ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN

INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Biometría Facial en la mejora del Proceso de Autenticación del Usuario en una Notaría Pública, Lima 2022

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

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

AUTOR:

Espinoza Beramendi, Juan Royer (orcid.org/0000-0001-6148-7973)

ASESOR:

Dr. Visurraga Agüero, Joel Martin (orcid.org/0000-0002-0024-668X)

CO - ASESOR:

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

LÍNEA DE INVESTIGACIÓN:

Sistemas de Información y Comunicaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA — PERÚ

2023

Dedicatoria

A mis queridos padres, por su apoyo incondicional y amor; por ser siempre mis grandes consejeros.

A mi esposa por su apoyo, amor y comprensión.

A mis hijas Aliz y Emma, porque son mi motor de vida.

Agradecimiento

A mis hijas y esposa, porque siempre me motivan a ser un mejor profesional y cumplir todas mis metas.

Índice de contenidos

Índice de tablas

Índice de gráficos y figuras

Resumen

En la actualidad las notarías deben contar con mecanismos de seguridad en los procesos de autenticación del usuario para asegurar la integridad jurídica en los servicios que ofrece.

Como objetivo general es determinar de qué manera la biometría facial mejora el proceso de autenticación del usuario en una notaría pública, Lima 2022.

Mediante esta tesis se mide los resultados del modelo tradicional de la autenticación biométrica dactilar vs la autenticación biométrica facial aplicada en la variable dependiente, para poder así identificar la mejora mediante los indicadores de validaciones con error, tiempo de consulta y riesgo de fallas. El tipo de investigación es aplicada y el diseño de investigación es experimental del tipo pre-experimental. La población es de 50 observaciones, como muestra a 50 observaciones obtenidas mediante el muestreo probabilístico aleatorio. La técnica de recolección de datos es la observación y como instrumento de recolección de datos es la guía de observación.

Se concluye que la implementación de la biometría facial mejora el proceso de autenticación de usuario, el primer indicador mejoró el 22.92% de las validaciones con error, el segundo mejoro el tiempo de consulta en 0:57 segundos, y el tercero mejoro el riesgo de fallas en 8.6666%.

Palabras clave: biometría facial, autenticación del usuario, mecanismos de seguridad.

Abstract

Currently, notary public offices must have security mechanisms in the user authentication process to ensure the legal integrity of the services offered.

The general objective is to determine how facial biometrics improves the user authentication process in a notary public's office, Lima 2022.

This thesis measures the results of the traditional model of fingerprint biometric authentication vs. facial biometric authentication applied to the dependent variable, in order to identify the improvement through the indicators of validations with error, consultation time and risk of failure. The type of research is applied and the research design is experimental of the pre-experimental type. The population is 50 observations, with a sample of 50 observations obtained by random probability sampling. The data collection technique is observation and the data collection instrument is the observation guide. It is concluded that the implementation of facial biometrics improves the user authentication process, the first indicator improved 22.92% of the validations with error, the second improved the query time by 0:57 seconds, and the third improved the risk of failure by 8.6666%.

Keywords: facial biometrics, user authentication, security mechanisms.

I. INTRODUCCIÓN

Actualmente se afronta un problema de seguridad en el proceso de autenticación del usuario que es la usurpación de identidad, que cada vez afecta a más personas a nivel mundial y es que aun en muchos países no se ha logrado contrarrestar este delito que perjudica a las personas despojándolas de sus propiedades que podrían ser una casa, un auto y hasta acciones de una empresa.

A nivel internacional la delincuencia y el crimen organizado han demostrado que vulnerar la autenticación de los usuarios ha sido algo sencillo, por tal razón las empresas refuerzan sus mecanismos de seguridad para autenticar a las personas y puedan estar completamente seguras que las personas sean las que dicen ser. En Colombia se ha comprobado que estas técnicas se pueden obtener por un muy bajo costo, incluso hay mucha información en internet de cómo hacerlo. Por todo esto muchos países desarrollados cambiaron la forma de autenticar a los usuarios e implementaron tecnologías más sofisticadas tales como reconocimiento con biometría facial, el de iris y voz, y entre las instituciones de alta seguridad como instalaciones militares, prisiones de máxima seguridad, bóvedas de bancos mundiales, usan las 3 en simultáneo. Gracias a la autenticación del usuario empleado con la tecnología del reconocimiento facial se ha logrado identificar y capturar a más de 650 delincuentes con orden de captura internacional, gracias al cambio de la biometría dactilar por la biometría facial instalada en los aeropuertos, colegios, centros comerciales, notarías, entre otros establecimientos. En Estonia las notarías ya identifican a los usuarios con biometría facial implementadas desde su página web, tanto cuando es a distancia, como presencialmente en el local, mediante una cámara o app del celular. Durante la pandemia del Covid-19, las organizaciones optaron por un cambio en la autenticación de sus empleados, para minimizar el contacto y así prevenir posibles contagios, muchos optaron por la tecnología de biometría facial, mientras que otros por la de iris ya que

eran las que tenían un contacto cero con el dispositivo. Leca (2022) demostró en su aplicación móvil de reconocimiento facial una mejora del 7% de neonatos autenticados, la cual redujo los contagios de COVID-19 que ya habían sucedió cuando no usaban la aplicación.

A nivel nacional, el problema de autenticación ha tenido su principal problema en la usurpación de identidad de los usuarios el cual ha traído grandes perjuicios económicos a los usuarios, sobre todo en los sectores bancarios, según el INEI (2021) indica que la usurpación de identidad tiene 8680 de casos denunciados en el año 2020 y van en aumento. Otro problema común es que los mecanismos de autenticidad no son los adecuados, existen diferentes maneras de autenticar una persona mediante la tecnología, cada una de ellas tiene un riesgo, un costo, y muchas empresas por no gastar en invertir en tecnología no usan los mecanismos apropiados el cual perjudica en la confiabilidad de los procesos de autenticación de los usuarios.

En las notarías se comenzaron a presentar problemas con las personas que tienen las huellas maltratadas y borrosas, porque el sistema que se usa actualmente que es de biometría dactilar no las autenticaba, el resultado era negativo a pesar que teníamos la certeza de que si eran las personas porque ya eran clientes antiguos, entonces estos usuarios teníamos que intentar muchas veces hasta que el sistemas les acepte las huellas y sino tenían que acercarse a RENIEC para actualizar sus huellas que están maltratadas y/o traer una constancia el cual acreditaban ser la persona que indicaba con su documento de identidad, esto causaba molestias a los usuarios y múltiples quejas; otros casos especiales eran con las personas que perdían sus dedos y el sistema exigía tales huellas, el mismo camino tenían que ir a la oficina de RENIEC a manifestar que ya no contaban con dicho dedo y/o mano que por accidente ya no lo tenían, para que actualicen en el sistema y el lector exija otra huella. Otro problema es por las caídas del servidor las cuales en muchas ocasiones ha causado que los clientes desistan del servicio notarial, causando pérdidas económicas a la notaría, ya que la ley del notariado dice que se debe contar

con la consulta biométrica dactilar o el servicio no podrá continuar su trámite, bajo este mandato se le tiene que devolver el dinero o no aceptar nuevos clientes hasta que se restablezca la conexión con el servidor de RENIEC, también presentaban fallas del cableado del lector biométrico, cada cierto sufría un desgaste y había que llevar para su mantenimiento, en algunas ocasiones también la ausencia del servicio de internet ocasionaba que no se pueda usar el sistema de autenticación ya que se conecta con RENIEC; asimismo, el acceso al servicio de autenticación biométrica dactilar toma un tiempo entre el ingreso, registro de huellas de una huella por cada mano y la validación de las dos huellas, lo cual si tenemos más de cinco usuarios en una sola operación se vuelve largo el proceso y sumándole a que muchas veces los usuarios tienen huellas maltratadas y hay que realizar varios intentos para cerciorarse que la autenticación del usuario no sea rechazada, esto nos lleva a demorar la operación causando muchas molestias a los usuarios, finalmente, está el riesgo latente de que un usuario consiga suplantar la identidad de otra usando las famosas gomas o implantes de tela en sus huellas y así usurpar la identidad de otro, ya que el lector no sería capaz de detectarlo, esto implica un gran riesgo para la seguridad jurídica en el oficio notarial y para el usuario a quien estén suplantando, un problema que hasta la fecha no ha podido ser controlado, existen algunas medidas de prevención pero muchas veces no se cumple por parte del personal y la notaría se expone a un riesgo de usurpación de identidad a pesar de haber cumplido con el correcto proceso de autenticar al usuario.

Dada la trascendencia de la realidad del problema de la investigación, se propone como problema general la siguiente pregunta: ¿De qué manera la biometría facial mejora el proceso de autenticación del usuario en una notaría pública, Lima 2022?

Asimismo, se propone como problemas específicos las siguientes preguntas: (i) ¿De qué manera la biometría facial mejora el indicador de la cantidad de validaciones con errores en el proceso de autenticación del usuario en una notaría pública, Lima 2022? (ii), ¿De qué manera la biometría facial mejora el

indicador tiempo de consulta en el proceso de autenticación del usuario en una notaría pública, lima 2022? (iii) y ¿De qué manera la biometría facial mejora el indicador porcentaje de riesgo de fallas en el proceso de autenticación del usuario en una notaría pública, Lima 2022?

Respecto a las justificaciones de esta investigación, la justificación epistemológica se basa en validar a una persona, en autenticarla de una forma más eficaz y segura, mediante el uso de la tecnología de biometría facial que reemplazará a la biometría dactilar que es la que se usa actualmente y que la biometría facial buscará mejorar todos los problemas que se viene experimentado con la biometría dactilar.

Además, en la justificación teórica se realiza con la idea de aportar conocimiento en búsqueda de la mejora del servicio de autenticación del usuario en una notaría pública, el cual va a generar conocimiento en cuanto a la autenticación de usuario, y de sus diferentes formas de autenticar a un usuario, de sus debilidades, fallas, así como sus fortalezas y ventajas de su nivel de riesgo y sus mejoras ante las tecnologías anteriores, de esta manera quedaría comprobado que el uso de la biometría facial mejora la autenticación del usuario.

Asimismo, en la justificación práctica, la biometría facial puede ser usada con un dispositivo móvil, la cual todos poseen, además nos da la ventaja de poder mover el equipo hacia la persona y ya no la persona hacia el lector lo que la hace más portátil y cómoda para el usuario, algo que la biometría dactilar lo permite pero con ciertas limitaciones y requiere de otros accesorios para completar esta tarea, tales como una laptop y además que la Aplicación móvil de reconocimiento con biometría facial hasta la fecha no ha registrado ninguna caída de su servicio.

Finalmente, en la justificación metodológica, para la mejora del proceso de autenticación del usuario mediante biometría facial se aplicó el método científico, asimismo, se utilizó un tipo de diseño experimental, por lo tanto, la

variable independiente es manipulada intencionalmente con el propósito de observar y posteriormente medir todos sus efectos respecto a la variable dependiente y así poder determinar la mejora. El software de Biometría facial una vez validado los resultados podrían usarse en diversas notarias.

Una vez planteados todos los problemas de la investigación y con el propósito de obtener las posibles soluciones, se plantea como objetivo general: Determinar de qué manera la biometría facial mejora el proceso de autenticación del usuario en una notaría pública, Lima 2022.

De la misma manera, como objetivos específicos (i) Determinar de qué manera la biometría facial mejora el indicador cantidad de validaciones con errores en el proceso de autenticación del usuario en una notaría pública, Lima 2022 (ii) Determinar de qué manera la biometría facial mejora el indicador tiempo de consulta en el proceso de autenticación del usuario en una notaría pública, Lima 2022 y (iii) Determinar de qué manera la biometría facial mejora el indicador porcentaje de riesgo de fallas en el proceso de autenticación del usuario en una notaría pública, Lima 2022.

Luego de los objetivos planteados, se realiza la hipótesis de los posibles resultados que se obtendrá en la investigación, se formula la hipótesis general: la biometría facial mejora significativamente el proceso de autenticación del usuario en una notaría pública, Lima 2022.

Asimismo, se plantean las hipótesis específicas: (i) la biometría facial mejora significativamente la cantidad de validaciones con errores en el proceso de autenticación del usuario en una notaría pública, Lima 2022, (ii) la biometría facial mejora significativamente el tiempo de consulta en el proceso de autenticación del usuario en una notaría pública, Lima 2022 y (iii) la biometría facial mejora significativamente el porcentaje de riesgo de fallas en el proceso de autenticación del usuario en una notaría pública, Lima 2022.

II. MARCO TEÓRICO.

En referencia a los estudios como antecedentes dentro del entorno a nivel nacional se destaca a Pinto et al. (2021), de la ciudad de Lima, Cuyo objeto de estudio era comprobar el proceso de validación en su web de ventas y reducir los errores de los usuarios en la autenticación antes de la compra. La pre-prueba fue de 30 transacciones y post-prueba también fue de 30 transacciones diarias, el resultado comprobó que el sistema de gestión de datos posee el efecto esperado en el rendimiento con un progreso significativo de una variación de 6% de transacciones autorizadas a 4% que era de transacciones denegadas por errores, bajo estos datos claramente se refleja que la implementación si influye; ya que fue posible disminuir las transacciones denegadas de un promedio de 18% a 14%; en septiembre del 2020 hubo 778 201 transacciones denegadas y con la implementación disminuyo a 607 344 transacciones a la fecha posterior de la implementacion.

