UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Sistema de Encriptación Homomórfica para Fortalecer la Seguridad de Datos en las Transacciones de Ventas en Lugar Expresivo SAC

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

AUTOR (ES):

Garro Murillo, George Anthonny Vicente (orcid.org/0000-0001-7461-8557)

Navarro Torres, Luis Reynaldo (orcid.org/0000-0003-4513-577X)

ASESOR:

Ing. Flores Chacón, Erick Giovanny (orcid.org/0000-0002-4028-8059)

LÍNEA DE INVESTIGACIÓN:

Sistema de Información y Comunicaciones

LÍNEA DE ACCIÓN DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo Económico, Empleo y Emprendimiento

LIMA – PERÚ

2022

Dedicatoria de George

Les dedico este trabajo a todas las personas que aplazaron estudios por cualquier motivo, pero que no solo hicieron pasar el tiempo, sino que se mantuvieron vigentes pues actualmente la conexión a Internet ha ayudado a compartir conocimiento. Y por supuesto, también a mis amigos que vienen porque afirman que no los contratan porque no tienen título 😎.

Dedicatoria de Luis

El presente trabajo está dedicado a mi madre Yolanda y a mi padre Luis, que por su insistencia, apoyo, y buenos consejos estoy logrando un objetivo más en mi vida.

Agradecimiento

Agradezco a todos los que colaboraron con la idea, personalmente a Walter Felipe por acercar el asunto de encriptación homomórfica y a Luis Navarro por tener un tema enfocado en la seguridad de datos que con este estudio lo hemos actualizado. (George Garro Murillo).

Agradezco a Dios por brindarnos sabiduría. A la Universidad César Vallejo, a los docentes, en especial a nuestro asesor Ms. Erick Giovanny Flores Chacón por compartirnos su experiencia y conocimientos en la realización de esta investigación. (Luis Navarro Torres).

Índice de contenido

Índice de tablas

Índice de figuras

Índice de anexos

Resumen

Esta investigación fue motivada por la poca seguridad aplicada al almacenamiento de datos privados de una empresa. Por ende, estuvo enfocada en el reforzamiento de la seguridad de datos dentro de la empresa Lugar Expresivo SAC, además de generar una estructura de almacenamiento para mitigar la infiltración de terceros a esos datos privados.

El motivo de esta investigación es demostrar cuánto contribuye la implementación de un sistema de encriptación homomórfica en las dimensiones de disponibilidad, integridad y confidencialidad en las transacciones de ventas de Lugar Expresivo SAC.

Esta investigación tiene un enfoque cuantitativo de tipo aplicada que se encargó de medir por medio de una intervención si el objetivo de estudio consigue el éxito. El diseño del trabajo fue de tipo pre experimental, el cual evaluó el mismo grupo de estudio en dos tiempos distintos (pre y post), dentro de una muestra que abarca la misma cantidad que la población y que fue definida por las transacciones de ventas aplicando una fórmula cuantitativa infinita.

Como resultado se obtuvo una mejora del 100%, cada hipótesis específica obtuvo un nivel de significancia menor que el 5% y el silogismo dio como resultado la aceptación de la hipótesis general presentada en este estudio.

Palabras clave: Encriptación Homomórfica, Seguridad de Datos, Privacidad, Criptografía.

Abstract

This research was motivated by the poor security applied to the storage of private data of a company. Therefore, it was focused on strengthening data security within the company Lugar Expresivo SAC, in addition to generating a storage structure to mitigate the infiltration of third parties to these private data.

The purpose of this research is to demonstrate how much the implementation of a homomorphic encryption system supports the dimensions of availability, integrity and confidentiality in the Lugar Expresivo SAC's sales transactions.

This research has a quantitative approach of applied type that was in charge of measuring by means of an intervention if the study objective achieves success. The design of the work was pre-experimental type, which evaluated the same study group in two different times (pre and post), within a sample that covers the same amount as the population and that was defined by the sales transactions applying an infinite quantitative formula.

As a result, a 100% improvement was obtained, each specific hypothesis obtained a significance level of less than 5% and the syllogism resulted in the acceptance of the general hypothesis presented in this study.

Keywords: Homomorphic Encryption, Data Security, Privacy, Cryptography.

I. INTRODUCCIÓN

En este primer capítulo se desarrollaron temas relacionados a la realidad problemática que evidencia la falta de seguridad en los datos en las organizaciones u otras entidades privadas. Asimismo, se realizó una justificación de forma teórica, metodológica y tecnológica sobre la investigación realizada. Por consiguiente, se planteó como problema general ver cuál fue el efecto que tuvo la implementación de un sistema para fortalecer la seguridad de datos y por último se plantean problemas específicos sobre los requerimientos que se deben cumplir para que la información sea considerada de calidad.

Según IPE (2021), indicó que: el presidente de la Confiep en 2017, Roque Benavides, la economía del Perú es movida por las pequeñas y medianas empresas. PQS indicó que en el 2018 el 96,5% de las empresas que existen, y sin contar que el Instituto Peruano de Economía menciona que el 76,8% es informal, logrando alcanzar una tasa elevada en los últimos 11 años. Esto habría significado un ingreso de casi 700 mil trabajadores informales con respecto al nivel pre pandemia. Todo esto está reafirmado por ComexPerú y que además afirma en su reporte de mypes en 2020 que la cantidad total de pymes se redujo en 48,8% comparado con el 2019 por la crisis causada por la covid-19, por lo que se afirma que los ingresos obtenidos son sólo para sobrevivir y que ser formal no es sinónimo de prosperidad, sino de estar realizando actividades dentro del reglamento, por lo que se deduce que estas pymes no desean invertir en más cosas que no estén relacionadas a su mercadería o productos.

Siguiendo ese camino, trabajar de manera formal también conlleva a más responsabilidades siendo la tributaria una de ellas y de esta forma estas empresas reciben el apelativo de contribuyente por estar inscritos en el Registro Único de Contribuyentes, RUC. Sunat (2018). Una de las mayores responsabilidades y más notorias en ese ámbito es la emisión de comprobantes de pagos electrónicos. Esta normativa de emisión de comprobantes, por ser obligatoria, exige a los contribuyentes la generación de comprobantes de pago electrónicos usando procesos computarizados durante la transacción.

En una reciente encuesta presentada por el Instituto Peruano de Economía los servicios tercerizados por empresas se observan que la mayor cantidad de servicios presentados por terceros son realizados por medio de computación e informática, de esta manera el servicio que las empresas formales adquieren a

terceros son más económicos y listos para usar. Entonces, a menos que el contribuyente desarrolle con o sin ayuda su propia solución para emitir comprobantes de pago electrónicos, deberá usar el emisor de comprobantes que tiene Sunat en su sitio web. Es menester mencionar que también hay empresas que actúan como intermediarios entre el contribuyente y Sunat conformados por proveedores de servicios electrónicos y operadores de servicios electrónicos. Sunat (2022). Sin embargo, de estas formas se evidencian inconvenientes y no solo los subjetivos como que la interfaz gráfica que usa sunat es muy vetusta y enemigadera entre diseñadores gráficos y programadores porque en los informes que la superintendencia presenta solo se observan análisis de procesamiento en servidores. Sunat (2019). Estos inconvenientes que están relacionados a la privacidad de los datos como el monto total de venta o quién es el adquirente que en la empresa intermediaria se puede filtrar y/o a la constante conexión a Internet para alcanzar al servidor que generará el comprobante de pago. Por supuesto que se necesita conexión a Internet, pero la prioridad de esa conexión es alcanzar el servidor de Sunat para informar de la existencia de los comprobantes de pago electrónicos emitidos.

Según Dueñas y Moreno (2018) indican que: los activos más valiosos para los propietarios en las empresas son los datos ya que pueden tomar mejores decisiones con más rapidez; sin embargo, Contero (2019) dijo que: la mayor parte de las empresas están centradas en la protección de la seguridad física, dando menos importancia entornos que se encuentran relacionados con el manejo y gestión de la información. Las organizaciones pueden sacar ventajas frente a su competencia si manejan correctamente este activo para así también perdurar en el mercado. Por lo tanto, existe la importancia de mantener actualizada la información y poder acceder a ella de manera oportuna para que no exista la incertidumbre. De igual manera existen datos que son personales de cada individuo y almacenarlos en cualquier lugar de forma legible es peligroso ya que cualquier persona que los vea puede hacer uso de ellos y hay usos que ponen en situación vulnerable al propietario de esos datos. Por eso es muy necesario proteger las transacciones que involucran asuntos monetarios.

Lugar Expresivo SAC es una organización que brinda servicios de publicidad para empresas, así como para personas naturales, dentro o fuera de Lima y estos

servicios terminan con la entrega de un producto publicitario como gigantografías, volantes, banners y otros productos similares dependiendo del requerimiento del cliente. Para sus efectos de emisión de comprobantes de pago utilizan una sola computadora que almacena todos los datos en una base de datos local por lo tanto dependen de esa computadora para generar los comprobantes de pago electrónicos y entregarlos al cliente. Asimismo, Lugar Expresivo SAC no contrata servicios de terceros para almacenar y procesar sus datos porque la administración de la empresa afirma creer que la filtración de sus datos de movimientos de dinero lo pondría en desventaja frente a la competencia. Por esos motivos se implementará un sistema con encriptación homomórfica para datos numéricos como base de un programa generador de comprobantes de pago electrónicos que permita además sumar los datos numéricos, que son los montos de las operaciones, por períodos pues estas son operaciones aritméticas básicas que se requieren para la declaración de impuestos pues si la suma se realiza en una base de datos, que alberga los datos de las transacciones en las ventas de la empresa que están sustentados por los comprobantes de pago electrónicos, en un servidor alojado fuera de los dominios de la empresa que debe ser accedido a través de Internet no se requiere previamente descifrar los datos numéricos. Estos comprobantes de pagos serán generados en un equipo local de propiedad y dentro de la empresa para que no haya ningún riesgo de que algún agente externo pueda observar los datos que están siendo usados por lo que el cifrado y descifrado de información solamente puede ser hecho en el equipo local que posee las claves respectivas.

Con todo lo anterior expuesto se presenta esta problemática general: ¿Cómo la seguridad de los datos en las transacciones de ventas mejora con el sistema de encriptación homomórfica en Lugar Expresivo SAC?, en consecuencia llevará a los siguientes problemas específicos: (a) ¿El sistema de encriptación homomórfica mejora la disponibilidad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC?, (b) ¿El sistema de encriptación homomórfica mejora la integridad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC?, y por último (c) ¿El sistema de encriptación homomórfica mejora la confidencialidad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC?

A continuación, se presentan las justificaciones teórica, metodológica y tecnológica. **La Justificación Teórica**, según Arias y Covinos (2021) indican que puede ser usada cuando el investigador quiera mejorar el conocimiento del problema que se encuentra estudiando. Es decir, esto se enfocó en la investigación de los sistemas de encriptación homomórfica, sus herramientas y sus principales aspectos de privacidad en la seguridad de datos frente a otros tipos de encriptación, además de la implementación de un sistema de encriptación homomórfica que fortalecerá la seguridad de datos de transacción al momento de efectuar una venta. **La Justificación Metodológica**, según Álvarez (2021) indicó que es importante describir y resaltar la importancia de utilizar la metodología planteada. En síntesis, se aplicarán los conocimientos necesarios para desarrollar el sistema de encriptación homomórfica con el fin de solucionar un problema específico relacionado a la seguridad de datos en las transacciones de ventas. **La Justificación Tecnológica,** según Rojas (2019) indicó que los resultados de la investigación sirven para producir activos en diversos campos como el económico, científico o industrial pues se dejan diseños, técnicas o herramientas que harán más fácil los trabajos. Es decir que la implementación de un sistema de encriptación homomórfica permitirá a entidades, que manejan información financiera, reducir riesgos al momento de generar transacciones de ventas por medio de comprobantes de pago electrónicos.

Las argumentaciones anteriores llevan a plantear un objetivo general que se desea alcanzar para esta investigación: Fortalecer la seguridad de los datos en las transacciones de ventas mediante el sistema de encriptación homomórfica en Lugar Expresivo SAC, además entre los objetivos específicos se plantea: (a) El sistema de encriptación homomórfica mejora **la disponibilidad** de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC, (b) El sistema de encriptación homomórfica mejora **la integridad** de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC, y (c) El sistema de encriptación homomórfica mejora **la confidencialidad** de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC.

Para la investigación se planteó la siguiente hipótesis general: El fortalecimiento de la seguridad de datos en las transacciones de ventas mejora con el sistema de encriptación homomórfica en Lugar Expresivo SAC, y por ende se

muestran las hipótesis específicas: (a) el sistema de encriptación homomórfica mejorará la disponibilidad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC, (b) el sistema de encriptación homomórfica mejorará la integridad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC, y por último (c) el sistema de encriptación homomórfica mejorará la confiabilidad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC.

II. MARCO TEÓRICO

En este capítulo se mostraron los estudios relacionados con el trabajo de investigación, se encontraron diversos estudios a nivel nacional e internacional entre artículos, tesis y libros diversos donde se priorizaron la problemática, desarrollo y resultados dentro de las revisiones efectuadas. Se explicaron teorías que se encuentran relacionadas al tema donde se detallan conceptos sobre la seguridad de datos, metodologías, herramientas e instrumentos que fueron utilizados para la investigación. Para obtener toda la información utilizada en esta investigación se realizó una extensa búsqueda en diferentes páginas, repositorios, artículos, base de datos y otros.

Se detallaron diversos antecedentes relacionados al tema, como la norma ISO 27001 (Narváez y Yungán 2022, Rojas 2019), ISO 27002:2013 (Cubillos 2020, Ortiz 2018, Contero 2019), Encriptación asimétrica (Fernández 2021, Nunes 2019), computación en la nube (Benítez, Granda y Jaramillo 2019) Cifrado homomórfico (, Plasencia 2018, García, van de Graaf y Montejano 2018, Garibaldi 2018, Araújo 2018), Encriptación Paillier (Schroeder 2018, Rugel 2019, Reis, Lara y Borges 2020). Asimismo, se detallaron los algoritmos que se utilizaron en esta investigación.

Narváez y Yungán (2022) en su investigación aplicaron la norma ISO 27001 para proteger la seguridad dentro de los sistemas de información, donde su objetivo estaba centrado en proteger a cualquier organización o institución de las pérdidas de datos o robos de los mismos, con el fin de asegurar la supervivencia de estas organizaciones. Narváez y Yungán (2022) como resultado obtuvieron que el uso de un sistema de gestión de seguridad de información (SGSI) dentro de una empresa puede mejorar continuamente el nivel de seguridad, disminuyendo los riesgos dentro de la misma; además Narváez y Yungán (2022) indicaron que su implementación puede ser manejado de forma segura y con total confidencialidad ante terceros.

Asimismo, Fernández (2021) en su estudio donde diseñaron mecanismos de protección de datos almacenados utilizando criptografía asimétrica PGP (pretty good privacy o privacidad bastante buena), aplicado en la seguridad informática dentro de la empresa Scharff Logistica Integrada SA. Fernández (2021) obtuvieron como resultado que el sistema basado en RSA (un sistema de encriptación de clave pública) cumplió con mejorar la seguridad y que a su vez se puede comprobar su

fiabilidad, por otro lado el sistema le brinda al jefe y dueños a decidir qué miembros pueden tener acceso a la información compartida y a quienes puede enviar la información cifrada de forma segura. De igual forma, Fernández (2021) recomendó la evaluación en la viabilidad del proyecto en caso se aplique a otros tipos de empresas, ampliando su alcance para la protección de la información de extremo a extremo para conseguir el éxito del proyecto en otras instituciones involucradas.

Asimismo, Cubillos (2020) en su estudio de protección de datos compartidos en entornos de nube, informó que la mayoría de emprendimientos y pymes utilizan tecnología de computación, que a su vez realizan almacenamiento en la nube para sus procesos de negocio; sin embargo, muchas de estas no toman en cuenta los protocolos de seguridad que garanticen la confidencialidad e integridad de la protección de su información. Cubillos (2020) propuso diseñar e implementar un prototipo que permita almacenar archivos en la nube y que se puedan compartir entre los usuarios autorizados, con el fin de garantizar la confidencialidad, integridad y la protección de los mismos. Cubillos (2020) concluyó que la implementación de un prototipo que combine el manejo de etiquetas dentro de confidencialidad e integridad, además de gestionar el acceso basado en roles permite generar un gobierno de datos que opera con las políticas de seguridad, y que a su vez fueron valoradas de forma positiva las pruebas realizadas con algoritmos de cifrado, los cuales permitieron identificar cuáles serían los más adecuados dependiendo del tipo de información.

Por otro lado, Reis, Lara y Borges (2020), en su estudio de Computação da Quadratura Gaussiana em um Esquema Criptográfico Parcialmente Homomórfico, evaluó la aplicabilidad de un sistema criptográfico parcialmente homomórfico de Paillier en el cálculo de aproximaciones de integrales definidas mediante la cuadratura Gaussiana (Gauss). Como resultado Reis *et al* (2020) obtuvieron que el tiempo de procesamiento aumenta con el nivel de precisión utilizado, elevándose a un valor en tiempo medio de 3234 utilizando una precisión de nueve cifras decimales. Reis *et al* (2020) concluyeron que utilizar criptografía homomórfica ralentizará el tiempo de procesamiento de archivos planos, que a su vez genera una ganancia en seguridad y privacidad que aporta el uso de la criptografía homomórfica.

Nunes (2019) tuvo como objetivo desarrollar un esquema criptográfico que pueda garantizar la confidencialidad, integridad, autenticidad, verificabilidad y el anonimato del voto en una elección electrónica. Nunes (2019) como resultado obtuvo que la aplicación del esquema propuesto de criptografía en las elecciones electrónicas garantiza el anonimato en la integridad, confidencialidad, autenticidad y verificabilidad de cada votante.

Contero (2019) desarrolló un análisis de la norma ISO/IEC 27002:2013, sustentándose en lo expuesto por el Esquema Gubernamental de Seguridad de la Información (EGSI). Contero (2019) concluyó que fue posible diseñar una política de seguridad para el sistema de botones, que a su vez fue aplicada a los procesos del manejo de servicios en la plataforma tecnológica y entornos administrativos del sistema de seguridad integral. Contero (2019) recomendó utilizar la metodología para proyectos, planes y procesos que requieran una estructura sistemática y organizada para la gestión de riesgos.

En un artículo de Benítez, Granda y Jaramillo (2019) centrado en análisis de información que brinda la literatura científica sobre el uso de computación en la nube (cloud computing) para fines educativos. En dicho trabajo Benítez et al (2019) utilizaron métodos de observación científica, revisiones bibliográficas, análisis de contenido, histórico - lógico y analítico - sintético. Benítez et al (2019) concluyeron que la computación en la nube permite el acceso a aplicaciones, servicios de almacenamiento y archivos con solo acceder a internet de forma privada y pública, comunitarias e híbridas.

Según Rojas (2019) en su investigación propone demostrar cuánto contribuye la implantación de la NTP ISO/IEC 27001:2014 en la base de datos del Reniec los cuales permiten una mejor gestión de los campos de disponibilidad, integridad y confidencialidad. Como resultado, Rojas (2019) detalló que la implementación de la ISO/IEC 27001 optimizó de manera significativa los indicadores de seguridad de datos cumpliendo con la implementación de nuevos controles de gestión relacionados con la seguridad de datos. Asimismo, Rojas (2019) recomendó a las investigaciones futuras profundizar con los temas de infraestructura, seguridad perimetral y desarrollo de un software que tengan incluidos la seguridad de datos e información.

Según Rugel (2019) en su proyecto analizó la seguridad dentro de los archivos utilizando herramientas de desarrollo actuales y acordes al tema. Como resultado del estudió Rugel (2019) comprobó que el cifrado homomórfico posee una estructura sólida y robusta, lo cual mantiene los datos encriptados de manera confiable.

Asimismo, Ortiz (2018) en su estudio realizó un análisis y gestión de riesgos de acuerdo con la metodología de Análisis y Gestión de Riesgos (MAGERIT) y se realizaron pruebas de intrusión en los sistemas informáticos y el uso de la Norma NTP-ISO/IEC 27005 para identificar las vulnerabilidades y riesgos asociados a la información. Como resultado, Ortiz (2018) confirmó con un 95% del nivel de confianza que la implementación de controles de seguridad de la norma ISO/IEC 27002:2013 permite mejorar la gestión de seguridad de la información en la Universidad Nacional Agraria de la Selva. Ortiz (2018) recomienda monitorear constantemente e ir implementando nuevos controles de ser necesarios para mitigar aún más los riesgos identificados.

