consumo RAM	,00	90	19,4278	,26031	,02744
	1,00	90	21,4278	,26031	,02744
Frame Length	,00	90	54,0000	,00000[a]	,00000
	1,00	90	,0000	,00000[a]	,00000
PayLoad	,00	90	36,0000	,00000[a]	,00000
	1,00	90	,0000	,00000[a]	,00000

a. t no se puede calcular porque las desviaciones estándar de ambos grupos son 0.

Elaboración propia

De la tabla 5 se observa que en la Media (Promedio): Respecto a la media en el Pre – Test, observa que existe una variación en los valores obtenidos respecto al pos test.

Tabla 6. *Prueba T: Prueba de Muestras independientes*

Prueba de muestras independientes										
		Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	t	gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
Tasa de Hash-rate Local	Se asumen varianzas iguales	0	1	-271,714	178	0	-52,68	0,19388	-53,0626	-52,2974
	No se asumen varianzas iguales			-271,714	178	0	-52,68	0,19388	-53,0626	-52,2974
Tasa de Hash-rate Efectivo	Se asumen varianzas iguales	104,53	0	-238,105	178	0	-33,2893	0,13981	-33,56523	-33,01344
	No se asumen varianzas iguales			-238,105	96,11	0	-33,2893	0,13981	-33,56685	-33,01182
Tiempo de Conexión	Se asumen varianzas iguales	167,084	0	-1065,99	178	0	-54,0556	0,05071	-54,15562	-53,95549
	No se asumen varianzas iguales			-1065,99	89	0	-54,0556	0,05071	-54,15631	-53,9548
Tasas de Consumo CPU	Se asumen varianzas iguales	0	1	-13,944	178	0	-1	0,07171	-1,14152	-0,85848
	No se asumen varianzas iguales			-13,944	178	0	-1	0,07171	-1,14152	-0,85848
Tasas de Consumo RAM	Se asumen varianzas iguales	0	1	-51,541	178	0	-2	0,0388	-2,07658	-1,92342
	No se asumen varianzas iguales			-51,541	178	0	-2	0,0388	-2,07658	-1,92342

Elaboración Propia

1) El p-valor es menor a 0.05, y conforme la Tabla 6, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, de que existe relación significativa de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, 2023.
2) El p-valor es menor a 0.05, y conforme la Tabla 6, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, de que existe relación significativa de la dimensión confidencialidad de la variable independiente red privada virtual en

la dimensión de eficiencia hashrate de la variable dependiente minería de criptomonedas en el hardware de la nube publica, 2023.

3) El p-valor es menor a 0.05, y conforme la Tabla 6, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, de que existe relación significativa de la dimensión confidencialidad de la variable independiente red privada virtual en la dimensión de conexión de la variable dependiente minería de criptomonedas en el hardware de la nube publica, 2023.

4) El p-valor es menor a 0.05, y conforme la Tabla 6, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, de que existe relación significativa de la dimensión confidencialidad de la variable independiente red privada virtual en la dimensión de rendimiento de la variable dependiente minería de criptomonedas en el hardware de la nube publica, 2023.

4.1.4 Análisis descriptivo de los resultados de Red Privada virtual

4.1.4.1 Análisis descriptivo de los resultados de Frame Length

Tabla 7.

Cuadro de estadística descriptiva de indicador frame length

	PRE/TEST		POS/TEST	
estadísticos Descriptivos	Estadístico	Desv. Error	Estadístico	Desv. Error
Media	54,0000	0,00000	0,0000	0,00000
95% de intervalo de confianza para la media Límite inferior	54,0000		0,0000	
Límite superior	54,0000		0,0000	
Media recortada al 5%	54,0000		0,0000	
Mediana	54,0000		0,0000	
Varianza	0,000		0,000	
Desv. Desviación	0,00000		0,00000	
Mínimo	54,00		0,00	
Máximo	54,00		0,00	
Rango	0,00		0,00	

Elaboración Propia

De la tabla 7, a continuación, se describe los resultados descriptivos y su interpretación:

1) Media (Promedio): La media en el Pre - Test es 54 bytes, lo que indica el valor típico de la variable. En este caso, representa un nivel moderado de la variable, respecto al pos test que es 0 bytes.
2) Error Estándar: El error estándar tanto para el pre/test y el pos/test es 0,000. Este valor indica la variabilidad esperada en la media de las muestras. Cuanto menor sea el error estándar, más precisa será la estimación de la media. En este caso, un error estándar relativamente bajo sugiere una estimación precisa de la media poblacional
3) Intervalo de Confianza al 95%: El intervalo de confianza proporciona un rango en el cual es probable que se encuentre la verdadera media de la población. En este caso, el intervalo inferior y superior es el mismo con 54 byte en el Pre - Test, mientras que para el Post - Test es 0 byte.
4) Media Recortada al 5%: La media recortada al 5% es 54 byte para el Pre - Test y para el Post - Test es 0 byte, se calcula eliminando el 5% de los valores

extremos. Esto es útil para reducir el impacto de valores atípicos en la estimación de la media.

5) Mediana: La mediana es 54 byte en el Pre - Test, que es similar a la media. Indica que la distribución de los datos no está sesgada de manera significativa, en cambio para el Post - Test es 0 byte.
6) Varianza y Desviación Estándar: La varianza es 0,00 y la desviación estándar es 0,000. Ambas medidas proporcionan información sobre la dispersión de los datos alrededor de la media. Tanto para el Pre - Test y en este caso el Post - Test, la desviación estándar muestra que hay una moderada dispersión alrededor de la media.
7) Mínimo y Máximo: El valor mínimo es 54 byte y el máximo es 54 byte. Mientras que en el Post - Test el valor mínimo y máximo se reduce a 0 byte. Esto proporciona información sobre el rango total de la variable en el pre y Post - Test, que es 0,00.
8) Rango: El rango es la diferencia entre el máximo y el mínimo (54 - 54 = 0,00) para el Pre - Test, siendo igual a 0 byte en el Post - Test, mostrando la extensión total de los datos.
9) Se observa que los resultados estadísticos de la media para el frame length después de ejecutar la red privada virtual muestran una reducción respecto al pre-test de 54 byte y 0 byte respectivamente, señalando que la red privada virtual ayudo a disminuir el frame length.

Estos estadísticos han proporcionado una descripción detallada de la distribución y la tendencia central del indicador frame length de la dimensión Confidencialidad de la variable independiente Red Privada Virtual con ello, se ha podido determinar la variabilidad y la forma de la distribución de los datos.

4.1.4.2 Análisis descriptivo de los resultados de PayLoad

Tabla 8.

Cuadro de estadística descriptiva de indicador PayLoad

		PRE - TEST		POSTTEST	
Estadísticos Descriptivos		Estadístico	Desv. Error	Estadístico	Desv. Error
Media		36,0000	0,00000	0,0000	0,00000
95% de intervalo de confianza para la media	Límite inferior	36,0000		0,0000	
	Límite superior	36,0000		0,0000	
Media recortada al 5%		36,0000		0,0000	
Mediana		36,0000		0,0000	
Varianza		0,000		0,000	
Desv. Desviación		0,00000		0,00000	
Mínimo		36,00		0,00	
Máximo		36,00		0,00	
Rango		0,00		0,00	

Elaboración Propia

De la tabla 8, a continuación, se describe los resultados descriptivos y su interpretación:

1) Media (Promedio): La media en el Pre - Test es 36 bytes, lo que indica el valor típico de la variable. En este caso, representa un nivel moderado de la variable, respecto al pos test que es 0 bytes.
2) Error Estándar: El error estándar tanto para el pre/test y el pos/test es 0,000. Este valor indica la variabilidad esperada en la media de las muestras. La estimación de la media será precisa cuanto más bajo se encuentre error estándar. En este caso, un error estándar relativamente bajo indica que la media poblacional es una estimación precisa.
3) Intervalo de Confianza al 95%: El intervalo de confianza proporciona un rango en el cual es probable que se encuentre la verdadera media de la población. En este caso, el intervalo inferior y superior es el mismo con 36 byte en el Pre - Test, mientras que para el Post - Test es 0 byte.
4) Media Recortada al 5%: La media recortada al 5% es 36 byte para el Pre - Test y para el Post - Test es 0 byte, se calcula eliminando el 5% de los valores extremos. Esto es útil para reducir el impacto de valores atípicos en la estimación de la media.

5) Mediana: La mediana es 36 byte en el Pre - Test, que es similar a la media. Indica que la distribución de los datos no está sesgada de manera significativa, en cambio para el Post - Test es 0 byte.
6) Varianza y Desviación Estándar: La varianza es 0,00 y la desviación estándar es 0,000. Ambas medidas proporcionan información sobre la dispersión de los datos alrededor de la media. Tanto para el Pre - Test y en este caso el Post - Test, la desviación estándar muestra que hay una moderada dispersión alrededor de la media.
7) Mínimo y Máximo: El valor mínimo es 36 byte y el máximo es 36 byte. Mientras que en el Post - Test el valor mínimo y máximo se reduce a 0 byte. Esto proporciona información sobre el rango total de la variable en el pre y Post - Test, que es 0,00.
8) Rango: El rango es la diferencia entre el máximo y el mínimo (54 - 54 = 0,00) para el Pre - Test, siendo igual a 0 byte en el Post - Test, mostrando la extensión total de los datos.
9) Se observa que los resultados estadísticos de la media para el payload después de ejecutar la red privada virtual muestran una reducción respecto al pre-test de 36 byte y 0 byte respectivamente, señalando que la red privada virtual ayudo a disminuir el payload.

Estos estadísticos han proporcionado una descripción detallada de la distribución y la tendencia central del indicador payload de la dimensión Confidencialidad de la variable independiente Red Privada Virtual Con ello, se ha podido determinar la variabilidad y la forma de la distribución de los datos.

4.1.4.3 Análisis descriptivo de Eficiencia de Hashrate Local

Tabla 9.

Cuadro de estadística descriptiva de indicador Eficiencia de Hashrate Local

		PRE - TEST		POSTTEST	
Estadísticos Descriptivos		Estadístico	Desv. Error	Estadístico	Desv. Error
Media		52,4870	0,13709	105,1670	0,13709
95% de intervalo de confianza para la media	Límite inferior	52,2146		104,8946	
	Límite superior	52,7594		105,4394	
Media recortada al 5%		52,5175		105,1975	
Mediana		52,5250		105,2050	
Varianza		1,692		1,692	
Desv. Desviación		1,30059		1,30059	
Mínimo		48,53		101,21	
Máximo		55,13		107,81	
Rango		6,60		6,60	

Elaboración Propia

De la tabla 9, a continuación, se describe los resultados descriptivos y su interpretación:

1) Media (Promedio): La media en el Pre - Test es 52,49 H/s, lo que indica el valor típico de la variable. En este caso, representa un nivel moderado de la variable, mientras que la media en el Post - Test es 105,17H/s, siendo favorable a la investigación.
2) Error Estándar: El error estándar es 0,13709 en el Pre - Test y Post - Test. Este valor indica la variabilidad esperada en la media de las muestras. Cuanto menor sea el error estándar, más precisa será la estimación de la media. En este caso, un error estándar relativamente bajo sugiere una estimación precisa de la media poblacional
3) Intervalo de Confianza al 95%: El intervalo de confianza proporciona un rango en el cual es probable que se encuentre la verdadera media de la población. En este caso, en el Pre - Test el intervalo va desde 48,53 H/s hasta los 55,13 H/s mientras que en el Post - Test va desde 101,21 H/S hasta 107,81 H/s.

4) Media Recortada al 5%: La media recortada al 5% en el Pre - Test es 52,52H/s mientras que en Post - Test se observa un incremento con 105,20 H/s. Se calcula eliminando el 5% de los valores extremos. Esto es útil para reducir el impacto de valores atípicos en la estimación de la media.
5) Mediana: La mediana en el Pre - Test es 52,53 H/s, que es similar a la media. Indica que la distribución de los datos no está sesgada de manera significativa, mientras que en el Post - Test observamos un aumento con 105,21 H/s.
6) Varianza y Desviación Estándar: En el Pre - Test y el Post - Test la varianza es 1,692 y la desviación estándar es 1,301. Ambas medidas proporcionan información sobre la dispersión de los datos alrededor de la media. En este caso, la desviación estándar muestra que hay una moderada dispersión alrededor de la media.
7) Mínimo y Máximo: En el Pre - Test el valor mínimo es 48,53 H/s y el máximo es 55,13 H/s. mientras que para el Post - Test el mínimo es 101,21 H/s y el máximo es 107,81 H/s. Esto proporciona información sobre el rango total de la variable, que es 6,60 H/s.
8) Rango: El rango es la diferencia entre el máximo y el mínimo, siendo para el Pre - Test y el Post - Test 6,6 H/s mostrando la extensión total de los datos.
9) Se observa que los resultados estadísticos de la media para la tasa de hashrate local después de ejecutar la red privada virtual muestran un aumento respecto al pre-test de 52,49H/s y 105,17 H/s respectivamente, señalando que la red privada virtual tuvo una variación sobre la tasa de hashrate local.
10) Estos estadísticos han proporcionado una descripción detallada de la distribución y la tendencia central del indicador tasa de hashrate local de la dimensión Eficiencia de Hashrate de la variable dependiente Minería de Criptomonedas Con ello, se ha podido determinar la variabilidad y la forma de la distribución de los datos.

4.1.4.4 Análisis descriptivo de Eficiencia de Hashrate Efectivo

Tabla 10.

Cuadro de estadística descriptiva de indicador Eficiencia de Hashrate efectivo

		PRE - TEST		POS-TEST	
Estadísticos Descriptivos		**Estadístico**	**Desv. Error**	**Estadístico**	**Desv. Error**
Media		10,4977	0,02742	43,7870	0,13709
95% de intervalo de confianza para la media	Límite inferior	10,4432		43,5146	
	Límite superior	10,5522		44,0594	
Media recortada al 5%		10,5038		43,8175	
Mediana		10,5050		43,8250	
Varianza		0,068		1,692	
Desv. Desviación		0,26015		1,30059	
Mínimo		9,71		39,83	
Máximo		11,03		46,43	
Rango		1,32		6,60	

Elaboración Propia

De la tabla 10, a continuación, se describe los resultados descriptivos y su interpretación:

1) Media (Promedio): La media en el Pre - Test es 10,50 H/s, lo que indica el valor típico de la variable. En este caso, representa un nivel moderado de la variable, mientras que la media en el Post - Test es 43,79H/s, lo que muestra una variación a la investigación.
2) Error Estándar: El error estándar es 0,02742 en el Pre - Test y 0,13709 en el Post - Test. Estos valores indican la variabilidad esperada en la media de las muestras. Cuanto menor sea el error estándar, más precisa será la estimación de la media. En este caso, un error estándar relativamente bajo sugiere una estimación precisa de la media poblacional.
3) Intervalo de Confianza al 95%: El intervalo de confianza proporciona un rango en el cual es probable que se encuentre la verdadera media de la población. En este caso, en el Pre - Test el intervalo va desde 10,44 H/s hasta los 10,55 H/s mientras que en el Post - Test va desde 43,51 H/S hasta 44,06 H/s.