De la misma forma, se menciona a Ruiz (2018), con su investigación usando validación biométrica facial para consultar y tramitar el DNI y/o el DNI electrónico en el RENIEC, en la ciudad de Lima. Como objetivo era Implementar la App “RENIEC móvil facial” usando validación biométrica facial para consultar y tramitar el DNI y/o el DNI electrónico en el RENIEC; la metodología usada fue SCRUM, porque se adapta mejor para este tipo de desarrollo de esta App. por el ahorro de tiempo, costos bajos, trabajo en equipo. Los resultados muestran que el trámite gestión del duplicado, rectificación de donación de órganos y rectificación del domicilio del DNI/DNIe en RENIEC, bajo a diez minutos a comparación del trámite que se tarda en la agencia, donde un civil tardaba hasta treinta minutos en hacer la cola y veinte minutos en gestionar el trámite en ventanilla, tardando un tiempo total de cincuenta minutos; por ende, se verifica que la implementación optimiza el trámite de estos servicios en RENIEC.

De igual modo, sobresale Cienfuegos (2017), en Lima, como objetivo era

mostrar cómo la biometría de voz puede mejorar los procesos de seguridad de la información; la pre-prueba y pos-prueba dieron resultados que muestran que la seguridad de la autenticación ha aumentado de66.30% a 94.10%, un aumento del 32,50%, lo que demuestra que la implementación de la biometría de voz mediante tecnologías de reconocimiento de hardware y software puede mejorar los procesos de seguridad de la información, que son fallas de seguridad muy peligrosas.

Así también, indica Oyola (2022), en Chiclayo, su finalidad es mejorar la seguridad de los sistemas web mediante un sistema de autenticación de tipo biométrico obtenido a partir de los hallazgos de las pruebas del software de autenticación de tipo biométrico aplicado a instituciones educativas, es decir el uso de la frecuencia del pulso como modelo de identidad contribuye a un modelo seguro para la información dentro del sistema de autenticación biométrica, permite ver el evento de presionar y soltar la tecla, la liberación de la tecla y la hora en que ocurrieron estos dos eventos, es decir se puede ver la velocidad de movimiento entre las claves a pesar de las credenciales correctas Para determinar aún si una persona está atrasada en la autenticación, los resultados muestran el nivel en el que las instituciones educativas deben implementar un sistema de autenticación biométrica con base en los resultados recopilados: Seguridad: Dimensión 60.0 % lo considera bueno, el 43.3% lo considera regular.

Por otro lado, comenta Correa et al. (2020), en su investigación optimiza el proceso de verificación usando la metodología Six Sigma en la organización ALIGNET S.A.C, su objetivo general es aumentar el porcentaje de verificación para el proceso de compras virtuales usando medios de pago digitales, como metodología se utilizó el SIx Sigma porque tiene un enfoque de gestión y además mejora los procesos en las compañías y empresas; también corrige los problemas en las actividades críticas, los resultados nos indican que se obtuvo el 79% de incrementos de las transacciones y también al mismo tiempo se autenticaba de formas eficaz, segura y rápida.

Por otro lado, respecto a los estudios en el entorno internacional se resalta a Luna (2015), en Bolivia. Cuyo objetivo fue crear un programa que autentique mediante la plataforma móvil de Android, sustentado con el Algoritmo de Libor Masek, que hará posible el tratamiento de imágenes del iris ocular de un ser humano con la finalidad de obtener su información biométrica que se usara para su autentificación; los resultados se hallaron usando cinco imágenes por cada ojo por cada muestra, luego se ingresó a la base de datos, se probaron a muchas personas registradas, los resultados fueron muy claros en el reconocimiento, ya que se detectó correctamente a las personas que si estaban registradas y a las que no, las detecto como no registradas, lo cual cumple el objetivo.

De la misma manera, se realza a Caicedo. (2019), con su tesis denominada Plataforma de Servicio de autenticación Biométrica Facial, en Bogotá. Su objetivo fue desarrollar e Implementar una plataforma de servicios de autenticación biométrica facial para el registro de sus trabajadores, la investigación es del tipo descriptiva, la metodología usada es la OMT que está basada en el análisis, diseño orientado a objetos, la codificación y pruebas. Los resultados luego del desarrollo e implementación del sistema facial fueron los esperados ya que se registró a todos los trabajadores almacenando sus fotografías, y se comprobó la validación, estos mecanismos optimizaron los tiempos de entrada de todos los trabajadores en todas las sucursales.

De igual modo, sobresale Espinosa (2013), en España, como objetivo de esta investigación es conocer las capacidades tecnológicas de nuevas cámaras IR, que sean accesibles para biometría de reconocimiento facial, también se buscaba comparar las imágenes faciales y las térmicas contra las de infrarrojo, como metodología se usó la Principal Component Analysis (PCA), porque actuaría como un extractor de características, y las técnicas de conjunto es la de submuestreo y el método de subespacio aleatorio (RSM) para realizar la etapa de clasificación. Como resultado al implementar el software hecho con la

capacidad de analizar de manera más eficiente las imágenes tomadas con baja luz, o las que salieron desenfocadas, para que el reconocimiento facial sea óptimo, se ha demostrado que la fusión supera el rendimiento en un 98%.

De igual modo, sobresale Estrela (2021), con su investigación titulada Autenticación continua basada en biometría de comportamiento para aplicaciones de banca móvil, en Brasil, plantea la ejecución de un sistema de autenticación continua para aplicaciones de banca móvil para detectar anomalías y generar alertas de autenticación basadas en patrones biométricos de comportamiento que interactúan con pantallas táctiles, ubicación registrada a través de GPS e información recopilada de varios sensores; los resultados mostraron que del 90,68% al 97,05% de los resultados provinieron de mejoras en la confiabilidad de la autenticación y del 9,85% al 1,88% de mejoras en la reducción de riesgos, y el uso de la biometría táctil conductual se probó en escenarios de autenticación biométrica por comportamiento como un aliado visual prometedor cuando se considera junto con métodos tradicionales como contraseñas en la definición de capas de seguridad para reducir el fraude de autenticación en aplicaciones de banca móvil.

Del mismo modo, se destaca a Mohamad (2013), cuya tesis se denomina Reconocimiento biométrico facial usando proyección multilineal e inteligencia artificial, en la Universidad NewCastle en Reino Unido, cuyo objetivo se centró en investigar el aprendizaje subespacial multilineal acerca del reconocimiento facial basado en la apariencia, se desarrolló algoritmos de aprendizaje subespaciales multilineales, los dos grandes problemas del reconocimiento facial está en la extracción que son la representación de objetos y la alta dimensionalidad, para solucionar este inconveniente se ha desarrollado un enfoque B2DNPP para el reconocimiento facial que comparado con el actual 2DNPP que solo opera en imágenes faciales 2-D, este nuevo método realiza descomposición curvilínea de imágenes faciales. Como resultados se vio que el método C-B2DNPP reduce la tasa de error del 5,9 % al 3,5
%, del 3,7 % al 2,0 % y del 19,7 % al 14,2 % empleando las bases de datos

ORL, AR y FERET en comparación con 2DNPP. Por lo tanto, logra disminuciones en la tasa de error de más del 40%, 45% y 27% y El método MNPP supervisado propuesto logró una disminución superior al 50,8%, 75,6% y 44,6% en la tasa de error utilizando las bases de datos ORL, AR y FERET respectivamente, en comparación con 2DNPP. Por lo tanto, los resultados demuestran que el enfoque MNPP obtiene el mejor rendimiento general en varios escenarios de aprendizaje.

Concerniente a las teorías que avalan la presente investigación tenemos a la teoría general de sistemas, von Bertalanffy(1989), demuestra que esta teoria es la formulación y derivación de todos los principios que se aplican a los sistemas como un todo. También hace aportes semánticos, que es donde están todos los conceptos técnicos pero con una semántica universal para el entendimiento de todos, destacan los conceptos como sistemas y dentro de este están las entradas, procesos y salidas. Skyttner (2005), indica que un sistema es intencional porque da a conocer un objetivo cuando internamente procesa una entrada en una salida y la salida vendría a ser una meta deseada, los clasifica como descomponibles, porque sus sub sistemas son independientes, también son casi descomponibles ya que sus sub sistemas son débiles, pero no despreciables y finalmente clasifica en no descomponibles, porque dependen de otros sistemas. Rodríguez et al. (2013), dice que la teoría general de sistemas Incluye un análisis del estado natural de los sistemas y la interacción entre estos sistemas. Paredes et al. (2022), dicen que la teoría general de sistemas se conceptualiza como un conjunto de principios e ideas con un orden al servicio del entendimiento de científicos, a la vez clasifica a los sistemas en naturales, en diseñados, de actividad humana y culturales. Indica que un sistema abierto se interrelaciona con el entorno que lo rodea, mientras que un sistema cerrado no lo hace, porque no intercambia energía con el entorno.

Como segunda teoría que avalan a la presente investigación con la teoría de la restricción, en este aspecto Goldratt (1979), menciona que esta teoría de la restricción es una limitación que está por arriba, la cual no se puede continuar,

todas las empresas tienen restricciones, cualquier proceso con diversas actividades pueden continuar solamente con menos velocidad, a esto lo denomino “cuello de botella”, existen varios tipos de restricciones, la lógica, la física, de mercado, de capacidad, logística, de materiales, de comportamiento, como propósito de la teoría de restricciones es la de maximizar las utilidades, consta de 5 pasos para su aplicación, el primero es identificar las restricciones, luego es explotar esas restricciones, luego subordinar todas las actividades a la decisión anterior, después elevar la restricción, se debe repetir los pasos por cada restricción encontrada. De igual modo, Cox III (2010), señaló que, la teoría de restricciones se define en hacer lo que se debe hacer y no hacer lo que no se debe hacer, no hay error más grave que no darle la importancia debida a la no restricción ya que esto afectaría en el rendimiento del sistema, las restricciones son mejores mientras haya más siempre y cuando no sobrepasen el umbral o si no estaríamos en “más es peor”, se enfoca que si perdemos una hora con un cuello de botella equivaldrá a perder esa hora. De igual forma, Groop (2012), aclara que la teoría de restricciones es cuando algún factor dificulta que un sistema alcance un rendimiento mayor al de su objetivo, ya que las restricciones establecen el desempeño directo del sistema como un todo, se debe mejorar el desempeño de todo el sistema, así permitirá el efectivo control de todo el sistema, se podría decir que las restricciones no son positivas ni negativas, también se dice que la restricción es un apalancamiento en donde el sistema podrá ser controlado y mejorado. Asimismo, Mccleskey (2020), aclara que una restricción es un factor que limita el rendimiento de un sistema y si ese factor pudiera utilizarse o explotarse de manera más eficiente, se obtendrían niveles más altos de rendimiento, se define como un cuello de botella, pero es más complicado que eso, es un recurso y su capacidad es menor que la demanda para su uso durante el periodo.

Referente al enfoque conceptual de la variable independiente Biometría facial, Browning (2018), define a la biometría como cualquier dato generado por mediciones automáticas de las características biológicas de in individuo, pero debe usarse bajo una normativa legal la cual no permita vulnerar la privacidad de

las personas, por tanto debe ser usado bajo consentimiento y solo debe ser exigido bajo ciertas medidas de seguridad para que otras personas no le saquen provecho de los datos biométricos registrados. De igual forma, Jasserand (2016), señalo que la biometría se define como propiedades biológicas, características fisiológicas, vida, rasgos o acciones repetibles donde esas características y/o acciones son únicas para esos individuos y son medibles, incluso si los patrones utilizados en la práctica para medir técnicamente involucran un cierto grado de probabilidad. Asimismo, Tikkinen-Piri, C. (2018), indicaron que los datos biométricos denotan cualquier dato en relacion con los rasgos físicos de la cara, manos, huellas o algunos se basan en el comportamiento de un individuo y que permite una identificación única (por ejemplo, imágenes faciales o datos dactiloscópicos). Del mismo modo, Arun et al. (2022), resalto que la biometría se refiere a la ciencia de reconocer a las personas a partir de sus atributos físicos y de comportamiento, denominadas modalidades biométricas, Si bien los datos biométricos se recopilan principalmente para verificar o establecer la identidad de una persona. También, Thenuwara et al. (2022), afirmaron que se puede decir que la biometría son medidas de patrones biológicos que pertenecen a individuos, como las huellas, el patrón del iris, la voz y la cara, la biometría facial y las huellas dactilares se pueden identificar como rasgos rentables y de fácil acceso en el dominio biométrico, las tecnologías biométricas consumen esos rasgos y autorizan a la persona para una determinada tarea denominada sistemas de autorización biométrica.