Plasencia (2018) en su investigación expresa que analizó la implementación de un sistema de votación electrónico que cumpla con tres características esenciales de multi autoridad, auditoría abierta y descentralizado en la red implementando tecnologías criptográficas como cifrado umbral y cifrado homomórfico y tecnología blockchain. Plasencia (2018) concluyó que el sistema puede ser adaptado y usado dentro de múltiples contextos luego de realizar unos pocos cambios. Plasencia (2018) recomendó adentrarse en la investigación de aplicaciones blockchain ya que podrían ser de uso más extendido.

Según García, van de Graaf y Montejano (2018) en su investigación presentaron una técnica para la optimización en el almacenamiento de sufragios con esquemas basados en el protocolo Non Interactive Dining Cryptographers (NIDC). Como resultado a su investigación, García et al (2018) recomendaron implementar un nuevo esquema de voto electrónico encargado de observar el comportamiento de un modelo teórico con el fin de detectar errores y proponer nuevas mejoras.

Según Garibaldi (2018) en su investigación tuvo como fin el estudiar el funcionamiento del homomorfismo en algoritmos de clave pública más utilizados y populares en el área de seguridad y criptoanálisis además de implementar un

programa con funcionalidad homomórfica para validar el estudio teórico. Garibaldi (2018) concluyó que el cifrado y descifrado de datos presentan una complejidad en ciertas aplicaciones, pero no se ven afectadas significativamente; también Garibaldi (2018) afirma que la ejecución del sistema puede llevarse a cabo sin exponer datos y garantizando su confidencialidad. Por último, Garibaldi (2018) recomendó para trabajos futuros basarse en su prototipo presentado en su investigación y crear un sistema más robusto con preocupaciones de seguridad o incluso explorar otros tipos de aplicaciones que utilizan encriptación.

Según Araújo (2018) en su proyecto desarrolló un esquema de voto electrónico utilizando encriptación homomórfica con ElGamal y esquemas que cumplan con la seguridad propuesta por la comunidad científica. Araújo (2018) concluyó que utilizar cifrado homomórfico y otros esquemas de compromiso para la construcción de un sistema de votación electrónica cumple con los requisitos del modelo que se propuso en la comunidad científica, además, Araújo (2018) demostró que la encriptación homomórfica con ElGamal llegó a resolver eficientemente el problema de la confianza al momento de brindar los resultados electorales por parte de autoridades.

Finalmente, Schroeder (2018) en su investigación Implementação de um sistema de eleição remoto secreto e verificável, estudió una solución remota para la seguridad y privacidad basados en el sistema ADDER y Paillier. Schroeder (2018) analizó e investigó las principales soluciones propuestas por medio de literaturas revisadas para el proyecto, con el fin de encontrar oportunidades de mejora. Schroeder (2018) concluyó que, la implementación que propuso necesita una verificación formal en sus aspectos de seguridad antes de utilizarlo en una elección a gran escala.

La presente investigación tomó como referencia las siguientes teorías: Seguridad de Datos, según Morales, Neyra y Vidal (2021) lo definieron como la protección por medio de procesos y herramientas asociadas a los activos de información confidencial que se encuentren ya sea en tránsito o en reposo; Narváez y Yungán (2022) indicaron que para tener confidencialidad, disponibilidad e integridad para enfrentar amenazas se requiere de un sistema que tenga controles de seguridad y esté documentado. Políticas de Seguridad, Contero (2019) dice que las organizaciones requieren cubrir la seguridad de los sistemas informáticos y para

lograrlo se necesitan objetivos que proporcionen roles que permitan delimitar y definir responsabilidades. Teoría de Criptografía, Garibaldi (2018), indicó que son un conjunto de técnicas que garantizan una comunicación con más seguridad y con mejor privacidad; en otras palabras, la criptografía se restringe al sentido literal de ocultar mensajes. Encriptación Asimétrica, según Cordova, Vega, Rodríguez y Escobedo (2020), explican que tiene una seguridad diferente a la encriptación simétrica; mientras que los dos se encargan de proteger los datos a accesos no autorizados, la encriptación asimétrica puede utilizar dos llaves de seguridad (una pública y una privada), mientras que la simétrica solo utiliza una. En otras palabras, la encriptación asimétrica genera dos llaves de cifrado al mismo tiempo, la cual una se encargará de encriptar y la otra de desencriptar. Encriptación Homomórfica, Rugel (2019) indicó que un texto que se encuentre cifrado homomórficamente tiene las propiedades de realizar operaciones directamente sin necesidad alguna de descifrarlos. Además, Rugel (2019) describe un esquema de cifrado homomórfico con los siguientes elementos:

- $Enc\ ()$ denota ser un esquema de cifrado probabilístico ($\oplus$, $\otimes$).
- $Dec\ ()$ denota el esquema de descifrado.
- M es el espacio mensaje (datos en claro) y tiene estructura de grupo bajo la operación.
- C es el resultado de la operación $\oplus$ y sus definiciones.

Donde:

$$c_1 = Enc_{k1}\ (m1)$$
$$c_2 = Enc_{k2}\ (m2)$$

Existe una clave k tal que:

$$c_1 \otimes c_2 = Enc_k\ (m1 \oplus m2)$$

Por consiguiente, el descifrado dentro de un procedimiento $\otimes$ en los valores cifrados son el resultado de adaptar la función $\oplus$ en los valores no cifrados.

Criptografía Paillier, según Morgado (2021) el algoritmo de Paillier es un sistema criptográfico parcialmente homomórfico pues solo realiza operaciones de

suma y multiplicación; es decir, las propiedades que posee son la adición de contenido cifrado con otro contenido cifrado, adición de contenido cifrado con otro contenido sin cifrar, y multiplicar contenido cifrado con otro contenido sin cifrar.

Clark (2020) presentó los pasos para generar una clave de cifrado según Paillier:

1. Elegir dos números primos grandes p y q de manera aleatoria e independiente. Confirmar que $gcd\,(pq, (p-1)\,(q-1))$ es 1, (donde $gcd(x, y)$ genera el máximo común divisor de x e y). En caso no sea el resultado entonces comenzar de nuevo.
2. Calcular $n = pq$.
3. Definir la función $L(x) = \frac{x-1}{n}$.
4. Calcular como $lcm\,(p-1, q-1)$ (donde $lcm(x, y)$, genera el mínimo común múltiplo de x e y).
5. Elegir un entero aleatorio g en el conjunto Z_{n2}^{*} (enteros entre 1 y n^2).
6. Calcular el inverso multiplicativo $\mu = (L\,(g^{\lambda}\, mod\, n^2))^{-1}$ mod n. Si μ no existe, comenzar otra vez desde el paso 1.
7. La clave pública es (n, g). Usar esto para cifrar.
8. La clave privada es λ. Usar esto para descifrar.

Certificado Digital, según Gallardo (2018) indicó que es un documento que se firma de forma digital que a su vez contiene la clave pública y la clave privada del poseedor. JavaScript de acuerdo a Villacres (2021) definió que es un lenguaje de programación que permite el diseño de contenido dinámico, imágenes animadas y otras acciones dentro de plantillas web. Es decir, Javascript es útil para darle interactividad a los datos y visualización en el navegador web sin la necesidad de que otro complemento o el mismo servidor deba procesar todo previamente. De esta manera se puede escribir cualquier programa y al ejecutar el procesamiento en el navegador web según se requiera. Mysql del mismo modo Villacres (2021), explicó que es un sistema gestor de base de datos relacional el cual permite relacionar tablas de forma organizada. Por tal sentido, Mysql permite administrar los datos realizando consultas de una manera estructurada a través del lenguaje SQL que son las iniciales de la definición anterior. Este motor de base de datos

proporciona la creación, lectura y modificación de los datos manteniendo la consistencia e integridad de los datos almacenados.

Para esta investigación fueron consideradas las siguientes definiciones para las variables y dimensiones respectivas. Variable Dependiente: Seguridad de datos en las transacciones de ventas; según Beynon (2018) definió que dispone de controles técnicos y administrativos que se encargan de proteger los datos ante todo tipo de amenazas. Sabogal (2021) indicó que la información es el activo más importante dentro de una empresa el cual es proveniente de los clientes y por ello la empresa tiene la obligación de asegurar su integridad y confidencialidad de estos mismos datos. Narváez y Yungán (2022) lo definió como un sistema de gestión documentado que contiene controles para la seguridad, los se encargan de resguardar la disponibilidad, integridad y confidencialidad de los activos frente vulneraciones y amenazas externas. En otras palabras, se encuentra enfocado en la protección del área computacional y todo lo que se encuentre relacionado con ella. Además, es una disciplina que se encarga de diseñar normas, métodos, técnicas y procedimientos que tienen como fin el de conseguir un sistema de información con más seguridad y un mayor nivel en confidencialidad.

Para la variable dependiente se presentan los siguientes principios y/o requerimientos que se deben cumplir para que una información sea considerada de calidad. Disponibilidad, Según De la Rosa (2021), indica que cuando los usuarios autorizados requieren acceder a los datos estos siempre estar al alcance, en otros términos, se encarga de proporcionar el mejor funcionamiento en los objetivos, de tal manera que sea seguro frente a ataques e interferencias que puedan perjudicar su correcto funcionamiento. Teniendo en cuenta nuestra dimensión de Disponibilidad se considera el siguiente indicador: Métricas de disponibilidad de transacciones, que corresponde a la evaluación y promedio total de la cantidad total de transacciones y la cantidad total de transacciones fallidas. Integridad, según Costales (2021), explicó que la información que se recibe debe ser igual a la información que se envía, esto puede confirmar con exactitud que el contenido no fue alterado o dañado durante la transmisión; es decir, se encarga de seleccionar qué usuarios pueden tener acceso al sistema, así como decidir cuándo y de qué forma brindarles acceso de la misma. Para esta dimensión se considera el indicador: Métricas de integridad de las transacciones, que corresponde para la

evaluación y promedio total de la cantidad de transacciones satisfactorias y la cantidad de las transacciones no disponibles. y por último Confidencialidad, según Camposano (2020) se debe mantener en reserva y no revelar información a personas que no tienen autorización para ver los procesos, en otras palabras, es uno de los principales pilares dentro de la seguridad informática, el cual, tiene como capacidad inicial el asegurar la fiabilidad y brindar un acceso seguro a los datos y recursos que son necesarios para realizar sus actividades. Teniendo en cuenta esta dimensión se consideró la variable Métrica de confidencialidad de las transacciones, que corresponde para la evaluación y el promedio total de la cantidad de reportes y cantidad de reportes legibles.

III. METODOLOGÍA

En este capítulo se definen conceptos como el tipo de investigación que se realiza, el nivel de experimento, su diseño y definiciones de las variables de operacionalización tanto para la dependiente e independiente, además, se detalla la población y muestra en la cual se aplica el estímulo incluyendo el tipo de instrumento de recolección de datos validado por expertos, entre otros.

3.1. Tipo y diseño de investigación

3.1.1. Tipo de investigación

Arias y Covinos (2021) explican que la problemática debe estar alineada al enfoque cuantitativo debido a que se habla de variables de investigación y medición de resultados. Según la intervención del investigador será de tipo Experimental con una planificación en la toma de datos de tipo Retrospectivo, el cual los datos serán tomados al momento de realizar la prueba pre test.

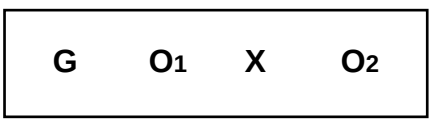
3.1.2. Nivel aplicativo

El nivel aplicativo cumple la finalidad de mejorar el entorno de investigación por medio de una intervención; además, sirve para el control de calidad que evalúa si el proyecto consigue el éxito o no. Para la variable de estudio será de tipo longitudinal, según Arias y Covinos (2021) indicaron que se estudia las características que obtiene una variable al momento de realizar un cambio en los procesos; para este caso no se manipula la variable, solo se observa el proceso en periodos.

3.1.3. Diseño de investigación

La investigación fue experimental del tipo preexperimental. Se analizó una sola variable. No se manipuló la variable independiente ni se usó un grupo control; no hubo la posibilidad de comparación de grupos. Arias y Covinos (2021) definió el diseño pre experimental con las siguientes características

Figura N° 1: Diseño pre experimental



Fuente: Arias y Covinos (2021)

G: Grupo de sujetos a evaluar.

X: Tratamiento, estímulo o condición experimental (Sistema de Encriptación homomórfica).

O_1: Medición del grupo **antes** de la implantación del estímulo (Seguridad de los datos).

O_2: Medición del grupo **después** de la implantación del estímulo (Seguridad de los datos).

3.2. Variables y operacionalización

Fue una variable cuantitativa con tipo de escala de razón, el cual se midió en forma de fracción cuantas unidades (según el tipo de indicador) son representadas del total. Según Arias y Covinos (2021) definieron que: el cero no se encuentra involucrado en la categoría en la que se mide. En otras palabras, el cero en los resultados dentro de esta escala sí indican la ausencia de este atributo, dando a entender que se define como un cero absoluto.

3.2.1. Variable independiente: sistema de encriptación homomórfica

a. Definición conceptual

El autor Rugel (2019) explicó que la encriptación homomórfica tiene las propiedades de realizar operaciones sobre texto directamente sin necesidad alguna de descifrarlos. Para García et. al (2018) lo definieron como una suma de operaciones matemáticas que se pueden realizar sobre las versiones cifradas dentro de la información.

b. Definición operacional

Sistema automatizado encargado de almacenar información de manera remota aplicando encriptación homomórfica, el cual tiene como finalidad la protección de toda información ingresada al momento de realizar una transacción de ventas por medio de un comprobante de pago electrónico.

3.2.2. Variable dependiente: seguridad de datos en las transacciones de ventas

a. Definición conceptual

El autor Beynon (2018), indicó que la seguridad de datos cuenta con controladores técnicos y administrativos que protegen datos ante todo tipo de amenazas. De igual forma, Narváez y Yungán (2022) definieron que son un conjunto de controles que protegen la disponibilidad, integridad y confidencialidad que actúan frente a amenazas y vulnerabilidades presentadas

b. Definición operacional

Contero (2019), definió que se deben adoptar medidas para proteger la información de un negocio para garantizar la integridad, disponibilidad y confidencialidad ya que esta información es un activo valioso. Entonces se establecen un conjunto de normas o políticas de seguridad que se encuentran desarrolladas para la protección de una base de datos, con el fin de proteger la información ante todo tipo de intrusos, posibles vulneraciones que puedan alterar los datos y fallas que puedan afectar la disponibilidad evitando el acceso a los servicios de información.

c. Indicadores

- **Métricas de disponibilidad de las transacciones (MDT)**, corresponde a la evaluación y promedio total de la cantidad total de transacciones (CTT) y la cantidad total de transacciones fallidas (CTT_F). (Rojas, 2019)

Figura N° 2: Métrica de disponibilidad de las transacciones

$$MDT = \frac{CTT - CTT\_F}{CTT} * 100$$

Fuente: Rojas (2019)

- **Métricas de integridad de las transacciones (MIT)**, que corresponde para la evaluación y promedio total de la cantidad de transacciones satisfactorias

(CTS) y la cantidad de las transacciones no disponibles (CTND). (Rojas, 2019)

Figura N° 3: Métrica de integridad de las transacciones

$$MIT = \frac{CTS - CTND}{CTS} * 100$$

Fuente: Rojas (2019)

- **Métrica de confidencialidad de las transacciones (MCT)**, que corresponde para la evaluación y el promedio total de la cantidad de reportes (CR) y cantidad de reportes legibles (CR_L). (Rojas, 2019)

Figura N° 4: Métrica de confidencialidad de las transacciones

$$MCT = \frac{CR - CR\_L}{CR} * 100$$

Fuente: Rojas (2019)

3.3. Población, muestra y muestreo

3.3.1. Población

Arias y Covinos (2021) definieron que las características similares de un conjunto de sujetos establecen la población.

Para esta investigación la población fue conformada por las transacciones de ventas que estaban siendo realizadas durante dos semanas dentro de Lugar Expresivo SAC, en estas se tomaron una semana para cada prueba respectiva (pre y post).

- **Criterios de inclusión:** Se recopilaron todas las transacciones de ventas que fueron procesadas con el sistema de facturación de la empresa durante el periodo establecido para la investigación.

- **Criterios de exclusión:** Las transacciones de ventas que se encuentran procesadas fuera de la fecha establecida (antes y después), no serán tomados dentro de la investigación.

3.3.2. Muestra

Asimismo, Arias y Covinos (2021) explicaron que: es un subgrupo que representa a una parte de la población o universo.

La muestra fue de la misma cantidad que la población, puesto que el total de las transacciones de ventas que fueron recolectados estuvieron dentro de un periodo de dos semanas, los cuales uno fue utilizado para la ejecución del pretest con un total de diecinueve (19) transacciones entre satisfactorias y fallidas al momento de ser efectuado (ver anexo), y el segundo para el postest luego de ser aplicado el estímulo que fue el sistema de encriptación homomórfica.

Figura N° 5: Fórmula cuantitativa infinita

$$n = \frac{z^2 s^2}{e^2}$$

Fuente: Arias y Covinos (2021)

3.3.3. Muestreo

Para el muestreo se utilizó un muestreo no probabilístico de tipo intencional. Hernández (2021) definió que los expertos validan los criterios para seleccionar los participantes.

3.3.4. Unidad observacional

Según Arias y Covinos (2021), indicaron que es el medio que se utiliza para la recopilación de información, donde en algunas ocasiones la unidad de análisis y la unidad de muestro vendrían a ser lo mismo. Para la unidad observacional se contemplaron todas las transacciones de ventas efectuadas en el sistema de encriptación homomórfica durante el periodo establecido.

3.4. Técnicas e instrumentos de recolección de datos

3.4.1. Técnicas

La técnica empleada para la recolección de datos fue la ficha de observación, que según Asqui, Charaja, Huanca, Huayanca, Mamani D. y Mamani H (2021)

definieron que consiste en describir y registrar de forma detallada hechos, personas o lugares que conformen el área de investigación. En otras palabras, la ficha de observación fue un instrumento de investigación que permitió la recolección y evaluación de los datos requeridos en un ambiente específico donde se determinaron las variables específicas.

La ficha de observación fue utilizada para averiguar las referencias relacionadas a las dimensiones para el manejo de información que se emplea dentro de la empresa Lugar Expresivo SAC con respecto a la seguridad en sus datos recolectados, los cuales fueron señalados y evaluados de acuerdo a los indicadores planteados dentro de esta investigación.

3.4.2. Instrumentos

El Instrumento respectivo que se utilizó para la investigación fue la ficha de observación (ver anexo) que consistió en reportes diarios de incidencias al momento de generar una transacción de venta en conjunción con el reporte de transacciones registradas en bases de datos. La unión de estos dos reportes generó los datos dicotómicos.

3.5. Procedimientos

3.5.1. Para su validación de los instrumentos

La validez de los instrumentos se realizó mediante un juicio de expertos donde se encargó de evaluar y corregir (en caso haya sido necesario) los ítems pertenecientes al instrumento (para la investigación será una ficha observación) para luego corroborar la validación y calificar si se encuentra aceptable para su aplicación.

3.5.2. Para su confiabilidad

Rojas (2019) indicó que un instrumento tiene diferentes procesos para que pueda tener un nivel de confiabilidad al momento de su medición, estos mismos usan técnicas y fórmulas que generan un coeficiente de fiabilidad.

Según Rojas (2019) indicó que en la validación de expertos para las dimensiones se obtuvieron como resultado las siguientes calificaciones:

Tabla N° 1: Validación de expertos

METRICA DE DISPONIBILIDAD								
	Puntuación por Item							Confiabilidad
Experto	1	2	3	4	5	6	7	
Dra. Romero Valencia, Monica	78.00%	78.00%	78.00%	78.00%	78.00%	78.00%	78.00%	78.00%
Mgtr. Galvez Tapia, Orleans Moisés	90.00%	90.00%	90.00%	90.00%	90.00%	90.00%	90.00%	90.00%
Mgtr. Huarote Zegarra, Raúl	95.00%	90.00%	85.00%	90.00%	95.00%	95.00%	90.00%	91.43%
							Grado de Confiabilidad	86.48%

Fuente: Rojas (2019)

Para el instrumento de confiabilidad por parte de tres (3) expertos consultados, Rojas (2019) interpreta el grado de confiabilidad con un promedio de 86.48% en la Métrica de Disponibilidad.

3.6. Método de análisis de datos

De acuerdo a Rojas (2019) se evaluará la consistencia de acuerdo a la correlación de los datos obtenidos. Para nuestro tipo de estudio se utilizó la estadística descriptiva el cual fue aplicada en un pretest y en un postest correspondiente a un diseño pre experimental.

Dentro del uso de prueba de normalidad se determinó que los datos utilizaron la prueba paramétrica de Shapiro-Wilk, donde el tamaño de la muestra fue establecido por un total de 5 días (una semana laboral). A partir de esto, luego de un análisis respectivo de los datos recolectados en “transacciones satisfactorias” y “transacciones fallidas” dentro de la ficha de observación, fueron distribuidos para cada indicador y se aplicaron las fórmulas respectivas las cuales fueron establecidas en esta investigación.