4) Media Recortada al 5%: La media recortada al 5% en el Pre - Test es 10,50 H/s mientras que en Post - Test se observa un incremento con 43,82 H/s. Se calcula eliminando el 5% de los valores extremos. Esto es útil para reducir el impacto de valores atípicos en la estimación de la media.
5) Mediana: La mediana en el Pre - Test es 10,51 H/s, que es similar a la media. Indica que la distribución de los datos no está sesgada de manera significativa, mientras que en el Post - Test observamos un aumento con 43,83 H/s.
6) Varianza y Desviación Estándar: En el Pre - Test la varianza es 0,068 y la desviación estándar es 0,260; para el Post - Test la varianza es 1,692 y la desviación estándar es 1,301. Ambas medidas tanto en el Pre - Test y Post - Test proporcionan información sobre la dispersión de los datos alrededor de la media. En este caso, la desviación estándar muestra que hay una moderada dispersión alrededor de la media.
7) Mínimo y Máximo: En el Pre - Test el valor mínimo es 9,71 H/s y el máximo es 11,03 H/s. mientras que para el Post - Test el mínimo es 39,83 H/s y el máximo es 46,43 H/s. Esto proporciona información sobre el rango total de la variable tanto en el Pre - Test con 1,32 H/s como en el pos test que es 6,60 H/s.
8) Rango: El rango es la diferencia entre el máximo y el mínimo, siendo para el Pre - Test 1,32 H/s y en el Post - Test 6,6 H/s mostrando la extensión total de los datos.
9) Se observa que los resultados estadísticos de la media para la tasa de hashrate efectiva después de ejecutar la red privada virtual muestran un aumento respecto al pre-test de 10,50H/s y 43,79 H/s respectivamente, señalando que la red privada virtual tuvo un impacto favorable sobre la tasa de hashrate efectiva.

Estos estadísticos han proporcionado una descripción detallada de la distribución y la tendencia central del indicador tasa de hashrate efectivo de la dimensión Eficiencia de Hashrate de la variable dependiente Minería de Criptomonedas con ello, se ha podido determinar la variabilidad y la forma de la distribución de los datos.

4.1.4.5 Análisis descriptivo de los resultados de Tiempo de Conexión

Tabla 11.

Cuadro de estadística descriptiva de la dimensión Conexión

		PRE - TEST		POS-TEST	
estadísticos Descriptivos		Estadístico	Desv. Error	Estadístico	Desv. Error
Media		5,9444	0,05071	60,0000	0,00000
95% de intervalo de confianza para la media	Límite inferior	5,8437		60,0000	
	Límite superior	6,0452		60,0000	
Media recortada al 5%		5,9414		60,0000	
Mediana		6,0000		60,0000	
Varianza		0,231		0,000	
Desv. Desviación		0,48107		0,00000	
Mínimo		5,00		60,00	
Máximo		7,00		60,00	
Rango		2,00		0,00	

Elaboración Propia

De la tabla 11, a continuación, se describe los resultados descriptivos y su interpretación:

1) Media (Promedio): La media en el Pre - Test es 5,94 minutos, lo que indica el valor típico de la variable. En este caso, representa un nivel moderado de la variable, mientras que la media en el Post - Test es 60 minutos, lo que muestra un impacto favorable a la investigación.
2) Error Estándar: El error estándar es 0,051 en el Pre - Test y 0,000 en el Post - Test. Estos valores indican la variabilidad esperada en la media de las muestras. Cuanto menor sea el error estándar, más precisa será la estimación de la media. En este caso, un error estándar relativamente bajo sugiere una estimación precisa de la media poblacional.
3) Intervalo de Confianza al 95%: El intervalo de confianza proporciona un rango en el cual es probable que se encuentre la verdadera media de la población. En este caso, en el Pre - Test el intervalo va desde 5,844 hasta los 6,045 minutos mientras que en el Post - Test va desde 60 hasta 60 minutos.
4) Media Recortada al 5%: La media recortada al 5% en el Pre - Test es 5,941 mientras que en Post - Test se observa un incremento con 60 minutos. Se

calcula eliminando el 5% de los valores extremos. Esto es útil para reducir el impacto de valores atípicos en la estimación de la media.

5) Mediana: La mediana en el Pre - Test es 6 minutos, que es similar a la media. Indica que la distribución de los datos no está sesgada de manera significativa, mientras que en el Post - Test observamos un aumento con 60 minutos.
6) Varianza y Desviación Estándar: En el Pre - Test la varianza es 0,231 y la desviación estándar es 0,481; para el Post - Test la varianza y la desviación estándar es 0,000. Ambas medidas tanto en el Pre - Test y Post - Test proporcionan información sobre la dispersión de los datos alrededor de la media. En este caso, la desviación estándar muestra que hay una moderada dispersión alrededor de la media.
7) Mínimo y Máximo: En el Pre - Test el valor mínimo es 5 minutos y el máximo es 7 minutos, mientras que para el Post - Test el mínimo es 60 y el máximo es 60 minutos. Esto proporciona información sobre el rango total de la variable tanto en el Pre - Test con 2 minutos como en el pos test que es 0 minutos.
8) Rango: El rango es la diferencia entre el máximo y el mínimo, siendo para el Pre - Test 2 minutos y en el Post - Test 0 minutos mostrando la extensión total de los datos.
9) Se observa que los resultados estadísticos de la media para el tiempo de conexión después de ejecutar la red privada virtual muestran un aumento respecto al pre-test de 5.94 y 60 minutos respectivamente, señalando que la red privada virtual tuvo una variación sobre el tiempo de conexión.

Estos estadísticos han proporcionado una descripción detallada de la distribución y la tendencia central del indicador tiempo de conexión de la dimensión Conexión de la variable dependiente Minería de Criptomonedas Con ello, se ha podido determinar la variabilidad y la forma de la distribución de los datos.

4.1.4.6 Análisis descriptivo de los resultados de tasa de consumo de CPU

Tabla 12.

Cuadro de estadística descriptiva de dimensión tasa de consumo de CPU

		PRE - TEST		POSTTEST	
estadísticos Descriptivos		Estadístico	Desv. Error	Estadístico	Desv. Error
Media		61,9444	0,05071	62,9444	0,05071
95% de intervalo de confianza para la media	Límite inferior	61,8437		62,8437	
	Límite superior	62,0452		63,0452	
Media recortada al 5%		61,9414		62,9414	
Mediana		62,0000		63,0000	
Varianza		0,231		0,231	
Desv. Desviación		0,48107		0,48107	
Mínimo		61,00		62,00	
Máximo		63,00		64,00	
Rango		2,00		2,00	

Elaboración Propia

De la tabla 12, a continuación, se describe los resultados descriptivos y su interpretación:

1) Media (Promedio): La media en el Pre - Test es 61,94%, lo que indica el valor típico de la variable. En este caso, representa un nivel moderado de la variable, mientras que la media en el Post - Test es 62,94%, lo que muestra un impacto favorable a la investigación.
2) Error Estándar: El error estándar es 0,051 en el Pre - Test y 0,051 en el Post - Test. Estos valores indican la variabilidad esperada en la media de las muestras. Cuanto menor sea el error estándar, más precisa será la estimación de la media. En este caso, un error estándar relativamente bajo sugiere una estimación precisa de la media poblacional.
3) Intervalo de Confianza al 95%: El intervalo de confianza proporciona un rango en el cual es probable que se encuentre la verdadera media de la población. En este caso, en el Pre - Test el intervalo va desde 61,84% hasta los 62,04% mientras que en el Post - Test va desde 62,84% hasta 63,05%.
4) Media Recortada al 5%: La media recortada al 5% en el Pre - Test es 61,94% mientras que en Post - Test se observa un incremento con 62,94%. Se calcula

eliminando el 5% de los valores extremos. Esto es útil para reducir el impacto de valores atípicos en la estimación de la media.

5) Mediana: La mediana en el Pre - Test es 62%, que es similar a la media. Indica que la distribución de los datos no está sesgada de manera significativa, mientras que en el Post - Test observamos un aumento con 63%.
6) Varianza y Desviación Estándar: En el Pre - Test la varianza es 0,231 y la desviación estándar es 0,481; para el Post - Test la varianza es 0,231 y la desviación estándar es 0,231. Ambas medidas tanto en el Pre - Test y Post - Test proporcionan información sobre la dispersión de los datos alrededor de la media. En este caso, la desviación estándar muestra que hay una moderada dispersión alrededor de la media.
7) Mínimo y Máximo: En el Pre - Test el valor mínimo es 61% y el máximo es 63%, mientras que para el Post - Test el mínimo es 62% y el máximo es 64%. Esto proporciona información sobre el rango total de la variable tanto en el Pre - Test con 2% como en el pos test que es 2%.
8) Rango: El rango es la diferencia entre el máximo y el mínimo, siendo para el Pre - Test 2% y en el Post - Test 2% mostrando la extensión total de los datos.
9) Se observa que los resultados estadísticos de la media para la tasa de consumo de CPU después de ejecutar la red privada virtual muestran un aumento respecto al pre-test de 61,94% y 62,94% respectivamente, señalando que la red privada virtual mantiene estable la tasa de consumo de CPU.

Estos estadísticos han proporcionado una descripción detallada de la distribución y la tendencia central del indicador tasa de consumo de CPU de la dimensión Rendimiento de la variable dependiente Minería de Criptomonedas Con ello, se ha podido determinar la variabilidad y la forma de la distribución de los datos.

4.1.4.7 Análisis descriptivo de los resultados de tasa de consumo de RAM

Tabla 13.

Cuadro de estadística descriptiva de indicador tasa de consumo de RAM

		PRE - TEST		POS-TEST	
estadísticos Descriptivos		**Estadístico**	**Desv. Error**	**Estadístico**	**Desv. Error**
Media		19,4278	0,02744	21,4278	0,02744
95% de intervalo de confianza para la media	Límite inferior	19,3733		21,3733	
	Límite superior	19,4823		21,4823	
Media recortada al 5%		19,4244		21,4244	
Mediana		19,5000		21,5000	
Varianza		0,068		0,068	
Desv. Desviación		0,26031		0,26031	
Mínimo		19,00		21,00	
Máximo		20,00		22,00	
Rango		1,00		1,00	

Elaboración Propia

De la tabla 13, a continuación, se describe los resultados descriptivos y su interpretación:

1) Media (Promedio): La media en el Pre - Test es 19,43%, lo que indica el valor típico de la variable. En este caso, representa un nivel moderado de la variable, mientras que la media en el Post - Test es 21,43%, lo que muestra un impacto favorable a la investigación.
2) Error Estándar: El error estándar es 0,027 en el Pre - Test y 0,027 en el Post - Test. Estos valores indican la variabilidad esperada en la media de las muestras. Cuanto menor sea el error estándar, más precisa será la estimación de la media. En este caso, un error estándar relativamente bajo sugiere una estimación precisa de la media poblacional.
3) Intervalo de Confianza al 95%: El intervalo de confianza proporciona un rango en el cual es probable que se encuentre la verdadera media de la población. En este caso, en el Pre - Test el intervalo va desde 19,37% hasta los 19,48% mientras que en el Post - Test va desde 21,37% hasta 21,48%.
4) Media Recortada al 5%: La media recortada al 5% en el Pre - Test es 19,42% mientras que en Post - Test se observa un incremento con 21,42%. Se calcula

eliminando el 5% de los valores extremos. Esto es útil para reducir el impacto de valores atípicos en la estimación de la media.

5) Mediana: La mediana en el Pre - Test es 19,5%, que es similar a la media. Indica que la distribución de los datos no está sesgada de manera significativa, mientras que en el Post - Test observamos un aumento con 21,5%.
6) Varianza y Desviación Estándar: En el Pre - Test la varianza es 0,068 y la desviación estándar es 0,260; para el Post - Test la varianza es 0,068 y la desviación estándar es 0,260. Ambas medidas tanto en el Pre - Test y Post - Test proporcionan información sobre la dispersión de los datos alrededor de la media. En este caso, la desviación estándar muestra que hay una moderada dispersión alrededor de la media.
7) Mínimo y Máximo: En el Pre - Test el valor mínimo es 19% y el máximo es 20%, mientras que para el Post - Test el mínimo es 21% y el máximo es 22%. Esto proporciona información sobre el rango total de la variable tanto en el Pre - Test con 1% como en el pos test que es 1%.
8) Rango: El rango es la diferencia entre el máximo y el mínimo, siendo para el Pre - Test 1% y en el Post - Test 1% mostrando la extensión total de los datos.
9) Se observa que los resultados estadísticos de la media para la tasa de consumo de RAM después de ejecutar la red privada virtual muestran un aumento respecto al pre-test de 19,43% y 21,43% respectivamente, señalando que la red privada virtual mantiene estable la tasa de consumo de RAM.

Estos estadísticos han proporcionado una descripción detallada de la distribución y la tendencia central del indicador tasa de consumo de RAM de la dimensión Rendimiento de la variable dependiente Minería de Criptomonedas Con ello, se ha podido determinar la variabilidad y la forma de la distribución de los datos.

4.2 Formulación de la Hipótesis

4.2.1 Formulación de la hipótesis general

La formulación de la hipótesis general de investigación es la siguiente:

Tabla 14.

Cuadro de formulación de hipótesis general

Hipótesis general de investigación	
Existe una relación significativa de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, 2023.	
Formulación de hipótesis estadística	
Hipótesis nula	Ho: No existe una relación significativa de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, 2023.
Hipótesis alternativa	Ha: Existe una relación significativa de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, 2023.

Elaboración Propia

La tabla 14 muestra la formulación de la hipótesis general.

4.2.2 Formulación de la hipótesis especificas

La formulación de las hipótesis específicas de investigación son las siguientes:

Tabla 15.

Cuadro de formulación de hipótesis especificas

Hipótesis específica 1 de investigación	
Existe una relación significativa de la confidencialidad en la eficiencia de hashrate en el hardware de la nube pública, 2023.	
Hipótesis nula	Ho: No existe una relación significativa de la confidencialidad en la eficiencia de hashrate en el hardware de la nube pública, 2023.
Hipótesis alternativa	Ha: Existe una relación significativa de la confidencialidad en la eficiencia de hashrate en el hardware de la nube pública, 2023.
Hipótesis específica 2 de investigación	
Existe una relación significativa de la confidencialidad en la Conexión en el hardware de la nube pública, 2023.	
Hipótesis nula	Ho: No existe una relación significativa de la confidencialidad en la Conexión en el hardware de la nube pública, 2023.
Hipótesis alternativa	Ha: Existe una relación significativa de la confidencialidad en la Conexión en el hardware de la nube pública, 2023.
Hipótesis específica 3 de investigación	
Existe relación significativa de la confidencialidad en el rendimiento en el hardware de la nube pública, 2023.	
Hipótesis nula	Ho: No existe relación significativa de la confidencialidad en el rendimiento en el hardware de la nube pública, 2023.
Hipótesis alternativa	Ha: Existe relación significativa de la confidencialidad en el rendimiento en el hardware de la nube pública, 2023.