Por otro lado, en cuanto a la variable dependiente proceso de autenticación de usuario, Prabhu et al. (2022), define la autenticación como uno de los métodos de control de acceso común y consistente, se requiere almacenar de forma segura las características biométricas en bases de datos digitales para hacer coincidir las plantillas biométricas correspondientes. De igual forma Vega (2021), establece que la autenticación es un conjunto de técnicas que utilizamos para atender un pedido de identidad como real. hay que tener claro que la autenticación se confirmara positivamente sólo si se cumple el pedido de

identidad de manera correcta, por ende, los registros deben ser lo más nítidos posibles para evitar rechazos. Asimismo, según Figueroa, Romero et al. (2018), La autentificación es un proceso que confirma algo como verdadero o cierto, no siempre se basa en verificar a una persona, ya que la autenticación no solamente está vinculada con personas, en otros casos se desea saber si un cambio o un dato es conforme o un sistema, aplicación y afines. Del mismo modo, Rodriguez et al. (2018), refirió que la autenticación es una consulta para la validación de la identidad manifestada por las personas, es indispensable que los métodos de autenticación sean los adecuados ya que es utilizado para muchos servicios y aplicaciones. Asimismo, Munandar et al. (2021), nos dicen que la autenticación es un proceso que prueba la identidad de un usuario en un sistema, uno de los esquemas utilizados es el de inicio de sesión, en la que un usuario debe demostrar su identidad como usuario válido para ingresar a un sistema, la autenticación de usuario es parte de la autenticación o identificación de la entidad, que es prueba de la identidad de una entidad, puede ser una persona, una tarjeta de crédito o una máquina.

La variable proceso de autenticación del usuario se operacionaliza por los siguientes indicadores: cantidad de validaciones con errores, tiempo de consulta y porcentaje de riesgo de fallas.

En relación al indicador tiempo de consulta, Sakshi et al. (2022), nos dice que el tiempo de consulta es un proceso que necesita algo de tiempo para ejecutarse, y el tiempo total tomado por cualquier proceso para completar el proceso se conoce como el tiempo de respuesta, todo proceso al ingresar para su ejecución depende de un algoritmo, y el tiempo que se tarda en responder a la solicitud realizada para responder se denomina tiempo de respuesta. Asimismo, para Abdulkareem (2014), el tiempo de espera es la reducción de las listas de esperas a los usuarios, de esta manera aumenta la eficiencia de la atención, acorta las esperas electivas y minimiza las cancelaciones, también aclara que reducir el tiempo de espera no compromete la calidad asistencial del usuario, sino todo lo contrario influye positivamente. Del mismo modo, Monge, A. et al.

(2014) lo define como tiempo de espera total para consulta que comienza con la primera vez que se busca el servicio de atención y termina cuando ya fue tratado, también indica que esta espera causa entre los usuarios una expectativa la cual al finalizar indicará un grado de satisfacción. También, Esfeh et al. (2022) dicen que el tiempo de espera es una función de la hora de salida deseada desde el origen y el punto de transferencia, y la hora de llegada deseada frente al horario del servicio, el tiempo de espera se reporta en la literatura como el costo más alto que experimentan los usuarios del servicio.

En relación al indicador cantidad de validaciones con errores, Zachos et al. (2003) indica que el error es natural y puede ser útil e informativo, asimismo es una meta valiosa para la educación científica, representa una amenaza para el conocimiento, pero se puede usar el error para aprender, el error se conceptualiza y modela tanto matemática como gráficamente, se hacen distinciones claras entre diferentes fuentes de error. Asimismo, Zhang et al. (2015), indica que el error es una equivocación, en un reporte y que su gravedad debe ser informado para decidir qué tan rápido se debe solucionar, para ello existen técnicas de predicciones que serán necesarios para detectar los errores, una de ellas es la de extracción de errores, se extrae la información de los reportes históricos y así construye un registro, asimismo se debe clasificar desde los más urgentes a los más leves. Del mismo modo Garrido et al. (2017), sobre el indicador cantidad de errores, manifestó que es la probabilidad de identificación incorrecta, debido a que la extracción de datos biométricos no es perfecta. También, Tolosa et al. (2019), sobre el indicador cantidad de errores, define que es el rechazo a un usuario legítimo ya que no se fue capaz de validar debidamente. De igual modo, Guerrero et al. (2013) sobre el indicador cantidad de errores, explica que un error es una oportunidad de aprendizaje, ya que dependerá del manejo que se le dé al error, puede crear un -aprendizaje significativo muy satisfactorio o viceversa.

En relación al indicador porcentaje de riesgo de fallas, Gabaldon (2022), lo define como hurto y fraude de identidad de una persona, mediante la creación de una ficticia identidad con el objetivo de defraudar. Asimismo, Friginal et al.

(2016), define el riesgo como la probabilidad que un problema o incidencia explote la debilidad de un proceso o sistema y, por lo tanto, cause daño a la organización. En otras palabras, el riesgo es una combinación de dos factores: la ocurrencia de un peligro potencial y las consecuencias del peligro. la amenaza que puede suponer para la víctima, también denominadas consecuencias negativas. Del mismo modo ARCIÓN (2013), manifestó que el porcentaje de riesgo de fallas es cuando el sujeto se apropia ilegalmente de la identidad de otra persona, afectando a la víctima, robando su identidad, exponiendo a despojarlo de sus pertenencias. Asimismo, según Faraldo (2010), el porcentaje de riesgo de fallas se define como hacerse pasar por otra persona con fines delictivos. Asimismo, Lindholm (2013), dice que el riesgo es la probabilidad de incurrir en una pérdida o soportar un impacto negativo, es crucial que el riesgo sea lo más bajo posible y que las organizaciones que desarrollan dispositivos deben abordar diferentes riesgos relacionado al rubro destinado del producto.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1. Tipo de investigación

La investigación es del tipo aplicada, el cual según Alvarez (2021) Dice que el propósito de la investigación aplicada es buscar nuevos conocimientos para resolver problemas prácticos. Asimismo, CONCYTEC (2019) dice que se utilizar el conocimiento científico para determinar formas de satisfacer una necesidad.

3.1.2. Diseño de investigación

Esta investigación es experimental del tipo pre experimental, el cual según Salas (2013), es cuando el experimentador intenta acercarse a un experimento, con un gran nivel exigencia en el control de variables que afectan a la validez de los datos experimentales.

A continuación, se presenta el diagrama del diseño de investigación que se ha utilizado:

Esquema:

RG: 01 → X → 02

RG: Pre-prueba → Biometría Facial → Post-prueba Leyenda:

R = Asignar aleatoriamente

G = grupo de prueba

X = Procedimiento

01 - 02 = Medición pre-prueba / post-prueba de la biometría facial.

3.2. Variables y Operacionalización

Variable independiente - Biometría Facial

La variable es Biometría Facial, que es cuantitativa de carácter discreta. Para Saiz (2017) la variable independiente es un elemento que va a generar un cambio. Asimismo, Contento (2019) define que la variable cuantitativa es discreta cuando poseen un conjunto contable de valores, es decir proceden de conteos.

Definición Conceptual de la variable independiente Biometría Facial

Según INCIBE (2016), la biometría facial es una manera de validar a las personas en función de sus rasgos fisiológicos del rostro; es un tipo de biometría estática porque mide una función directa de la cara.

Variable dependiente proceso de autenticación del usuario

En esta investigación se analiza a la variable proceso de autenticación del usuario, se trata de una variable tipo cuantitativa de carácter discreta y con una escala de tipo porcentual. Según Espinoza (2018), una variable dependiente es una variable que cambia debido a la acción de la variable independiente. Establecen una meta para iniciar resultados.

Definición Conceptual de la variable dependiente - proceso de autenticación del usuario

Según Bernal (2022). Es el proceso digital que permite la identificación electrónica de un sujeto de manera física, a la vez de su fuente y su integridad de datos de forma digital.

Definición Operacional de la variable dependiente proceso de autenticación del usuario

Para la variable dependiente autenticación del usuario, esta ha sido medida por tres indicadores: (i) cantidad de validaciones con errores, (ii) tiempo de consulta y (iii) porcentaje de riesgo de fallas; y para que cada indicador sea cuantificado su valor en el anexo 2 se muestran las fórmulas usadas, en donde los resultados se consideraron en porcentaje.

3.3. Población, muestra y muestreo

3.3.1. Población

La población para este estudio consistirá en 50 observaciones para cada indicador. Según Condori (2020), la población son todos los elementos disponibles o unidades de análisis que pertenecen al lugar donde se realizó el estudio; en ese sentido Hernandez (2019), considera que la muestra sirve para delimitar a la población a través de una selección.

Tabla 1

Población de la Investigación

Población	Cantidad	Indicador
Observaciones	50	cantidad de validaciones con errores
Observaciones	50	tiempo de consulta
Observaciones	50	porcentaje de riesgo de fallas

Nota. Elaboración propia

3.3.2. Muestreo

Para la presente investigación se usó un muestreo probabilístico aleatorio simple, ya que según Tamayo (2021), es un método de selección de n unidades, extraídas de una población homogénea de tamaño N, por ende, cada una de las muestras, tengan la misma opción de ser elegidas.

3.3.3. Unidad de análisis

Son cada una de las observaciones aplicadas por el investigador, ya que según Posada (2016) es el elemento objeto de estudio, que puede ser un objeto, una persona, un grupo de personas o un acontecimiento. La unidad debe corresponder al tipo de investigación a realizar, se debe tener en cuenta que las características de los elementos no sean inequívocas, comprensibles y permitan mediciones y comparaciones.

3.4. Técnicas e instrumentos de recolección de datos

Técnicas de recolección de datos

El método de recolección de datos de este estudio fue la observación, ya que según Arias (2020), consiste cuando el investigador desea medir, analizar o calificar un objetivo en específico; es decir, extraer información del objeto.

Instrumentos de recolección de datos

El instrumento usado para la recolección de datos, fue la guía de observación y se aplicó en la pre-prueba y post-pruebat; considerando los parámetros fecha, tiempo inicial, tiempo final, DNI, cantidad de intentos fallidos, cantidad de intentos, fallas detectadas, total riesgos registrados, como se indica en el anexo 3. Para Valle et al.

(2022), la ficha de observación, es donde describimos cautelosamente lo que va pasando mientras visualizamos.

Tabla 2

Ficha técnica del Instrumento

Nombre del instrumento:	Guía de observación de medición del indicador
Autor:	Juan Royer Espinoza Beramendi
Año:	2022
Descripción:	
Tipo de Instrumento:	Guía de Observación
Objetivo:	Determinar de qué manera la biometría facial mejora el proceso de autenticación del usuario en una notaría pública, Lima 2022.
Indicadores:	a) Cantidad de validaciones conerrores b) Tiempo de consulta c) Porcentaje de riesgo de fallas.
Número de observaciones a recolectar :	50
Aplicación:	Presencial

Nota. Elaboración propia

Validez

Se empleó la validación por juicio de expertos como herramienta de recolección de datos de la investigación, en la cual un experto temático y dos metodológicos emitieron un juicio de aplicabilidad, mediante la constancia de validez, el cual se señala en el anexo 4. Para Benini et al. (2017) dice que es la opinión de expertos dada en el contexto de una decisión, la opinión de expertos son datos y contexto proporcionados por personas con habilidades o conocimientos superiores cuando las consideraciones de disponibilidad, calidad, tiempo y costo descartan los datos de fuentes tradicionales.

Tabla 3

Validación del Instrumento de recolección de datos

DNI	Experto	Procedencia	Especialista	Calificación
73041890	Mg. Yañez Romero Robinson Manuel	Universidad Cesar Vallejo	Metodólogo	aplicable
42243830	Mg. Morales Fernandez Santos Ivan	Universidad Cesar Vallejo	Metodólogo	aplicable
42097456	Mg. Acuña Benite Marlon Frank	Universidad Cesar Vallejo	Temático	aplicable

Nota. Elaboración propia.

3.5. Procedimientos

Se consideraron cuatro etapas principales, la primera es la recolección de datos; se valida el instrumento con base en criterios de opinión de expertos en la segunda etapa; en la tercera etapa se realizó la recolección de datos usando métodos observacionales y finalmente usando los programas Microsoft Excel e IBM SPSS V26 para realizar trabajos de oficina y a los resultados aplicar el análisis estadístico.

3.6. Método de análisis de datos

Se emplearon dos herramientas digitales, software SPSS y Microsoft Excel para el apoyo en la pre-prueba y post-prueba por cada indicador; para el análisis descriptivo se usó las tablas y figuras para mostrar la tendencia central, y los

resultados de cada indicador se explicarán utilizando los valores de media, desviación estándar, mediana, mínimo y máximo de cada indicador. Se usó Shapiro-Wilk, para el análisis inferencial, la prueba de normalidad de cada indicador y la prueba de hipótesis utiliza Wilcoxon y t de Student.

3.7. Aspectos éticos

Para confirmar la integridad y regularidad de este estudio, este trabajo se realizó de acuerdo con las normas y principios morales de la Universidad Cesar Vallejo, de acuerdo con la Resolución de Consejo n. 0262-2020UCV.

De igual forma, en este estudio se utilizaron normas ajustadas por los estándares APA 7. Considerando la veracidad de todo lo expuesto en la presente investigación, se asume la responsabilidad y el cumplimiento legal y ético, respetuoso y confidencial del uso de la información sensible. Además, el software de Turnitin se usa para cumplir con las pautas antiplagio.