3.7. Aspectos éticos

Esta investigación persigue objetivos académicos, todo dato o información que fue proporcionado por la empresa Lugar Expresivo SAC fue tratado con discreción y tuvo una máxima confidencialidad.

Se mantuvo un respeto de los argumentos utilizados dentro de los documentos, libros virtuales, repositorios, tesis y artículos publicados que sirvieron como fuente de información y conocimiento para efectuar nuestra investigación por medio de citas textuales con sus respectivas referencias bibliográficas siguiendo el estándar de la ISO 690, y no buscamos adueñarnos de trabajos que no son de

nuestra autoría sino que damos los créditos a las personas que hicieron trabajos que estamos usando para sustentar el nuestro. De esta manera esperamos cumplir con las normativas académicas de colegios, institutos u otros organismos profesionales que velan por la ética, la conducta profesional y la calidad de la información que pueden repercutir en la humanidad. Y como una manera más de demostrar lo que indicamos, esta investigación puede estar disponible para que sea revisada por cualquier persona que requiera contrastar asuntos de cualquier índole no necesariamente partiendo desde la óptica de la ingeniería.

IV. RESULTADOS

Para el presente capítulo se describieron de forma detallada los resultados que se obtuvieron dentro de la investigación con base en la recolección de datos usando la ficha de observación y base de datos durante el periodo establecido para el pretest y postest. Estos datos fueron recolectados dentro de 2 variables: transacciones satisfactorias y transacciones fallidas. Estos resultados, por medio de un análisis previo, dieron origen a los datos necesarios para la aplicación de las fórmulas de las "métricas de disponibilidad de las transacciones", "métricas de integridad de las transacciones" y "métricas de confidencialidad de las transacciones", para lo cual se utilizó el programa IBM SPSS Statistics 26.

4.1. Prueba de hipótesis específica 1: disponibilidad

HE1$_0$: El sistema de encriptación homomórfica **no mejorará** la disponibilidad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC.
HE1$_a$: El sistema de encriptación homomórfica **mejorará** la disponibilidad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC.

Para este indicador de métrica de disponibilidad de las transacciones se realizó el análisis de un grupo de transacciones obtenidos dentro del sistema de encriptación homomórfica en un plazo de una semana, y la ficha de observación planteado para la investigación fue valorada en dos rangos: transacciones satisfactorias (0) y transacciones fallidas (1) (ver anexo), los cuales, luego de un análisis previo se definieron las siguientes variables para el indicador de disponibilidad: Cantidad total de las transacciones (0) y Cantidad total de las transacciones fallidas (1). Para el análisis de disponibilidad se ejecutó la fórmula planteada en esta investigación por cada día de muestra, donde:
MDT = Métrica de Disponibilidad de las Transacciones
CTT = Cantidad Total de las Transacciones
CTT_F = Cantidad Total de las Transacciones Fallidas

Figura N° 6: Fórmula de métricas de disponibilidad de las transacciones

$$MDT = \frac{(CTT - CTT\_F)}{CTT} * 100$$

Fuente: Rojas (2019)

De tal forma que los resultados para el indicador de disponibilidad generaron un nuevo resultado equivalente a las variables iniciales para la observación del pretest y postest.

Tabla N° 2: Datos de disponibilidad pre y post respectivos

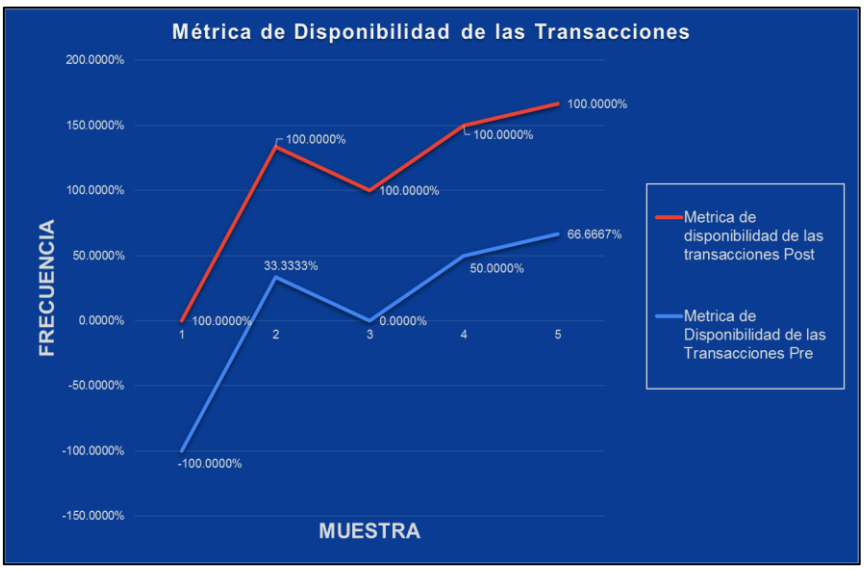
Datos pre test			
Muestras para Disponibilidad			
Días	Transacciones Satisfactorias	Transacciones Fallidas	Metrica de Disponibilidad de las Transacciones Pre
1	1	2	-100.0000%
2	3	2	33.3333%
3	2	2	0.0000%
4	2	1	50.0000%
5	3	1	66.6667%
Total	11	8	

Datos pos test			
Muestras para Disponibilidad			
Días	Cantidad total de transacciones satisfactorias	Cantidad total de transacciones fallidas	Metrica de disponibilidad de las transacciones Post
1	0	0	100.0000%
2	5	0	100.0000%
3	1	0	100.0000%
4	1	0	100.0000%
5	3	0	100.0000%
Total	10	0	

Fuente: Elaboración propia

Según Espinoza (2021) definió que: en estadística se acostumbra dar resultados con un número de dos cifras decimales y significativas, pero en ciertas circunstancias es común representarlas con tres o más cifras significativas. Se presenta el siguiente gráfico del incremento en la métrica de disponibilidad de las transacciones:

Figura N° 7: Gráfico de comparación pre y post de disponibilidad



Fuente: Elaboración propia

A continuación, se detallan los cuadros estadísticos según la ficha de observación pre y post donde se consiguió medir el nivel de disponibilidad al finalizar el uso del sistema de encriptación homomórfica.

4.1.1. Indicador del nivel de disponibilidad

En la tabla N° 3 se muestran los promedios (media) de las pruebas que se realizaron en el pre y post dentro de la métrica de disponibilidad de las transacciones donde las variables transacciones satisfactorias y transacciones fallidas fueron implementadas en el estudio para el indicador.

Tabla N° 3: Indicador de mejora de disponibilidad de las transacciones

	N		Media	Mediana	Moda	Desv. Estandar
	Válido	Perdidos				
Metricas de Disponibilidad de las Transacciones Antes	5	0	0,1000	0,3333	-1,0000	0,6625
Metricas de Disponibilidad de las Transacciones Despues	5	0	1,0000	1,0000	1,0000	0,0000

Fuente: Elaboración propia

En la tabla N° 3 se visualiza la mejora en la seguridad de datos en las transacciones a nivel de disponibilidad adquirida de la recopilación de transacciones por medio de la ficha de observación, donde se identificó que en el pretest (antes de implementar el estímulo) se obtuvo una media de 0.1000 (10.00%) en la métrica de disponibilidad de las transacciones; por otro lado, en la ficha de observación postest (después de implementar el estímulo) se obtuvo una media de 1.0000 (100.00%) en la métrica de disponibilidad de las transacciones, demostrando una mejora de 0.9000 (90.00%).

4.1.2. Prueba de Normalidad

Según C. E. Flores y K. L. Flores (2021) citando a Novales (2010) indicaron que esta prueba se utiliza para verificar la normalidad cuando el tamaño de la muestra es menor a 50, mientras que a las muestras más grandes le corresponden a la prueba de Kolmogórov-Smirnov.

En la prueba de normalidad se aplicó la prueba de Shapiro-Wilk, ya que la muestra para el indicador estuvo compuesta por un total de una semana laboral, recolectando un total de 19 transacciones en el pretest y 10 transacciones en el postest, y cuando la cantidad de la muestra es menor a 50 se usa este método. A continuación, se detallan los resultados de las pruebas pre y post de esta

investigación. Para este indicador de disponibilidad fueron analizados bajo un nivel de confiabilidad del 5%, esto indica que si el valor de significancia (***Sig.***) en los datos postest es:

- **Sig. >= 0.05 (5.00%)**, la muestra se ajusta a una distribución normal.
- **Sig. < 0.05 (5.00%)**, la muestra no se ajusta a una distribución normal.

Tabla N° 4: Comparación de significancia pre y post de disponibilidad

	Kolmogorov-Smirnov			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Metrica de Disponibilidad de las Transacciones Antes	0,240	5	0,200	0,860	5	0,227
Metrica de Disponibilidad de las Transacciones Despues	0,000	5	0,000	0,000	5	0,000

Fuente: Elaboración propia

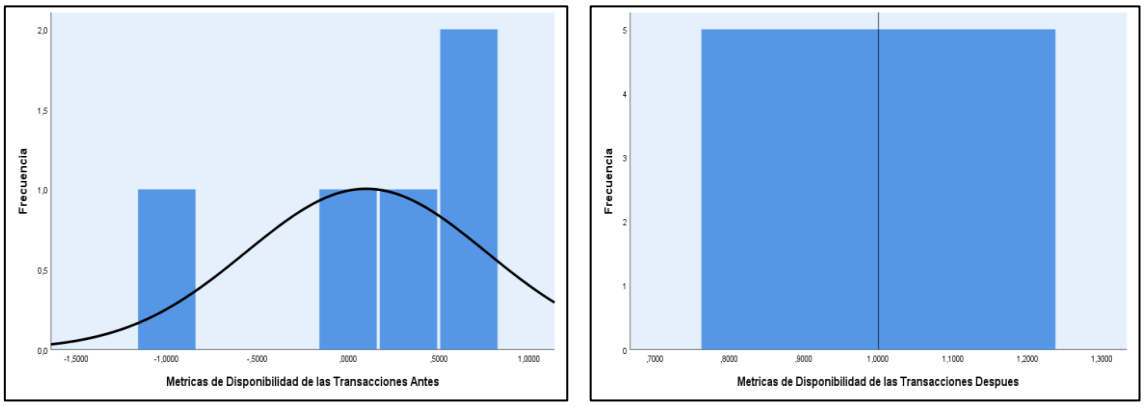
b. Disponibilidad pretest

Los resultados obtenidos en la prueba de normalidad (ver tabla N° 4) a partir de los datos en la disponibilidad pretest, se obtuvo que el nivel de significancia (*Sig.*) en la métrica de disponibilidad de las transacciones fue de 0.227 (22.70%), siendo mayor a 0.05 (5.00%).

c. Disponibilidad postest

Los resultados obtenidos en la prueba de normalidad (ver tabla N° 4) a partir de los datos en la disponibilidad postest, se obtuvo que el nivel de significancia (*Sig.*) en la métrica de disponibilidad de las transacciones fue de 0.000 (0.00%), siendo menor a 0.05 (5.00%).

Figura N° 8: Diagramas de normalidad de datos disponibilidad



Fuente: Elaboración propia

Los histogramas para la métrica de disponibilidad de las transacciones (ver Figura N° 8) indican que la muestra no se ajusta a una distribución normal.

d. Prueba de rangos con signos de Wilcoxon

En la tabla N° 5 se muestra la prueba con signos de Wilcoxon de forma más detallada.

Tabla N° 5: Rangos con signos de Wilcoxon de disponibilidad

		N	Rango promedio	Suma de rangos
Metrica de Disponibilidad de las Transacciones Despues - Metrica de Disponibilidad de las Transacciones Antes	Rangos negativos	0[a]	0,00	0,00
	Rangos positivos	5[b]	3,00	15,00
	Empates	0[c]		
	Total	5		

Fuente: Elaboración propia

- Métrica de Disponibilidad de las Transacciones Después < Métrica de Disponibilidad de las Transacciones Antes
- Métrica de Disponibilidad de las Transacciones Después > Métrica de Disponibilidad de las Transacciones Antes
- Métrica de Disponibilidad de las Transacciones Después = Métrica de Disponibilidad de las Transacciones Antes

En la tabla N° 5 se puede apreciar que, dentro del total de días aplicado en la muestra (total = 5), ninguna métrica de transacción fue afectada en los resultados negativos dentro de la prueba de disponibilidad; por otro lado, en los rangos

positivos se identifica que 5 métricas de disponibilidad de las transacciones fueron afectadas, el cual equivale al total de la muestra establecida para este estudio.

Tabla N° 6: Estadística de prueba Z en disponibilidad

	Metrica de Disponibilidad de las Transacciones Despues - Metrica de Disponibilidad de las Transacciones Antes
Z	-2,023
Sig. asintótica(bilateral)	0,043

Fuente: Elaboración propia

Luego de realizar el análisis de datos mediante el programa SPSS en la zona Z mostrada en la tabla N° 6, se consiguió una región de rechazo de -2.023 y se obtuvo un nivel de significancia (*Sig.*) = 0.043 (4.30%) siendo menor a 0.05 (5.00%), dicho este resultado se rechazó la hipótesis nula (**HE1$_0$**) y se aceptó la hipótesis alternativa (**HE1$_a$**); en otras palabras, la media obtenida entre las pruebas realizadas para el pretest y postest en el indicador de disponibilidad, los cuales fueron diferentes de forma significativa, tuvieron como resultado la aceptación de que "El sistema de encriptación homomórfica **mejorará** la disponibilidad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC", con un incremento de satisfacción del 0.9000 (90.00%).

4.2. Prueba de hipótesis específica 2: integridad

HE2$_0$: El sistema de encriptación homomórfica **no mejorará** la integridad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC.
HE2$_a$: El sistema de encriptación homomórfica **mejorará** la integridad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC.

Para este indicador de métrica de integridad de las transacciones se realizó el análisis de un grupo de transacciones obtenidos dentro del sistema de encriptación homomórfica en un plazo de una semana, y la ficha de observación planteado para la investigación fue valorada en dos variables: transacciones satisfactorias (0) y transacciones fallidas (1) (ver anexo), los cuales, luego de un análisis previo se definieron las siguientes variables para el indicador de integridad: Cantidad de transacciones satisfactorias (0) y Cantidad de transacciones no

disponibles (1). Para el análisis de integridad se ejecutó la fórmula planteada en esta investigación por cada día de muestra, donde:

MIT = Métricas de Integridad de las Transacciones
CTS = Cantidad de Transacciones Satisfactorias
CTND = Cantidad de Transacciones No Disponibles

Figura N° 9: Fórmula de métricas de integridad de las transacciones

$$MIT = \frac{(CTS - CTND)}{CTS} * 100$$

Fuente: Rojas (2019)

De tal forma que los resultados para el indicador de integridad generaron un nuevo resultado equivalente a las variables iniciales para la observación del pretest y postest.

Tabla N° 7: Datos respectivos de integridad pre y post

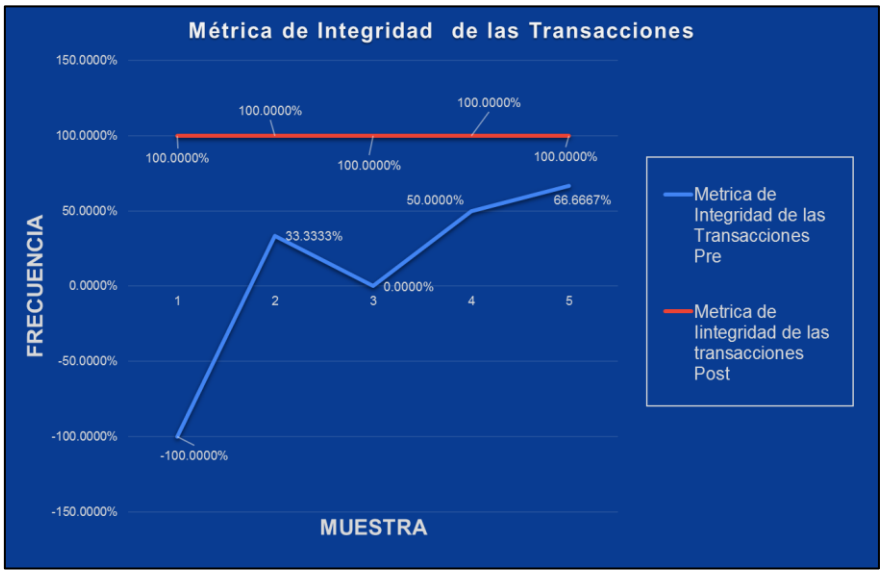
Datos pre test			
Muestras para Integridad			
Días	Cantidad de transacciones Satisfactorias	Cantidad de transacciones no disponibles	Metrica de Integridad de las Transacciones Pre
1	1	2	-100.0000%
2	3	2	33.3333%
3	2	2	0.0000%
4	2	1	50.0000%
5	3	1	66.6667%
Total	11	8	

Datos pos test			
Muestras para Integridad			
Días	Cantidad de transacciones Satisfactorias	Cantidad de transacciones no disponibles	Metrica de lintegridad de las transacciones Post
1	0	0	100.0000%
2	5	0	100.0000%
3	1	0	100.0000%
4	1	0	100.0000%
5	3	0	100.0000%
Total	10	0	

Fuente: Elaboración propia

Se presenta el siguiente gráfico del incremento en la métrica de integridad de las transacciones.

Figura N° 10: Gráfico de comparación pre y post de integridad



Fuente: Elaboración propia

A continuación, se detallan los cuadros estadísticos según la ficha de observación pre y post donde se consiguió medir el nivel de integridad al finalizar el uso del sistema de encriptación homomórfica.

4.2.1. Indicador del nivel de integridad

En la tabla N° 8 se muestran los promedios (media) de las pruebas que se realizaron en el pre y post dentro de la métrica de integridad de las transacciones donde las variables cantidad de transacciones satisfactorias y cantidad de transacciones no disponibles fueron implementadas en el estudio para el indicador.

Tabla N° 8: Indicador de mejora de integridad de las transacciones

	N		Media	Mediana	Moda	Desv. Estandar
	Válido	Perdidos				
Metricas de Integridad de las Transacciones Antes	5	0	0,1000	0,3333	-1,0000	0,6625
Metricas de Integridad de las Transacciones Despues	5	0	1,0000	1,0000	1,0000	0,0000

Fuente: Elaboración propia

En la tabla N° 8 se visualiza la mejora en la seguridad de datos en las transacciones a nivel de integridad adquirida de la recopilación de transacciones por medio de la ficha de observación, donde se identificó que en la pretest (antes

de implementar el estímulo) se obtuvo una media de 0.1000 (10.00%) en la métrica de integridad de las transacciones; por otro lado, en la ficha de observación postest (después de implementar el estímulo) se obtuvo una media de 1.0000 (100.00%) en la métrica de integridad de las transacciones, demostrando una mejora de 0.9000 (90.00%).

4.2.2. Prueba de Normalidad

En la prueba de normalidad se aplicó la prueba de Shapiro-Wilk, ya que la muestra para el indicador estuvo compuesta por un total de una semana laboral, recolectando un total de 19 transacciones en el pretest y 10 transacciones en el postest, y cuando la cantidad de la muestra es menor a 50 se usa este método. A continuación, se detallan los resultados de las pruebas pre y post de esta investigación. Para este indicador de integridad fueron analizados bajo un nivel de confiabilidad del 5%, esto indica que si el valor de significancia (***Sig.***) en los datos postest es:

- **Sig. >= 0.05 (5.00%)**, la muestra se ajusta a una distribución normal.
- **Sig. < 0.05 (5.00%)**, la muestra no se ajusta a una distribución normal.

Tabla N° 9: Comparación de significancia pre y post integridad

	Kolmogorov-Smirnov			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Metricas de Integridad de las Transacciones Antes	0,240	5	0,200	0,860	5	0,227
Metricas de Integridad de las Transacciones Despues	0,000	5	0,000	0,000	5	0,000

Fuente: Elaboración propia

a. Integridad pretest

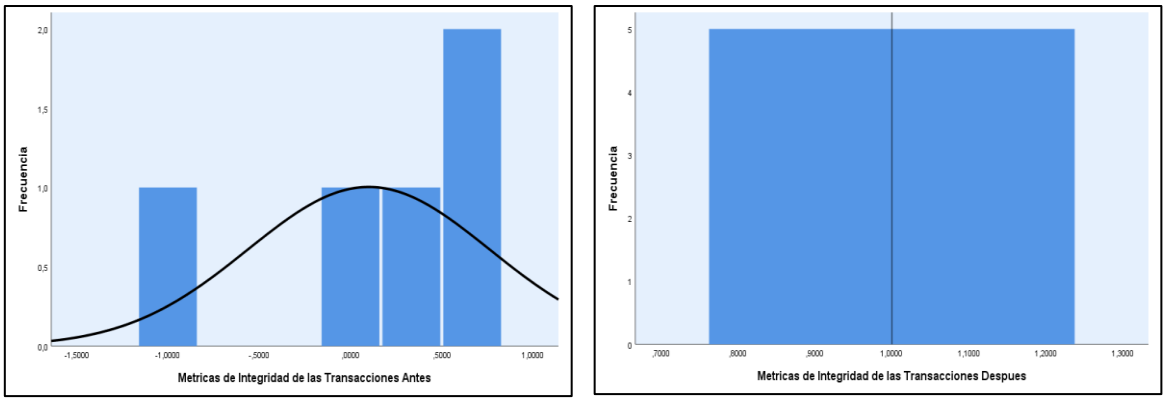
Los resultados obtenidos en la prueba de normalidad (ver tabla N° 9) a partir de los datos en la integridad pretest, se obtuvo que el nivel de significancia (*Sig.*) en la métrica de integridad de las transacciones fue de 0.227 (22.70%), siendo mayor a 0.05 (5.00%).

b. Integridad postest

Los resultados obtenidos en la prueba de normalidad (ver tabla N° 9) a partir de los datos en la integridad postest, se obtuvo que el nivel de significancia (*Sig.*)

en la métrica de integridad de las transacciones fue de 0.000 (0.00%), siendo menor a 0.05 (5.00%).