En la tabla 15 se reflejó el cuadro de formulación de hipótesis específicas.

4.3 Pruebas de Correlación

Para realizar las pruebas de correlaciones de la variable dependiente minería de criptomonedas y variable independiente red privada virtual, de la hipótesis general, se formuló las hipótesis respectivas en la tabla 16 :

Tabla 16.

Formulación de hipótesis para pruebas de correlaciones

Pruebas de Correlaciones	Detalle
Ho	Ho: No existe una relación significativa de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, 2023.
Ha	Ha: Existe una relación significativa de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, 2023.
α	95%(0.950)
Error: α	5%(0.050)
Tipo de Prueba de Correlación	Distribución normal: Pearson Distribución no normal: Spearman
Criterio de evaluación	0.050 > p-valor Aprobar Ha Declinar Ho 0.050=< p-valor Declinar Ha Aprobar Ho
Interpretación de p-valor	Se considera inversa, correlación negativa muy fuerte cuando p-valor se encuentra de -1,0 hasta -0,8 inclusive. Se considera inversa, correlación negativa fuerte cuando p-valor se encuentra de -0,79 hasta -0,6 inclusive. Se considera inversa, correlación negativa moderada cuando p-valor se encuentra de -0,59 hasta -0,4 inclusive. Se considera inversa, correlación negativa débil cuando p-valor se encuentra de -0,39 hasta -0,2 inclusive. Se considera inversa, correlación negativa muy débil cuando p-valor se encuentra de -0,19 hasta -0,01 inclusive. Se considera correlación neutra cuando p-valor es 0. Se considera directa, correlación positiva muy débil cuando p-valor se encuentra de 0,19 hasta 0,01 inclusive. Se considera directa, correlación positiva débil cuando p-valor se encuentra de 0,2 hasta 0,39 inclusive. Se considera directa, correlación positiva moderada cuando p-valor se encuentra de 0,4 hasta 0,59 inclusive. Se considera directa, correlación positiva fuerte cuando p-valor se encuentra de 0,6 hasta 0,79 inclusive. Se considera directa, correlación positiva muy fuerte cuando p-valor se encuentra de 0,8 hasta 1,0 inclusive.

Elaboración Propia

Los resultados de las pruebas de correlación, se evidencia en la tabla siguiente:

Tabla 17.

Prueba de correlaciones entre Red privada virtual y Minería de criptomonedas

Correlaciones			***Red Privada Virtual***
Rho Spearman	***Minería de Criptomonedas***	Coeficiente de correlación	-,866
		Sig. (bilateral)	,000
		N	180

Elaboración Propia

La interpretación de los resultados de la Tabla 17, son:

1) Coeficiente de Correlación de Spearman (Rho) entre Minería de Criptomonedas y la red privada virtual es de -0,866. Este coeficiente indica la fuerza y dirección de la relación entre las dos variables.
2) Significancia Estadística: La correlación es significativa a un nivel de significancia del 0.000 (bilateral).
3) El p-valor es menor a 0.05, y conforme la Tabla 16, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, de que existe una relación significativa de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, 2023.
4) La correlación de -0.866 sugiere una correlación negativa muy fuerte entre la minería de criptomonedas en la muestra analizada. La significancia estadística respalda que las variables están relacionadas. Por lo tanto, existe una asociación significativa y positiva entre la minería de criptomonedas y la red privada virtual en la muestra analizada.

Para realizar las pruebas de correlaciones de las dimensiones confidencialidad y eficiencia de hashrate, se formuló las hipótesis respectivas en la tabla 18:

Tabla 18. *Formulación de hipótesis para pruebas de correlaciones*

Pruebas de Correlaciones	**Detalle**
Ho	Ho: No existe una relación significativa de la confidencialidad en la eficiencia de hashrate en el hardware de la nube pública, 2023.
Ha	Ha: Existe una relación significativa de la confidencialidad en la eficiencia de hashrate en el hardware de la nube pública, 2023.
α	95%(0.950)
Error: α	5%(0.050)
Tipo de Prueba de Correlación	Distribución normal: Pearson Distribución no normal: Spearman
Criterio de evaluación	0.050 > p-valor Aprobar Ha Declinar Ho 0.050=< p-valor Declinar Ha Aprobar Ho
Interpretación de p-valor	Se considera inversa, correlación negativa muy fuerte cuando p-valor se encuentra de -1,0 hasta -0,8 inclusive. Se considera inversa, correlación negativa fuerte cuando p-valor se encuentra de -0,79 hasta -0,6 inclusive. Se considera inversa, correlación negativa moderada cuando p-valor se encuentra de -0,59 hasta -0,4 inclusive. Se considera inversa, correlación negativa débil cuando p-valor se encuentra de -0,39 hasta -0,2 inclusive. Se considera inversa, correlación negativa muy débil cuando p-valor se encuentra de -0,19 hasta -0,01 inclusive. Se considera correlación neutra cuando p-valor es 0. Se considera directa, correlación positiva muy débil cuando p-valor se encuentra de 0,19 hasta 0,01 inclusive. Se considera directa, correlación positiva débil cuando p-valor se encuentra de 0,2 hasta 0,39 inclusive. Se considera directa, correlación positiva moderada cuando p-valor se encuentra de 0,4 hasta 0,59 inclusive. Se considera directa, correlación positiva fuerte cuando p-valor se encuentra de 0,6 hasta 0,79 inclusive. Se considera directa, correlación positiva muy fuerte cuando p-valor se encuentra de 0,8 hasta 1,0 inclusive.

Elaboración Propia

Los resultados de las pruebas de correlación, se evidencia en la tabla siguiente:

Tabla 19.

Prueba de correlaciones de Confidencialidad y Eficiencia de Hashrate

Correlaciones			***Confidencialidad***
Rho Spearman	***Eficiencia de Hashrate***	Coeficiente de correlación	-,866
		Sig. (bilateral)	,000
		N	180

Elaboración Propia

La interpretación de los resultados de la Tabla 19, son:

1) Coeficiente de Correlación de Spearman (Rho) entre eficiencia de hashrate y la confidencialidad es de -0,866. Este coeficiente indica la fuerza y dirección de la relación entre las dos variables.

2) Significancia Estadística: La correlación es significativa a un nivel de significancia del 0.000 (bilateral).

3) El p-valor es menor a 0.05, y conforme la Tabla 18, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, de que existe una relación significativa de la confidencialidad en la eficiencia de hashrate en el hardware de la nube pública, 2023.

4) La correlación de -0.866 sugiere una correlación negativa muy fuerte entre la eficiencia de hashrate y la confidencialidad en la muestra analizada. La significancia estadística respalda que las dimensiones están relacionadas. Por lo tanto, existe una asociación significativa y positiva entre eficiencia de hashrate y la confidencialidad en la muestra analizada.

Para realizar las pruebas de correlaciones de las dimensiones confidencialidad y conexión, se formuló las hipótesis respectivas en la tabla 20:

Tabla 20.

Formulación de hipótesis para pruebas de correlaciones

Pruebas de Correlaciones	**Detalle**
Ho	Ho: No existe una relación significativa de la confidencialidad en la Conexión en el hardware de la nube pública, 2023.
Ha	Ha: Existe una relación significativa de la confidencialidad en la Conexión en el hardware de la nube pública, 2023.
α	95%(0.950)
Error: α	5%(0.050)
Tipo de Prueba de Correlación	Distribución normal: Pearson Distribución no normal: Spearman
Criterio de evaluación	0.050 > p-valor Aprobar Ha Declinar Ho 0.050=< p-valor Declinar Ha Aprobar Ho
Interpretación de p-valor	Se considera inversa, correlación negativa muy fuerte cuando p-valor se encuentra de -1,0 hasta -0,8 inclusive. Se considera inversa, correlación negativa fuerte cuando p-valor se encuentra de -0,79 hasta -0,6 inclusive. Se considera inversa, correlación negativa moderada cuando p-valor se encuentra de -0,59 hasta -0,4 inclusive. Se considera inversa, correlación negativa débil cuando p-valor se encuentra de -0,39 hasta -0,2 inclusive. Se considera inversa, correlación negativa muy débil cuando p-valor se encuentra de -0,19 hasta -0,01 inclusive. Se considera correlación neutra cuando p-valor es 0. Se considera directa, correlación positiva muy débil cuando p-valor se encuentra de 0,19 hasta 0,01 inclusive. Se considera directa, correlación positiva débil cuando p-valor se encuentra de 0,2 hasta 0,39 inclusive. Se considera directa, correlación positiva moderada cuando p-valor se encuentra de 0,4 hasta 0,59 inclusive. Se considera directa, correlación positiva fuerte cuando p-valor se encuentra de 0,6 hasta 0,79 inclusive. Se considera directa, correlación positiva muy fuerte cuando p-valor se encuentra de 0,8 hasta 1,0 inclusive.

Elaboración Propia

Los resultados de las pruebas de correlación, se evidencia en la tabla siguiente:

Tabla 21.

Prueba de correlaciones de la dimensión confidencialidad y la dimensión conexión

Correlaciones			***Confidencialidad***
Rho Spearman	***Conexión***	Coeficiente de correlación	-,928
		Sig. (bilateral)	,000
		N	180

Elaboración Propia

La interpretación de los resultados de la Tabla 21, son:

1) Coeficiente de Correlación de Spearman (Rho) entre conexión y la confidencialidad es de -0,928. Este coeficiente indica la fuerza y dirección de la relación entre las dos variables.

2) Significancia Estadística: La correlación es significativa a un nivel de significancia del 0.000 (bilateral).

3) El p-valor es menor a 0.05, y conforme la Tabla 20, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, de que existe una relación significativa de la confidencialidad en la Conexión en el hardware de la nube pública, 2023.

4) La correlación de -0.928 sugiere una correlación negativa muy fuerte entre la conexión y la confidencialidad en la muestra analizada. La significancia estadística respalda que las dimensiones están relacionadas. Por lo tanto, existe una asociación significativa y positiva entre conexión y la confidencialidad en la muestra analizada.

Para realizar las pruebas de correlaciones de las dimensiones confidencialidad y rendimiento, se formuló las hipótesis respectivas en la tabla 20:

Tabla 22.

Formulación de hipótesis para pruebas de correlaciones

Pruebas de Correlaciones	**Detalle**
Ho	Ho: No existe relación significativa de la confidencialidad en el rendimiento en el hardware de la nube pública, 2023.
Ha	Ha: Existe relación significativa de la confidencialidad en el rendimiento en el hardware de la nube pública, 2023.
α	95%(0.950)
Error: α	5%(0.050)
Tipo de Prueba de Correlación	Distribución normal: Pearson Distribución no normal: Spearman
Criterio de evaluación	0.050 > p-valor Aprobar Ha Declinar Ho 0.050=< p-valor Declinar Ha Aprobar Ho
Interpretación de p-valor	Se considera inversa, correlación negativa muy fuerte cuando p-valor se encuentra de -1,0 hasta -0,8 inclusive. Se considera inversa, correlación negativa fuerte cuando p-valor se encuentra de -0,79 hasta -0,6 inclusive. Se considera inversa, correlación negativa moderada cuando p-valor se encuentra de -0,59 hasta -0,4 inclusive. Se considera inversa, correlación negativa débil cuando p-valor se encuentra de -0,39 hasta -0,2 inclusive. Se considera inversa, correlación negativa muy débil cuando p-valor se encuentra de -0,19 hasta -0,01 inclusive. Se considera correlación neutra cuando p-valor es 0. Se considera directa, correlación positiva muy débil cuando p-valor se encuentra de 0,19 hasta 0,01 inclusive. Se considera directa, correlación positiva débil cuando p-valor se encuentra de 0,2 hasta 0,39 inclusive. Se considera directa, correlación positiva moderada cuando p-valor se encuentra de 0,4 hasta 0,59 inclusive. Se considera directa, correlación positiva fuerte cuando p-valor se encuentra de 0,6 hasta 0,79 inclusive. Se considera directa, correlación positiva muy fuerte cuando p-valor se encuentra de 0,8 hasta 1,0 inclusive.

Elaboración Propia

Los resultados de las pruebas de correlación, se evidencia en la tabla siguiente:

Tabla 23.

Prueba de correlaciones de la dimensión confidencialidad y la dimensión rendimiento

Correlaciones			***Confidencialidad***
Rho Spearman	***Rendimiento***	Coeficiente de correlación	-,868
		Sig. (bilateral)	,000
		N	180

Elaboración Propia

La interpretación de los resultados de la Tabla 23, son:

1) Coeficiente de Correlación de Spearman (Rho) entre conexión y el rendimiento es de
   -0,868. Este coeficiente indica la fuerza y dirección de la relación entre las dos variables.
2) Significancia Estadística: La correlación es significativa a un nivel de significancia del 0.000 (bilateral).
3) El p-valor es menor a 0.05, y conforme la Tabla 22, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, de que existe relación significativa de la confidencialidad en el rendimiento en el hardware de la nube pública, 2023.
4) La correlación de -0.868 sugiere una correlación negativa muy fuerte entre el rendimiento y la confidencialidad en la muestra analizada. La significancia estadística respalda que las dimensiones están relacionadas. Por lo tanto, existe una asociación significativa y positiva entre rendimiento y la confidencialidad en la muestra analizada.

V. DISCUSIÓN

En esta investigación, sobre Red privada virtual y la minería de criptomonedas en el hardware de la nube pública, 2023, se tiene la dimensión confidencialidad, donde obtuvo una reducción en el indicador frame length con 54 byte(Pre – Test), con 0 bytes(Post – Test), obteniendo una reducción de 100%. Adicionalmente, para el indicador payload con 36 byte(Pre – Test), con los 0 bytes(Post – Test), obteniendo una reducción de 100%. Para ello, a través de las pruebas de Spearman, el sig bilateral igual a 0,00 está siendo menor a $\alpha = 0.05$, a través del cual se observa que existe una relación de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, siendo esto beneficioso para la investigación.

Estos resultados fueron confirmados por Surantha y Rino(2018) en su investigación, utilizaron una red privada virtual, lograron encapsular el tráfico de los datos, esto resultados fueron verificados con la herramienta wireshark.

Así mismo, los resultados de la investigación son respaldados con lo mencionado por Sun et al.(2022), quienes detectaron el comportamiento de la minería de criptomonedas con la utilización de técnicas de aprendizaje automático y análisis de tráfico de red. Su técnica, basada en características convolucionales, lograron diferenciar con gran precisión entre los flujos de minería y los flujos normales, mencionaron que la identificación del tráfico de minería requería un tamaño de payload mínimo de 20 bytes y un mínimo de frame length requerido para detectar el tráfico de minería de 46 hasta 566 byte. Ambos estudios resaltan la importancia de detectar comportamientos tempranos en la minería de criptomonedas.