IV. Resultados

Análisis descriptivos

Medidas descriptivas del indicador: Cantidad de validaciones con errores

Tabla 4

Medidas descriptivas del indicador: Cantidad de validaciones con errores

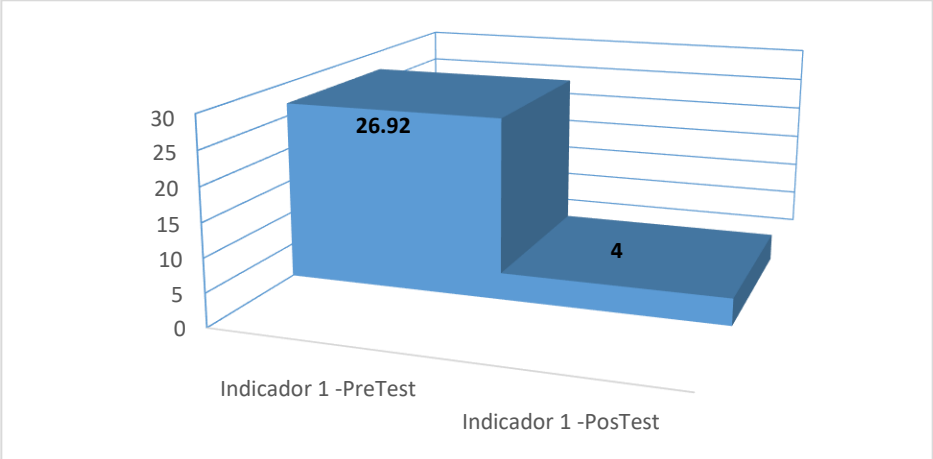
	N	Mínimo	Máximo	Media	Desv. Desviación
I1 PrePrueba	50	0	94	26.92	36.826
I1 PosPrueba	50	0	50	4.00	13.702
N válido (por lista)	50				

Nota. La tabla tiene asistencia del spss

En la tabla 4 se visualiza las medidas descriptivas del indicador *Cantidad de validaciones con errores*, en el cual el valor de la media calculada en la pre-prueba tuvo un valor de 26.92 y en la post-prueba tuvo un valor de 4.0; esto indica que hay una reducción de 22.92 de validaciones con errores después de implementar la biometría facial. Asimismo, los valores del rango mínimo y máximo en la pre-prueba tuvieron un valor de 0 y 94 respectivamente y en la post-prueba tuvieron un valor de 0 y 50 respectivamente; esto es que los valores de las validaciones con errores en la pre-prueba se posicionaron entre 0 y 94 y en la post-prueba se posicionaron entre 0 y 50, en ambos casos la media se acerca a los rangos mínimos. Tambien, la desviación estándar promedio en la pre-prueba tuvo un valor de 36.826 y en la post-prueba tuvo un valor de 13.702; esto es que en promedio la *Cantidad de validaciones con errores* en la pre-prueba se desvía 36.826 de la media y en la post-prueba se desvía 13.702 de la media.

Figura 1

Histograma de la media de Cantidad de validaciones con errores tiempo de consulta



Nota. Material utilizado Microsoft Excel.

En la figura 1 se representa la media del indicador *Cantidad de validaciones con errores* antes y después de la ejecución de la biometría facial, en base a los datos conseguidos en la guía de observación, por lo que se puede sustentar que la *Cantidad de validaciones con errores disminuyo* un 22.92.

Asimismo, en el anexo 5a se representa gráficamente el comportamiento de las medias del indicador *Cantidad de validaciones con errores* respecto a la pre-prueba y post-prueba, el cual muestra que el indicador *Cantidad de validaciones con errores* fue cambiante.

Medidas descriptivas del indicador: tiempo de consulta

Tabla 5

Medidas descriptivas del indicador: tiempo de consulta

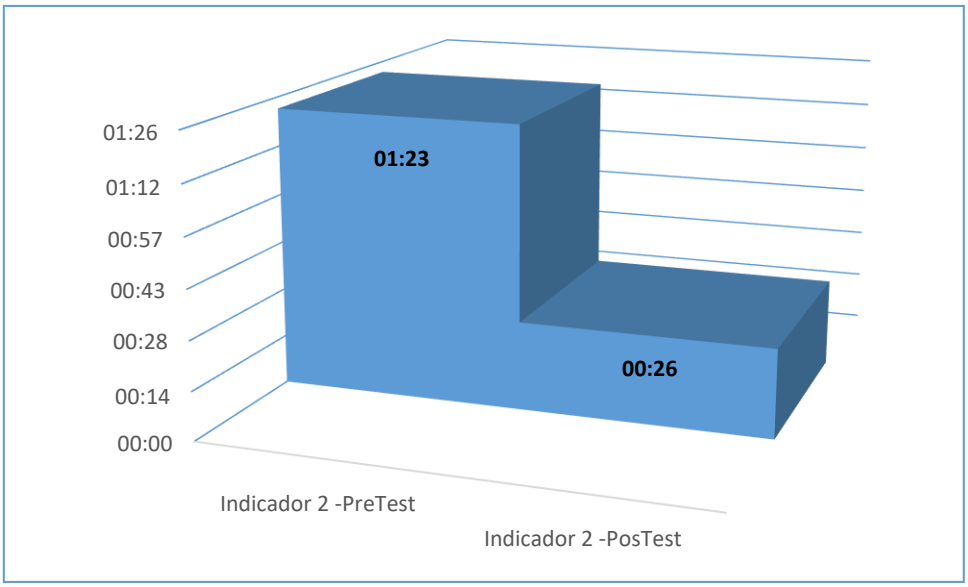
	N	Mínimo	Máximo	Media	Desv. Desviación
I2 PrePrueba -	50	00:52	01:53	01:23	00:16
I2 PosPrueba	50	00:17	00:39	00:26	00:04
N válido (por lista)	50				

Nota. La tabla tiene asistencia del spss

En la tabla 5 se visualizan las medidas descriptivas del indicador *tiempo de consulta*, en donde el valor de la media obtenida en la pre-prueba fue 01:23 segundos y en la post-prueba fue 0:26 segundos; lo cual indica que hay una reducción de 00:57 segundos del *tiempo de consulta* después de implementar la biometría facial. Adicionalmente, el rango mínimo y máximo en la pre-prueba fue 0:52 y 01:53 segundos respectivamente y en la post-prueba fue 0:17 y 0:39 segundos respectivamente; esto es que los valores del *tiempo de consulta* en la pre-prueba se posicionaron entre 0:52 y 01:53 segundos y en la post-prueba se posicionaron entre 0:17 y 0:39 segundos, en ambos casos la media se acerca a los rangos maximos. Tambien, la desviación estándar promedio en la pre-prueba fue 0:16 y en la post-prueba fue 0:04; esto es que en promedio el *tiempo de consulta* en la pre-prueba se desvía 0:16 de la media y en la post-prueba se desvía 0:04 de la media.

Figura 2

Histograma de la media de tiempo de consulta



Nota. Material utilizado Microsoft Excel.

En la figura 2 se representa la media del indicador *tiempo de consulta* antes y después de la ejecucion de la biometría facial, en base a los datos conseguidos en la guía de observación, por lo que se puede sustentar que el *tiempo de consulta disminuyo* un 00:57 segundos.

Asimismo, en el anexo 5b se representa gráficamente el comportamiento de las medias del indicador *tiempo de consulta* respecto a la pre-prueba y post-prueba, el cual indica que el indicador *tiempo de consulta* fue cambiante.

Medidas descriptivas del indicador: riesgo de falla

Tabla 6

Medidas descriptivas del indicador: riesgo de falla

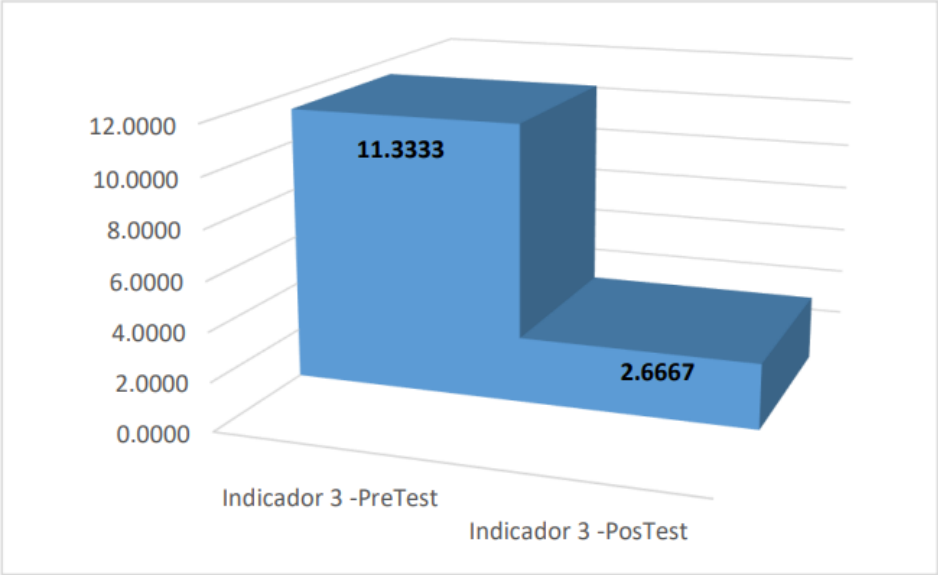
	N	Mínimo	Máximo	Media	Desv. Desviación
I3 - PrePrueba	50	0.00	33.33	11.3333	15.95060
I3 - PosPrueba	50	0.00	33.33	2.6667	9.13492
N válido (por lista)	50				

Nota. La tabla tiene asistencia del spss

En la tabla 6 se visualizan las medidas descriptivas del indicador *riesgo de falla*, en donde el valor de la media conseguida en la pre-prueba fue 11.3333 y en la post-prueba fue 2.6667; lo cual indica que hay una reducción de 8.6666 del *riesgo de falla* después de la ejecución de la biometría facial. Adicionalmente, el rango mínimo y máximo en la pre-prueba fue 0 Y 33.33 respectivamente y en la post-prueba fue 0 Y 33.33 respectivamente; esto es que los valores del *riesgo de falla* en la pre-prueba se posicionaron entre 0 Y 33.33 y en la post-prueba se posicionaron entre 0 Y 33.33, en ambos casos la media se acerca a los rangos mínimos. Tambien, la desviación estándar promedio en la pre-prueba fue 15.95060 y en la post-prueba fue 9.13492; esto es que en promedio el *riesgo de falla* en la pre-prueba se desvía 15.95060 de la media y en la post-prueba se desvía 9.13492 de la media.

Figura 3

Histograma de la media de riesgo de falla



Nota. Material utilizado Microsoft Excel.

En la figura 3 se representa la media del indicador *riesgo de falla* antes y después de la ejecución de la biometría facial, en base a los datos conseguidos en la guía de observación, por lo que se puede sustentar que el *riesgo de falla disminuyo* un 8.6666. Adicionalmente, en el anexo 5c se representa gráficamente el comportamiento de las medias del indicador *riesgo de falla* respecto a la pre-prueba y post-prueba, el cual revela que el indicador *riesgo de falla* fue cambiante.

Análisis Inferencial

Prueba de Normalidad

Para realizar la prueba de normalidad de los indicadores cantidad de validaciones con errores, tiempo de consulta, porcentaje de riesgo de falla, se ha usado la prueba de shapiro-wilk, porque la muestra para cada indicador es de 50 observaciones; esta prueba se hizo con la ayuda del software IBM SPSS V26, y cuenta con un nivel de confianza de 95%. En este aspecto, Hanusz, Tarasinska y Zieliński (2016) y Romero (2016) Indican que si la muestra es igual o menor a 50; en este caso se

aplicara shapiro-wilk y aplicando como nivel de significancia 0.05, si el valor de p es mayor que 0.05, la distribución se considera normal, caso contrario será no normal.

Prueba de normalidad del Indicador: cantidad de validaciones con errores

Formulación de hipótesis estadística

H0: Los datos del indicador cantidad de validaciones con errores poseen una distribución normal.

H1: Los datos del indicador cantidad de validaciones con errores no poseen una distribución normal.

Tabla 7

Prueba de normalidad del indicador cantidad de validaciones con errores

	Shapiro-Wilk Estadístico	gl	Sig.
I1 - PrePrueba	0.671	50	0.000
I1 - PosPrueba	0.303	50	0.000

Nota. La tabla tiene asistencia del spss

En la tabla 7 se aprecia el nivel de significancia (p) cuyo valor es de 0.000, entonces como es menor a 0.05, se rechaza la hipótesis nula (H0) y se acepta la hipótesis alterna (H1); el cual indica que, los datos del indicador cantidad de validaciones con errores poseen una distribución no normal, antes y después de la implementación de la biometría facial.

Prueba de normalidad del Indicador: tiempo de consulta

Formulación de hipótesis estadística

H0: Los datos del indicador tiempo de consulta poseen una distribución normal.

H1: Los datos del indicador tiempo de consulta no poseen una distribución normal.

Tabla 8

Prueba de normalidad del indicador tiempo de consulta

	Shapiro-Wilk Estadístico	gl	Sig.
I2 - PrePrueba	0.961	50	0.097
I2 - PosPrueba	0.973	50	0.297

Nota. La tabla tiene asistencia del spss

En la tabla 8 se aprecia el nivel de significancia (p) que en la pre-prueba fue 0.097 y post-prueba fue 0.297, entonces como en ambos casos es mayor a 0.05, se acepta la hipótesis nula (H0) y se rechaza la hipótesis alterna (H1); el cual revela que, los datos del indicador tiempo de consulta poseen una distribución normal, antes y después de la implementación de la biometría facial.

Prueba de normalidad del Indicador: riesgo de falla

Formulación de hipótesis estadística

H0: Los datos del indicador riesgo de falla poseen una distribución normal.

H1: Los datos del indicador riesgo de falla no poseen una distribución normal.