Figura N° 11: Diagramas de normalidad de datos de integridad



Fuente: Elaboración propia

Los histogramas para la métrica de integridad de las transacciones (antes y después) indican que la muestra no se ajusta a una distribución normal.

c. Prueba de rangos con signos de Wilcoxon

En la tabla N° 10 se muestra la prueba con signos de Wilcoxon de forma más detallada.

Tabla N° 10: Rango con signos de Wilcoxon de integridad

		N	Rango promedio	Suma de rangos
Metricas de Integridad de las Transacciones Despues - Metricas de Integridad de las Transacciones Antes	Rangos negativos	0	0,00	0,00
	Rangos positivos	5	3,00	15,00
	Empates	0		
	Total	5		

Fuente: Elaboración propia

- Métricas de Integridad de las Transacciones Después < Métricas de Integridad de las Transacciones Antes
- Métricas de Integridad de las Transacciones Después > Métricas de Integridad de las Transacciones Antes
- Métricas de Integridad de las Transacciones Después = Métricas de Integridad de las Transacciones Antes

En la tabla N° 10 se puede apreciar que, dentro del total de días aplicado en la muestra (total = 5), ninguna métrica de transacción fue afectada en los resultados negativos dentro de la prueba de integridad; por otro lado, en los rangos positivos se identifica que 5 métricas de integridad de las transacciones fueron afectados, el cual equivale al total de la muestra establecida para este estudio.

Tabla N° 11: Estadística de prueba Z en integridad

	Metrica de Integridad de las Transacciones Despues - Metrica de Integridad de las Transacciones Antes
Z	-2,023
Sig. asintótica(bilateral)	,043

Fuente: Elaboración propia

Luego de realizar el análisis de datos mediante el programa SPSS en la zona Z mostrada en la tabla N° 11, se consiguió una región de rechazo de -2.023 y se obtuvo un nivel de significancia (*Sig.*) = 0.043 (4.30%) siendo menor a 0.05 (5.00%), dicho este resultado se rechazó la hipótesis nula (**HE2$_0$**) y se aceptó la hipótesis alternativa (**HE2$_a$**); en otras palabras, la media obtenida entre las pruebas realizadas para el pretest y postest en el indicador de integridad, los cuales fueron diferentes de forma significativa, tuvieron como resultado la aceptación de que “El sistema de encriptación homomórfica **mejorará** la integridad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC”, con un incremento de satisfacción del 0.9000 (90.00%).

4.3. Prueba de hipótesis específica 3: confidencialidad

HE3$_0$: El sistema de encriptación homomórfica **no mejorará** la confidencialidad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC.
HE3$_a$: El sistema de encriptación homomórfica **mejorará** la confidencialidad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC.

Para este indicador de métrica de confidencialidad de las transacciones se realizó el análisis de un grupo de transacciones obtenidos dentro del sistema de encriptación homomórfica en un plazo de una semana, y la ficha de observación

planteado para la investigación fue valorada en dos rangos: transacciones satisfactorias (0) y transacciones fallidas (1) (ver anexo), de los cuales, luego de un análisis previo se definieron las siguientes variables para el indicador de integridad: Cantidad de reportes (0) y Cantidad de reportes legibles (1). Para el análisis de confidencialidad se ejecutó la fórmula planteada en esta investigación por cada día de muestra, donde:

MCT = Métricas de Confidencialidad de las Transacciones
CR = Cantidad de Reportes
CR_L = Cantidad de Reportes Legibles

Figura N° 12: Fórmula de métricas de confidencialidad de las transacciones

$$MCT = \frac{(CR - CR\_L)}{CR} * 100$$

Fuente: Rojas (2019)

De tal forma que los resultados para el indicador de confidencialidad generaron un nuevo resultado equivalente a las variables iniciales para la observación del pretest y postest.

Tabla N° 12: Datos respectivos de confidencialidad pre y post

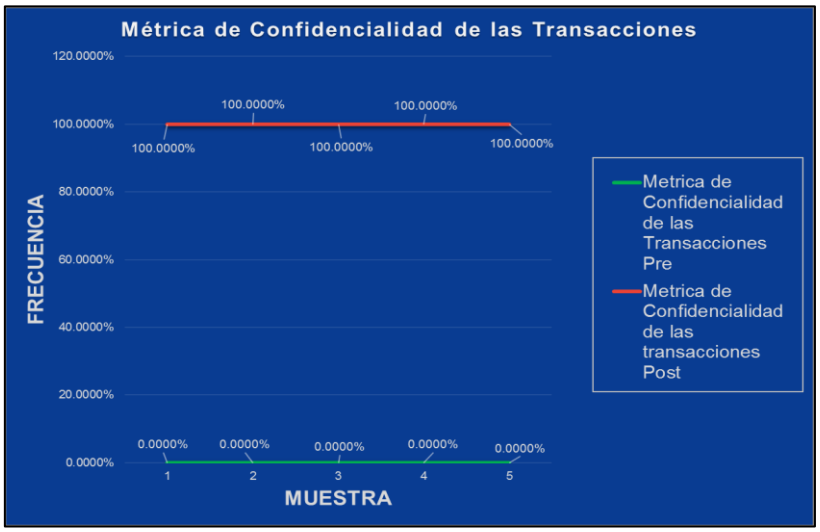
Datos pre test			
Muestras para Condifencialidad			
Días	Cantidad de reportes	Cantidad de reportes legibles	Metrica de Confidencialidad de las Transacciones Pre
1	1	1	0.0000%
2	3	3	0.0000%
3	2	2	0.0000%
4	2	2	0.0000%
5	3	3	0.0000%
Total	11	11	

Datos pos test			
Muestras para Condifencialidad			
Días	Cantidad de reportes	Cantidad de reportes legibles	Metrica de Confidencialidad de las transacciones Post
1	0	0	100.0000%
2	5	0	100.0000%
3	1	0	100.0000%
4	1	0	100.0000%
5	3	0	100.0000%
Total	10	0	

Fuente: Elaboración propia

Se presenta el siguiente gráfico para la métrica de confidencialidad de las transacciones.

Figura N° 13: Gráfico de comparación pre y post de confidencialidad



Fuente: Elaboración propia

A continuación, se detallan los cuadros estadísticos según la ficha de observación pre y post donde se consiguió medir el nivel de confidencialidad al finalizar el uso del sistema de encriptación homomórfica.

4.3.1. Indicador del nivel de confidencialidad

En la tabla N° 13 se muestran los promedios (media) de las pruebas realizadas en el pre y post en las variables cantidad de reportes y la cantidad de reportes legibles implementadas en el estudio para el indicador de confidencialidad.

Tabla N° 13: Indicador de mejora de confidencialidad de las transacciones

	N		Media	Mediana	Moda	Desv. Estándar
	Válido	Perdidos				
Metricas de Confidencialidad de las Transacciones Antes	5	0	0,0000	0,0000	0,0000	0,0000
Metricas de Confidencialidad de las Transacciones Despues	5	0	1,0000	1,0000	1,0000	0,0000

Fuente: Elaboración propia

En la tabla N° 13 se visualiza la mejora en la seguridad de datos en las transacciones a nivel de confidencialidad adquirida de la recopilación de transacciones por medio de la ficha de observación, donde se identificó que en el pretest (antes de implementar el estímulo) se obtuvo una media de 0.0000 (0.00%)

en la métrica de confidencialidad de las transacciones; por otro lado, en la ficha de observación postest (después de implementar el estímulo) se obtuvo una media de 1.0000 (100.00%) en la métrica de confidencialidad de las transacciones, demostrando una mejora de 1.0000 (100.00%).

4.3.2. Prueba de Normalidad

En la prueba de normalidad se aplicó la prueba de Shapiro-Wilk, ya que la muestra para el indicador estuvo compuesta por un total de una semana laboral, recolectando un total de 19 transacciones en el pretest y 10 transacciones en el postest, y cuando la cantidad de la muestra es menor a 50 se usa este método. A continuación, se detallan los resultados de las pruebas pre y post de esta investigación. Para este indicador de confidencialidad fueron analizados bajo un nivel de confiabilidad del 5%, esto indica que si el valor de significancia (***Sig.***) en los datos postest es:

- **Sig. >= 0.05 (5.00%)**, la muestra se ajusta a una distribución normal.
- **Sig. < 0.05 (5.00%)**, la muestra no se ajusta a una distribución normal.

Tabla N° 14: Comparación de significancia pre y post en confidencialidad

	Kolmogorov-Smirnov			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Metricas de Confidencialidad de las Transacciones Antes	0,000	5	0,000	0,000	5	0,000
Metricas de Confidencialidad de las Transacciones Despues	0,000	5	0,000	0,000	5	0,000

Fuente: Elaboración propia

a. Confidencialidad pretest

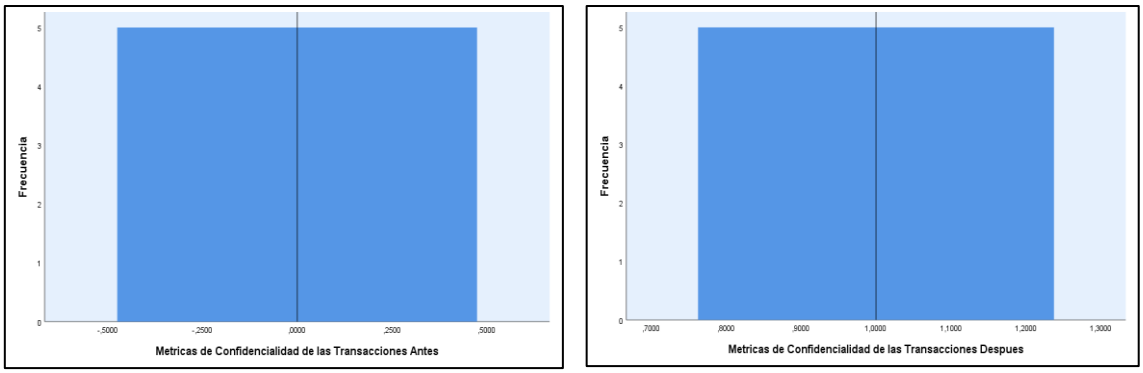
Los resultados obtenidos en la prueba de normalidad (ver tabla N° 14) a partir de los datos en la confidencialidad pretest, se obtuvo que el nivel de significancia (*Sig.*) en la métrica de confidencialidad de las transacciones fue de 0.0000 (0.00%), siendo menor a 0.05 (5.00%).

a. Confidencialidad postest

Los resultados obtenidos en la prueba de normalidad (ver tabla N° 14) a partir de los datos en la confidencialidad postest, se obtuvo que el nivel de

significancia (*Sig.*) en la métrica de confidencialidad de las transacciones fue de 0.000 (0.00%), siendo menor a 0.05 (5.00%).

Figura N° 14: Diagramas de normalidad de datos confidencialidad



Fuente: Elaboración propia

Los histogramas para la métrica de confidencialidad de las transacciones indican que la muestra no se ajusta a una distribución normal.

b. Prueba de rangos con signos de Wilcoxon

En la tabla N° 15 se muestra la prueba con signos de Wilcoxon de forma más detallada.

Tabla N° 15: Rangos con signos de Wilcoxon de confidencialidad

		N	Rango promedio	Suma de rangos
Metricas de Confidencialidad de las Transacciones Despues - Metricas de Confidencialidad de las Transacciones Antes	Rangos negativos	0	0,00	0,00
	Rangos positivos	5	3,00	15,00
	Empates	0		
	Total	5		

Fuente: Elaboración propia

- Métricas de Confidencialidad de las Transacciones Después < Métricas de Confidencialidad de las Transacciones Antes
- Métricas de Confidencialidad de las Transacciones Después > Métricas de Confidencialidad de las Transacciones Antes
- Métricas de Confidencialidad de las Transacciones Después = Métricas de Confidencialidad de las Transacciones Antes

En la tabla N° 15 se puede apreciar que, dentro del total de días aplicado en la muestra (total = 5), ninguna métrica de transacción fue afectada en los resultados negativos dentro de la prueba de confidencialidad; por otro lado, en los rangos positivos se identifica que 5 métricas de confidencialidad de las transacciones fueron afectados, el cual equivale al total de la muestra establecida para este estudio.

Tabla N° 16: Estadística de prueba Z en confidencialidad

	Metricas de Confidencialidad de las Transacciones Despues - Metricas de Confidencialidad de las Transacciones Antes
Z	-2,236
Sig. asintótica(bilateral)	0,025

Fuente: Elaboración propia

Luego de realizar el análisis de datos mediante el programa SPSS en la zona Z mostrada en la tabla N° 16, se consiguió una región de rechazo de -2.236 y se obtuvo un nivel de significancia (*Sig.*) = 0.025 (2.50%) siendo menor a 0.05 (5.00%), dicho este resultado se rechazó la hipótesis nula (**HE3$_0$**) y se aceptó la hipótesis alternativa (**HE3$_a$**); en otras palabras, la media obtenida entre las pruebas realizadas para el pretest y postest en el indicador de confidencialidad, los cuales fueron diferentes de forma significativa, tuvieron como resultado la aceptación de que “El sistema de encriptación homomórfica **mejorará** la confidencialidad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC”, con un incremento de satisfacción del 1.0000 (100.00%).

4.4 Prueba de hipótesis general

Según López (2020) indica que: la propiedad transitiva o silogismo hipotético se cumple cuando dos elementos se relacionan, un primer elemento con un segundo, y este último elemento con un tercero, por consiguiente: $P \rightarrow Q. \mid Q \rightarrow R. \mid$ Entonces, $P \rightarrow R$. Dado que las hipótesis específicas 1, 2 y 3 fueron aceptadas, se determinó que la hipótesis general: “El fortalecimiento de la seguridad de datos en las transacciones de ventas mejora con el sistema de encriptación homomórfica en Lugar Expresivo SAC”, también fuera aceptada por unanimidad.

4.5. Resumen de las hipótesis

A continuación, se presenta la tabla N° 17 indicando el resumen de los resultados en las hipótesis planteadas y su comprobación en este estudio:

Tabla N° 17: Resumen de resultados de hipótesis

Codigo	Hipótesis	Resultado (Aceptada o Rechazada)
HE1	El sistema de encriptación homomórfica mejorará la disponibilidad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC	**Aceptada**
HE2	El sistema de encriptación homomórfica mejorará la integridad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC	**Aceptada**
HE3	El sistema de encriptación homomórfica mejorará la confidencialidad de la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC	**Aceptada**
HG	El fortalecimiento de la seguridad de datos en las transacciones de ventas mejora con el sistema de encriptación homomórfica en Lugar Expresivo SAC	**Aceptada**

Fuente: Elaboración propia

Como se detalla en la tabla N° 17, los resultados lograron demostrar que las hipótesis planteadas en esta investigación fueron aceptadas, llegando a cumplir los objetivos específicos, y a su vez el objetivo general; además, se logró un incremento considerable del 90.00% a nivel de disponibilidad, un incremento del 90.00% a nivel de integridad, por último, un incremento del 100.00% a nivel de confidencialidad luego de aplicar el sistema de encriptación homomórfico que permitió fortalecer la seguridad de los datos al momento de generar una transacción.

V. DISCUSIÓN

En el presente capítulo aceptamos la hipótesis general de acuerdo a los resultados obtenidos en el capítulo previo por cada hipótesis específica. Así afirmamos que el sistema de encriptación homomórfica mejoró la seguridad de los datos en las transacciones generadas dentro de Lugar Expresivo SAC. Esto indica que un sistema de encriptación homomórfica fortalece la seguridad de otro sistema que genera transacciones para que solo el personal que cuenta con las llaves pueda hacer uso de los datos e información.

Esta afirmación, desprendida de los resultados para esta investigación, señala que el indicador de Disponibilidad obtuvo una mejora del 90%, respecto al indicador de Integridad obtuvo una mejora del 90%. Y para finalizar, en el indicador de confidencialidad llegó a conseguir una mejora del 100%.

Para el estudio de Rojas (2019), tuvo como resultados en el nivel de disponibilidad una media en el pretest de 96.35% y luego de implementar su estímulo obtuvo una media de 99.97%, de igual forma, en el indicador de integridad su valor de la media del pretest fue de 76% y luego del estímulo aumentó significativamente a 90.59%; por último, para el indicador de confidencialidad su valor de la media en el índice de pretest fue de 96.35%, y en el postest fue de 98,58%. En el estudio de Rojas (2019), implementó la NTP ISO/IEC 27001:2014 en la base de datos de la Reniec para mejorar la seguridad de los datos en los campos de disponibilidad, integridad y confidencialidad. Para esta investigación se tomó como referencia los campos para la dimensión que dieron como resultado la mejora del 90% y 100% en la seguridad de información aplicada a las transacciones.

Para el estudio de Rugel (2019), obtuvo como resultados en el valor de la media en el pretest un 82.3% y luego de aplicar el estímulo ganó un valor exponencial del 2747% para el tiempo de encriptación. El motivo de este valor exponencial es porque estaba siendo analizado por el tiempo de encriptación por archivo, el cual, debido a la longitud del código y el tamaño de los archivos, el tiempo de cifrado fue mayor de lo esperado generando un déficit; por otro lado, recomendó aplicar protocolos de enrutamiento dinámico como una solución al tráfico para información. En esta investigación el tiempo resultante es aceptable para evitar la demora en los procesos de facturación ya que los datos procesados dentro de los mismos son solamente números enteros por lo que los tiempos para encriptar y desencriptar se han mantenido constantes.

Plasencia (2018) realizó una encuesta virtual de 4 preguntas en un rango de tiempo de 10 horas en un mismo día para usuarios de edad universitaria consiguiendo de forma exitosa que el sistema puede ser adaptado en múltiples contextos haciendo referencia en sus decisiones técnicas el uso de firmas digitales para garantizar la integridad del dato; una de estas adaptaciones planteadas por el autor fue planteada dentro de esta investigación la cual estuvo aplicada al sector comercial en los procesos de generación de comprobante de pago electrónico cambiando la firma que se ha de generar con la clave privada a solamente usar un esquema de seguridad con clave simétrica para resguardar el par de llaves.

De la misma forma, para García et al. (2018) utilizaron métodos de encriptación cuya seguridad demostró que puede ser probada de manera matemática y permitió garantizar el anonimato del votante; además, el uso de esquemas homomórficos permitieron realizar operaciones matemáticas sobre información cifrada. Para esta investigación se aplicaron los esquemas homomórficos en el ámbito comercial, dentro de las transacciones para el procesamiento de sumas algebraicas en los reportes mensuales lo que concluyó con una mejora significativa en la seguridad de datos al momento de realizar estas consultas mensuales.

Para la investigación de Araujo (2018), utilizó el algoritmo ElGamal para la construcción del sistema de voto electrónico con encriptación homomórfica, el cual resolvió el problema de la falta de confidencialidad por parte de externos o cualquier usuario con acceso a Internet que pueda editar los resultados electorales. El presente estudio, al igual que Araujo (2018), consiguió resolver el problema de la falta de confidencialidad aplicado dentro de las transacciones utilizando el algoritmo de cifrado Paillier, el cual cumple la misma función que ElGamal, siendo los dos de la clase de criptografía asimétrica los cuales funcionan con dos tipos de claves al momento de cifrar: clave pública y clave privada. El algoritmo Paillier es un algoritmo de criptografía asimétrica probabilística por lo que encriptar más de una vez un dato no resultará en otro idéntico. Esta aleatoriedad sumada a que aún no se han documentado vulnerabilidades en su computación hizo que nos decidamos por usar el algoritmo de Paillier.