Sin embargo, mientras que la investigación actual se enfoca en la utilización de la red privada virtual y la minería de criptomonedas en la nube pública, Sun et al., se concentraron en la creación de un método efectivo para detectar el tráfico minero. Ambas investigaciones, cada una desde su punto de vista único, destacan la importancia de abordar y detectar comportamientos de minería de criptomonedas. Integrando los resultados de ambos estudios, podemos obtener una comprensión más completa de las técnicas de seguridad respecto a la minería de criptomonedas en la nube pública.

Sería fascinante ampliar la investigación a otros contextos donde el uso de la red privada virtual puede ser beneficiosa en otras aplicaciones de su uso en la nube pública y así reducir los riesgos asociados con la minería de criptomonedas.

Además, con respecto a la dimensión eficiencia de hashrate, donde obtuvo un aumento en el indicador tasa de hashrate local con 52,49H/s(Pre – Test), hacia los 105,17 H/s(Post- Test), reflejando un aumento de 100.36%. Adicionalmente, para el indicador tasa de hashrate efectivo con 10,5H/s(Pre – Test), hacia los 43,79H/s(Post- Test), reflejando un aumento de 317,04%. Para ello, a través de las pruebas de Spearman, el sig bilateral igual a 0,00 está siendo menor a $\alpha = 0.05$, a través del cual se observa que existe una relación significativa de la confidencialidad en la eficiencia de hashrate en el hardware de la nube pública, siendo esto beneficioso para la investigación.

Comparando los hallazgos de la investigación actual con el estudio de Shuaib et al.(2022), donde mostraron un aumento significativo en la eficiencia de hashrate de 10,5 H/s hacia los 43,79H/s respecto a las tasas de hashrate en la investigación actual, y en el estudio de Shuaib et al., de 60 MH/s hacia 73.91 MH/s.

Estos resultados en contraste por los presentados por Gundaboina et al.(2022), se observaron un aumento en la eficiencia de hashrate en la minería de criptomonedas que oscilaban de 26 MH/s hasta los 121 MH/s.

Sin embargo, mientras la presente investigación intenta determinar la relación de la confidencialidad en la eficiencia de hashrate en el hardware de la nube pública, Shuaib et al. y Gundaboina et al., se enfocaron en la optimización de unidades de procesamiento gráfico (GPU) mediante sobrecalentamiento y subcalentamiento. Así mismo en la investigación actual se tiene que las pruebas de Spearman respaldan la mejora en la eficiencia de hashrate.

Sería fascinante ampliar la investigación a otros contextos donde la red privada virtual, pueden ser cruciales para aumentar la eficiencia de hashrate en la minería de criptomonedas sobre hardware de GPU en la nube pública, contribuyendo a la sostenibilidad y rentabilidad de la práctica global.

Además, con respecto a la dimensión conexión, donde se obtuvo un aumento en el indicador tiempo de conexión con 5,94 minutos(Pre – Test), hacia los 60 minutos(Post – Test), obteniendo un aumento de 926,75%. Para ello, a través de las pruebas de Spearman, el sig bilateral igual a 0.00 está siendo menor a α = 0.05, a través del cual se observa que existe una relación significativa de la confidencialidad en la Conexión en el hardware de la nube pública, siendo esto beneficioso para la investigación.

Confirmando lo que Cruz et al.(2022) quienes usando GPU basado en pruebas con tiempo de duración, tuvo una disponibilidad de 6 horas de minado; logró obtener el aumento de la tasa de hashrate de 1.9681 KH/s hacia los 12 MH/s, mostrando una conexión prolongada en la minería.

Por otro lado, el estudio de Runchao et al. (2019), a través de 100 ejecuciones de 60 segundos cada una, logro obtener una mejora en la eficiencia de hashrate de 0,79KH/s hacia los 926,61KH/s. a través de la optimización de algoritmos de prueba de trabajo (PoW) de memoria para contrarrestar la centralización, así como el aumento de costos para la energía consumida con la proliferación de hardware específico.

En contraste al estudio evidenciado por Sukharev (2020) quien investigó sobre “Overclocking De Hardware Para Mejorar La Eficiencia De La Minería De Criptomonedas Ethereum”, el cual se llevó a cabo sobre un tiempo de conexión favorable de 10 minutos sin dañar el hardware utilizado, logro incrementar hasta 77% la eficiencia de hashrate de la minería de criptomonedas.

Por otro lado, para Iyer et al.(2018), se enfocaron en la minería de criptomonedas utilizando GPU y CPU, con un enfoque particular en el análisis financiero y la optimización del rendimiento. Se utilizó una metodología experimental para minar una variedad de criptomonedas en un entorno controlado durante un período de 24 horas. La implementación de overclocking en las GPU a través de "EVGA PrecisionX" fue una parte importante de su enfoque, lo que resultó en un aumento significativo del 20% en los hashrates (H/S) en comparación con los valores iniciales. El estudio también examinó el uso de energía del hardware utilizado, notando que la NVIDIA GTX 1060 requería 120 vatios de energía mientras que la NVIDIA GTX 1050 Ti requería 75 vatios. Las conclusiones destacan el valor del sobrecalentamiento para mejorar el rendimiento de la minería de

criptomonedas. Además, al evaluar la rentabilidad de las operaciones mineras, se enfatiza la necesidad de considerar el equilibrio entre el consumo de energía y el hashrate. Este estudio ayuda a comprender la optimización de recursos en este campo tecnológico en constante evolución y proporciona información útil sobre las prácticas efectivas y rentables en el contexto de la minería de criptomonedas.

Las investigaciones presentadas respecto a la conexión, respaldado por las pruebas de Spearman que demostraron una correlación significativa en la investigación actual muestran una continuidad de la conexión en el contexto de la minería de criptomonedas.

Sería fascinante ampliar la investigación a otros contextos donde la red privada virtual aborde otros aspectos relacionados con la confidencialidad y la conexión medible en tiempo de la minería de criptomonedas en otras regiones geográficas de la nube pública.

Por otra parte, el indicador tasa de consumo de CPU, se logró obtener 61,94%(Pre – Test), hacia los 62,94%(Post – Test), Para ello, a través de las pruebas de Spearman, el sig bilateral igual a 0.00 está siendo menor a $\alpha = 0.05$, a través del cual se observa un aumento moderado en la tasa de consumo de CPU siendo esto beneficioso para la investigación.

Por un lado, Gomes et al. (2020) examinaron el uso de la CPU para detectar el malware de minería de criptomonedas. La investigación experimental, realizada en un entorno de hardware de la nube pública, evaluó la presencia de scripts de minería en páginas web utilizando métricas de uso de CPU recopiladas en intervalos de 60 segundos. Los hallazgos indicaron que la detección de malware tenía una alta precisión, con una tasa de falsos positivos cercana al 0%.

Según Gomes et al., el método de análisis se concentró en descubrir patrones distintivos relacionados con la ejecución de scripts de minería al observar el comportamiento de la CPU en páginas web específicas. La conclusión principal fue que el uso de métricas de CPU, que aumentan el consumo del 50% al 100%, permite la detección efectiva de malware de minería. Además, los autores destacaron la necesidad de tener en cuenta el comportamiento de múltiples núcleos de CPU para una detección más precisa. Este estudio proporciona datos valiosos para abordar amenazas relacionadas con la minería de criptomonedas y establece

un cimiento sólido para otros estudios futuros en ciberseguridad y detección de malware.

Comparando los hallazgos de la investigación actual con el estudio de Wu et al.(2022) ambos abordan el uso excesivo de CPU relacionado con la minería de criptomonedas, pero desde diferentes ángulos. Wu et al. presentan MinerGuard, una solución que detecta aplicaciones basadas en navegador que realizan minería y destaca los efectos negativos de la minería en el uso de la CPU, mientras que este estudio evalúa la relación de la confidencialidad sobre la tasa de consumo de CPU y muestra un aumento moderado del 61.94% al 62.94%.

Aunque los estudios varían en su enfoque, ambos señalan que la eficiencia de la CPU es importante para la minería de criptomonedas. Wu et al., presentan MinerGuard, una solución proactiva que demuestra ser más precisa que los mecanismos de lista negra y reduce la carga de mantenimiento humano, mientras que la investigación actual proporciona datos específicos sobre la tasa de consumo de CPU. Estos hallazgos sugieren que, para contrarrestar la amenaza de la minería de criptomonedas basada en el navegador, es fundamental abordar directamente la tasa de consumo de CPU y implementar soluciones sofisticadas y efectivas como MinerGuard para proteger de manera proactiva la seguridad cibernética y la privacidad en línea.

Sin embargo, el estudio de Alkaeed et al. (2020) se enfoca en la minería de criptomonedas con CPU y GPU y ofrece un análisis más detallado de las características y ventajas de ambos procesadores. Alkaeed et al., examinaron minuciosamente la minería de criptomonedas con CPU y GPU, destacando los beneficios de estas unidades de procesamiento. Los autores contrastaron las diferencias arquitectónicas entre CPU y GPU en áreas como la mejora de la capacidad para realizar cálculos simultáneos.

Alkaeed et al., Realizaron comparaciones detalladas entre CPUs de Intel y GPUs de AMD, abordando características clave como la memoria y su ancho de banda, frecuencia y número de núcleos. El estudio también examinó el desarrollo de arquitecturas CPU-GPU y la herramienta de programación CUDA de NVIDIA. Como resultado, presentaron comparativas de pools de minería, obteniendo 4.8 KH/s para Sulsh y 750.9 KH/s para XMRPool. Además, exploraron las aplicaciones de la minería de criptomonedas en redes eléctricas inteligentes y proporcionaron

un marco integral para analizar los beneficios derivados de la utilización de CPUs y GPUs en la minería de criptomonedas. Mencionando que para entender los beneficios generales de utilizar CPUs y GPUs en la minería de criptomonedas, el análisis del desarrollo de arquitecturas CPU-GPU y la herramienta de programación CUDA de NVIDIA brindan un contexto más amplio.

En resumen, aunque la investigación actual muestra que un aumento moderado en la tasa de consumo de CPU es un indicador favorable, la discusión con otros estudios resaltaron la importancia de comprender las características y beneficios de las unidades de procesamiento en el contexto de la minería de criptomonedas. Los estudios mencionados, que examinan aspectos específicos y generales, ayudan a comprender mejor este campo tecnológico en constante cambio a nivel mundial.

Los resultados de la investigación actual, respaldados por las pruebas de Spearman, sugieren un aumento moderado en la tasa de consumo de CPU, lo que podría interpretarse como un impacto favorable en la minería de criptomonedas en la nube pública. Sin embargo, Wu et al. señalaron que el hacking de criptografía puede resultar en un consumo del 100% de la CPU, lo que destaca la importancia de abordar este problema en futuras investigaciones.

Por otra parte, el indicador tasa de consumo de RAM, se logró obtener 19,43%(Pre – Test), hacia los 21,43%(Post – Test), Para ello, a través de las pruebas de Spearman, el sig bilateral igual a 0.00 está siendo menor a $\alpha = 0.05$, a través del cual se observa un aumento moderado en la tasa de consumo de RAM siendo esto beneficioso para la investigación.

Sin embargo, el estudio de Jayasinghe et al.(2020), mostraron una perspectiva útil sobre cómo la minería de criptomonedas afecta el consumo de CPU y la RAM en la nube pública. Para Jayasinghe et al. señalaron que la táctica utilizada por los atacantes para evitar generar sospechas controlando minuciosamente el uso de la CPU mediante herramientas de minería como XMRig. Explicaron específicamente cómo se utilizan estas herramientas para asignar un número de núcleos específico, establecer límites y prioridades en el uso de la CPU, lo que permite una minería independiente que escapa a la detección de sistemas de seguridad.

En este contexto, Jayasinghe et al, señalaron que la tasa de consumo de la RAM y su aumento en la investigación actual adquiere relevancia porque Jayasinghe et al. sugieren que el monitoreo de RAM puede ser un indicador adicional crucial para detectar actividades maliciosas relacionadas con la minería de criptomonedas en entornos de infraestructura en la nube pública.

Ambos estudios coinciden en que comprender y vigilar de cerca el consumo de recursos, como RAM, es crucial para identificar actividades de minería de criptomonedas ilegales en entornos de nube pública. Además, destacan la importancia de desarrollar técnicas de detección que puedan detectar patrones de comportamiento relacionados con la minería de criptomonedas, incluso si los atacantes utilizan estrategias de evasión complejas. Estos resultados y sugerencias, en conjunto, ayudan a fortalecer la seguridad del entorno digital contra las amenazas potenciales de la minería de criptomonedas no autorizadas.

VI. CONCLUSIONES

1. Se determinó la relación de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, 2023. Con una correlación negativa muy fuerte de -0.866 entre ambas variables.

2. Se determinó la relación de la confidencialidad en la eficiencia de hashrate en el hardware de la nube pública, 2023. Con una correlación negativa muy fuerte de -0.866 entre ambas dimensiones.

3. Se determinó la relación de la confidencialidad en la Conexión en el hardware de la nube pública, 2023. Con una correlación negativa muy fuerte de -0.928 entre ambas dimensiones.

4. Se determinó la relación de la confidencialidad en el rendimiento en el hardware de la nube pública, 2023. Con una correlación negativa muy fuerte de -0.868 entre ambas dimensiones.

VII. RECOMENDACIONES

1. En futuros estudios, se recomienda a los investigadores que profundicen en nuevos protocolos y configuraciones de red privada virtual para comparar hardware de CPU y hardware de GPU en la nube pública.
2. En futuros estudios, se recomienda a los investigadores que puedan realizar un seguimiento de la confidencialidad en diferentes regiones de la nube publica, para así determinar donde se encuentra la mayor eficiencia de hashrate.
3. En futuros estudios, se recomienda a los investigadores que profundicen en varias plataformas de la nube publica, para determinar la confidencialidad que produce una red privada virtual y el tiempo de conexión para la minería de criptomonedas.
4. En futuros estudios, se recomienda a los investigadores ejecutar una red privada virtual y minería de criptomonedas sobre nuevas instancias de máquinas con hardware de CPU y GPU en diversas regiones de la nube publica con el fin de determinar si se mantiene estable el rendimiento del hardware.