Tabla 9

Prueba de normalidad del indicador riesgo de falla

	Shapiro-Wilk Estadístico	gl	Sig.
I3 - PrePrueba	0.599	50	0.000
I3 - PosPrueba	0.303	50	0.000

Nota. La tabla tiene asistencia del spss

En la tabla 9 se aprecia el nivel de significancia (p) cuyo valor es de 0.000, por lo tanto, ya que es menor a 0.05, se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1); el cual indica que, los datos del indicador riesgo de falla poseen una distribución no normal, antes y después de la implementación de la biometría facial.

Prueba de Hipótesis

Para los indicadores cantidad de validaciones con errores, porcentaje de riesgo de falla, se ha empleado la prueba no paramétrica de Wilcoxon, como prueba de hipótesis, porque los datos muestreados en cada indicador tuvieron una distribución no normal y para el indicador tiempo de consulta, se ha empleado la prueba de t de student por tener una distribución normal; estas pruebas fueron hechas con la ayuda del software IBM SPSS V26 y con 95% de nivel de confianza.

Prueba de Hipótesis especifica 1: Indicador cantidad de validaciones con errores

Formulación de hipótesis estadística:

H_0: La biometría facial no mejora significativamente la cantidad de validaciones con errores en el proceso de autenticación del usuario en una notaría pública, Lima 2022.

H_1: La biometría facial mejora significativamente la cantidad de validaciones con errores en el proceso de autenticación del usuario en una notaría pública, Lima 2022.

Contrastación de hipótesis

Observando el resultado de la prueba de normalidad del indicador cantidad de validaciones con errores, el cual revela que los datos del indicador poseen una distribución no normal, se aplicó la prueba no paramétrica de Wilcoxon.

Tabla 10

Prueba de rangos con signos de Wilcoxon del indicador cantidad de validaciones con errores

Rangos

		N	Rango promedio	Suma de rangos
I1 Pos-Prueba - I1 Pre-Prueba	Rangos negativos	18[a]	13.39	241.00
	Rangos positivos	4[b]	3.00	12.00
	Empates	28[c]		
	Total	50		

Nota. La tabla tiene asistencia del spss

a. Post-Prueba - indicador 1 < Pre-Prueba - indicador 1

b. Post-Prueba - indicador 1 > Pre-Prueba - indicador 1

c. Post-Prueba - indicador 1 = Pre-Prueba - indicador 1

Para la contrastación de la hipótesis del indicador cantidad de validaciones con errores, se empleó la prueba no paramétrica de rangos con signos de Wilcoxon, como puede visualizarse en la tabla 10, que los pares muestrales en los rangos negativos y positivos son 18 y 4 respectivamente, ello revela una prevalencia de los pares muestrales ubicados en los rangos positivos, que demuestran que el indicador cantidad de validaciones con errores (post-prueba) es mayor a la cantidad de validaciones con errores en situación inicial (pre-prueba).

Tabla 11

Estadísticos de prueba de Wilcoxon del indicador cantidad de validaciones con errores

Estadísticos de prueba	Post-Prueba I1 - Pre-Prueba I1
Z	-3,740[b]
Sig. asintótica(bilateral)	0.000

Nota. La tabla tiene asistencia del spss

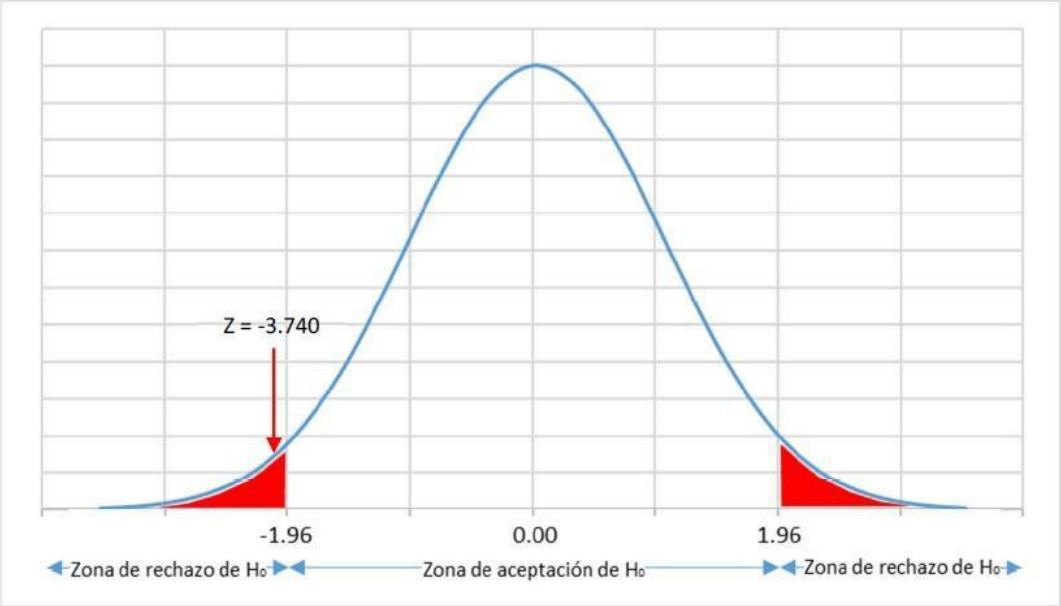
a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Siguiendo con la contrastación de hipótesis del indicador cantidad de validaciones con errores, en la tabla 11 se visualiza que el estadístico de prueba (z) conseguido es -3.740, el que por ser menor a -1.96 se localiza en la zona de rechazo de la hipótesis nula (ver figura 4); adicionalmente, el nivel de significancia (p) fue 0.000 el cual es menor a 0.05, por lo cual se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1); el cual revela que, la biometría facial mejora significativamente el indicador cantidad de validaciones con errores.

Figura 4

Contrastación bilateral de la hipótesis del indicador cantidad de validaciones con errores



Nota. Material utilizado Microsoft Excel.

Prueba de Hipótesis especifica 2: Indicador tiempo de consulta

Formulación de hipótesis estadística:

H_0: La biometría facial no mejora significativamente el tiempo de consulta en el proceso de autenticación del usuario en una notaría pública, Lima 2022.

H_1: La biometría facial mejora significativamente el tiempo de consulta en el proceso de autenticación del usuario en una notaría pública, Lima 2022.

Contrastación de hipótesis

Respetando el resultado de la prueba de normalidad del indicador tiempo de consulta, en donde se revela que los datos del indicador poseen una distribución normal, se aplicó la prueba de *t de student*

Tabla 12

Prueba de t de student para medidas de muestras relacionadas del indicador tiempo de consulta

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Pre-Test – Pos-Test	00:56	00:17	00:02	00:51	01:01	22.689	49	0.000

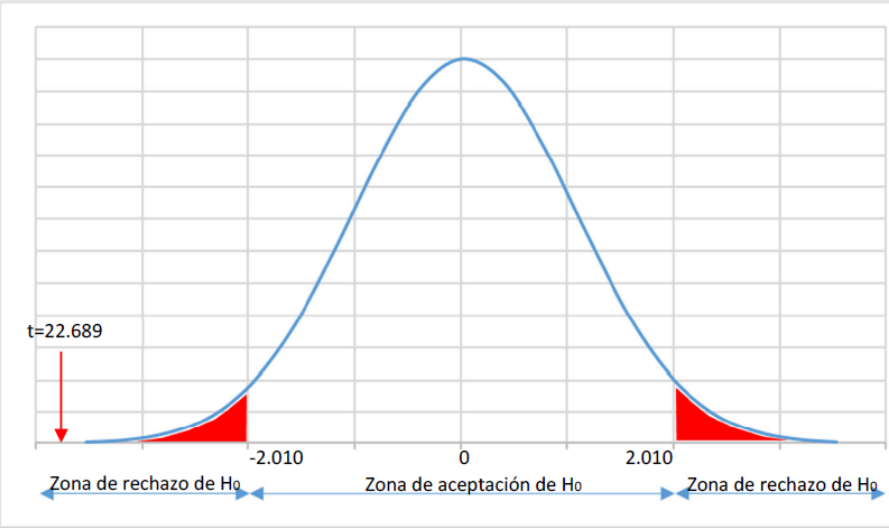
Nota. La tabla tiene asistencia del spss

El indicador tiempo de consulta en su contrastación de la hipótesis, se empleó la prueba de t de student, como puede visualizarse en la tabla 12, estadísticamente el valor de 22.689 corresponde al t de Student, localizándose hipótesis nula en la zona de rechazo.

Adicionalmente, en la figura 5 se visualiza la prueba t Student con su representación gráfica tomando referencia los grados de libertad (gl), fueron gl=n-1=49 y 0.05 de nivel de significancia; gracias a estos valores se ha localizado e interpolado en la tabla de distribución t, el valor de t crítico consiguiendo el valor de ± 2.010 ubicándose este valor en la zona de rechazo por lo que se rechaza la hipótesis nula (Ho) y se acepta la hipótesis alterna (H1); y se debe a que hay una diferencia significativa en las medias del tiempo de consulta antes y después de la implementación de la biometría facial y se tiene efectos significativos de un 01:23 a un 0:26 segundos.

Figura 5

Contrastación bilateral de la hipótesis del indicador tiempo de consulta



Nota. Material utilizado Microsoft Excel.

Prueba de Hipótesis especifica 3: Indicador porcentaje de riesgo de fallas

Formulación de hipótesis estadística:

H_0: La biometría facial no mejora significativamente el porcentaje de riesgo de fallas en el proceso de autenticación del usuario en una notaría pública, Lima 2022.

H_1: La biometría facial mejora significativamente el porcentaje de riesgo de fallas en el proceso de autenticación del usuario en una notaría pública, Lima 2022.

Contrastación de hipótesis

Respetando el resultado de la prueba de normalidad del indicador porcentaje de riesgo de fallas, se revela que los datos del indicador poseen una distribución no normal, se aplicó la prueba no paramétrica de Wilcoxon.

Tabla 13

Prueba de rangos con signos de Wilcoxon del indicador porcentaje de riesgo de fallas

Rangos

		N	Rango promedio	Suma de rangos
Post-Prueba I3 – Pre-Prueba I3	Rangos negativos	17[a]	11.00	187.00
	Rangos positivos	4[b]	11.00	44.00
	Empates	29[c]		
	Total	50		

Nota. La tabla tiene asistencia del spss

a. Post-Prueba del indicador 3 < Pre-Prueba del indicador 3

b. Post-Prueba del indicador 3 > Pre-Prueba del indicador 3

c. Post-Prueba del indicador 3 = Pre-Prueba del indicador 3

Para la contrastación de la hipótesis del indicador porcentaje de riesgo de fallas, se empleó la prueba no paramétrica de Wilcoxon, como puede visualizarse en la tabla 13, que los pares muestrales en los rangos negativos y positivos son 17 y 4 respectivamente, ello revela una prevalencia de los pares muestrales localizados en los rangos positivos, que demuestran que el indicador porcentaje de riesgo de fallas (post-prueba) es superior al porcentaje de riesgo de fallas en situación inicial (pre-prueba).

Tabla 14

Estadísticos de prueba de Wilcoxon del indicador porcentaje de riesgo de fallas

Estadísticos de prueba[a]	
	Post-Prueba I3 – Pre-Prueba I3
Z	-2,837[b]
Sig. asintótica(bilateral)	0.005

Nota. La tabla tiene asistencia del spss

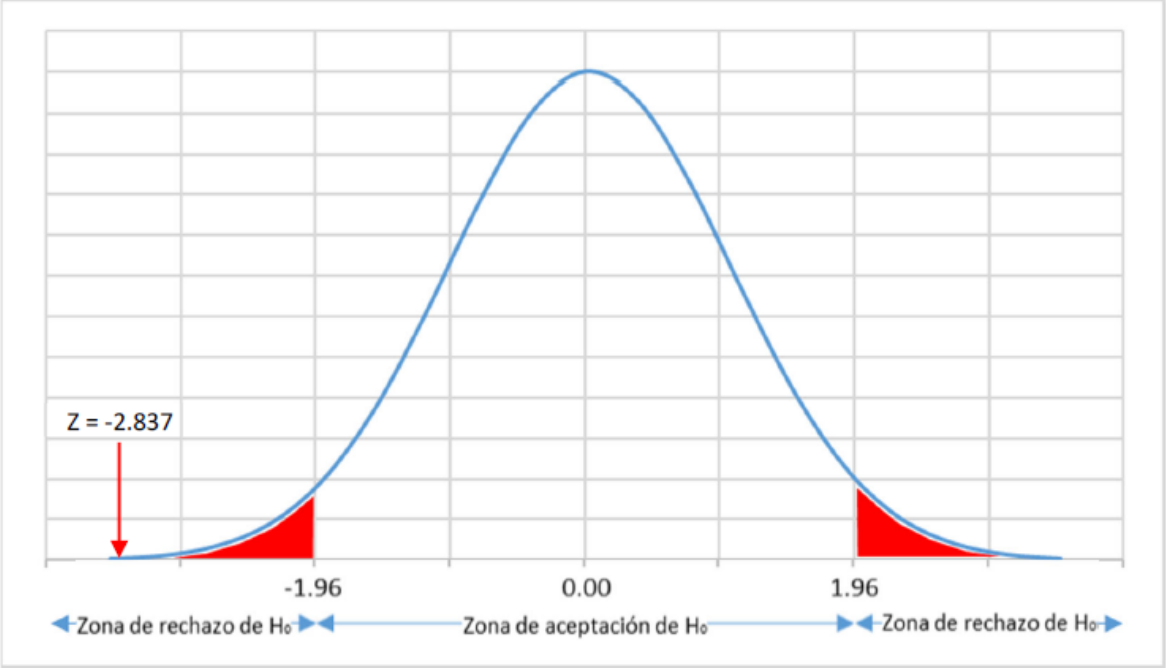
a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Siguiendo con la contrastación de hipótesis del indicador porcentaje de riesgo de fallas, en la tabla 14 se visualiza que el estadístico de prueba (z) conseguido es -2.837, el que por ser inferior a -1.96 se localiza en la zona de rechazo de la hipótesis nula (ver figura 6); Adicionalmente, el nivel de significancia (p) fue 0.005 el cual es menor a 0.05, por tanto se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1); el cual revela que, la biometría facial mejora significativamente el indicador porcentaje de riesgo de fallas.