De igual manera, para Garibaldi (2018), luego de realizar una comparación con otros algoritmos de cifrado, utilizó el algoritmo Paillier, el cual obtuvo como

resultado que la utilización de esquemas con algoritmos de cifrado se llegan a comprometer para construir un sistema de voto electrónico con mayor seguridad y transparencia, demostrando que a pesar de la complejidad de usar algoritmos de cifrado garantizan que la ejecución llega a producirse sin necesidad de exponer los datos, consiguiendo la confidencialidad de los mismos. Para este estudio se revisó las comparaciones de otros algoritmos de cifrado presentados por Garibaldi (2018) y se planteó utilizar el algoritmo de pailler como módulo principal para la creación del sistema de encriptación homomórfica, siendo implementado en el área comercial por motivo de proteger los datos generados dentro de las transacciones.

Schroeder (2018) utilizó el algoritmo de Paillier para la creación de un sistema de voto electrónico remoto para apoyar las elecciones gestionadas por las autoridades, aunque su diseño cumplió con tareas en su cometido tiene un límite en su función, como el conteo de votos y la protección de los mismos, lo que hace que delegue algunas tareas a terceros con el fin de disminuir la responsabilidad y extender las ejecuciones simultáneas dentro del sistema. La presente investigación utilizó el algoritmo de Paillier para la creación del sistema de encriptación homomórfica que se encargó de proteger los datos generados al momento de crear los comprobantes de pago electrónicos dentro de la empresa Lugar Expresivo SAC y la limitación de las operaciones que se pueden realizar con este algoritmo de Paillier sí logran satisfacer los requerimientos necesarios para todos los menesteres en la facturación y posterior uso de los datos para presentar al fisco.

Por último, Fernández (2021) diseñó un sistema de cifrado de archivos por lotes, implementando un script de programación (elaborado por el mismo autor) para el cifrado donde se empleó el estándar PGP (Pretty good privacy / privacidad bastante buena) con el lenguaje de programación Python; además de diseñar una arquitectura para el cifrado de mensajes por correo saliente que cumplan las condiciones establecidas en las políticas internas de la empresa. Dicho proyecto validó que el algoritmo RSA con llaves públicas es fiable, ya que por su complejidad y longitud de las mismas al momento de encriptar la información lo hace muy robusta, garantizando la confidencialidad e integridad de los datos, de tal forma que la información que está siendo transmitida siempre se mantendrá protegida de extremo a extremo. De igual manera, en el presente estudio los datos numéricos encriptados que se guardan en bases de datos de servidores remotos no requieren

ser transferidos en su totalidad hacia la persona que debe tener acceso a los mismos, sino que se pueden realizar operaciones dentro del servidor y transmitir únicamente los resultados necesarios. Es por eso que se puede ahorrar en la transferencia de grandes volúmenes de datos al operarlos previamente sin comprometer su confidencialidad por medio de las llaves de cifrado generadas al momento de procesar una transacción.

VI. CONCLUSIONES

Para la presente investigación se presentan las siguientes conclusiones:

a. Se logró cumplir el objetivo de esta investigación para el índice de Disponibilidad, donde el análisis de resultados dio como positivo en la medición de la Media con una diferencia de 10.00% en el pretest respecto a la Media del índice postest que es del 100.00%, logrando una mejora del 90.00% en esta dimensión. Esto significa que la variable independiente influenció de forma considerada al momento de ser implementada dentro de la organización.

b. Se logró cumplir el objetivo dentro de esta investigación para el índice de Integridad, donde el análisis de los resultados dio como positivo en la medición de la Media con una diferencia de 10.00% en el pretest respecto a la Media del índice postest que es del 100.00%, logrando una mejora del 90.00% en esta dimensión. Esto significa que la variable independiente influenció de forma considerada al momento de ser implementada dentro de la organización.

c. Se logró cumplir el objetivo de la investigación en el índice de Confidencialidad, donde el análisis de los resultados dio como positivo en la medición de la Media con una diferencia de 0.00% en el pretest respecto a la Media del índice postest que es del 100%, logrando una mejora del 100% en esta dimensión. Esto significa que la variable independiente obtuvo una gran influencia al momento de ser implementada dentro de la organización.

d. Al considerar que las tres dimensiones fueron aceptadas dentro del estudio, se determinó que se cumplió el cometido dentro de esta investigación, el cual afirma que la implementación de un sistema de encriptación homomórfica en la empresa Lugar Expresivo SAC optimizó significativamente los indicadores en la seguridad de los datos en el proceso de facturación.

e. De los estudios referenciados, así como del presente estudio, se puede concluir que los algoritmos de cifrado, implementados en un sistema de

encriptación homomórfica causan efectos positivos en la seguridad de los datos ya que poseen una estructura sólida y robusta, y puede ser usado dentro de organizaciones que manejen información valiosa, además, existe una mejora y adaptación al momento de implementar algoritmos de cifrado dentro del área comercial.

VII. RECOMENDACIONES

Las recomendaciones para investigaciones futuras son las siguientes:

1. Para la empresa, y sobre todo quien tenga poder de decisión dentro de ella, debe estar dispuesta a cambiar el esquema de seguridad de los datos, porque los datos generados se encriptan y no hay manera de desencriptar si se pierde la contraseña. Por este motivo el esquema debe involucrar métodos o formas de respaldar las contraseñas y las llaves privadas sin exponerlas, para eso se pueden usar esquemas de secreto compartido.

2. Se recomienda revisar periódicamente el sistema de encriptación ya que conforme avanzan los estudios también algunos algoritmos se vuelven vulnerables y los atacantes podrían acceder a los datos. Por ello, se debe actualizar el sistema con algoritmos más seguros y remover los algoritmos obsoletos.

3. Se recomienda a las empresas encriptar los datos de sus comprobantes de pagos con un sistema de encriptación homomórfica, porque el proceso de generación de comprobantes de pago no sufre modificaciones y la seguridad es fortalecida en todas sus dimensiones.

4. Se recomienda a los trabajos futuros implementar la encriptación homomórfica en otros ámbitos más allá de los relacionados al sufragio electrónico y la generación de comprobantes de pagos electrónicos.

5. Se recomienda el estudio e implementación de la encriptación completamente homomórfica para realizar mayor cantidad de operaciones lógicas y aritméticas para abarcar a otros sistemas diferentes de los generadores de comprobantes de pago.

REFERENCIAS

Alvarez, A. (2020). Justificación de la Investigación. Universidad de Lima. Facultad de Ciencias Empresariales y Económicas, Carrera de Negocios Internacionales. 9, 1-3.

Morales, J., Neyra, A. y Vidal, A. (2021). Método de Análisis Cuantitativo de Riesgos de Ciberseguridad Enfocado a la Seguridad de datos en Entidades Financieras (Universidad Peruana de Ciencias Aplicadas. Escuela de Postgrado, Perú). Recuperado de https://repositorioacademico.upc.edu.pe/handle/10757/660721

Narváez, C. y Yungán, J (2022). Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información (Ciencias Tecnologías de la Información y la Comunicación, Ecuador). Recuperado de https://dominiodelasciencias.com/ojs/index.php/es/article/view/2854

Contero, W. (2019). Diseño de una política de seguridad de la información basada en la norma ISO 27002:2013, para el sistema de botones de seguridad del Ministerio del Interior (Facultad de Arquitectura e Ingeniería, Ecuador). Recuperado de https://repositorio.uisek.edu.ec/bitstream/123456789/3345/1/TESIS%20MC%2026_03_2019.pdf

Trabajadores Informales ganan 15% menos que antes de la pandemia. (2022). INSTITUTO PERUANO DE ECONOMÍA - IPE. Recuperado de https://www.ipe.org.pe/portal/trabajadores-informales-ganan-15-menos-que-antes-de-pandemia/

Guzmán, C. (2018). Mypes: por qué son importantes para la economía peruana. Publicado el 18 de abril de 2018. Recuperado de https://pqs.pe/actualidad/economia/mypes-por-que-son-importantes-para-la-economia-peruana/

Las micro y pequeñas empresas en el Perú Resultados en 2020 (2020). COMEXPERU. Recuperado de https://www.comexperu.org.pe/upload/articles/reportes/reporte-mypes-2020.pdf

Beynon, P. (2018). *Sistemas de Bases de Datos.* Barcelona, España: © Editorial Reverté. Recuperado de https://www.digitaliapublishing.com/visor/67908

Hernández, O. (2021). Aproximación a los distintos tipos de muestreo no probabilístico que existen. 37 (3), 1-3. Recuperado de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-21252021000300002

Garibaldi, J. (2018). Aplicabilidade de Criptografia Homomórfica (Universidade Federal do Rio Grande do Sul, instituto de informática, Brasil). Recuperado de https://www.lume.ufrgs.br/bitstream/handle/10183/175084/001065175.pdf?sequence=1&isAllowed=y

Reis, P., Lara, P. y Borges, F. (2020). Computação da Quadratura Gaussiana em um Esquema Criptográfico Parcialmente Homomórfico (Simpósio Brasileiro De Segurança Da Informação E De Sistemas Computacionais, Brasil). Recuperado de https://sol.sbc.org.br/index.php/sbseg/article/view/19262

Andrade, E., Lunardi, R. y Ramos, N. (2018). Conceitos Básicos de Criptografia. (Brasil). Recuperado de https://www.researchgate.net/profile/Roben-Lunardi/publication/359514048_Conceitos_basicos_de_Criptografia/links/624214e17931cc7ccf009b99/Conceitos-basicos-de-Criptografia.pdf

Morgado, D. (2021). Do Cripto-Esquema Homomórfico para a Classificação de Solvabilidade no Crédito ao Consumo à Engenharia do Direito, não Artificial (Engenharia do Direito da Inteligência Artificial, Brasil). Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881839

Madeira, M. (2018). Towards more Secure and Efficient Password Databases (Faculdade de Ciências e Tecnologia e a Universidade NOVA de Lisboa, Portugal). Recuperado de https://run.unl.pt/handle/10362/61549

Felipe, A. (2018). Implementación Facturación electrónica en Colombia (Universidad Católica de Colombia, Colombia). Recuperado de https://repository.ucatolica.edu.co/handle/10983/22477

Benítez, C., Granda, D. y Jaramillo, J. (2019). LA COMPUTACIÓN EN LA NUBE EN LOS ESPACIOS EDUCATIVOS (Revista del Instituto Tecnológico Superior Jubones, (2) 1, 1-9. Recuperado de http://institutojubones.edu.ec/ojs/index.php/societec/article/view/67/388

Cordova, J., Vega, H., Rodríguez, C. y Escobedo, F. (2020). FIRMA DIGITAL BASADA EN CRIPTOGRAFÍA ASIMÉTRICA PARA GENERACIÓN DE HISTORIAL CLÍNICO (Universidad Nacional Mayor de San Marcos, Perú). Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=7678811

Fernández, N. (2021). Diseño de un Sistema de Criptografía Asimétrica para dotar Seguridad de Confidencialidad e Integridad a las Comunicaciones SMTP y SFTP para Scharff Logística Integrada S.A (Universidad Peruana de Ciencias Aplicadas, Perú). Recuperado de https://repositorioacademico.upc.edu.pe/handle/10757/656271

Rojas, M. (2019). Seguridad en los datos e implantación de la NTP-ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC (Universidad César Vallejo, Perú). Recuperado de https://repositorio.ucv.edu.pe/handle/20.500.12692/43660

Cubillos, G. (2020). Protección de datos compartidos en entornos de nube. Universidad de los Andes (Facultad de Ingeniería, Colombia). Recuperado de https://repositorio.uniandes.edu.co/bitstream/handle/1992/48674/u833337.pdf

Arias, J. y Covinos, M. (2021). *Diseño y metodología de investigación*. Perú: Editorial Enfoques Consulting EIRL. Recuperado de http://repositorio.concytec.gob.pe/handle/20.500.12390/2260

Baena, G. (2022). Metodología de la investigación (3ª ed.). México: Grupo Editorial Patria®. Recuperado de https://repositorio.eesppjsco.edu.pe/handle/JOSACO/8

Clark, W (2020). What is the paillier cryptosystem?. Publicado el 9 de julio de 2020. Recuperado de https://blog.openmined.org/the-paillier-cryptosystem/

Shacklett, M. (2021). What is a digital certificate?. *s.f.* Recuperado de https://www.techtarget.com/searchsecurity/definition/digital-certificate

Plasencia, E. (2018). Sistema de votación electrónica basado en blockchain (Universidad de La Laguna, España). Recuperado de https://riull.ull.es/xmlui/bitstream/handle/915/9462/Sistema%20de%20votacion%20electronica%20basado%20en%20blockchain.pdf?sequence=1

Araújo, P. (2018). Transparência e privacidade em urnas eletrônicas através de encriptação homomórfica e de esquemas de comprometimento (Universidade Federal do Maranhão, Brasil). Recuperado de https://rosario.ufma.br/jspui/handle/123456789/3525

Schroeder, R. (2018). Implementação de um sistema de eleição remoto secreto e veriicável (Universidade Federal de Santa Catarina - UFSC, Brasil). Recuperado de https://repositorio.ufsc.br/handle/123456789/192304

Nunes, R. (2019). Uma abordagem criptográfica a sistemas eleitorais (Universidade do Minho, Portugal). Recuperado de http://repositorium.uminho.pt/handle/1822/65272

De la Rosa, M. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001 (Revista Universidad y Sociedad, Ecuador). Recuperado de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000500495

Costales, C. (2021). Desarrollo de un plan de seguridad informática que permita la confidencialidad, integridad y disponibilidad de la información en el Juzgado de la Niñez y Adolescencia de la ciudad de Quito (Escuela Superior Politécnica de Chimborazo, Ecuador). Recuperado de http://dspace.espoch.edu.ec/handle/123456789/14689

Pereira, H. (2021). Introdução à criptografia completamente homomórfica com implementação em Sage (XXI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, Brasil). Recuperado de https://sol.sbc.org.br/livros/index.php/sbc/catalog/download/71/308/564-1?inline=1

Gallardo, I. (2018). Certificados digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada (Tesis de Maestría, Universidad Nacional de la Plata, Argentina). Recuperado de http://sedici.unlp.edu.ar/handle/10915/72076

Molina, J. (2021). Modelo de evaluación de metodologías de desarrollo de software web. Universidade da Coruña (Programa de doctorado en Tecnologías de la Información y las Comunicaciones, España). Recuperado de https://ruc.udc.es/dspace/handle/2183/28902

Osuna, V. (2019). “Propuestas de mejoras para asegurar la calidad del software” (Universidad Politécnica De Sinaloa, México). Recuperado de http://repositorio.upsin.edu.mx/Fragmentos/tesinas/262016030167OsunaOsunaVanessa6141.pdf

Córdova, L., López, R., Pacheco, S. y Vera, D. (2019). Análisis de la metodología RUP en el desarrollo de software académico mediante la herramienta DJANGO (Revista Ciencia Mundo de la Investigación y el Conocimiento, Ecuador). Recuperado de https://recimundo.com/~recimund/index.php/es/article/view/486

Sabogal, C. (2021). Análisis de la seguridad informática en las transacciones electrónicas para el comercio electrónico (Universidad Nacional Abierta y a Distancia UNAD, Colombia). Recuperado de https://repository.unad.edu.co/handle/10596/44132

Camposano, G. (2020). Propuesta para el control y seguridad de la información de la empresa de ventas en Línea Buy Now aplicando Norma ISO 27001 (Universidad Técnica de Babahoyo, Ecuador). Recuperado de http://dspace.utb.edu.ec/handle/49000/8614

Dueñas, B. y Moreno, J. (2018). Sistemas de información empresarial: la información como recurso estratégico. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=6255073

Villacres, K. (2021). Estudio de Factibilidad de la Seguridad para el Desarrollo de un Prototipo Web de Voto Electrónico en la Universidad de Guayaquil (Universidad de Guayaquil, Ecuador). Recuperado de http://repositorio.ug.edu.ec/handle/redug/56860

Superintendencia Nacional de Administración Tributaria. Informe técnico previo de evaluación de software n°. 12-2019-SUNAT/1U4100. Recuperado de https://www.sunat.gob.pe/cuentassunat/adquisiciones/ley28612/2019/1U4100/informe-012-2019-1U4100.pdf

Ortiz, E. (2018). Controles de Seguridad según la Norma ISO/IEC 27002:2013 para el mejoramiento de la Gestión de Seguridad de la Información en la Universidad Nacional Agraria de la Selva (Universidad Nacional Agraria de la Selva, Perú). Recuperado de http://repositorio.unas.edu.pe/handle/UNAS/1710

Proveedor de Servicios Electrónicos - PSE. Superintendencia Nacional de Aduanas y de Administración Tributaria - Sunat. Publicado el 18 de agosto de 2022. Recuperado de: https://cpe.sunat.gob.pe/aliados/pse

Operadores de Servicios Electrónicos. Superintendencia Nacional de Aduanas y de Administración Tributaria - Sunat. Publicado el 26 de octubre del 2021. Recuperado de: https://cpe.sunat.gob.pe/aliados/ose

Obtener el RUC. Emprender Sunat. Publicado 2018. Recuperado de: https://emprender.sunat.gob.pe/emprendiendo/decido-emprender/obtener-ruc

Serie “27000”. Guías de referencia útiles para la implantación, mantenimiento, auditoría y certificación de los Sistemas de Gestión de la Seguridad de la Información. Recuperado de: https://www.iso27000.es/iso27000.html

Gutiérrez, A. (2020). *Cómo entender estadística fácilmente.* México: Instituto Mexicano de Contadores Públicos. Recuperado de: https://n9.cl/tnbew

Asqui, C., Huanca, H., Mamani, D. y Mamani, H. (2021). Habilidades lingüísticas y comprensión lectora en la oquedad del siglo XXI: una mirada a la Institución Educativa Politécnica de Puno - Perú. Perú: Horizontes Revista de Investigación en Ciencias de la Educación. Recuperado de http://www.scielo.org.bo/scielo.php?pid=S2616-79642021000200537&script=sci_arttext

Rugel, B. (2019). Seguridad En El Sistema De Gestión De Datos Medidos De Energía Eléctrica Aplicando Cifrado Homomórfico (Universidad Politécnica Salesiana Sede Quito, Ecuador). Recuperado de https://dspace.ups.edu.ec/handle/123456789/16923

García, P., van de Graaf, J., Montejano, G. (2018). Voto Electrónico Seguro con Criptografía Homomórfica. XX Workshop de Investigadores en Ciencia de la Computación. Argentina. Recuperado de http://sedici.unlp.edu.ar/handle/10915/68315

Espinoza, J. (2021). *Apuntes de probabilidad y estadística*. México. Recuperado de http://www.ptolomeo.unam.mx:8080/jspui/bitstream/132.248.52.100/3302/1/APUNTES%20DE%20PROBABILIDAD%20Y%20ESTAD%C3%8DSTICA.pdf

López (2020). Relaciones entre la lógica y la filosofía de la ciencia (ensayo) (Universidad Autónoma de Nayarit, México). Recuperado de: http://www.protrepsis.cucsh.udg.mx/index.php/prot/article/view/268

C. E. Flores y K. L. Flores (2021). Pruebas para comprobar la normalidad de datos en procesos productivos: Anderson–Darling, Ryan-Joiner, Shapiro-Wilk y Kolmogórov-Smirnov (Universidad de Panamá, Panamá) Recuperado de: http://portal.amelica.org/ameli/journal/341/3412237018/3412237018.pdf

ANEXOS

Anexo: Ficha de recolección de datos

Reporte semanal de incidencias generando transacciones

Trabajador:		Luis Garro Acuña		
Fecha de inicio:		10/10/22	Fecha de fin:	
Cant.	(G)enerando o (L)eyendo	Observaciones		
2	G	Tuve que rehacer la fact. no se generaba o sunatizaba		
2	G	A pesar de este problema se genera el pdf y se archiva		
2	G	Malogra el orden y causa incomodidad.		
1	G	No se como jalar la razón social y ruc del nuevo cliente		
	G	Debe de haber una base de datos (clientes) en el		
		programa y agilizar el comprobante.		
1	G	No encuentro forma de hacer la Guía de remisión		

Fuente: Rojas, Moisés (2019)