REFERENCIAS

Abbas, H., Emmanuel, N., Amjad, M. F., Yaqoob, T., Atiquzzaman, M., Iqbal, Z., Shafqat, N., Shahid, W. Bin, Tanveer, A., & Ashfaq, U. (2023). Security Assessment and Evaluation of VPNs: A Comprehensive Survey. *ACM Computing Surveys*, *55*(13s). https://doi.org/10.1145/3579162

Aggarwal, S., & Kumar, N. (2021). Architecture of blockchain☆. In *Advances in Computers* (1st ed., Vol. 121). Elsevier Inc. https://doi.org/10.1016/bs.adcom.2020.08.009

Alkaeed, M. K. (2020). *Highlight on Cryptocurrencies Mining w ith CPUs and GPUs and their B enefits B ased on their C haracteristics*. *November*, 67–72. https://doi.org/10.1109/ICSET51301.2020.9265386

Almukaynizi, M., Paliath, V., Shah, M., Shah, M., & Shakarian, P. (2018). Finding cryptocurrency attack indicators using temporal logic and darkweb data. *2018 IEEE International Conference on Intelligence and Security Informatics, ISI 2018*, 91–93. https://doi.org/10.1109/ISI.2018.8587361

Alsindi, W. Z., & Lotti, L. (2021). Mining. *Internet Policy Review*, *10*(2), 1–9. https://doi.org/10.14763/2021.2.1551

Aye, G. C., Demirer, R., Gupta, R., & Nel, J. (2023). The pricing implications of cryptocurrency mining on global electricity markets: Evidence from quantile causality tests. *Journal of Cleaner Production*, *397*(November 2022), 136572. https://doi.org/10.1016/j.jclepro.2023.136572

Celina Oviedo, H., & Campo-Arias, A. (2005). Revista Colombiana de Psiquiatría Aproximación al uso del coeficiente alfa de Cronbach. *Revista Colombiana de Psiquiatría*, *XXXIV*(1), 571–580. http://www.redalyc.org/pdf/806/80634409.pdf%0Ahttp://www.redalyc.org/pdf/806/80650839004.pdf

Chauhan, M., & Shiaeles, S. (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. *Network*, *3*(3), 422–450. https://doi.org/10.3390/network3030018

Chen, X., Zhang, X., Elliot, M., Wang, X., & Wang, F. (2022). Fix the leaking tap: A survey of Trigger-Action Programming (TAP) security issues, detection techniques and solutions. *Computers and Security*, *120*, 102812.

https://doi.org/10.1016/j.cose.2022.102812

Chua, C. H., & Ng, S. C. (2022). Open-Source VPN Software: Performance Comparison for Remote Access. *ACM International Conference Proceeding Series*, 29 – 34. https://doi.org/10.1145/3561877.3561882

CISCO. (2018). Cisco 2018 Annual Cybersecurity Report. *Cisco 2018 Annual Cybersecurity Report*, 68. http://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf

CISCO. (2019). *Resolver fragmentación de IPv4 y problemas de MTU , MSS y PMTUD con GRE e IPSEC*. https://www.cisco.com/c/es_mx/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.pdf

CLOUDFLARE. (2023). *Conocimientos básicos de la red*. https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-computer-port/

Coonjah, I., Catherine, P. C., & Soyjaudah, K. M. S. (2018). Design and Implementation of UDP Tunneling-based on OpenSSH VPN. *Proceedings - IEEE 2018 International Conference on Advances in Computing, Communication Control and Networking, ICACCCN 2018*, 640 – 645. https://doi.org/10.1109/ICACCCN.2018.8748849

Crawshaw, D. (2021). Everything VPN is new again. *Communications of the ACM*, *64*(4), 130–134. https://doi.org/10.1145/3434230

Cruz, J., Lomeli, L., Mario Cortes Rodríguez, J., Iván, E., & Osuna, A. (2022). *Rendimiento Del Hardware De Un Equipo Personal En La Minería De Criptomoneda*. *6*, 58–63. https://doi.org/https://doi.org/10.18800/iusetveritas.201901.008

De Vries, A. (2023). Cryptocurrencies on the road to sustainability: Ethereum paving the way for Bitcoin. *Patterns*, *4*(1), 100633. https://doi.org/10.1016/j.patter.2022.100633

Dudani, S., Baggili, I., Raymond, D., & Marchany, R. (2023). The current state of cryptocurrency forensics. *Forensic Science International: Digital Investigation*, *46*, 301576. https://doi.org/10.1016/j.fsidi.2023.301576

Duong Le, V. T., Tran, T. H., Pham, H. L., Lam, D. K., & Nakashima, Y. (2021). MRSA: A High-Efficiency Multi ROMix Scrypt Accelerator for Cryptocurrency Mining and Data Security. *IEEE Access*, *9*, 168383–168396. https://doi.org/10.1109/ACCESS.2021.3131558

García Villalba, L. J., Sandoval Orozco, A. L., & Maestre Vidal, J. (2017). Advanced Payload Analyzer Preprocessor. *Future Generation Computer Systems*, *76*, 474–485.

https://doi.org/10.1016/j.future.2016.10.032

Gomes, F., & Correia, M. (2020). Cryptojacking Detection with CPU Usage Metrics. *2020 IEEE 19th International Symposium on Network Computing and Applications, NCA 2020*. https://doi.org/10.1109/NCA51143.2020.9306696

Gundaboina, L., Badotra, S., Bhatia, T. K., Sharma, K., Mehmood, G., Fayaz, M., & Khan, I. U. (2022). Mining Cryptocurrency-Based Security Using Renewable Energy as Source. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/4808703

Han, R., Foutris, N., & Kotselidis, C. (2019). Demystifying Crypto-Mining: Analysis and Optimizations of Memory-Hard PoW Algorithms. *Proceedings - 2019 IEEE International Symposium on Performance Analysis of Systems and Software, ISPASS 2019*, 22–33. https://doi.org/10.1109/ISPASS.2019.00011

Hauser, F., Haberle, M., Schmidt, M., & Menth, M. (2020). P4-IPsec: Site-to-Site and Host-to-Site VPN with IPsec in P4-Based SDN. *IEEE Access*, *8*, 139567–139586. https://doi.org/10.1109/ACCESS.2020.3012738

Heinonen, H. T., Semenov, A., Veijalainen, J., & Hamalainen, T. (2022). A Survey on Technologies Which Make Bitcoin Greener or More Justified. *IEEE Access*, *10*(June), 74792–74814. https://doi.org/10.1109/ACCESS.2022.3190891

Hernández, R., Fernández, C., & Baptista, M. (2014). *Metodología de la Investigación - 6ta ed.*

Hernández, R., & Mendoza, C. (2018). Metodología de la investigación: las tres rutas cuantitativa, cualitativa y mixta. In *Mc Graw Hill* (Vol. 1, Issue Mexico).

Iyer, S. G., & Dipakumar Pawar, A. (2018). GPU and CPU accelerated mining of cryptocurrencies and their financial analysis. *Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2018*, 599 – 604. https://doi.org/10.1109/I-SMAC.2018.8653733

Jakóbczyk, M. T. (2020). Practical Oracle Cloud Infrastructure: Infrastructure as a Service, Autonomous Database, Managed Kubernetes, and Serverless. *Practical Oracle Cloud Infrastructure: Infrastructure as a Service, Autonomous Database, Managed Kubernetes, and Serverless*, 1–566. https://doi.org/10.1007/978-1-4842-5506-3

Jayasinghe, K., & Poravi, G. (2020). A Survey of Attack Instances of Cryptojacking Targeting Cloud Infrastructure. *ACM International Conference Proceeding Series*, *115*, 100–107. https://doi.org/10.1145/3379310.3379323

Karmakar, K. K., Varadharajan, V., Tupakula, U., Nepal, S., & Thapa, C. (2020). Towards a security enhanced virtualised network infrastructure for internet of medical things (IoMT). *Proceedings of the 2020 IEEE Conference on Network Softwarization: Bridging the Gap Between AI and Network Softwarization, NetSoft 2020*, 257–261. https://doi.org/10.1109/NetSoft48620.2020.9165387

Kheirkhah, M., Phan, T. K., Wei, X., Griffin, D., & Rio, M. (2020). UCIP: User controlled internet protocol. *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2020*, 279 – 284. https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162833

KINGSTON. (2023). *Glosario de Kingston*. https://www.kingston.com/latam/memory/kingston-glossary

Lackorzynski, T., Kopsell, S., & Strufe, T. (2019). A Comparative Study on Virtual Private Networks for Future Industrial Communication Systems. *IEEE International Workshop on Factory Communication Systems - Proceedings, WFCS*, *2019-May*. https://doi.org/10.1109/WFCS.2019.8758010

Lasla, N., Al-Sahan, L., Abdallah, M., & Younis, M. (2022). Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm. *Computer Networks*, *214*(May), 109118. https://doi.org/10.1016/j.comnet.2022.109118

Laszewski, T., & Nauduri, P. (2012). Migrating to the Cloud. *Migrating to the Cloud*, 1–19. https://doi.org/10.1016/b978-1-59749-647-6.00001-6

Li, C., Fang, L., Sun, S., An, T., & Wang, C. (2023). The Optimal UDP Data Length in Ethernet. *Lecture Notes in Electrical Engineering*, *917 LNEE*, 1050 – 1057. https://doi.org/10.1007/978-981-19-3387-5_126

López Miranda, L. (2019). Bitcoin: ¿Tenerla o ignorarla? Una aproximación hacia el tratamiento tributario peruano de la criptomoneda más famosa del mundo. *Ius Et Veritas*, *2929*(58), 140–153. https://doi.org/10.18800/iusetveritas.201901.008

Nani, A. (2022). The doge worth 88 billion dollars: A case study of Dogecoin. *Convergence*, *28*(6), 1719–1736. https://doi.org/10.1177/13548565211070417

Parthasarathy, R., Loong, S. S., Ayyappan, P., Hamid, Z. A., & Kumar, A. S. (2022). Implementation of Site-To-Site IPSEC Virtual Private Network For Enterprise Network Design Using Cisco Packet Tracer Simulation Tool. *International Journal of Mechanical Engineering*, *7*(1), 1293 – 1305. https://www.scopus.com/inward/record.uri?eid=2-s2.0-

85122393699&partnerID=40&md5=64bdc693c3ab6025b0a9dc0dd3057374

Peru21. (2021). *¿Cómo deberían estar reguladas las criptomonedas en nuestro país?* https://peru21.pe/economia/como-deberian-estar-reguladas-las-criptomonedas-en-nuestro-pais-ncze-noticia/

Peters, K. (2019). 21st Century Crime: How Malicious Artificial Intelligence Will Impact Homeland Security. *Homeland Security Affairs*. https://www.proquest.com/scholarly-journals/21st-century-crime-how-malicious-artificial/docview/2266265939/se-2?accountid=37408

Pineda, A. P., Sojos, G. L., & Calle, M. P. (2019). Análisis del Sistema Turístico de la Parroquia Casacay, Pasaje, Ecuador. *Revista Interamericana de Ambiente y Turismo*, *15*(2), 162–169. https://doi.org/10.4067/s0718-235x2019000200162

Poongodi, T., Ilango, S. S., Gupta, V., & Prasad, S. K. (2022). Influence of blockchain technology in pharmaceutical industries. In *Blockchain Technology for Emerging Applications: A Comprehensive Approach*. Elsevier Inc. https://doi.org/10.1016/B978-0-323-90193-2.00009-0

Reedy, P. (2023). Interpol review of digital evidence for 2019–2022. *Forensic Science International: Synergy*, *6*(January), 100313. https://doi.org/10.1016/j.fsisyn.2022.100313

RPP. (2021). *Cada vez más hackers infectan PC para minar criptomonedas y Perú es uno de los países más afectados*. https://rpp.pe/tecnologia/mas-tecnologia/criptomonedas-cada-vez-mas-hackers-infectan-pc-para-minar-bitcoins-y-peru-es-uno-de-los-paises-mas-afectados-noticia-1350915

Safaei Pour, M., Nader, C., Friday, K., & Bou-Harb, E. (2023). A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security. *Computers and Security*, *128*, 103123. https://doi.org/10.1016/j.cose.2023.103123

Salman, F. A. (2017). *Implementation of IPsec-VPN Tunneling using GNS3*. *7*(3), 855–860. https://doi.org/10.11591/ijeecs.v7.i3.pp855-860

Sampieri, R. (2018). Las rutas Cuantitativa Cualitativa y Mixta. In *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta*. shorturl.at/mwS39

Seraj, S., Khodambashi, S., Pavlidis, M., & Polatidis, N. (2023). MVDroid: an android malicious VPN detector using neural networks. *Neural Computing and Applications*, *35*(29), 21555–21565. https://doi.org/10.1007/s00521-023-08512-1

Shaikh, K. A., Karthik Bhat, A., & Moharir, M. (2018). A Survey on SSL Packet Structure.

2nd International Conference on Computational Systems and Information Technology for Sustainable Solutions, CSITSS 2017. https://doi.org/10.1109/CSITSS.2017.8447634

Shuaib, M., Badotra, S., Khalid, M. I., Algarni, A. D., Ullah, S. S., Bourouis, S., Iqbal, J., Bharany, S., & Gundaboina, L. (2022). A Novel Optimization for GPU Mining Using Overclocking and Undervolting. *Sustainability (Switzerland)*, *14*(14). https://doi.org/10.3390/su14148708

Sibande, X., Demirer, R., Balcilar, M., & Gupta, R. (2023). On the pricing effects of bitcoin mining in the fossil fuel market: The case of coal. *Resources Policy*, *85*(PB), 103539. https://doi.org/10.1016/j.resourpol.2023.103539

Steenkiste, P. (2023). IP and TCP. *Synthesis Lectures on Mobile and Pervasive Computing*, 89 – 103. https://doi.org/10.1007/978-3-031-27466-4_5

Sukharev, P. V. (2020). Hardware Overclocking to Improve the Efficiency of Ethereum Cryptocurrency Mining. *Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus 2020*, 1873–1877. https://doi.org/10.1109/EIConRus49466.2020.9039491

Sukharev, P. V., & Silnov, D. S. (2018). Asynchronous Mining of Ethereum Cryptocurrency. *Proceedings of the 2018 International Conference "'Quality Management, Transport and Information Security, Information Technologies'", IT and QM and IS 2018*, 731–735. https://doi.org/10.1109/ITMQIS.2018.8524929

Sun, P., Lyu, M., Li, H., Yang, B., & Peng, L. (2022). An early stage convolutional feature extracting method using for mining traffic detection. *Computer Communications*, *193*(July), 346–354. https://doi.org/10.1016/j.comcom.2022.06.044

Surantha, N., & Rino. (2018). Secure Portable Virtual Private Network with Rabbit Stream Cipher Algorithm. *Procedia Computer Science*, *135*, 259–266. https://doi.org/10.1016/j.procs.2018.08.173

Taylor, M. B. (2017). The evolution of bitcoin hardware. *Computer*, *50*(9), 58–66. https://doi.org/10.1109/MC.2017.3571056

Tekiner, E., Acar, A., Uluagac, A. S., Kirda, E., & Selcuk, A. A. (2021). SoK: Cryptojacking malware. *Proceedings - 2021 IEEE European Symposium on Security and Privacy, Euro S and P 2021*, 120–139. https://doi.org/10.1109/EuroSP51992.2021.00019

Tovanich, N., Soulie, N., & Isenberg, P. (2021). Visual Analytics of Bitcoin Mining Pool

Evolution: On the Road Toward Stability? *2021 11th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2021*. https://doi.org/10.1109/NTMS49979.2021.9432675