Figura 6

Contrastación bilateral de la hipótesis del indicador porcentaje de riesgo de fallas



Nota. Material utilizado Microsoft Excel.

V. Discusión

Debido a los resultados hallados en el estudio, ya que nos brindan todos los cambios en la variable dependiente en el proceso de autenticación del usuario, se realizan las siguientes comparaciones.

En el análisis descriptivo del indicador 1 Cantidad de validaciones con errores, en la pre-prueba la media fue 26.92 y en la post-prueba fue de 4, esto quiere decir que hay una mejora de 22.92, después de ejecutar la biometría facial. También, para la prueba de normalidad del análisis inferencial, se empleó la prueba de Shapiro-Wilk, en donde en la pre-prueba y post-prueba resulto con un nivel de significancia (p) igual a 0.000 y por ser inferior a 0.05 no se aceptó la hipótesis nula (H0) y la hipótesis alterna se acepta (H1); el cual revela como los datos del indicador Cantidad de validaciones con errores poseen una distribución no normal.

Partiendo de la contrastación de los resultados del indicador Cantidad de validaciones con errores y de los antecedentes, se visualiza una mejora significativa respecto a cada uno de ellos: En ese sentido Pinto et al. (2021) obtuvo como resultado de la pre- prueba y post-prueba aplicado al proceso de validación para emisores en la organización Alignet S.A.C, en la ciudad de Lima, que el sistema de gestión de datos posee el efecto esperado en el rendimiento ya que fue posible disminuir las transacciones denegadas por error de un promedio de 18% a 14%, afirmando que si influye, el cual se revela en la reducción del 4% de transacciones denegadas. Asimismo, Correa et al. (2020), obtuvo como resultado, que las transacciones se incrementaron de 46% a 79%, afirmando que la metodología Six Sigma mejora el proceso de ventas autenticadas con tarjetas digitales. Por otra parte, Luna (2015), obtuvo como resultado de la pre-prueba y post-prueba aplicada a la autenticación de usuarios mediante biometría facial del iris, que los falsos negativos en la autenticación se redujeron de un 0.238% a 0.005%, afirmando que la biometría facial por iris mejora en la reducción de los falsos negativos. Asimismo, Mohamad (2013), obtuvo como resultado de la pre-prueba y post-prueba aplicada a la proyección

multilineal del Reconocimiento biométrico facial, que el error en las imágenes faciales 2-D es de 5.9% y al aplicar el método de curvilíneo paso a 3.5% de error, por lo tanto, hubo una mejora del 2.4%, afirmando que la proyección multilineal si mejora el reconocimiento facial. Asimismo, Caicedo (2019), obtuvo como resultado que las transacciones se incrementaron de 46% a 79%, afirmando que la metodología Six Sigma mejora el proceso de ventas autenticadas con tarjetas digitales. De igual modo, Estrela (2021), con su investigación titulada Autenticación contínua basada en biometría de comportamiento para aplicaciones de banca móvil; los resultados mostraron que del 90,68% al 97,05% de los resultados provinieron de mejoras en la confiabilidad de la autenticación y del 9,85% al 1,88% de mejoras en la reducción de riesgos, afirmando que la biométrica contínua mejora el proceso de autenticación en la banca móvil.

En el análisis descriptivo del indicador 2 tiempo de consulta, se evidenció que la media de las muestras en la pre-prueba y post-prueba fueron 01:23 y 0:26 segundos respectivamente, entonces hay una mejora de 00:57 segundos, después de implementar biometría facial. Asimismo, en el análisis inferencial para la prueba de normalidad se empleó la prueba de Shapiro-Wilk, en donde en la preprueba fue 0.097 y post-prueba fue 0.297, entonces como en ambos casos es mayor a 0.05 se acepta la hipótesis nula (H0) y se rechaza la hipótesis alterna (H1); el cual revela que, los datos del indicador tiempo de consulta poseen una distribución normal.

Partiendo de la contrastación de los resultados del indicador tiempo de consulta y de los antecedentes, se visualiza una mejora significativa respecto a cada uno de ellos: En ese sentido Ruiz (2018), obtuvo como resultado de la pre-prueba y post-prueba aplicado para la consulta y tramite del DNI y/o el DNI electrónico en el RENIEC, en la ciudad de Lima, que la app “RENIEC móvil facial” usando validación biométrica facial posee el efecto esperado en el rendimiento ya que fue posible disminuir la gestión de los tramites de un promedio de 50 minutos a 10 minutos, afirmando que la app “RENIEC móvil facial” usando validación

biométrica facial si influye en el proceso de consulta y tramite del DNI y/o el DNI electrónico en el RENIEC, el cual se revela en la reducción de 40 minutos de espera. De igual forma, Oyola (2022) obtuvo como resultado en una institución educativa, aplicando un Sistema de autenticación biométrica de tecleo, que los tiempos de pulsacion como patron de identidad son un aporte a la seguridad de la información, dentro del marco de un sistema de autenticación biométrica que permite ver los sucesos de pulsar luego soltar la tecla, nuevamente soltar la tecla para pulsar otra vez la tecla y al momento en que pasa estos dos eventos, es decir la velocidad del desplazamiento que transcurre entre tecla y tecla podrá determinar si la persona es la está detrás de la autenticación a pesar de tener la credencial correcta.

Los resultados del análisis descriptivo del indicador 3 porcentaje de riesgo de fallas muestran que las medias en la pre-prueba fueron de 11,3333 y en la post-prueba fue de 2,6667, respectivamente, lo que implica una mejora de 8,6666 tras introducir la biometría facial. Para el análisis inferencial de la prueba de normalidad se utilizó la prueba de Shapiro-Wilk, donde la pre y post prueba obtuvo un nivel de significación (p) igual a 0.000 y se rechazó la hipótesis nula (H0) por ser menor a 0.05, se acepta la hipótesis alterna (H1); esto indica que el porcentaje de riesgo de fallas está distribuido de manera no normal.

Partiendo del indicador porcentaje de riesgo de fallas y de los antecedentes, la contrastación de los resultados se visualiza una mejora significativa en referencia a cada uno de ellos: En ese aspecto, Espinosa (2013), logro como resultado de comparar la biometría facial general con la biometría facial con reconocimiento térmico, que la biometría facial aplicado con machine learning, el cual al comparar el facial general con el facial térmico se mostró una mejora del error causado por la baja iluminación donde está expuesta el lente del dispositivo que captura el rostro, la mejora fue de un 95.1% a 100% de reducción del error de validación por baja iluminación. Por otra parte, Cienfuegos (2017) obtuvo como resultado de la pre-prueba y post-prueba, una mejora de 66.30 a 94.10, se obtuvo un aumento de 32.50% en la implementación de la

biometría de voz.

Respecto al Objetivo General

Después de investigar la forma de determinar de qué manera la biometría facial mejora el proceso de autenticación del usuario en una Notaría Pública, Lima 2022; se consigue resultados favorables del indicador cantidad de validaciones con errores, en la cual la pre-prueba fue de 26.92% y post-prueba fue de 4% respectivamente, evidenciando que las validaciones con errores disminuyo un 22.92%; análogamente se lograron resultados a favor del indicador tiempo de consulta, la pre-prueba fue de 01:23 y la post-prueba fue de 0:26 segundos respectivamente, evidenciando que el tiempo de consulta disminuyo 00:57 segundos y del indicador riesgo de fallas, en la pre-prueba fue de 11.3333 y post-prueba fue de 2.6667% respectivamente, evidenciando que el riesgo de fallas disminuyo un 8.6666%. Se afirma que La implementación de biometría facial mejora así el proceso de autenticación de usuarios para notarios, Lima 2022; 00:57 segundos menos de tiempo de consulta debido a una reducción del 22,92% en verificaciones falsas, eliminando el riesgo de errores en un 8,6666%;

Esta afirmación concuerda con, los autores Pinto y Zúñiga (2021), Correa y Panizo (2020), Luna (2015), Mohamad (2013), Caicedo (2019), Ruiz (2018), Oyola (2022), Espinosa (2013), Cienfuegos (2017), Estrela (2021), sustentan que la biometría facial, mejoro todos los procesos relacionados con la autenticación, minimizo las fallas de conexión tanto de software como hardware, y redujo las validaciones con error, también conocidos como falsos negativos.

Respecto a la Metodología

El método científico se utiliza en el presente estudio, porque nos aproxima a la solución que se plantea en la investigación y la investigación del tipo aplicada se enfoca en solucionar problemas reales. Además, como diseño experimental, permite el control de variables para lograr el objetivo planteado; las variables son

cuantitativas y fáciles de medir; y también se utiliza el muestreo probabilístico para garantizar que toda la población tenga la misma probabilidad de ser seleccionada.

El uso de métodos de observación permite la obtención de los datos a medir. El uso de modelos observacionales como herramienta de recolección de datos contribuye al desarrollo de la tecnología porque los investigadores recolectan datos; asimismo, la disponibilidad de herramientas de evaluación expertas asegura la confiabilidad de los datos obtenidos.

VI: Conclusiones

Primera: Se concluye de acuerdo a los resultados, que la biometría facial mejora significativamente el proceso de autenticación de usuarios en una Notaría Pública de Lima 2022, pues los tres indicadores denominados, validaciones con errores, tiempo de consulta y riesgo de fallas, sí demostraron la existencia de mejoras de acuerdo a la post-prueba luego de corroborarlo contra la pre-prueba, y la prueba de hipótesis se efectuó la prueba no paramétrica de rangos con signos de Wilcoxon para validar los indicadores validaciones con errores, tiempo de consulta y riesgo de fallas.

Segunda: La biometría facial significativamente mejoro las validaciones con errores, porque los resultados muestran que existe un 22.92% de mejora en la post- prueba después de haber sido comparado contra la pre-prueba, adicionalmente se utilizó la prueba no paramétrica de Wilcoxon según la contrastación de hipótesis donde z tiene como valor -3.740 y 0.000 de significancia, la hipótesis tiene su área de rechazo dentro del valor donde se encuentra z y la significancia es menor a 0.05.

Tercera: La biometría facial significativamente mejoro el tiempo de consulta, porque los resultados muestran que existe un 00:57 segundos de mejora en la post-prueba después de haber sido comparado contra la pre-prueba, adicionalmente se utilizó como distribución de probabilidad la t de student según la contrastación de hipótesis donde t tiene como valor 22.689 y 0.000 de significancia, la hipótesis tiene su área de rechazo dentro del valor donde se encuentra t y la significancia es menor a 0.05.

Cuarta: La biometría facial significativamente mejoro el riesgo de fallas,

porque los resultados muestran que existe un 8.6666% de mejora en la post-prueba después de haber sido comparado contra la pre-prueba, adicionalmente se utilizó la prueba no paramétrica de Wilcoxon según la contrastación de hipótesis donde z tiene como valor -2.837 y 0.005 de significancia, la hipótesis tiene su área de rechazo dentro del valor donde se encuentra z y la significancia es menor a 0.05.

VII. Recomendaciones

Primera: Con la finalidad de mantener los resultados a favor, en el proceso de autenticación de usuarios en una Notaría Pública, Lima 2022; se recomienda al notario; implementar este proceso de autenticación mediante la biometría facial a todos sus servicios sin excepción, porque garantiza una autenticación más fiable que la biometría dactilar; asimismo innovar en tecnología de punta en los dispositivos de captura para la biometría facial, porque funcionaran más rápido y con menos probabilidad de fallas técnicas. Finalmente, se le recomienda al notario proponer que la tecnología de biometría facial reemplace a la dactilar dentro del marco legal del decreto Legislativo del *Notariado, Decreto* Legislativo Nº1049 ya que según esta investigación la biometría facial mejora el proceso de autenticación del usuario cuando se usa biométrica dactilar.

Segunda: Con la finalidad de mantener los resultados a favor, el indicador cantidad de validaciones con errores; se recomienda al notario; capturar las imágenes con biometría facial en un área con mucha iluminación, de preferencia luz blanca y fondo blanco, los cuales contribuyen a una mejor muestra de la captura de la imagen con biometría facial y pueda validarse correctamente y no caer en validaciones con error o falsos negativos.

Tercera: Con la finalidad de mantener los resultados a favor, el indicador tiempo de consulta; se recomienda al notario; usar dispositivos de captura con biometría facial con un lente de óptima calidad, que pueda disparar la captura de manera inmediata y así ganar más segundos en el tiempo de consulta, asimismo fijar el dispositivo de captura y fijar también la ubicación del usuario para que al momento de realizar la captura no se pierda tiempo tratando de cuadrar el rostro de la persona.