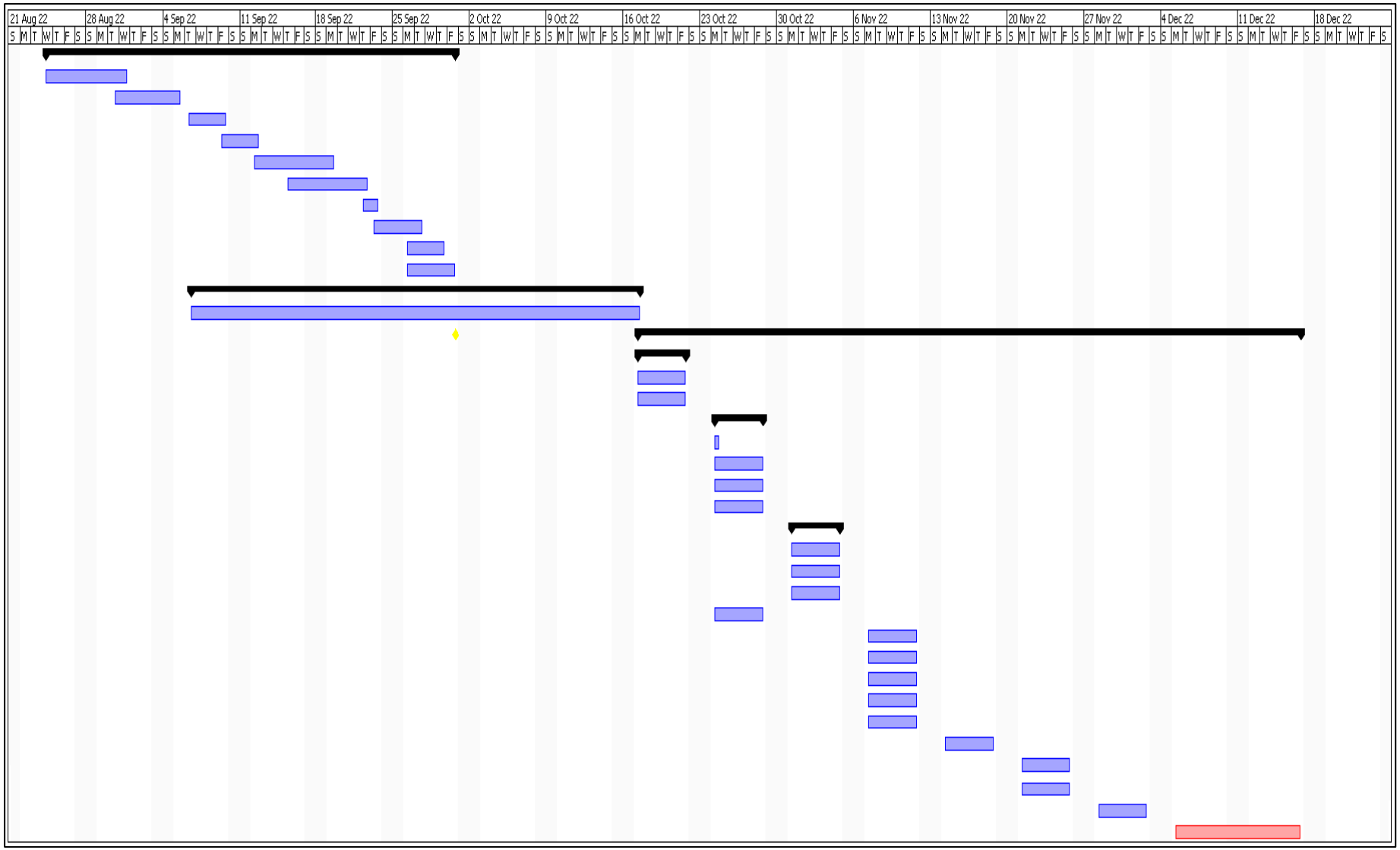
Anexo: Tabla de datos pretest

Datos pretest			
Disponibilidad			
Muestra	Transacciones Satisfactorias	Transacciones Fallidas	Metrica de Disponibilidad de las Transacciones Pre
1	1	2	-100.0000%
2	3	2	33.3333%
3	2	2	0.0000%
4	2	1	50.0000%
5	3	1	66.6667%
Total	11	8	

Promedio Pretest (media)	0.1000
Mediana	0.3333
Moda	0.0000
Desviación estandar	0.6625

Anexo: Cronograma de ejecución

		Name	Duration	Start	Finish
1		**Elección del Tema de P. I**	**28 days**	**8/24/22 8:00 AM**	**9/30/22 5:00 PM**
2		Recopilación de Información y Referencias	6 days	8/24/22 8:00 AM	8/31/22 5:00 PM
3		Planteamiento de la Problemática, Hipótesis y O.	4 days	8/30/22 2:00 PM	9/5/22 2:00 PM
4		Creación del Plan de Trabajo	4 days	9/6/22 8:00 AM	9/9/22 5:00 PM
5		Definición de Variables	2 days	9/9/22 8:00 AM	9/12/22 5:00 PM
6		Fundamentación de la Introducción	6 days	9/12/22 8:00 AM	9/19/22 5:00 PM
7		Fundamentación del Marco Teórico	6 days	9/15/22 8:00 AM	9/22/22 5:00 PM
8		Formulación de la Entrevista	2 days	9/22/22 8:00 AM	9/23/22 5:00 PM
9		Fundamentación de la Metodología	3 days	9/23/22 8:00 AM	9/27/22 5:00 PM
10		Ordenar el Trabajo	4 days	9/26/22 8:00 AM	9/29/22 5:00 PM
11		Corregir Errores	5 days	9/26/22 8:00 AM	9/30/22 5:00 PM
12		**Desarrollo del Software**	**29 days**	**9/6/22 1:00 PM**	**10/17/22 1:00 ...**
13		Desarrollo del Sistema	29 days	9/6/22 1:00 PM	10/17/22 1:00 PM
14		**Seguimiento de la Investigacion**	**45 days**	**10/17/22 8:00 ...**	**12/16/22 5:00 ...**
15		**Ejecución de Pre Test**	**5 days**	**10/17/22 8:00 ...**	**10/21/22 5:00 ...**
16		Recopilación de datos con la Ficha de Observ..	5 days	10/17/22 8:00 AM	10/21/22 5:00 PM
17		Consultas / Retroalimentacion	5 days	10/17/22 8:00 AM	10/21/22 5:00 PM
18		**Implementacion del Estímulo**	**5 days**	**10/24/22 8:00 ...**	**10/28/22 5:00 ...**
19		Implementacion del Sistema	1 day	10/24/22 8:00 AM	10/24/22 5:00 PM
20		Capacitacion a los trabajadores	5 days	10/24/22 8:00 AM	10/28/22 5:00 PM
21		Acompañamiento y consultas	5 days	10/24/22 8:00 AM	10/28/22 5:00 PM
22		Normalización	5 days	10/24/22 8:00 AM	10/28/22 5:00 PM
23		**Ejecucion del Post Test**	**5 days**	**10/31/22 8:00 ...**	**11/4/22 5:00 PM**
24		Recopilacion de datos de la Ficha de Observa..	5 days	10/31/22 8:00 AM	11/4/22 5:00 PM
25		Monitoreo	5 days	10/31/22 8:00 AM	11/4/22 5:00 PM
26		Consultas / Retroalimentacion	5 days	10/31/22 8:00 AM	11/4/22 5:00 PM
27		Exposicion de Primera Jornada	5 days	10/24/22 8:00 AM	10/28/22 5:00 PM
28		Resultado de investigacion	5 days	11/6/22 3:00 PM	11/11/22 5:00 PM
29		Análisis de Resultados	5 days	11/6/22 4:00 PM	11/11/22 5:00 PM
30		Resultado de investigacion	5 days	11/7/22 8:00 AM	11/11/22 5:00 PM
31		Análisis de Resultados	5 days	11/7/22 8:00 AM	11/11/22 5:00 PM
32		Discusión de resultados de investigación	5 days	11/7/22 8:00 AM	11/11/22 5:00 PM
33		Conclusiones y Recomendaciones de Investigac.	5 days	11/14/22 8:00 AM	11/18/22 5:00 PM
34		Correspondencia entre los Objetivos, Conclusio.	5 days	11/21/22 8:00 AM	11/25/22 5:00 PM
35		Informe preliminar de Investigación	5 days	11/21/22 8:00 AM	11/25/22 5:00 PM
36		Revision de Informe de Investigación	5 days	11/28/22 8:00 AM	12/2/22 5:00 PM
37		Exposición de Segunda Jornada de Investigación	10 days	12/5/22 8:00 AM	12/16/22 5:00 PM

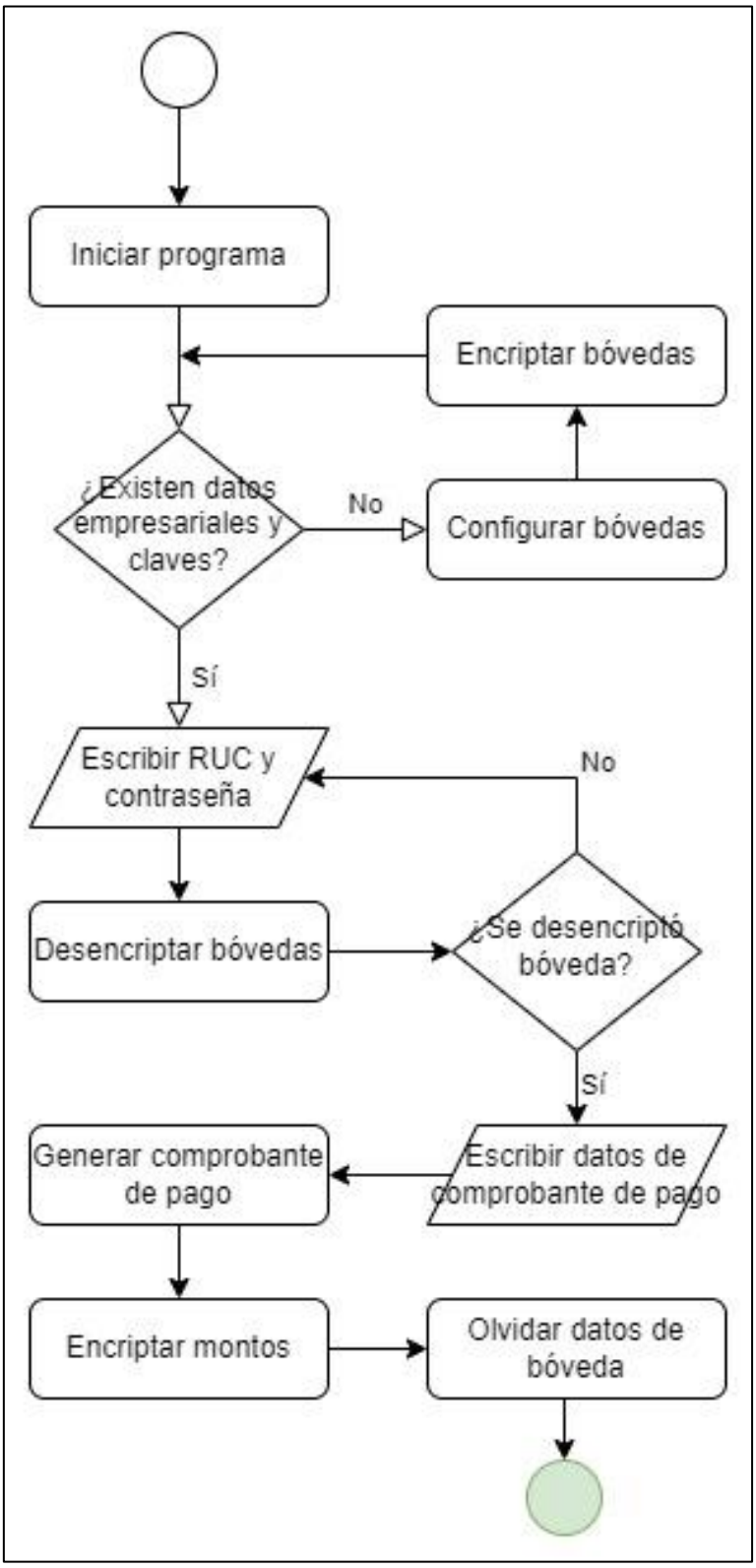

21 Aug 22
28 Aug 22
4 Sep 22
11 Sep 22
18 Sep 22
25 Sep 22
2 Oct 22
9 Oct 22
16 Oct 22
23 Oct 22
30 Oct 22
6 Nov 22
13 Nov 22
20 Nov 22
27 Nov 22
4 Dec 22
11 Dec 22
18 Dec 22

Anexo: Matriz de consistencia.

SISTEMA DE ENCRIPTACIÓN HOMOMÓRFICA PARA FORTALECER LA SEGURIDAD DE DATOS EN LAS TRANSACCIONES DE VENTAS EN LUGAR EXPRESIVO SAC

PROBLEMA	OBJETIVOS	HIPOTESIS	Variable Independiente: X = SISTEMA DE ENCRIPTACIÓN HOMOMÓRFICA					
Problema principal	**Objetivo principal**	**Hipótesis principal**	**Variable**	**Definición conceptual**	**Definición Operacional**	**Dimensión**	**Indicadores**	**Escala de medición**
¿Cómo la seguridad de los datos en las transacciones de ventas mejora con el sistema de encriptación homomórfica en Lugar expresivo SAC?	Fortalecer la seguridad de los datos en las transacciones de ventas mediante el sistema de encriptación homomórfica en Lugar Expresivo SAC	El fortalecimiento de la seguridad de datos en las transacciones de ventas mejora con el sistema de encriptación homomórfica en Lugar Expresivo SAC	SISTEMA DE ENCRIPTACIÓN HOMOMÓRFICA	La encriptación homomórfica tiene las propiedades de realizar operaciones sobre texto directamente sin necesidad alguna de descifrarlos. Rugel (2019). Una suma de operaciones matemáticas que se pueden realizar sobre las versiones cifradas dentro de la información. García, van de Graaf y Montejano (2018)	Sistema automatizado encargado de almacenar información de manera local y remota aplicando encriptación homomórfica, el cual tiene como finalidad la protección de toda información ingresada al momento de realizar una transacción de ventas por medio de un comprobante de pago electrónico.			
Problemas específicos	**Objetivos específicos**	**Hipótesis específicos**	**Variable Dependiente: Y = SEGURIDAD DE DATOS EN LAS TRANSACCIONES DE VENTAS**					
			Variable	**Definición conceptual**	**Definición Operacional**	**Dimensión**	**Indicadores**	**Escala de medición**
¿El sistema de encriptacion homomórfica mejora la disponibilidad de la seguridad de datos en las transacciones de ventas en Lugar expresivo SAC?	El sistema de encriptación homomórfica mejora la dispobilidad de la seguridad de datos en las transacciones de ventas en lugar expresivo SAC	El sistema de encriptación homomórfica mejorará la disponibilidad de la seguridad de datos en las transacciones de ventas en lugar expresivo SAC	SEGURIDAD DE DATOS EN LAS TRANSACCIONES DE VENTAS	La seguridad de datos cuenta con controladores técnicos y administrativos que protegen datos ante todo tipo de amenazas. (Beynon, 2018). son un conjunto de controles que protegen la disponibilidad, integridad y confidencialidad que actúan frente a amenazas y vulnerabilidades presentadas. (Narváez y Yungán,2022)	Se deben adoptar medidas para proteger la información de un negocio para garantizar la integridad, disponibilidad y confidencialidad ya que esta información es un activo valioso. Contero (2019)	Disponibilidad	Métrica de Disponibilidad de las Transacciones. (Rojas, 2019)	Razón [0 - 1] Transaccion Satisfactoria Transaccion Fallida
¿El sistema de encriptacion homomórfica mejora la integridad de la seguridad de datos en las transacciones de ventas en Lugar expresivo SAC?	El sistema de encriptación homomórfica mejora la integridad de la seguridad de datos en las transacciones de ventas en lugar expresivo SAC	El sistema de encriptación homomórfica mejorará la integridad de la seguridad de datos en las transacciones de ventas en lugar expresivo SAC				Integridad	Métrica de Integridad de las Transacciones (Rojas, 2019)	
¿El sistema de encriptacion homomórfica mejora la confidencialidad de la seguridad de datos en las transacciones de ventas en Lugar expresivo SAC?	El sistema de encriptación homomórfica fortalece la confidencialidad de la seguridad de datos en las transacciones de ventas en lugar expresivo SAC	El sistema de encriptación homomórfica mejorará la confidencialidad de la seguridad de datos en las transacciones de ventas en lugar expresivo SAC				Confidencialidad	Métrica de Confidencialidad de las Transacciones (Rojas, 2019)	

Anexo: Diagrama de flujo del sistema



- **Descripción de módulos**

Módulo de configuración de bóvedas

En este módulo se podrá realizar el siguiente proceso:

a. Almacenar llaves para generar firma de comprobante de pago.
b. Almacenar llaves para el algoritmo de encriptación homomórfica.
c. Almacenar los datos de la organización.

Módulo de encriptación

En este módulo se podrá realizar el siguiente proceso:

a. Encriptar datos del sistema con una clave simétrica en una bóveda.
b. Desencriptar datos del sistema con una clave simétrica en una bóveda.
c. Olvidar las llaves de la bóveda.

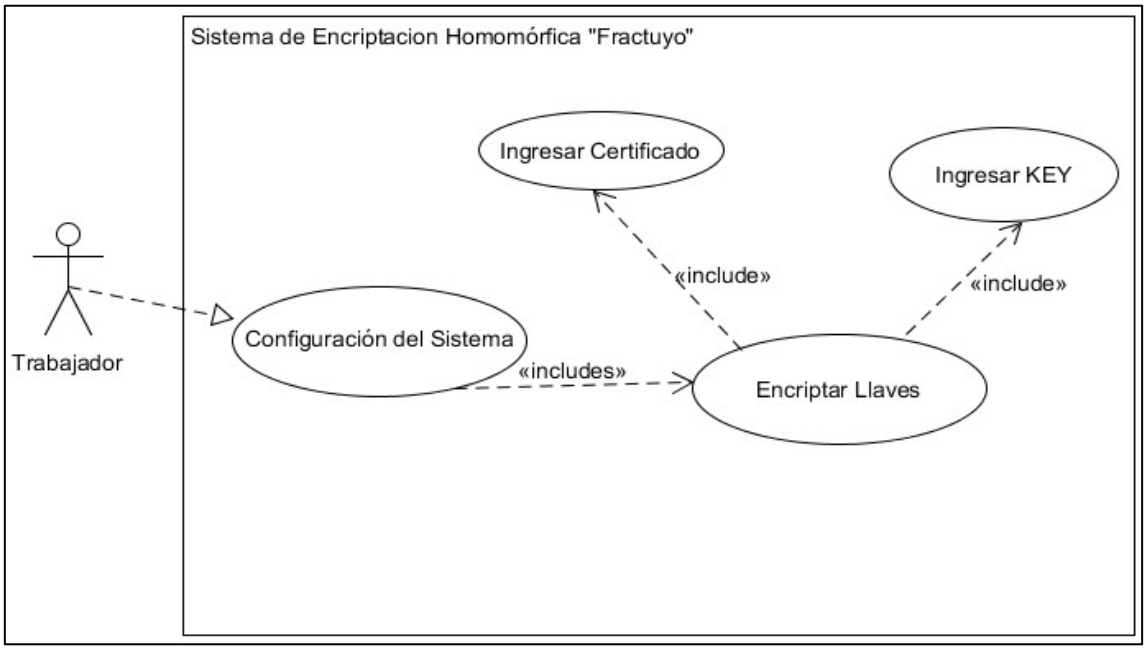
Módulo de facturación

En este módulo se podrán realizar los siguientes procesos:

a. Guardar Factura.
b. Imprimir Factura.