Turner, S. (2014). Transport layer security. *IEEE Internet Computing*, *18*(6), 60–63. https://doi.org/10.1109/MIC.2014.126

Vargas Cordero, Z. R. (2009). La Investigación aplicada: Una forma de conocer las realidades con evidencia científica. *Revista Educación*, *33*(1), 155–165. https://doi.org/DOI 10.15517/REVEDU.V33I1.538

WHIRESHARK. (2020). *Ethernet (IEEE 802.3)*. https://wiki.wireshark.org/Ethernet

WIRESHARK. (2021). *¿Qué es la carga útil en un cuadro y dónde puedo encontrarla después de la captura?* https://ask.wireshark.org/question/21236/what-is-payload-in-a-frame-and-where-i-can-find-it-after-capture/

Wu, M. H., Lai, Y. J., Hwang, Y. L., Chang, T. C., & Hsu, F. H. (2022). MinerGuard: A Solution to Detect Browser-Based Cryptocurrency Mining through Machine Learning. *Applied Sciences (Switzerland)*, *12*(19). https://doi.org/10.3390/app12199838

Zhou, D., Yan, Z., Fu, Y., & Yao, Z. (2018). A survey on network data collection. *Journal of Network and Computer Applications*, *116*(May), 9–23. https://doi.org/10.1016/j.jnca.2018.05.004

ANEXOS

Anexo 1:Matriz de operacionalización de variable dependiente

Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición	Instrumentos
VD: minería de criptomonedas	La minería de criptomonedas, (también conocida como *minería de bitcoin*) es el proceso que se usa para crear criptomonedas nuevas y verificar transacciones(Google 2023), implica utilizar hardware para resolver problemas computacionales, su objetivo es generar ganancias. (Alsindi & Lotti, 2021)	Al medir cada indicador a través de las propias aplicaciones donde se ejecuta la minería se procederá a anotar en una ficha de registros, bajo las escalas validadas por expertos, se obtendrá a través del uso de instrumentos elaborado por el investigador.	Eficiencia de Hashrate	*Tasa de Hashrate Local (THL > 0 H/s) $THL=(\sum HL)/CHL$ THL= Tasa De Hashrate Local ∑HL=Sumatoria de Hashrate Local CHL=Cantidad Hashrate Local	Razón	Ficha de Registro
				*Tasa de Hashrate Efectivo (THL > 0 H/s) $THE=(\sum HE)/CHE$ THE= Tasa De Hashrate Efectivo ∑HE=Sumatoria de Hashrate Efectivo CHE=Cantidad Hashrate Efectivo	Razón	
			Conexión	*Tiempo de conexión $TC=(\sum TC)/CTC$ TC= Tiempo de conexión ∑TC=Sumatoria Tiempo de conexión CTC=Cantidad Tiempo de conexión	Razón	Ficha de Registro
			Rendimiento	*Tasa consumo de CPU $TCCPU=(\sum TCCPU)/CTCPU$ TCCPU= Tasa de Consumo CPU ∑TCCPU=Sumatoria Tasa de Consumo CPU CTCCPU=Cantidad Tasa de Consumo CPU	Razón	Ficha de Registro
				*Tasa de consumo de RAM $TCRAM=(\sum TCRAM)/CTCRAM$ TCRAM= Tasa de Consumo RAM ∑TCRAM=Sumatoria Tasa de Consumo RAM CTCRAM=Cantidad Tasa de Consumo RAM	Razón	Ficha de Registro

Anexo 2:Matriz de operacionalización de variable independiente

Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición	Instrumentos
VI: **Red privada virtual**	La red privada virtual se define como una conexión directa entre el usuario y un servidor, permitiendo ocultar la ubicación geográfica, además de asegurar el anonimato y la privacidad de la información, a través de un proveedor de nube pública (Safaei Pour et al.2023).	Mediante la red privada virtual, se pretende lograr una conexión segura de dispositivos y al medir cada indicador a través de las propias aplicaciones donde se ejecuta la red privada virtual, se procederá a anotar en una ficha de registros, bajo las escalas validadas por expertos, ello se obtendrá a través del uso de instrumentos elaborado por el investigador.	Confidencialidad	*Frame Length $FL=(\sum FL)/CFL$ FL= Frame Length ∑FL=Sumatoria de Frame Length CFL=Cantidad Frame Length	Razón	Ficha de Registro
				*PayLoad $PL=(\sum PL)/CPL$ PL= PayLoad ∑PL=Sumatoria de PayLoad CPL=Cantidad PayLoad	Razón	

Anexo 3:Matriz de Consistencia - "Red privada virtual y la minería de criptomonedas en el hardware de la nube pública, 2023".

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES E INDICADORES	METODOS Y TECNICAS DE INVESTIGACION
PROBLEMA GENERAL ¿ Existe una relación de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, 2023? **PROBLEMAS ESPECIFICOS** ▪ PE1: ¿Existe una relación de la confidencialidad impacta en la eficiencia de hashrate en el hardware de la nube pública, 2023? ▪ PE2: ¿Existe una relación de la confidencialidad en la **Conexión** en el hardware de la nube pública, 2023? PE3: ¿Existe una relación de la confidencialidad en el rendimiento en el hardware de la nube pública, 2023?	**OBJETIVO GENERAL** Determinar la relación de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, 2023. **OBJETIVOS ESPECIFICOS** ▪ OE1: Determinar la relación de la confidencialidad en la eficiencia de hashrate en el hardware de la nube pública, 2023. ▪ OE2: Determinar la relación de la confidencialidad en la **Conexión** en el hardware de la nube pública, 2023. ▪ OE3: Determinar la relación de la confidencialidad en el rendimiento en el hardware de la nube pública, 2023.	**HIPÓTESIS GENERAL** Existe una relación significativa de la red privada virtual en la minería de criptomonedas en el hardware de la nube pública, 2023. **HIPÓTESIS ESPECIFICOS** ▪ HE1: Existe una relación significativa de la confidencialidad en la eficiencia de hashrate en el hardware de la nube pública, 2023. ▪ HE2: Existe una relación significativa de la confidencialidad en la **Conexión** en el hardware de la nube pública, 2023. ▪ HE3: Existe relación significativa de la confidencialidad en el rendimiento en el hardware de la nube pública, 2023.	**VARIABLE INDEPENDIENTE:** **Red privada virtual** • **Dimensión: Confidencialidad** Frame Length Payload **VARIABLE DEPENDIENTE:** **Minería de criptomonedas** • **Dimensión: Eficiencia de hashrate** -Indicador: -Tasa de Hashrate local -Tasa de Hashrate efectivo • **Dimensión: Conexión** -Indicador: Tiempo de conexión • **Dimensión: Rendimiento** -Indicadores: -% Tasa de Consumo de CPU. -% Tasa de Consumo DE RAM.	**Métodos:** **Tipo:** Aplicada **Nivel:** Correlacional **Diseño**: Experimental Tipo: Cuasi Experimental Tipo: Cuantitativo pre y post Grupo | Antes | Intervención | Después GE: | 0_1 | X | 0_2 ▪ GE: Instancia de máquinas virtuales en la nube. ▪ O1: Aplicación de instrumentos según indicadores antes de la implementación de la red privada virtual (pre-test). ▪ X: red privada virtual. ▪ O2: Aplicación de instrumentos según indicadores después de la implementación de la red privada virtual(post-test). ▪ Población: instancia en la nube publica, Muestra: 6 máquinas virtuales N1- us-central1-a, de las cuales se tomará 180 observaciones. **Técnicas:** ▪ De recolección de datos Observación por: Ficha de Registro en función de los indicadores.

Anexo 4: Validación de instrumentos a través de juicio de experto N°1.

CARTA DE PRESENTACIÓN

Señor Ingeniero:

Marlon Frank Acuña Benites

Presente

Asunto: **VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO**.

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, siendo estudiante del Programa de Maestría en Ingeniería de Sistemas con mención en Tecnologías de la Información de la Escuela de Posgrado de la UCV, en la sede Lima norte 202302, requiero validar los instrumentos con los cuales se recogerá la información necesaria para poder desarrollar mi investigación y con la que sustentaré mis competencias investigativas en la experiencia curricular de diseño y desarrollo del trabajo de investigación.

El título de mi investigación es "Red privada virtual y la minería de criptomonedas en el hardware de la nube pública, 2023". Cumplimiento normativo y Sentencias, siendo imprescindible contar con la aprobación de expertos del tema para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación, que le hago llegar contiene:

- Carta de presentación.
- Formato de validación.
- Certificado de validez de contenido de los instrumentos.

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

……

Carlos Alberto Bueno Torres
Alumno del programa de maestría grupo 202302
D.N.I 45883622

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento para medir las variables Red privada virtual y minería de criptomonedas. La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente. Agradezco su valiosa colaboración.

1. Datos generales del juez:

Nombre del juez:	Marlon Frank Acuña Benites
Grado profesional:	Maestría ( ) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa (x) Organizacional ( )
Áreas de experiencia profesional:	Educación
Institución donde labora:	Universidad César Vallejo sede Lima Norte
Tiempo de experiencia profesional en el área:	2 a 4 años (x) Más de 5 años ( )
Experiencia en Investigación (si corresponde)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Soporte teórico

Breve detalle de las variables de la investigación

VI. Red privada virtual: La red privada virtual permite una conexión directa entre el usuario y un servidor sin importar la ubicación geográfica dando como resultado el anonimato y la privacidad de la información permitiendo conectarse a un proveedor de nube pública (Safaei Pour et al.2023).

VD. Minería de criptomonedas: La minería de criptomonedas implica utilizar hardware para resolver problemas computacionales, su objetivo es que las ganancias comienzan a llegar, para ello la tasa de hashrate debe superar los 0 H/s.(Alsindi & Lotti, 2021).

4. Presentación de instrucciones para el juez

A continuación, a usted le presento la ficha de datos conformada por las 2 variables de mi investigación detalladas con sus dimensiones y su detalle respectivo, elaborado por Carlos Alberto Bueno Torres. De acuerdo con lossiguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem secomprende fácilmente, esdecir, su sintácticay semántica son adecuadas.	1. No cumple con el criterio	El indicador no es claro.
	2. Bajo Nivel	El indicador requiere bastantes modificaciones o unamodificación muy grande en el uso de las palabras de acuerdo con su significado o por laordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica dealgunos de los términos del ítem.
	4. Alto nivel	El indicador es claro, tiene semántica y sintaxisadecuada.
COHERENCIA El ítem tiene relación lógica conla dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (nocumple con el criterio)	El indicador no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El indicador tiene una relación tangencial /lejana conla dimensión.
	3. Acuerdo (moderado nivel)	El indicador tiene una relación moderada con ladimensión que se está midiendo.
	4. Totalmente de Acuerdo (altonivel)	El indicador se encuentra está relacionado con ladimensión que está midiendo.
RELEVANCIA El ítem es esencialo importante, es decir debe ser incluido.	1. No cumple con el criterio	El indicador puede ser eliminado sin que se veaafectada la medición de la dimensión.
	2. Bajo Nivel	El indicador tiene alguna relevancia, pero otro ítempuede estar incluyendo lo que mide éste.
	3. Moderado nivel	El indicador es relativamente importante.
	4. Alto nivel	El indicador es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brindesus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

Primera dimensión: Confidencialidad

Objetivos de la Dimensión: Contiene indicadores que evidencia los datos visibles capturados en el tráfico de red.

Variable	Dimensión	Indicadores	Claridad				Coherencia				Relevancia				
			1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	Observaciones/ Recomendaciones
VI:Red Privada Virtual	Confidencialidad	Frame Length				X				X				X	
		PayLoad				X				X				X	

Instrumento-FICHA DE REGISTRO: Frame Length y PayLoad					
Investigadores	Carlos Bueno Torres	**Tipo de Prueba**	☐ Pre -Test ☐ Post - Test		
Lugar de Investigación	Entorno Virtual Controlado				
Motivo de Estudio	**Frame Length y PayLoad**				
Fecha de Inicio		**Fecha Final**			
Variable	Red Privada Virtual				
FORMULA	**FL=(∑FL)/CFL**		**PL=(∑PL)/CPL**		
	FL= Frame Length ∑FL=Sumatoria de Frame Length CFL=Cantidad Frame Length		PL= PayLoad ∑PL=Sumatoria de PayLoad CPL=Cantidad PayLoad		
Procedimiento de Uso:	1.-Instalar en el dispositivo con windows, el app unmineable, wireshark y OpenVPN(Post test) 2.-Ejecutar la aplicacion WIRESHARK durante 10 minutos y presionar start para iniciar la captura de datos 3.-Ejecutar aplpicaciones openVPN y presionar start(Solo en post Test) 4.-Ejecutar aplicacion unmineable 4.-Presionar STOP en wireshard 5.-filtrar ip de unmineable en wireshark: ip.dst == 161.35.250.173 6.-Ésto se debe realizar en cada instancia elegido para esta investigación y registrar lo solicitado.				
N° INSTANCIA	**Fecha**	**Frame Length**	**FL**	**PayLoad**	**PL**

SEGUNDA dimensión: Eficiencia de Hashrate

Objetivos de la Dimensión: Contiene indicadores que evidencia los datos de eficiencia de hashrate de la minería de criptomonedas.

Variable	Dimensión	Indicadores	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
			1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	
VD: Minería de Criptomonedas	Eficiencia de Hash Rate	Tasa de Hashrate local				X				X				X	
		Tasa de Hashrate efectivo				X				X				X	

Instrumento-FICHA DE REGISTRO: Tasa de Hashrate Local y Tasa de Hashrate Efectivo					
Investigadores	Carlos Bueno Torres	Tipo de Prueba	☐ Pre -Test ☐ Post - Test		
Lugar de Investigación	Entorno Virtual Controlado				
Motivo de Estudio	Tasa de Hashrate Local y Tasa de Hashrate Efectivo				
Fecha de Inicio		Fecha Final			
Variable	Minería de Criptomonedas				
FORMULA	THL=(∑HL)/CHL		THE=(∑HE)/CHE		
	THL= Tasa De Hashrate Local		THE= Tasa De Hashrate Efectivo		
	∑HL=Sumatoria de Hashrate Local		∑HE=Sumatoria de Hashrate Efectivo		
	CHL=Cantidad Hashrate Local		CHE=Cantidad Hashrate Efectivo		
Procedimiento de Uso:	1.Instalar en el dispositivo con windows, el app unmineable y OpenVPN(Post Test) 2.-Ejecutar la aplicaciones durante 1 hora y presionar start para iniciar la medicion del minado 3.-Presionar STOP 4.-Ésto se debe realizar en cada instancia elegido para esta investigación y registrar lo solicitado.				
N° INSTANCIA	Fecha	Hashrate Local	THL	Hashrate Efectivo	THE

TERCERA dimensión: Conexión

Objetivos de la Dimensión: Contiene indicadores que evidencia los datos del tiempo de conexión de la minería de criptomonedas.