Cuarta: Con la finalidad de mantener los resultados a favor, el indicador riesgo de fallas; se recomienda al notario; contar con un internet independiente para este servicio, para que la conexión entre la notaría y RENIEC no se pierda y sea fluida, sin interferencias; asimismo, los dispositivos de captura con biometría facial deben contar un lente de óptima calidad, para que no haya fallas por capturas de baja calidad, finalmente Mantener una comunicación con el área de soporte de RENIEC ante una posible caída del servicio.

REFERENCIAS

Abdulkareem, I. (2014). The surgical waiting time initiative: A review of the Nigerian situation. Department of Trauma and Orthopaedic Surgery, Leeds University Teaching Hospitals, Leeds, West Yorkshire, United Kingdom. Nigerian Medical Journal, 55(6), 443-451. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4262837/pdf/NMJ-55-443.pdf

Alvarez, A. (2021). Clasificación de las investigaciones. Universidad de Lima, 1-3. https://repositorio.ulima.edu.pe/handle/20 500.12724/10818

ARCION (2013). La suplantación de identidad. Colectivo ARCION, Dirección General de Investigación, 6-7. http://revista.cleu.edu.mx/new/descargas/1301/articulos/01_La_suplantacion_de_identidad_de_tipo_fisico,_informatico_y_de_telecomunicaciones_como_nueva_manifestacion_de_consductas_antisociales.pdf

Arias, J. (2020). Técnicas e instrumentos de investigación científica. Enfoques Consulting EIRL, 14. https://repositorio.concytec.gob.pe/handle/20 500.12390/2238

Arun, R., Sudipta, B. y Chowdhury, A. (2022). Deducing health cues from biometric data. Department of Computer Science and Engineering, Michigan State University, East Lansing, MI, USA, 221, 1-2. https://reader.elsevier.com/reader/sd/pii/S1077314222000522?token=4A878B2050F4B3D6EA997C79EFBC3A1BA959A75D132D53962AC9FE5C658F79F027393FEB5D6273B2F7731199E9BBEFEC&originRegion=us-east-1&originCreation=20221018044219

Benini, A., Chataigner, P., Noumri, N., Parham, N., Sweeney J. y Tax, L. (2017). The Use of Expert Judgment in Humanitarian Analysis – Theory, Methods, Applications. Geneva, Assessment Capacities Project – ACAPS, 29-30. https://www.acaps.org/sites/acaps/files/resources/files/acaps_expert_judgment_-_full_study_august_2017.pdf

Bernal, M. (2022). La identificación y autenticación electrónica ante la administración de la comunidad autónoma de Aragón. Revista Aragonesa de Administración Pública, 302. https://dialnet.unirioja.es/descarga/articulo/8514302.pdf

Browning, J. (2018). The battle over biometrics. Texas Bar Journal, 81, 674-676. https://www.inei.gob.pe/media/MenuRecursivo/boletines/estadisticas_de_criminalidad_seguridad_ciudadana_abr-jun2021.pdf

Caicedo, J. (2019). *Plataforma de Servicio de Identificación Biométrica Facial*. https://reunir.unir.net/bitstream/handle/123456789/8254/CAICEDO%20GONZALEZ%2C%20JOSE%20LUIS.pdf?sequence=1&isAllowed=y

Cienfuegos, S. (2017). Biometría de voz en la seguridad de la información en las notarías públicas peruanas. https://repositorio.ucv.edu.pe/handle/20.500.12692/16295

CONCYTEC (2019). Memoria Institucional 2019. Consejo Nacional de Ciencia, Tecnología e innovación Tecnológica, 6-18. http://repositorio.concytec.gob.pe/bitstream/20.500.12390/2197/1/memoria_institucional_Concytec_2019.pdf

Condori, P. (2020). Universo, población y muestra. Creative Commons, 3. https://www.aacademica.org/cporfirio/18.pdf

Contento, M. (2019). *Estadística con aplicaciones en R. Editorial Utadeo*, 47. https://www.utadeo.edu.co/sites/tadeo/files/node/publication/field_attached_file/libro_estadistica_con_aplicaciones_en_r_def_ago_11.pdf

Correa, C. y Panizo, M. (2020). *Mejora en el proceso de autenticación utilizando la metodología six sigma en la empresa Alignet S.A.C*. https://repositorio.ulima.edu.pe/handle/20.500.12724/12777

Cox, J. y Schleier, J. (2010). *Theory of constraints handbook*, 10-11. https://coloradoleancollege.com/wp-content/uploads/2019/12/theory_of_constraints_handbook.pdf

Esfeh, M., Saidi, S., Wirasinghe, S. y Kattan, L. (2022). Waiting time and headway modeling considering unreliability in transit service. Transportation Research Part A: Policy and Practice, 155, 1-3. https://www.sciencedirect.com/science/article/pii/S0965856421003001

Espinosa, V. (2013). *Face recognition by means of advanced contributions in machine learning. Universitat Politecnica de Catalunya Barcelonatech*.

https://www.tdx.cat/bitstream/handle/10803/128872/TVED1de1.pdf?sequence=1

Espinoza, F. (2018). Las variables y su operacionalización en la investigación educativa. Universidad técnica de machala, 14(65), 41. https://www.researchgate.net/profile/Eudaldo-Espinoza-Freire/publication/328268666_Las_variables_y_su_operacionalizacion_en_la_investigacion_educativa_Parte_I/links/5bc261bd458515a7a9e72bdc/Las-variables-y-su-operacionalizacion-en-la-investigacion-educativa-Parte-I.pdf

Estrela, P. (2021). Autenticação contínua baseada em biometria comportamental para aplicações bancárias mobile. https://repositorio.unb.br/handle/10482/39850

Faraldo, P. (2010). Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico. Revista de derecho penal y criminología, 3(3), 2-11. http://e-spacio.uned.es/fez/eserv/bibliuned:revistaDerechoPenalyCriminologia-2010-3-5030/Documento.pdf

Friginal, J., Guiochet, J. y Killijian, M. (2016). Towards a privacy Assessment methodology for location-Based systems. Hal Open Sciencie, 748-753. https://adsp.ngo/wp-content/uploads/2018/12/A-72_REPORT-OF-THE-PUBLIC-INQUIRY-INTO-LAND-USURPATION.pdf

Gabaldon, L. (2008). Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico. Sociologias,10(20),164-190. https://www.redalyc.org/pdf/868/86819551008.pdf

Garrido, R. y Becker, S. (2017). La biometría en Chile y sus riesgos. Revista chilena de derecho y tecnología, 6,67-91. https://scielo.conicyt.cl/pdf/rchdt/v6n1/0719-2584-rchdt-6-01-00067.pdf

Goldratt, E. (1979). *Theory of constraints*, 4-8. http://brharnetc.edu.in/br/wp-content/uploads/2018/11/5.pdf

Groop, J. (2012). *Theory of Constraints in Field Service*, 26-28. http://lib.tkk.fi/Diss/2012/isbn9789526045948/isbn9789526045948.pdf

Guerrero, J., Sigifredo, E., Chamorro, H. y Isaza, G. (2013). El error como oportunidad de aprendizaje desde la diversidad en las prácticas evaluativas. Plumilla educativa, 12(2), 375. https://dialnet.unirioja.es/servlet/articulo?codigo=4757466 Hanusz, Z., Tarasinska, J. & Zieliński, W. (2016). Shapiro–Wilk test with known mean. 14. 89-100. https://www.researchgate.net/publication/298706800_Shapiro-Wilk_test_with_known_mean

Hernandez, C. (2019). Introducción a los tipos de muestreo. Alerta, Revista Científica del Instituto Nacional de Salud, 2, 2-3. https://www.lamjol.info/index.php/alerta/article/view/7535/7746

INCIBE (2016). Tecnologías biométricas aplicadas a la ciberseguridad. Instituto Nacional de Ciberseguridad, 6. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

INEI (2021). Estadísticas de la criminalidad, seguridad ciudadana y violencia. Informe técnico INEI, 49. https://www.inei.gob.pe/media/MenuRecursivo/boletines/estadisticas_de_criminalidad_seguridad_ciudadana_abr-jun2021.pdf

Jasserand, C. (2016). Legal nature of biometric data: From “generic” personal data to sensitive data. University of Groningen Faculty of Law, 2, 297-311. https://deliverypdf.ssrn.com/delivery.php?ID=255100081087114089124119113013001023016039060039010087100115109070069092029101065022019117103061008030027113127018103097080076043075078051054005004109031104090123105003079016087009089027103019122089002113006004105079076015068100085126120079112082003027&EXT=pdf&INDEX=TRUE

Leca-Principe J.H., Alcántara-Moreno O.R., Cieza-Mostacero S.E. (2022). Facial recognition mobile application to improve the neonatal care process in a hospital in El Porvenir [Aplicación Móvil de Reconocimiento Facial para Mejorar el Proceso de Atención Neonatal en un Hospital de El Porvenir]. CISCI 2022 - Vigesima Primera Conferencia Iberoamericana en Sistemas, Cibernetica e Informatica, Decimo Noveno Simposium Iberoamericano en Educacion, Cibernetica e Informatica – Memorias. https://www.scopus.com/inward/record.uri?eid=2-s2.0-

85137281686&doi=10.54808%2fCISCI2022.01.152&partnerID=40&md5=658c86dc03c97a2b837600b167af8edf

Lindholm, C. (2013). A case study on software risk análisis and planning in medical device development. Group Departamento of computer Sciencie, Faculty of Engineering, Lund University, 5. https://fileadmin.cs.lth.se/cs/Personal/Christin_Lindholm/A_case_study_on_software_risk.pdf

Luna, A. (2015). *Autentificación de un usuario basado en la biometría facial del iris empleando patrones de reconocimiento de imagen para clientes móviles Android*. https://repositorio.umsa.bo/xmlui/handle/123456789/8715

Mccleskey, J. (2020). Forty years and still evolving: the theory of constraints. American Journal of Management, 20(3), 65. http://www.m.www.na-businesspress.com/AJM/AJM20-3/6_McCleskeyFinal.pdf

Mohamad, A. (2013). *Biometric face recognition using multilinear projection and artificial intelligence*. https://core.ac.uk/download/pdf/153778411.pdf

Monge, A., Murillo, G., Calderón, A. y Vega, A. y Aguilar, A. (2014). Listas de Espera. Acta Médica Costarricense, 56(2), 3. http://www.redalyc.org/articulo.oa?id=43431275007

Munandar, M. y Rahman, A. (2021). Analisis keamanan pair based text authentication pada skema login. Seminar Nasional Sistem Informasi Indonesia, 2-3. https://www.researchgate.net/publication/356844273_ANALISIS_KEAMANAN_PAIR_BASED_TEXT_AUTHENTICATION_PADA_SKEMA_LOGIN

Oyola, H. (2022). Sistema de autenticación biométrica de tecleo para mejorar la seguridad en un sistema web de una I.E.N. - Chiclayo. https://repositorio.ucv.edu.pe/handle/20 500.12692/85412

Paredes, E. y Velasco, M. (2022). *Teoría general de sistemas*, 10-11. https://docplayer.es/18932892-Teoria-general-de-sistemas.html

Pinto, K. y Zuñiga, K. (2021). *Sistema de gestión de datos en el proceso de autenticación para emisores en la empresa ALIGNET S.A.C*. https://repositorio.ucv.edu.pe/handle/20 500.12692/73856

Posada, G. (2016). *Elementos básicos de estadística descriptiva para el análisis de datos.* Editorial Luis Amigo. 15. https://www.funlam.edu.co/uploads/fondoeditorial/120_Ebook-elementos_basicos.pdf

Prabhu, D., Bhanu, S. y Suthir, S. (2022). Privacy preserving steganography based biometric authentication system for cloud computing environment. Department of Computer Science and Engineering, Annamalai University, India, 24, 1-2. https://reader.elsevier.com/reader/sd/pii/S2665917422001453?token=9AB239F2BCBBFEB2D55FCD3985DA33635A3A270F91384CF77F896BF32142E704EB3F551661D7F605881C6E6CDB923557&originRegion=us-east-1&originCreation=20221018031529

Rodríguez, G., Schuch, C., Antunez, M. y Piovesan, C. (2021). General Systems Theory and Remanufacturing. Id Online Rev. Psicho, 16(59), 1-2. https://idonline.emnuvens.com.br/id/article/view/3220/5307

Rodriguez, R. y Ribon, J. (2018). Políticas de seguridad informática (PSI). Departamento de Tecnología Organización Inca, 10. https://www.centroinca.com/centro_inca/documentos/politica_seguridad_informatica.pdf

Romero, M., Figueroa, G., Vera, D., Alava, J., Parrales, G., Alava, C., Murillo, A. y Castillo, M. (2018). Introducción a la seguridad Informática y el análisis de vulnerabilidades. 3ciencias, 16. https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Ruiz, F. (2018). *Implementación de la aplicación "RENIEC Móvil Facial" utilizando autenticación biométrica facial para consultas y trámites de DNI/DNIE en el RENIEC*. https://cybertesis.unmsm.edu.pe/handle/20 500.12672/17750

Saiz, M. (2017). Gestión de calidad. Universidad de Burgos, 9. https://riubu.ubu.es/bitstream/handle/10259/4889/Tema_3_metodologia_para_la_evaluacion.pdf

Sakshi, C., Sharma, C., Sharma, S., Kautish, S., Alsallami, S., Khalil, E., Mohamed, A. (2022). A new median-average round Robin scheduling algorithm: An optimal

approach for reducing turnaround and waiting time. Alexandria University, 61, 1-3. https://www.sciencedirect.com/science/article/pii/S1110016822002599