Anexo: Diagrama de casos de uso

- **Caso de uso configuración del sistema**



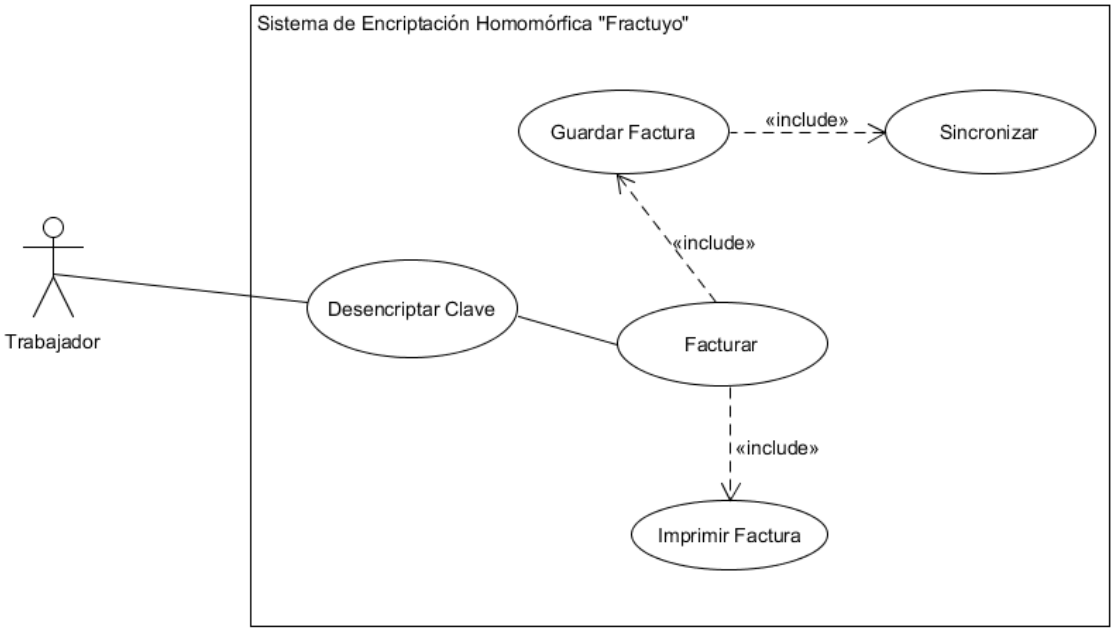
Fuente: elaboración propia

Descripción del caso de uso configuración del sistema

Cu:	**Cu_01**
Descripción:	Proceso de facturación
Condiciones:	El sistema debe estar en funcionamiento.
	El usuario debe desencriptar los datos de configuración.
Escenarios:	Se procede a llenar los campos por obligación.
	Elegir la ruta de ubicación del directorio de trabajo.
	Encriptar los datos escritos en un archivo llamado bóveda.

fuente: elaboración propia

- **Caso de uso facturación**



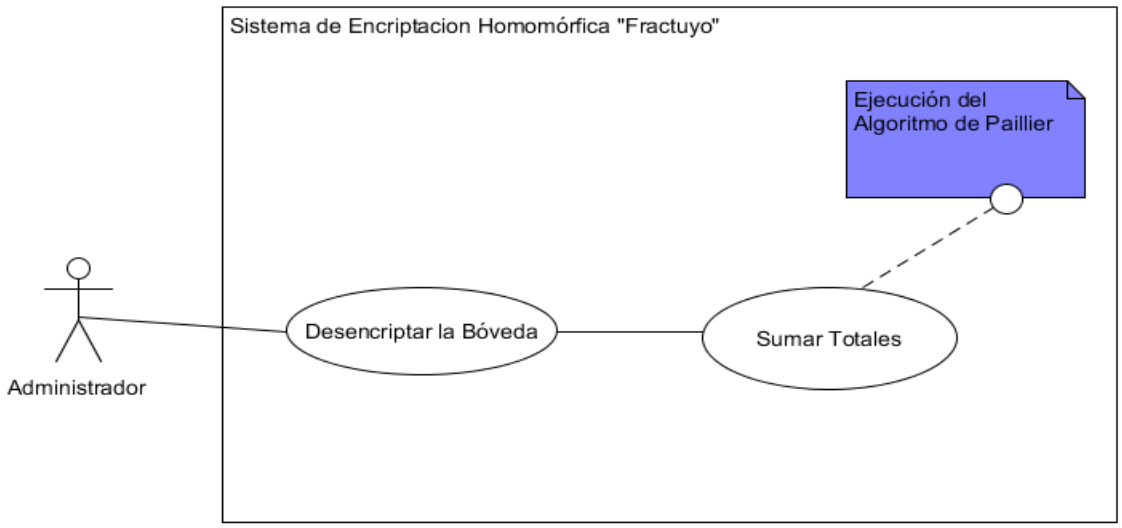
Fuente: elaboración propia

Descripción del caso de uso facturación

Cu:	**Cu_02**
Descripción:	Proceso de configuración del sistema
Condiciones:	El sistema debe estar en funcionamiento.
Escenarios:	a. Se procede a llenar los campos por obligación.
	b. Seleccionar el botón facturar.
Post condición:	Seleccionar botón “candado” al finalizar una cantidad n de facturas que estén en cola.

fuente: elaboración propia

- **Caso de uso reporte mensual**



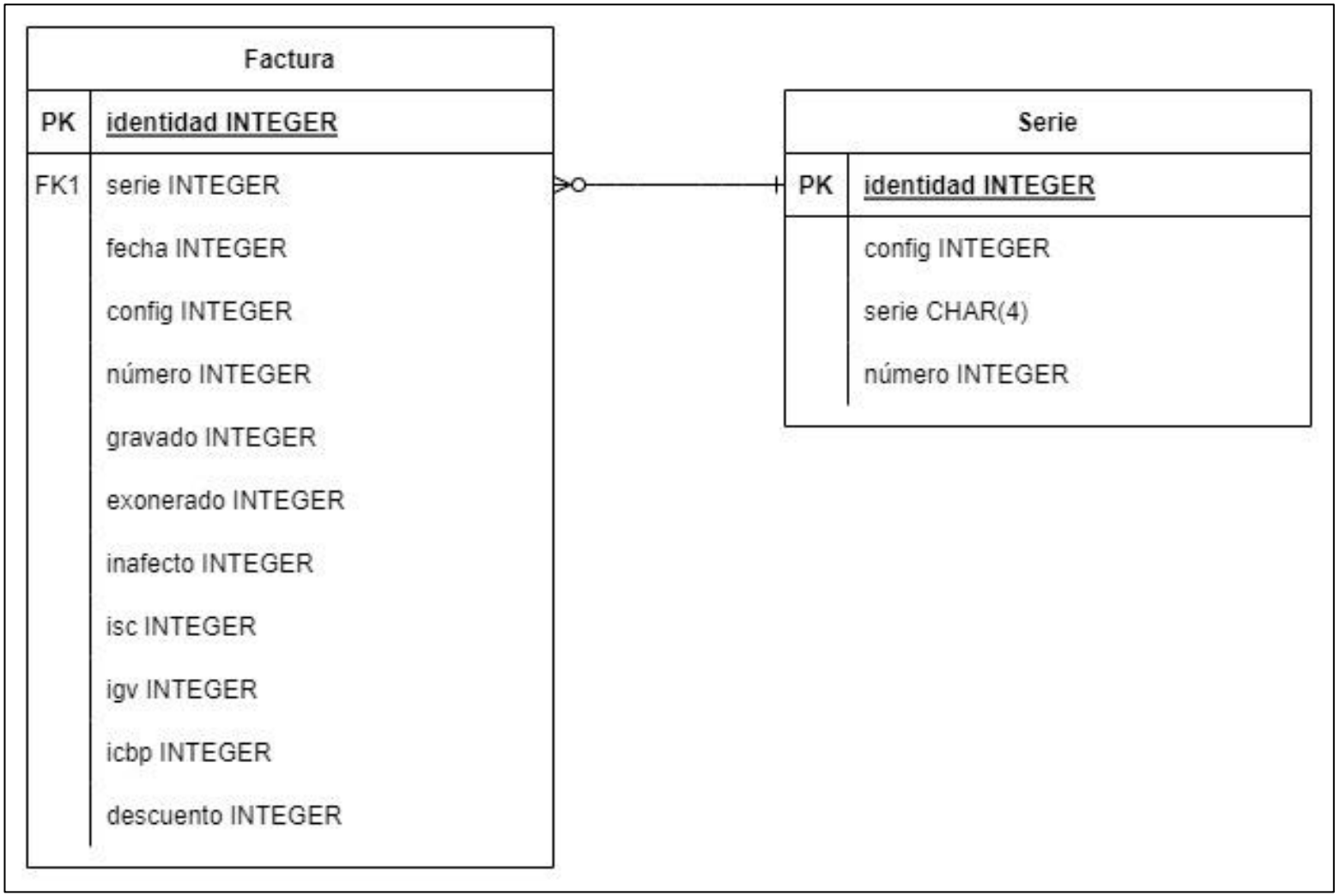
Fuente: elaboración propia

Descripción del caso de uso reporte mensual

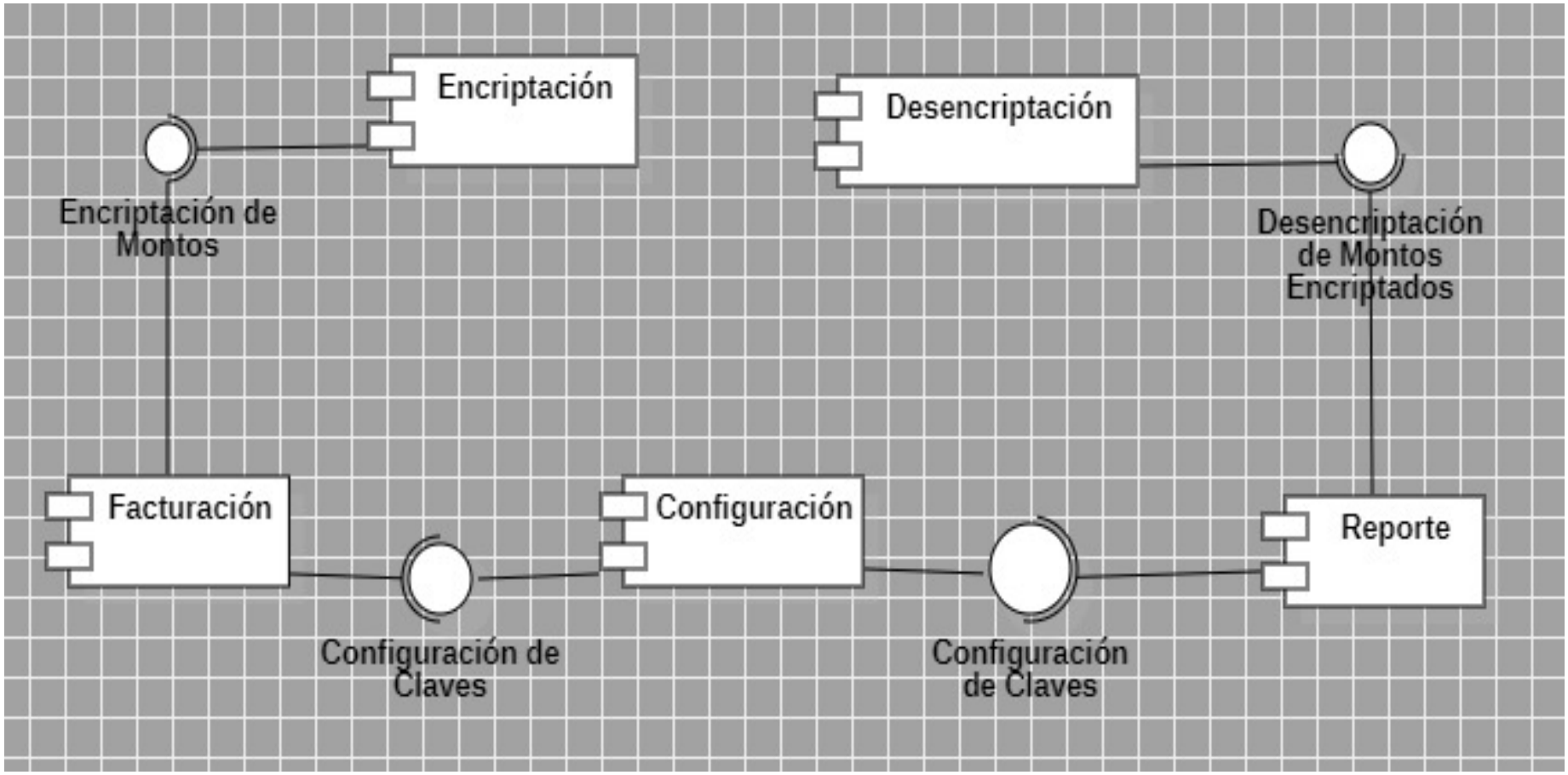
Cu:	**Cu_03**
Descripción:	Proceso de reporte mensual
Condiciones:	El sistema debe estar en funcionamiento.
	El usuario debe desencriptar los datos de la bóveda.
Escenarios:	a. Elegir el periodo necesitado para generar el reporte.
	b. Seleccionar botón reportar.