Variable	Dimensión	Indicadores	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
			1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	
VD: Minería de Criptomonedas	Conexión	Tiempo de Conexión				X				X				X	

Instrumento-FICHA DE REGISTRO: Tiempo de Conexión			
Investigadores	Carlos Bueno Torres	Tipo de Prueba	☐ Pre -Test ☐ Post - Test
Lugar de Investigación	Entorno Virtual Controlado		
Motivo de Estudio	TIEMPO DE CONEXIÓN		
Fecha de Inicio		Fecha Final	
Variable	Minería de Criptomonedas		
FORMULA	TC=(∑TC)/CTC		
	TC= Tiempo de conexión ∑TC=Sumatoria Tiempo de conexión CTC=Cantidad Tiempo de conexión		
Procedimiento de Uso:	1.Instalar en el dispositivo con windows, el app unmineable y OpenVPN(Post Test) 2.-Ejecutar la aplicaciones durante 1 hora y presionar start para iniciar la medicion del minado 3.-Presionar STOP 4.-Ésto se debe realizar en cada instancia elegido para esta investigación y registrar lo solicitado.		
N° ESTUDIANTE	Fecha	Tiempo de Conexión	TC

Primera dimensión: Rendimiento

Objetivos de la Dimensión: Contiene indicadores que evidencia los datos de consumo de hardware de la minería de criptomonedas.

Variable	Dimensión	Indicadores	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
			1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	
VD: Minería de Criptomonedas	Rendimiento	Tasa de consumo de CPU				X				X				X	
		Tasa de consumo de RAM				X				X				X	

Instrumento-FICHA DE REGISTRO: Tasa consumo CPU y Tasa consumo RAM					
Investigadores	Carlos Bueno Torres	Tipo de Prueba	☐ Pre -Test ☐ Post - Test		
Lugar de Investigación	Entorno Virtual Controlado				
Motivo de Estudio	Tasa consumo CPU y Tasa consumo RAM				
Fecha de Inicio		Fecha Final			
Variable	Minería de Criptomonedas				
FORMULA	TCCPU=(∑TCCPU)/CTCPU		TCRAM=(∑TCRAM)/CTCRAM		
	TCCPU= Tasa de Consumo CPU ∑TCCPU=Sumatoria Tasa de Consumo CPU CTCCPU=Cantidad Tasa de Consumo CPU		TCRAM= Tasa de Consumo RAM ∑TCRAM=Sumatoria Tasa de Consumo RAM CTCRAM=Cantidad Tasa de Consumo RAM		
Procedimiento de Uso:	1.-Instalar en el dispositivo con windows, el app unmineable y OpenVPN(Post Test) 2.-Ejecutar la aplicaciones durante 1 hora y presionar start para iniciar la medicion del minado 3.-Ejecutar aplpicacion administrador de tareas 4.-Presionar STOP 5.-Ésto se debe realizar en cada instancia elegido para esta investigación y registrar lo solicitado.				
N° INSTANCIA	Fecha	Hashrate Local	THL	Hashrate Efectivo	THE

Observaciones (precisar si hay suficiencia): El instrumento presenta suficiencia_____

Opinión de aplicabilidad: Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: …Marlon Acuña Benites**…..**

Especialidad del validador: Docente…Investigador……

10 de noviembre del 2023.

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Dr. Marlon Acuña Benites
DNI: 42097456
Ing. de Sistemas / Investigador

Firma del Experto validador

DNI: ……

Anexo 5: Validación de instrumentos a través de juicio de experto N°2.

CARTA DE PRESENTACIÓN

Señor Ingeniero:

Roberto Juan Tejada Ruiz

Presente

Asunto: **VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO**.

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, siendo estudiante del Programa de Maestría en Ingeniería de Sistemas con mención en Tecnologías de la Información de la Escuela de Posgrado de la UCV, en la sede Lima norte 202302, requiero validar los instrumentos con los cuales se recogerá la información necesaria para poder desarrollar mi investigación y con la que sustentaré mis competencias investigativas en la experiencia curricular de diseño y desarrollo del trabajo de investigación.

El título de mi investigación es "Red privada virtual y la minería de criptomonedas en el hardware de la nube pública, 2023". Cumplimiento normativo y Sentencias, siendo imprescindible contar con la aprobación de expertos del tema para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación, que le hago llegar contiene:

- Carta de presentación.
- Formato de validación.
- Certificado de validez de contenido de los instrumentos.

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

……

Carlos Alberto Bueno Torres
Alumno del programa de maestría grupo 202302
D.N.I 45883622

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento para medir las variables Red privada virtual y minería de criptomonedas. La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente. Agradezco su valiosa colaboración.

1. Datos generales del juez:

Nombre del juez:	Roberto Juan Tejada Ruiz
Grado profesional:	Maestría (x) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa (x) Organizacional (x)
Áreas de experiencia profesional:	Educación
Institución donde labora:	Universidad César Vallejo sede Lima Norte
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)
Experiencia en Investigación (si corresponde)	Docente tesis, jurado tesis, asesor tesis

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Soporte teórico

Breve detalle de las variables de la investigación

VI. Red privada virtual: La red privada virtual permite una conexión directa entre el usuario y un servidor sin importar la ubicación geográfica dando como resultado el anonimato y la privacidad de la información permitiendo conectarse a un proveedor de nube pública (Safaei Pour et al.2023).

VD. Minería de criptomonedas: La minería de criptomonedas implica utilizar hardware para resolver problemas computacionales, su objetivo es que las ganancias comienzan a llegar, para ello la tasa de hashrate debe superar los 0 H/s.(Alsindi et al. 2021).

4. Presentación de instrucciones para el juez

A continuación, a usted le presento la ficha de datos conformada por las 2 variables de mi investigación detalladas con sus dimensiones y su detalle respectivo, elaborado por Carlos Alberto Bueno Torres. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, esdecir, su sintácticay semántica son adecuadas.	1. No cumple con el criterio	El indicador no es claro.
	2. Bajo Nivel	El indicador requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica dealgunos de los términos del ítem.
	4. Alto nivel	El indicador es claro, tiene semántica y sintaxisadecuada.
COHERENCIA El ítem tiene relación lógica conla dimensión o indicador que estámidiendo.	1. totalmente en desacuerdo (nocumple con el criterio)	El indicador no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El indicador tiene una relación tangencial /lejana conla dimensión.
	3. Acuerdo (moderado nivel)	El indicador tiene una relación moderada con ladimensión que se está midiendo.
	4. Totalmente de Acuerdo (altonivel)	El indicador se encuentra está relacionado con ladimensión que está midiendo.
RELEVANCIA El ítem es esencialo importante, es decir debe ser incluido.	1. No cumple con el criterio	El indicador puede ser eliminado sin que se veaafectada la medición de la dimensión.
	2. Bajo Nivel	El indicador tiene alguna relevancia, pero otro ítempuede estar incluyendo lo que mide éste.
	3. Moderado nivel	El indicador es relativamente importante.
	4. Alto nivel	El indicador es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brindesus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

Primera dimensión: Confidencialidad

Objetivos de la Dimensión: Contiene indicadores que evidencia los datos visibles capturados en el tráfico de red.

Variable	Dimensión	Indicadores	Claridad				Coherencia				Relevancia				
			1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	Observaciones/ Recomendaciones
VI:Red Privada Virtual	Confidencialidad	Frame Length				X				X				X	
		PayLoad				X				X				X	

Instrumento-FICHA DE REGISTRO: Frame Length y PayLoad					
Investigadores	Carlos Bueno Torres	**Tipo de Prueba**	☐ Pre -Test ☐ Post - Test		
Lugar de Investigación	Entorno Virtual Controlado				
Motivo de Estudio	**Frame Length y PayLoad**				
Fecha de Inicio		**Fecha Final**			
Variable	Red Privada Virtual				
FORMULA	**FL=(∑FL)/CFL**		**PL=(∑PL)/CPL**		
	FL= Frame Length ∑FL=Sumatoria de Frame Length CFL=Cantidad Frame Length		PL= PayLoad ∑PL=Sumatoria de PayLoad CPL=Cantidad PayLoad		
Procedimiento de Uso:	1.-Instalar en el dispositivo con windows, el app unmineable, wireshark y OpenVPN(Post test) 2.-Ejecutar la aplicacion WIRESHARK durante 10 minutos y presionar start para iniciar la captura de datos 3.-Ejecutar aplpicaciones openVPN y presionar start(Solo en post Test) 4.-Ejecutar aplicacion unmineable 4.-Presionar STOP en wireshard 5.-filtrar ip de unmineable en wireshark: ip.dst == 161.35.250.173 6.-Ésto se debe realizar en cada instancia elegido para esta investigación y registrar lo solicitado.				
N° INSTANCIA	**Fecha**	**Frame Length**	**FL**	**PayLoad**	**PL**

SEGUNDA dimensión: Eficiencia de Hashrate

Objetivos de la Dimensión: Contiene indicadores que evidencia los datos de eficiencia de hashrate de la minería de criptomonedas.

Variable	Dimensión	Indicadores	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
			1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	
VD: Minería de Criptomonedas	Eficiencia de HashRate	Tasa de Hashrate local				X				X				X	
		Tasa de Hashrate efectivo				X				X				X	

Instrumento-FICHA DE REGISTRO: Tasa de Hashrate Local y Tasa de Hashrate Efectivo					
Investigadores	Carlos Bueno Torres	Tipo de Prueba	☐ Pre -Test ☐ Post - Test		
Lugar de Investigación	Entorno Virtual Controlado				
Motivo de Estudio	Tasa de Hashrate Local y Tasa de Hashrate Efectivo				
Fecha de Inicio		Fecha Final			
Variable	Minería de Criptomonedas				
FORMULA	THL=(∑HL)/CHL		THE=(∑HE)/CHE		
	THL= Tasa De Hashrate Local		THE= Tasa De Hashrate Efectivo		
	∑HL=Sumatoria de Hashrate Local		∑HE=Sumatoria de Hashrate Efectivo		
	CHL=Cantidad Hashrate Local		CHE=Cantidad Hashrate Efectivo		
Procedimiento de Uso:	1.Instalar en el dispositivo con windows, el app unmineable y OpenVPN(Post Test) 2.-Ejecutar la aplicaciones durante 1 hora y presionar start para iniciar la medicion del minado 3.-Presionar STOP 4.-Ésto se debe realizar en cada instancia elegido para esta investigación y registrar lo solicitado.				
N° INSTANCIA	Fecha	Hashrate Local	THL	Hashrate Efectivo	THE

TERCERA dimensión: Conexión

Objetivos de la Dimensión: Contiene indicadores que evidencia los datos del tiempo de conexión de la minería de criptomonedas.

Variable	Dimensión	Indicadores	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
			1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	
VD: Minería de Criptomonedas	Conexión	Tiempo de Conexión				X				X				X	

Instrumento-FICHA DE REGISTRO: Tiempo de Conexión			
Investigadores	Carlos Bueno Torres	**Tipo de Prueba**	☐ Pre -Test ☐ Post - Test
Lugar de Investigación	Entorno Virtual Controlado		
Motivo de Estudio	**TIEMPO DE CONEXIÓN**		
Fecha de Inicio		**Fecha Final**	
Variable	Minería de Criptomonedas		
FORMULA	**TC=(∑TC)/CTC**		
	TC= Tiempo de conexión ∑TC=Sumatoria Tiempo de conexión CTC=Cantidad Tiempo de conexión		
Procedimiento de Uso:	1.Instalar en el dispositivo con windows, el app unmineable y OpenVPN(Post Test) 2.-Ejecutar la aplicaciones durante 1 hora y presionar start para iniciar la medicion del minado 3.-Presionar STOP 4.-Ésto se debe realizar en cada instancia elegido para esta investigación y registrar lo solicitado.		
N° ESTUDIANTE	**Fecha**	**Tiempo de Conexión**	**TC**

Primera dimensión: Rendimiento

Objetivos de la Dimensión: Contiene indicadores que evidencia los datos de consumo de hardware de la minería de criptomonedas.

Variable	Dimensión	Indicadores	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
			1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	
VD: Minería de Criptomonedas	Rendimiento	Tasa de consumo de CPU				X				X				X	
		Tasa de consumo de RAM				X				X				X	

Instrumento-FICHA DE REGISTRO: Tasa consumo CPU y Tasa consumo RAM					
Investigadores	Carlos Bueno Torres	Tipo de Prueba	☐ Pre -Test ☐ Post - Test		
Lugar de Investigación	Entorno Virtual Controlado				
Motivo de Estudio	Tasa consumo CPU y Tasa consumo RAM				
Fecha de Inicio		Fecha Final			
Variable	Minería de Criptomonedas				
FORMULA	TCCPU=(∑TCCPU)/CTCPU		TCRAM=(∑TCRAM)/CTCRAM		
	TCCPU= Tasa de Consumo CPU ∑TCCPU=Sumatoria Tasa de Consumo CPU CTCCPU=Cantidad Tasa de Consumo CPU		TCRAM= Tasa de Consumo RAM ∑TCRAM=Sumatoria Tasa de Consumo RAM CTCRAM=Cantidad Tasa de Consumo RAM		
Procedimiento de Uso:	1.-Instalar en el dispositivo con windows, el app unmineable y OpenVPN(Post Test) 2.-Ejecutar la aplicaciones durante 1 hora y presionar start para iniciar la medicion del minado 3.-Ejecutar aplpicacion administrador de tareas 4.-Presionar STOP 5.-Ésto se debe realizar en cada instancia elegido para esta investigación y registrar lo solicitado.				
N° INSTANCIA	Fecha	Hashrate Local	THL	Hashrate Efectivo	THE

Observaciones (precisar si hay suficiencia): El instrumento presenta suficiencia si___

Opinión de aplicabilidad: Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: … Roberto Juan Tejada Ruiz.

Especialidad del validador: Docente… ingeniero industrial

10 de noviembre del 2023.

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto validador

DNI: 17930425

Ms. Roberto Juan Tejada Ruiz
INGENIERO INDUSTRIAL - C.I.P. 242352

Anexo 6: Tabla de datos utilizado en SPS.

pre_post	THL	THE	Tiempo de Conexión	Tasa consumo CPU	Tasa de Consumo de RAM	FL	PL
0	51,55	10,31	5,5	61,5	19,25	54	36
0	53,71	10,74	6,5	62,5	19,75	54	36
0	50,69	10,14	5,5	61,5	19,25	54	36
0	52,94	10,59	6	62	19,5	54	36
0	51,1	10,22	5,25	61,25	19	54	36
0	51,46	10,29	5,5	61,5	19,25	54	36
0	50	10	5,25	61,25	19	54	36
0	53,21	10,64	6,5	62,5	19,75	54	36
0	53,43	10,69	6	62	19,5	54	36
0	50,79	10,16	5,25	61,25	19	54	36
0	52,98	10,6	5,75	61,75	19,25	54	36
0	54,29	10,86	6,5	62,5	19,75	54	36
0	52,92	10,58	6	62	19,5	54	36
0	49,71	9,94	5	61	19	54	36
0	53,78	10,76	6,5	62,5	19,75	54	36
0	52,53	10,51	5,75	61,75	19,25	54	36
0	52,75	10,55	6	62	19,5	54	36
0	51,44	10,29	5,5	61,5	19	54	36
0	54,66	10,93	7	63	20	54	36
0	54,33	10,87	6,5	62,5	19,75	54	36
0	51,88	10,38	6	62	19,5	54	36
0	52,54	10,51	6	62	19,5	54	36
0	51,65	10,33	6	62	19,5	54	36

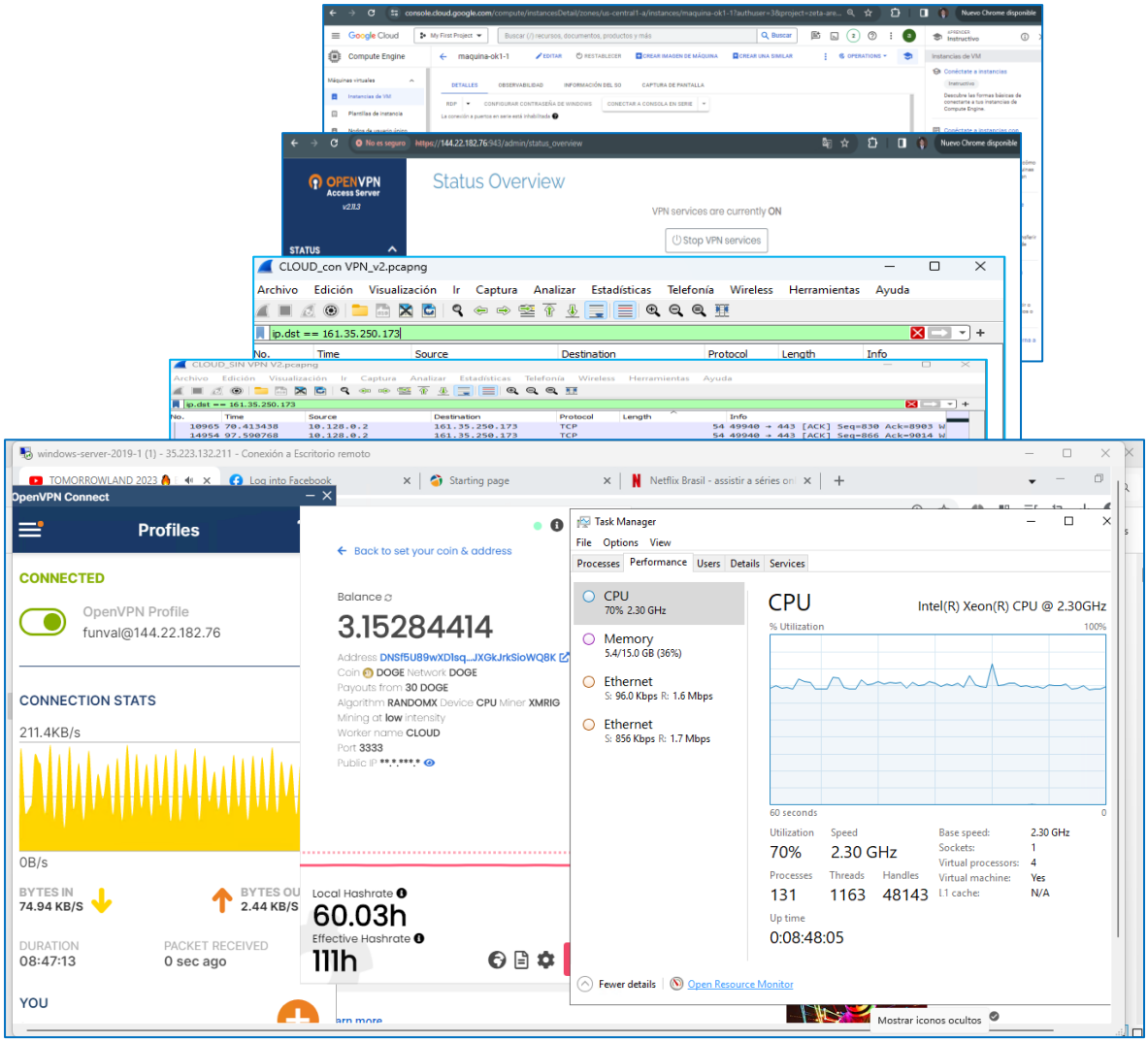
0	51,43	10,29	5,75	61,75	19,25	54	36
0	52,24	10,45	6	62	19,5	54	36
0	51,73	10,35	6	62	19,5	54	36
0	54,63	10,93	6,5	62,5	19,75	54	36
0	53,17	10,63	6	62	19,5	54	36
0	54,76	10,95	7	63	20	54	36
0	50,67	10,13	5,25	61,25	19	54	36
0	53,26	10,65	6	62	19,5	54	36
0	52,78	10,56	6	62	19,5	54	36
0	53,49	10,7	6,25	62,25	19,5	54	36
0	52,39	10,48	5,5	61,5	19,25	54	36
0	53,78	10,76	6,75	62,75	19,75	54	36
0	53,28	10,66	6	62	19,5	54	36
0	52,07	10,41	6	62	19,5	54	36
0	52,15	10,43	6	62	19,5	54	36
0	52,52	10,5	6,25	62,25	19,5	54	36
0	51,23	10,25	5,75	61,75	19,25	54	36
0	53,76	10,75	6,75	62,75	19,75	54	36
0	52,63	10,53	5,75	61,75	19,25	54	36
0	54,16	10,83	6,5	62,5	19,75	54	36
0	52,58	10,52	6	62	19,5	54	36
0	55,13	11,03	7	63	20	54	36
0	54,18	10,84	6,5	62,5	19,75	54	36
0	52,72	10,54	6	62	19,5	54	36
0	51,73	10,35	5,5	61,5	19,25	54	36
0	54,59	10,92	6,5	62,5	19,75	54	36
0	51,37	10,27	5,5	61,5	19,25	54	36
0	51,84	10,37	5,5	61,5	19,25	54	36
0	50,89	10,18	5	61	19	54	36
0	51,42	10,28	5,5	61,5	19,25	54	36
0	53,41	10,68	6,5	62,5	19,75	54	36
0	51,3	10,26	5,5	61,5	19,25	54	36
0	53,08	10,62	6,25	62,25	19,5	54	36
0	48,53	9,71	5	61	19	54	36
0	53,08	10,62	6	62	19,5	54	36
0	52,64	10,53	5,75	61,75	19,25	54	36

0	51,99	10,4	5,75	61,75	19,25	54	36
0	52,67	10,53	6,25	62,25	19,5	54	36
0	51,94	10,39	5,5	61,5	19,25	54	36
0	53,85	10,77	6,5	62,5	19,75	54	36
0	51,8	10,36	6,25	62,25	19,5	54	36
0	52,88	10,58	6	62	19,5	54	36
0	52,18	10,44	5,75	61,75	19,25	54	36
0	50,22	10,04	5	61	19	54	36
0	51,82	10,36	5,5	61,5	19,25	54	36
0	52,01	10,4	5,5	61,5	19	54	36
0	53,52	10,7	6,25	62,25	19,5	54	36
0	49,83	9,97	5,25	61,25	19	54	36
0	54,52	10,9	6,5	62,5	19,75	54	36
0	52,56	10,51	5,75	61,75	19,25	54	36
0	52	10,4	6	62	19,5	54	36
0	54,87	10,97	6,5	62,5	19,75	54	36
0	52,18	10,44	5,75	61,75	19,25	54	36
0	51,62	10,32	5,5	61,5	19,25	54	36
0	51,25	10,25	6	62	19,5	54	36
0	54,2	10,84	6,5	62,5	19,75	54	36
0	53,61	10,72	6	62	19,5	54	36
0	51,32	10,26	5,5	61,5	19,25	54	36
0	51,4	10,28	5,75	61,75	19,25	54	36
0	52,47	10,49	6,25	62,25	19,5	54	36
0	52,07	10,41	5,5	61,5	19,25	54	36
0	53,77	10,75	6,5	62,5	19,75	54	36
0	51,54	10,31	6	62	19,5	54	36
0	53,63	10,73	6,75	62,75	19,75	54	36
0	53,77	10,75	6	62	19,5	54	36
0	51,97	10,39	5,5	61,5	19,25	54	36
0	51,41	10,28	5,5	61,5	19	54	36
1	104,23	42,85	60	62,5	21,25	0	0
1	106,39	45,01	60	63,5	21,75	0	0
1	103,37	41,99	60	62,5	21,25	0	0
1	105,62	44,24	60	63	21,5	0	0
1	103,78	42,4	60	62,25	21	0	0
1	104,14	42,76	60	62,5	21,25	0	0
1	102,68	41,3	60	62,25	21	0	0
1	105,89	44,51	60	63,5	21,75	0	0
1	106,11	44,73	60	63	21,5	0	0
1	103,47	42,09	60	62,25	21	0	0

1	105,66	44,28	60	62,75	21,25	0	0
1	106,97	45,59	60	63,5	21,75	0	0
1	105,6	44,22	60	63	21,5	0	0
1	102,39	41,01	60	62	21	0	0
1	106,46	45,08	60	63,5	21,75	0	0
1	105,21	43,83	60	62,75	21,25	0	0
1	105,43	44,05	60	63	21,5	0	0
1	104,12	42,74	60	62,5	21	0	0
1	107,34	45,96	60	64	22	0	0
1	107,01	45,63	60	63,5	21,75	0	0
1	104,56	43,18	60	63	21,5	0	0
1	105,22	43,84	60	63	21,5	0	0
1	104,33	42,95	60	63	21,5	0	0
1	104,11	42,73	60	62,75	21,25	0	0
1	104,92	43,54	60	63	21,5	0	0
1	104,41	43,03	60	63	21,5	0	0
1	107,31	45,93	60	63,5	21,75	0	0
1	105,85	44,47	60	63	21,5	0	0
1	107,44	46,06	60	64	22	0	0
1	103,35	41,97	60	62,25	21	0	0
1	105,94	44,56	60	63	21,5	0	0
1	105,46	44,08	60	63	21,5	0	0
1	106,17	44,79	60	63,25	21,5	0	0
1	105,07	43,69	60	62,5	21,25	0	0
1	106,46	45,08	60	63,75	21,75	0	0
1	105,96	44,58	60	63	21,5	0	0
1	104,75	43,37	60	63	21,5	0	0
1	104,83	43,45	60	63	21,5	0	0
1	105,2	43,82	60	63,25	21,5	0	0
1	103,91	42,53	60	62,75	21,25	0	0
1	106,44	45,06	60	63,75	21,75	0	0
1	105,31	43,93	60	62,75	21,25	0	0
1	106,84	45,46	60	63,5	21,75	0	0
1	105,26	43,88	60	63	21,5	0	0
1	107,81	46,43	60	64	22	0	0
1	106,86	45,48	60	63,5	21,75	0	0
1	105,4	44,02	60	63	21,5	0	0
1	104,41	43,03	60	62,5	21,25	0	0
1	107,27	45,89	60	63,5	21,75	0	0
1	104,05	42,67	60	62,5	21,25	0	0

1	104,52	43,14	60	62,5	21,25	0	0
1	103,57	42,19	60	62	21	0	0
1	104,1	42,72	60	62,5	21,25	0	0
1	106,09	44,71	60	63,5	21,75	0	0
1	103,98	42,6	60	62,5	21,25	0	0
1	105,76	44,38	60	63,25	21,5	0	0
1	101,21	39,83	60	62	21	0	0
1	105,76	44,38	60	63	21,5	0	0
1	105,32	43,94	60	62,75	21,25	0	0
1	104,67	43,29	60	62,75	21,25	0	0
1	105,35	43,97	60	63,25	21,5	0	0
1	104,62	43,24	60	62,5	21,25	0	0
1	106,53	45,15	60	63,5	21,75	0	0
1	104,48	43,1	60	63,25	21,5	0	0
1	105,56	44,18	60	63	21,5	0	0
1	104,86	43,48	60	62,75	21,25	0	0
1	102,9	41,52	60	62	21	0	0
1	104,5	43,12	60	62,5	21,25	0	0
1	104,69	43,31	60	62,5	21	0	0
1	106,2	44,82	60	63,25	21,5	0	0
1	102,51	41,13	60	62,25	21	0	0
1	107,2	45,82	60	63,5	21,75	0	0
1	105,24	43,86	60	62,75	21,25	0	0
1	104,68	43,3	60	63	21,5	0	0
1	107,55	46,17	60	63,5	21,75	0	0
1	104,86	43,48	60	62,75	21,25	0	0
1	104,3	42,92	60	62,5	21,25	0	0
1	103,93	42,55	60	63	21,5	0	0
1	106,88	45,5	60	63,5	21,75	0	0
1	106,29	44,91	60	63	21,5	0	0
1	104	42,62	60	62,5	21,25	0	0
1	104,08	42,7	60	62,75	21,25	0	0
1	105,15	43,77	60	63,25	21,5	0	0
1	104,75	43,37	60	62,5	21,25	0	0
1	106,45	45,07	60	63,5	21,75	0	0
1	104,22	42,84	60	63	21,5	0	0
1	106,31	44,93	60	63,75	21,75	0	0
1	106,45	45,07	60	63	21,5	0	0
1	104,65	43,27	60	62,5	21,25	0	0
1	104,09	42,71	60	62,5	21	0	0

Anexo 7:Propuesta de ingeniería



Para descargar el instructivo de Usuario, ingresar al siguiente link:

https://drive.google.com/drive/folders/1Qp_nf48XdiLaPZZ9dqnBniJJzR3_XvSO?usp=sharing

Anexo 8:Registro en CONCYTEC

BUENO TORRES CARLOS ALBERTO

Identificadores

Orcid Id 0000-0002-2274-6298
Scopus Id
Wos Id

Contacto

Teléfono 993439794
Correo cabt1314@gmail.com

Fecha de última actualización: 22/12/2023

Ficha CTI Vitae: 369982

Fecha de exportación: 07/01/2024 01:02:08

Resumen

Datos Personales

Sexo	Masculino
Tipo de Documento de Identidad	DNI
Número de Documento de Identidad	45883622
País de Nacimiento	Perú
Fecha de Nacimiento	13/08/1989
Dirección	Av. De Los Ingenieros 536 Urb. Pablo Canepa
Departamento	LIMA
Provincia	LIMA
Distrito	LA MOLINA

Datos Actuales

Pagina web personal	http://
E-mail	cabt1314@gmail.com
Dirección actual	Calle Australia Mz. A Lt. 24 Los Portales De Javier Prado 1ra Etapa Ate
País	Perú
Teléfono de contacto	993439794
Celular	993439794
Departamento	Lima
Provincia	Lima
Distrito	Ate

Otros Identificadores

Scopus Author ID	
ORCID ID	0000-0002-2274-6298
Web of Science	

Anexo 9: Examen aprobado de Conducta Responsable en Investigación