fuente: elaboración propia

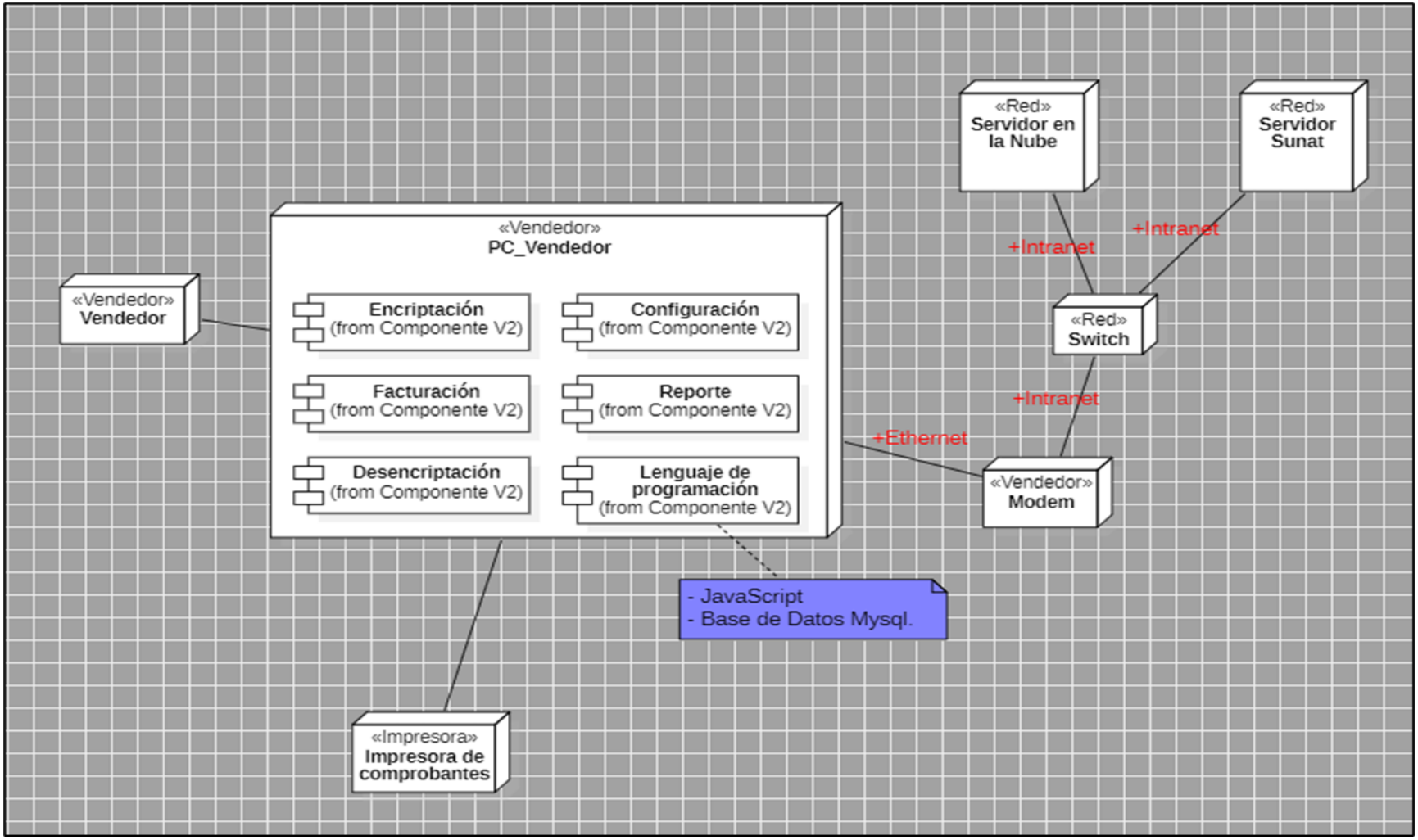
Anexo: Modelo de datos



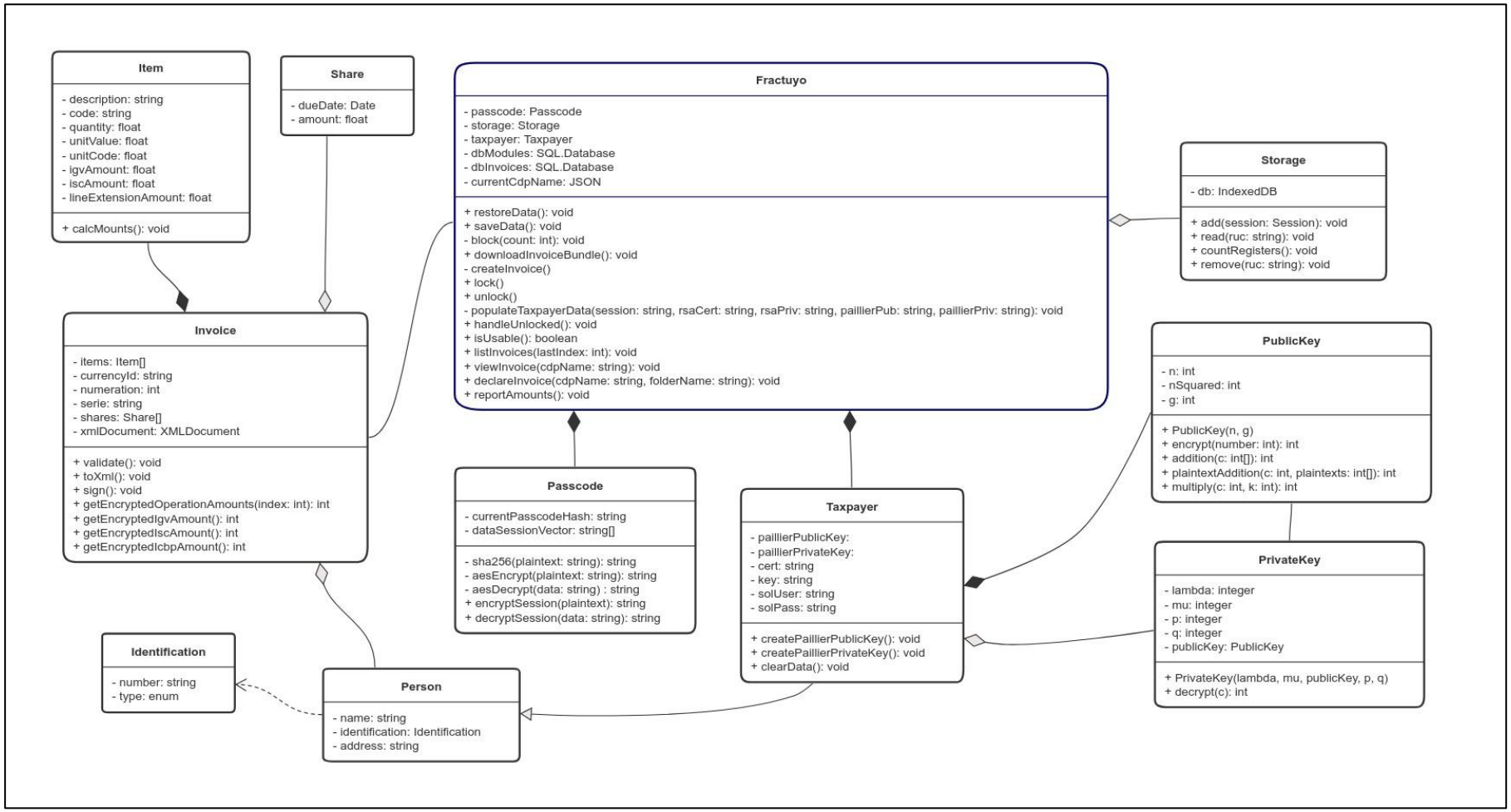
Anexo: Diagrama de componentes



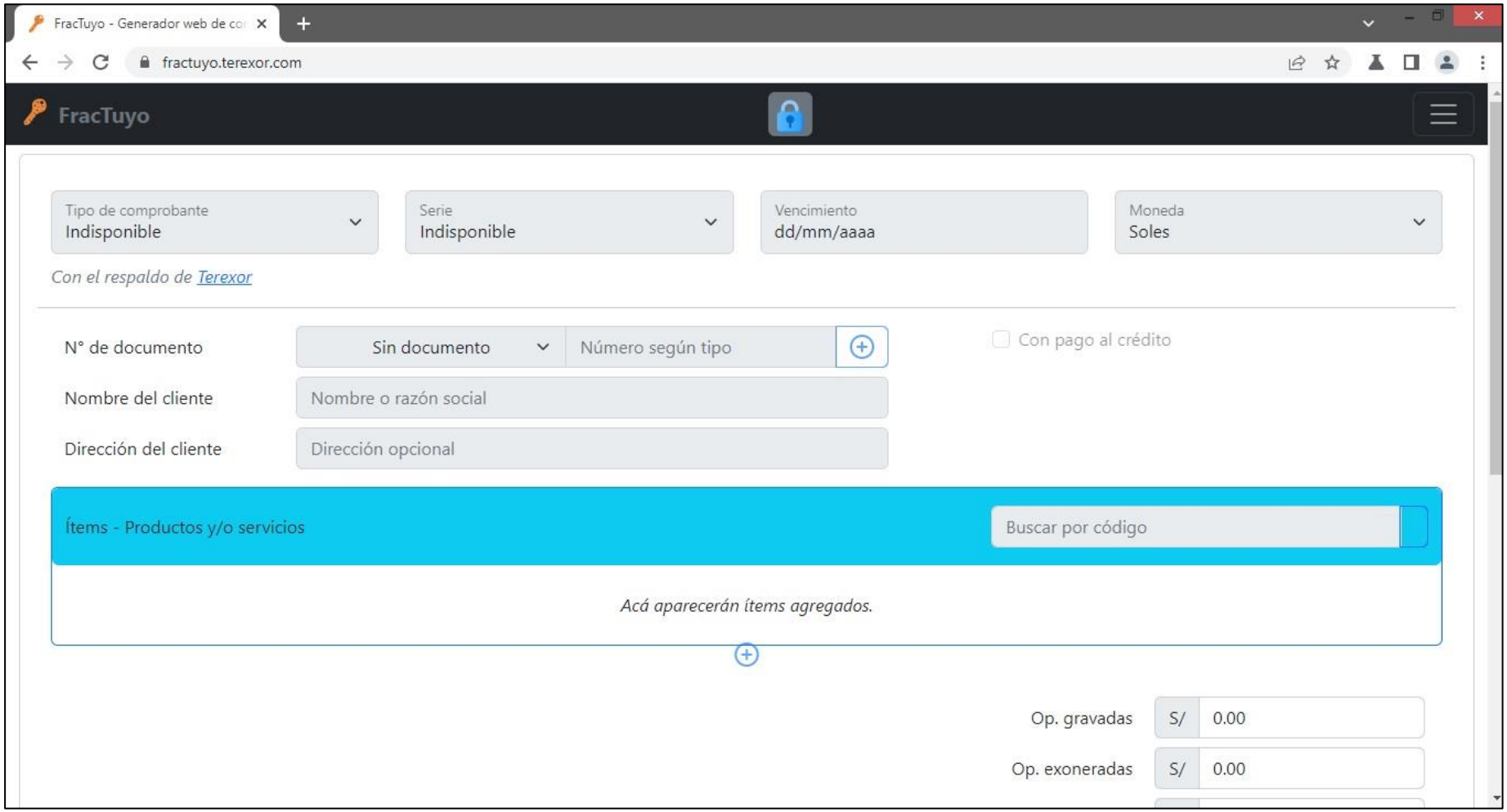
Anexo: Diagrama de despliegue

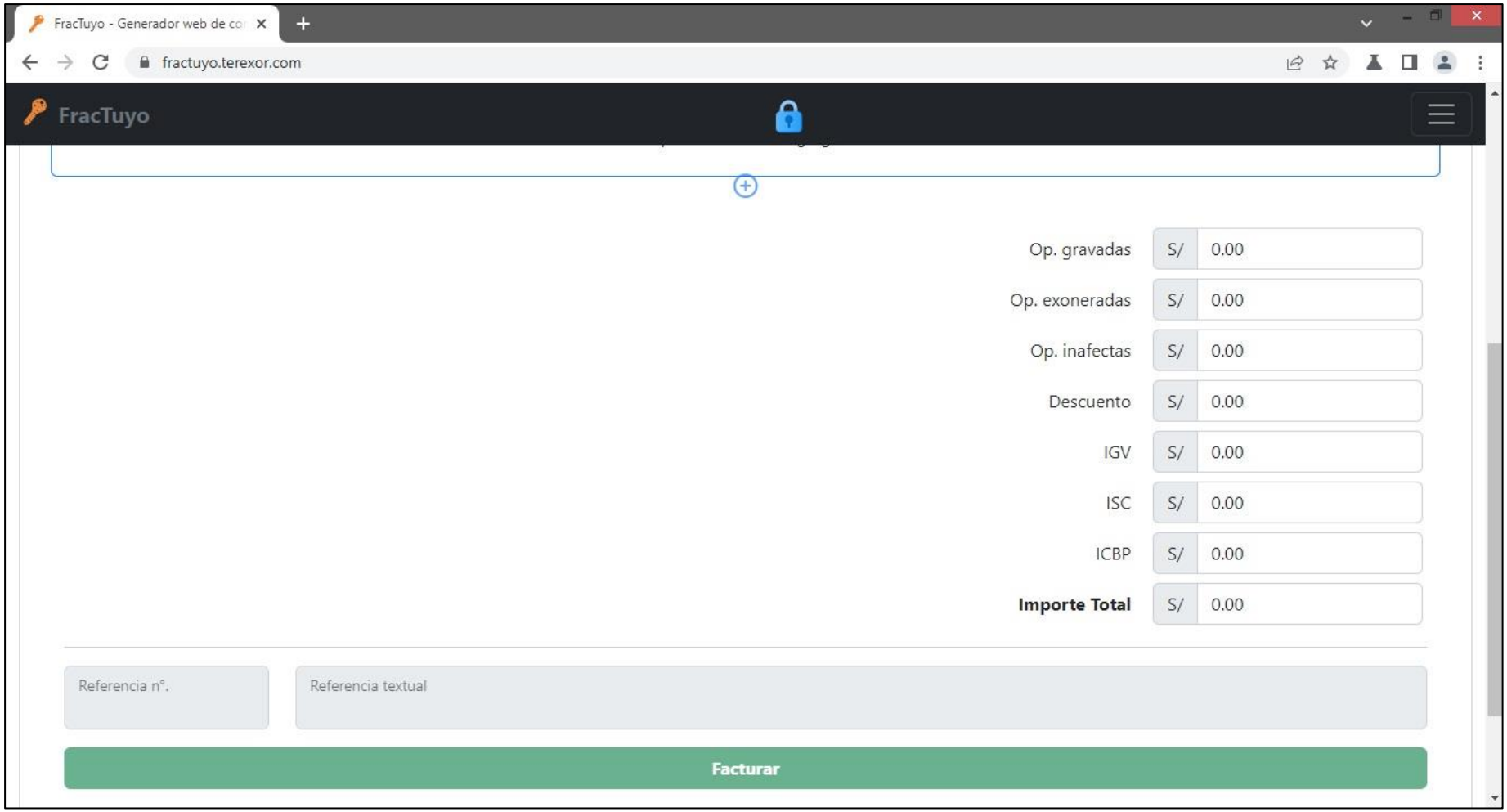


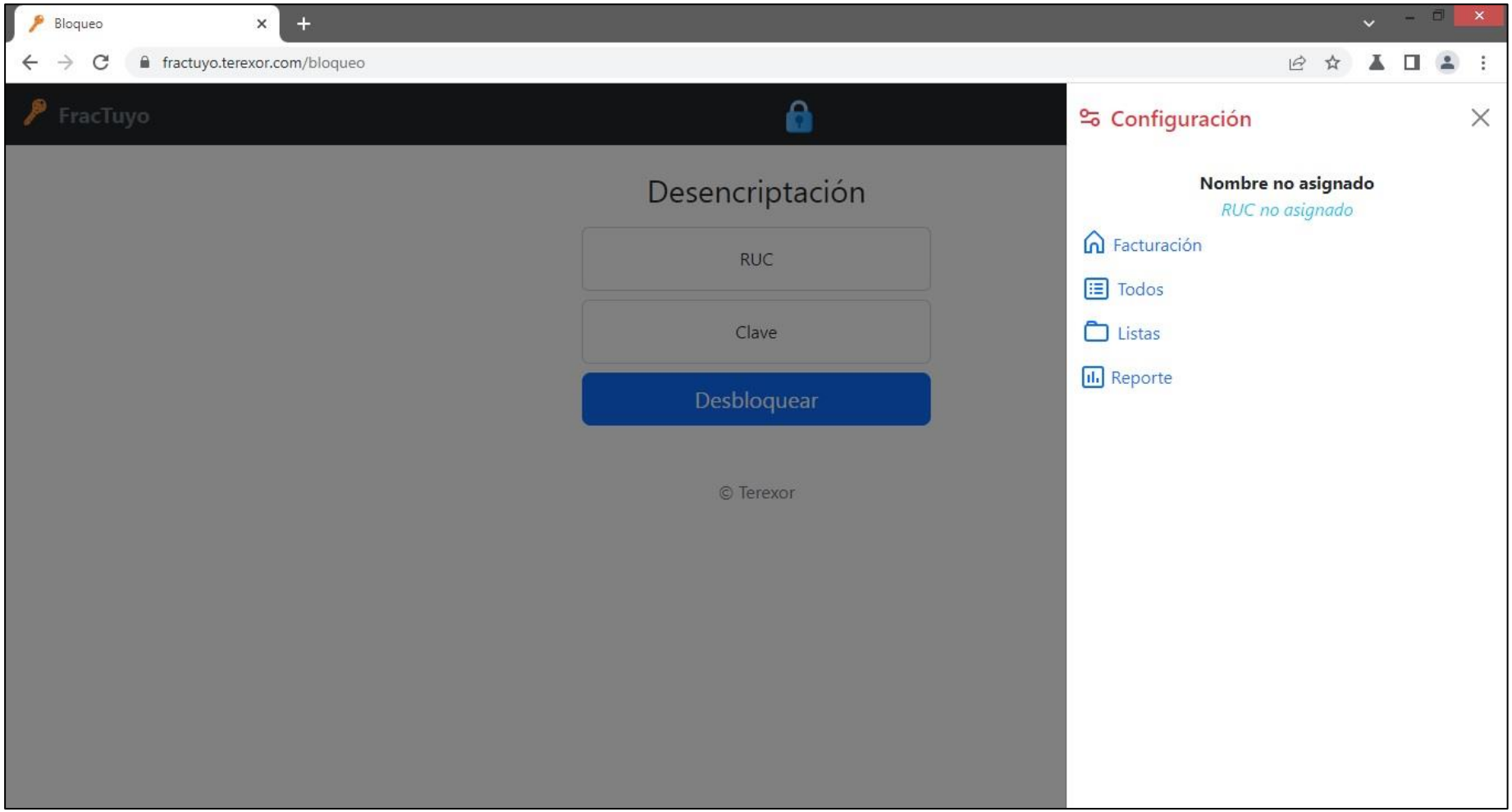
Anexo: Diagrama de clases



Anexo: Interfaz gráfica del usuario




FracTuyo - Generador web de co
fractuyo.terexor.com
FracTuyo
Op. gravadas S/ 0.00
Op. exoneradas S/ 0.00
Op. inafectas S/ 0.00
Descuento S/ 0.00
IGV S/ 0.00
ISC S/ 0.00
ICBP S/ 0.00
Importe Total S/ 0.00
Referencia n°.
Referencia textual
Facturar


Bloqueo
fractuyo.terexor.com/bloqueo
FracTuyo
Desencriptación
RUC
Clave
Desbloquear
© Terexor
Configuración
Nombre no asignado
RUC no asignado
Facturación
Todos
Listas
Reporte

Anexo: Carta de autorización

Lima, 10 de octubre de 2022

Señores

Escuela Profesional de Ingeniería

Universidad César Vallejo – Campus Lima Este

A través del presente, yo Luis Antenor Gamo Acuña, identificado (a) con DNI N° 09320067 representante de la empresa **Lugar Expresivo SAC,** con el cargo de Gerente, me dirijo a su representante a fin de dar a conocer que los siguientes estudiantes:

- **Garro Murillo, George Anthonny Vicente** (Orcid.org/0000-0001-7461-8557).
- **Navarro Torres, Luis Reynaldo** (Orcid.org/0000-0003-4513-577X).

Se encuentran autorizados para:

a. Recoger datos de nuestra organización con el fin de la realización de su proyecto y posterior tesis titulada **Sistema de encriptación homomórfica para fortalecer la seguridad de datos en las transacciones de ventas en Lugar Expresivo SAC.**

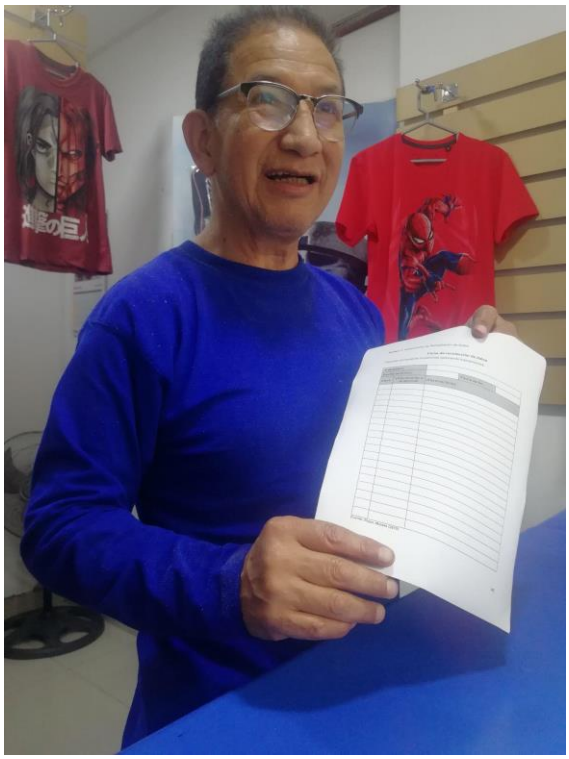
b. Disponer del nombre de nuestra organización dentro de su tema de trabajo.

Atentamente:

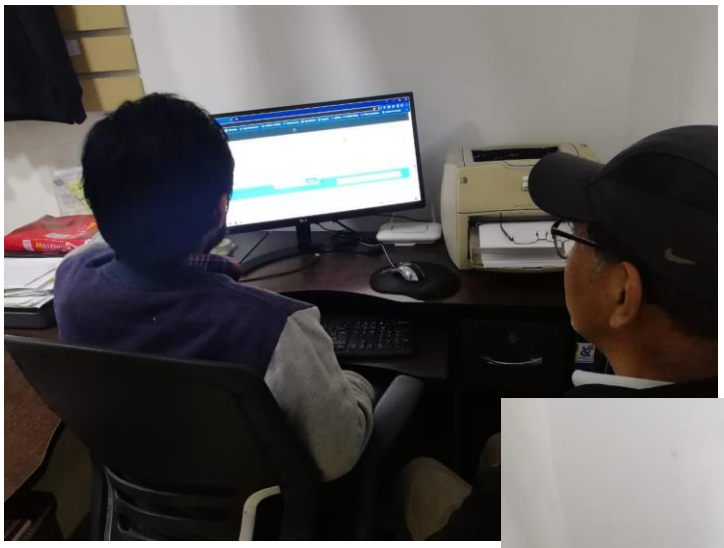
LUGAR EXPRESIVO Arte & Publicidad

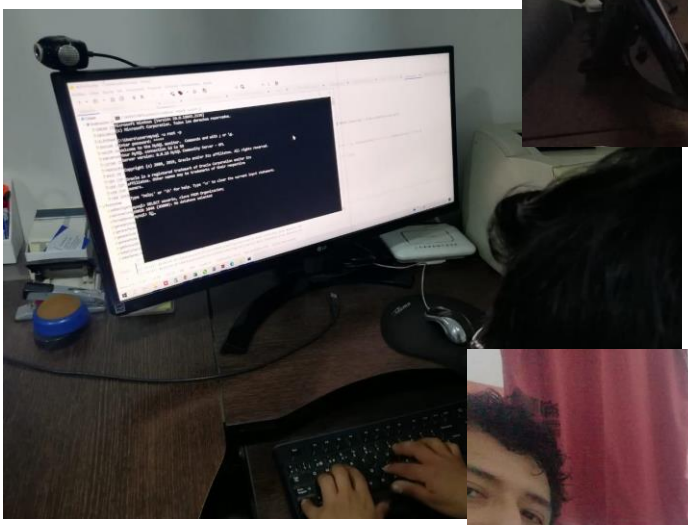
Firma y Sello

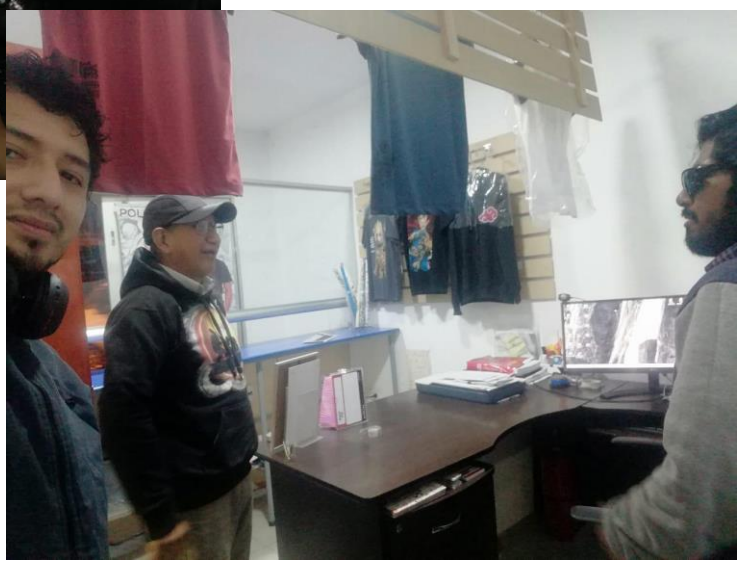
Anexo: Interacción con el gerente pretest



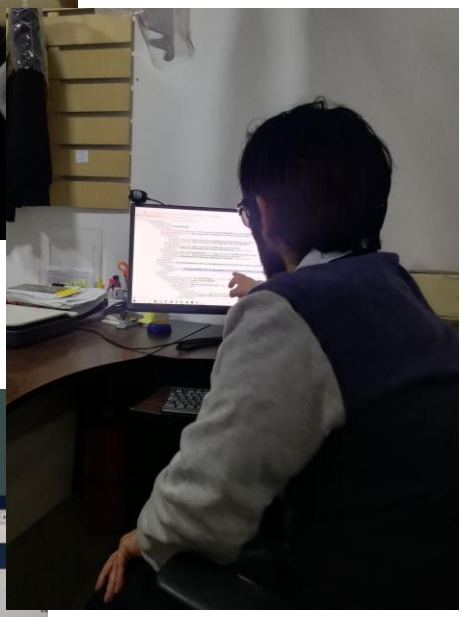
Anexo: Implementación del estímulo

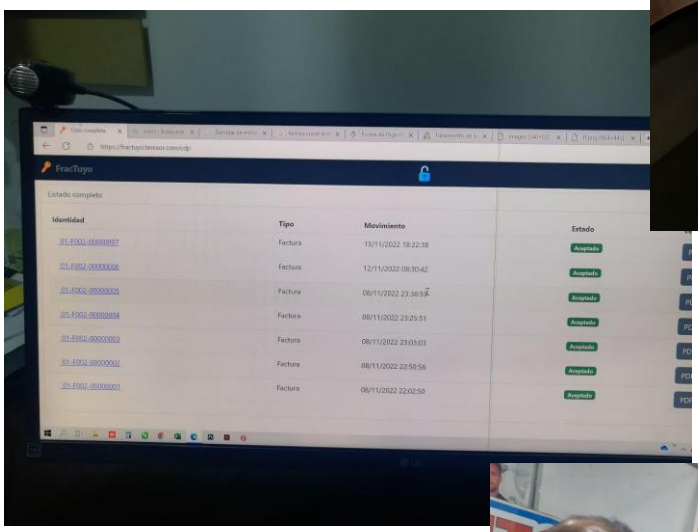


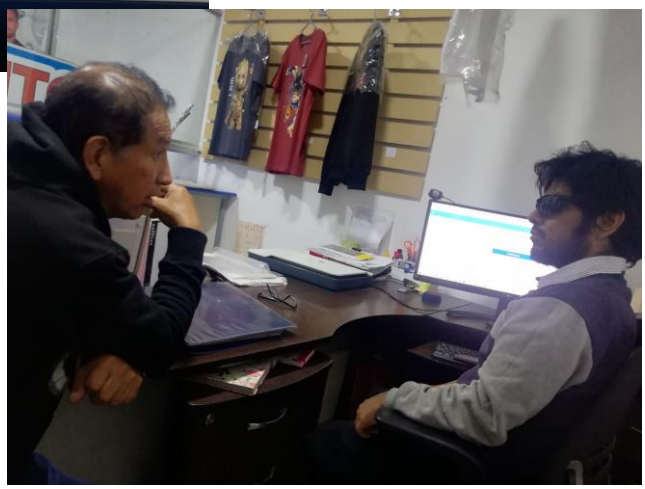




Anexo: Recopilación de datos postest







UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, ERICK GIOVANNY FLORES CHACÓN, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, asesor de Tesis titulada: "SISTEMA DE ENCRIPTACIÓN HOMOMÓRFICA PARA FORTALECER LA SEGURIDAD DE DATOS EN LAS TRANSACCIONES DE VENTAS EN LUGAR EXPRESIVO SAC", cuyos autores son NAVARRO TORRES LUIS REYNALDO, GARRO MURILLO GEORGE ANTHONNY VICENTE, constato que la investigación tiene un índice de similitud de 14.00%, 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, 01 de Diciembre del 2022

Apellidos y Nombres del Asesor:	**Firma**
ERICK GIOVANNY FLORES CHACÓN **DNI:** 07964931 **ORCID:** 0000-0002-4028-8059	Firmado electrónicamente por: EFLORESCH01 el 04-12-2022 10:22:09

Código documento Trilce: TRI - 0466811

INVESTIGA UCV