Salas, E. (2013). Pre-Experimental designs in Psychology and education: a conceptual review. Universidad de San Martín de Porres, Perú, 1-4. http://dev.scielo.org.pe/pdf/liber/v19n1/a13v19n1.pdf

Skyttner, L. (2005). *General systems theory. Worl Scientific*, 2, 5-20. https://books.google.com.pe/books?id=38NoDQAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Tamayo, G. (2021). Diseños muestrales en la investigación. Universidad de Medellín, 4(7), 4-5. https://dialnet.unirioja.es/servlet/articulo?codigo=5262273

Thenuwara, S., Premachandra, C. y Kawanaka, H. (2022). A multi-agent based enhancement for multimodal biometric system at border control. Department of Electronic Engineering, Shibaura Institute of Technology, Tokyo, Japan, 14, 1-2. https://www.sciencedirect.com/science/article/pii/S2590005622000327

Tikkinen-Piri, C. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34, 134-152. http://jultika.oulu.fi/files/nbnfi-fe201802203509.pdf

Tolosa, C. y Giz, A. (2019). Sistemas Biométricos. Universidad Nacional Jose Faustino Sanchez Carrion, 14. https://www.dsi.uclm.es/personal/miguelfgraciani/mikicurri/docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

Valle, A. y Manrique, L. (2022). La Investigación Descriptiva con Enfoque Cualitativo en Educación. Pontificia Universidad Católica del Perú, 35-36. https://files.pucp.education/facultad/educacion/wp-content/uploads/2022/04/28145648/GUIA-INVESTIGACION-DESCRIPTIVA-20221.pdf

Vega, E. (2021). Seguridad de la información. 3ciencias, 28. https://www.3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIO%CC%81N.pdf

Von Bertalanffy, L. (1989). *Teoría general de los sistemas*, 4, 1-5. https://fad.unsa.edu.pe/bancayseguros/wp-content/uploads/sites/4/2019/03/Teoria-General-de-los-Sistemas.pdf

Zachos, P., Pruzek, R. y Hick, T. (2003). Approaching Error in Scientific Knowledge and Science Education. International History, Philosophy of Science and Science Teaching Conference Proceedings, Winnipeg, 7, 1-11. https://acase.org/files/approachingerror.pdf

Zhang, T., Yang, G., Lee, B. y Chan, A. (2015). Predicting severity of bug report by mining bug repository with concept profile. The ACM Digital Library is published by the Association for Computing Machinery, 1553-1558. https://dl.acm.org/doi/pdf/10.1145/2695664.2695872

ANEXOS

Anexo 1: Matriz de Consistencia

TÍTULO: **Biometría Facial en la mejora del proceso de autenticación del usuario en una Notaría Pública, Lima 2022.**
AUTOR: JUAN ROYER ESPINOZA BERAMENDI.

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES
Problema principal: ¿De qué manera la biometría facial mejora el proceso de autenticación del usuario en una notaría Pública, Lima 2022?	**Objetivo principal:** Determinar de qué manera la biometría facial mejora el proceso de autenticación del usuario en una notaría Pública, Lima 2022.	**Hipótesis principal:** La biometría facial mejora significativamente el proceso de autenticación del usuario en una notaría Pública, Lima 2022	**Variable - 1:** Biometría Facial **Variable - 2:** en la mejora del proceso de autenticación del usuario en una Notaría Pública, Lima 2022.
Problemas específicos: (i) ¿De qué manera la biometría facial mejora el indicador de la cantidad de validaciones con errores en el proceso de autenticación del usuario en una notaría Pública, Lima 2022?	**Objetivos específicos:** (i) Determinar de qué manera la biometría facial mejora el indicador cantidad de validaciones con errores en el proceso de autenticación del usuario en una notaría Pública, Lima 2022.	**Hipótesis específicas:** (i) La biometría facial mejora significativamente la cantidad de validaciones con errores en el proceso de autenticación del usuario en una notaría Pública, Lima 2022.	
(ii) ¿De qué manera la biometría facial mejora el indicador tiempo de consulta en el proceso de autenticación del usuario en una notaría Pública, Lima 2022?	ii) Determinar de qué manera la biometría facial mejora el indicador tiempo de consulta en el proceso de autenticación del usuario en una notaría Pública, Lima 2022.	(ii) La biometría facial mejora significativamente el tiempo de consulta en el proceso de autenticación del usuario en una notaría Pública, Lima 2022.	

Indicadores	**Unidad de medida**
Cantidad de validaciones con errores.	Porcentual
Tiempo de consulta.	Minutos
Porcentaje de riesgo de fallas.	Porcentual

TÍTULO: **Biometría Facial en la mejora del proceso de autenticación del usuario en una Notaría Pública, Lima 2022.** **AUTOR: JUAN ROYER ESPINOZA BERAMENDI.**			
PROBLEMA	**OBJETIVOS**	**HIPÓTESIS**	**VARIABLES E INDICADORES**
(iii) ¿De qué manera la biometría facial mejora el indicador porcentaje de riesgo de fallas en el proceso de autenticación del usuario en una notaría Pública, Lima 2022?	(iii) Determinar de qué manera la biometría facial mejora el indicador porcentaje de riesgo de fallas en el proceso de autenticación del usuario en una notaría Pública, Lima 2022.	(iii) La biometría facial mejora significativamente el porcentaje de riesgo de fallas en el proceso de autenticación del usuario en una notaría Pública, Lima 2022.	

Metodología

TIPO Y DISEÑO	**POBLACIÓN Y MUESTRA**	**TÉCNICAS E INSTRUMENTOS**	**ESTADÍSTICA POR UTILIZAR**
Tipo: Aplicada. **Diseño:** Experimental-pre experimental.	**Población:** 50 validaciones de usuarios. **Muestreo:** aleatorio.	**Técnicas:** Observación y recolección de datos. **Instrumentos:** Guía de Observación.	**Descriptiva**: se usará tablas y figuras, exponiendo medidas de tendencia central usando la media, se realizará su interpretación o lectura por cada indicador. **Inferencial**: Comprobación de la normalidad de los datos obtenidos mediante la prueba Test de Shapiro Wilk.

Anexo 2: Matriz de Operacionalización de Variables

TÍTULO: Biometría Facial en la mejora del proceso de autenticación del usuario en una notaría Pública, Lima 2022.

AUTOR: Juan Royer Espinoza Beramendi

INDICADOR	DEFINICIÓN	INSTRUMENTO	UNIDAD DE MEDIDA	FÓRMULA
Cantidad de validaciones con errores.	Zhang et al. (2015), indica que el error es una equivocación en un reporte y que su gravedad debe ser informado para decidir qué tan rápido se debe solucionar.	Guía de observación	Porcentual	Cantidad de validaciones con errores = Cantidad de intentos fallidos / Cantidad de intentos x100
Tiempo de consulta.	Esfeh et al. (2022) dicen que el tiempo de espera es una función de la hora de salida deseada desde el origen y el punto de transferencia, y la hora de llegada deseada frente al horario del servicio	Guía de observación	Minutos	Tiempo de consulta = Tiempo Final – Tiempo Inicial
Porcentaje de riesgo de fallas	Friginal et al. (2016), define el riesgo como el potencial de que una amenaza dada aproveche las vulnerabilidades de un activo y por lo tanto cause daño a la organización.	Guía de observación	Porcentual	Riesgo de fallas = cantidad de fallas presentadas / cantidad de fallas registradas x100

Anexo 3: Instrumento de Recolección de Datos

Ficha de observación N° 1. Indicador cantidad de validaciones con errores

Ficha de observación de medición del indicador cantidad de validaciones con errores / Preprueba				
Investigador:			Juan Royer Espinoza Beramendi	
Proceso observado:			proceso de autenticación del usuario	
Pre-Test				
N° de Obs.	DNI	Fecha	Error	Cantidad de validaciones con errores = Cantidad de intentos fallidos / Cantidad de intentos x 100
1				
2				
3				
4				
5				
6				
N				

Ficha de observación de medición del indicador cantidad de validaciones con errores / Postprueba				
Investigador:			Juan Royer Espinoza Beramendi	
Proceso observado:			proceso de autenticación del usuario	
Post -Test				
N° de Obs.	DNI	Fecha	Error	Cantidad de validaciones con errores = Cantidad de intentos fallidos / Cantidad de intentos x 100
1				
2				
3				
4				
5				
6				
N				

Ficha de observación N° 2. Indicador tiempo de consulta

Ficha de observación de medición del indicador tiempo de consulta / Preprueba					
Investigador:			Juan Royer Espinoza Beramendi		
Proceso observado:			proceso de autenticación del usuario		
Pre-Test					
N° de Obs.	DNI	Fecha	Tiempo inicial	Tiempo Final	Tiempo de consulta = Tiempo Final – Tiempo Inicial
1					
2					
3					
4					
5					
6					
N					

Ficha de observación de medición del indicador tiempo de consulta / Post prueba					
Investigador:			Juan Royer Espinoza Beramendi		
Proceso observado:			proceso de autenticación del usuario		
Post-Test					
N° de Obs.	DNI	Fecha	Tiempo inicial	Tiempo Final	Tiempo de consulta = Tiempo Final – Tiempo Inicial
1					
2					
3					
4					
5					
6					
N					

Ficha de observación N° 3. Indicador porcentaje de riesgo de fallas

Ficha de observación de medición del indicador porcentaje de riesgo de fallas / Preprueba					
Investigador:			Juan Royer Espinoza Beramendi		
Proceso observado:			proceso de autenticación del usuario		
Pre-Test					
N° de Obs.	DNI	Fecha	Fallas Presentadas	Fallas Registradas	Riesgo de fallas = cantidad de fallas presentadas / cantidad de fallas registradas x 100
1					
2					
3					
4					
5					
6					
N					

Ficha de observación de medición del indicador porcentaje de riesgo de fallas / Postprueba					
Investigador:			Juan Royer Espinoza Beramendi		
Proceso observado:			proceso de autenticación del usuario		
Post-Test					
N° de Obs.	DNI	Fecha	Fallas Presentadas	Fallas Registradas	Riesgo de fallas = cantidad de fallas presentadas / cantidad de fallas registradas x 100
1					
2					
3					
4					
5					
6					
N					

Anexo 4: Certificado de Validación del Instrumento de Recolección de Datos

Validación del Experto N°1

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO

VARIABLE: PROCESO DE AUTENTICACIÓN DEL USUARIO

Nº	INDICADORES	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
		Si	No	Si	No	Si	No	
1	INDICADOR 1: Cantidad de validaciones con errores **Cantidad de validaciones con errores** = Cantidad de intentos fallidos x 100 / Cantidad de intentos	X		X		X		
2	INDICADOR 2: Tiempo de consulta **Tiempo de consulta** = Tiempo Final – Tiempo Inicial	X		X		X		
3	INDICADOR 3: Porcentaje de riesgo de usurpación **Porcentaje de riesgo de usurpación** = Alertas detectadas x margen de error del dispositivo	X		X		X		

Observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA

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

17 de octubre del 2022

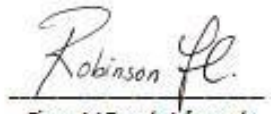
Apellidos y nombres del juez evaluador: Yañez Romero Robinson Manuel DNI: 73041890

Especialista: Metodólogo [X] Temático [ ]

Grado: Maestro [X] Doctor [ ]

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

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



Firma del Experto Informante

Validación del Experto N°2

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO

VARIABLE: PROCESO DE AUTENTICACIÓN DEL USUARIO

N°	INDICADORES	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
		Si	No	Si	No	Si	No	
1	**INDICADOR 1: Cantidad de validaciones con errores** Cantidad de validaciones con errores = Cantidad de intentos fallidos x 100 / Cantidad de intentos	X		X		X		
2	**INDICADOR 2: Tiempo de consulta** Tiempo de consulta = Tiempo Final – Tiempo Inicial	X		X		X		
3	**INDICADOR 3: Porcentaje de riesgo de usurpación** Porcentaje de riesgo de usurpación = Alertas detectadas x margen de error del dispositivo	X		X		X		

Observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA

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

Apellidos y nombres del juez evaluador: MORALES FERNANDEZ SANTOS IVAN **DNI: 42243830**

Especialista: Metodólogo [X] Temático [ ]

Grado: Maestro [X] Doctor [ ]

17 de octubre del 2022

ING. MORALES FERNÁNDEZ SANTOS IVÁN

Firma del Experto Informante

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

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

Validación del Experto N°3

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO

VARIABLE: PROCESO DE AUTENTICACIÓN DEL USUARIO

N°	INDICADORES	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
		Si	No	Si	No	Si	No	
1	**INDICADOR 1: Cantidad de validaciones con errores** **Cantidad de validaciones con errores** = Cantidad de intentos fallidos x 100 / Cantidad de intentos	X		X		X		
2	**INDICADOR 2: Tiempo de consulta** **Tiempo de consulta** = Tiempo Final – Tiempo Inicial	X		X		X		
3	**INDICADOR 3: Porcentaje de riesgo de usurpación** **Porcentaje de riesgo de usurpación** = Alertas detectadas x margen de error del dispositivo	X		X		X		

Observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez evaluador: **ACUÑA BENITE MARLON FRANK** **DNI: 42097456**

17 de OCTUBRE del 2022

Especialista: Metodólogo [ ] **Temático [X]**

Grado: Maestro [X] **Doctor [ ]**

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

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

Firma del Experto Informante

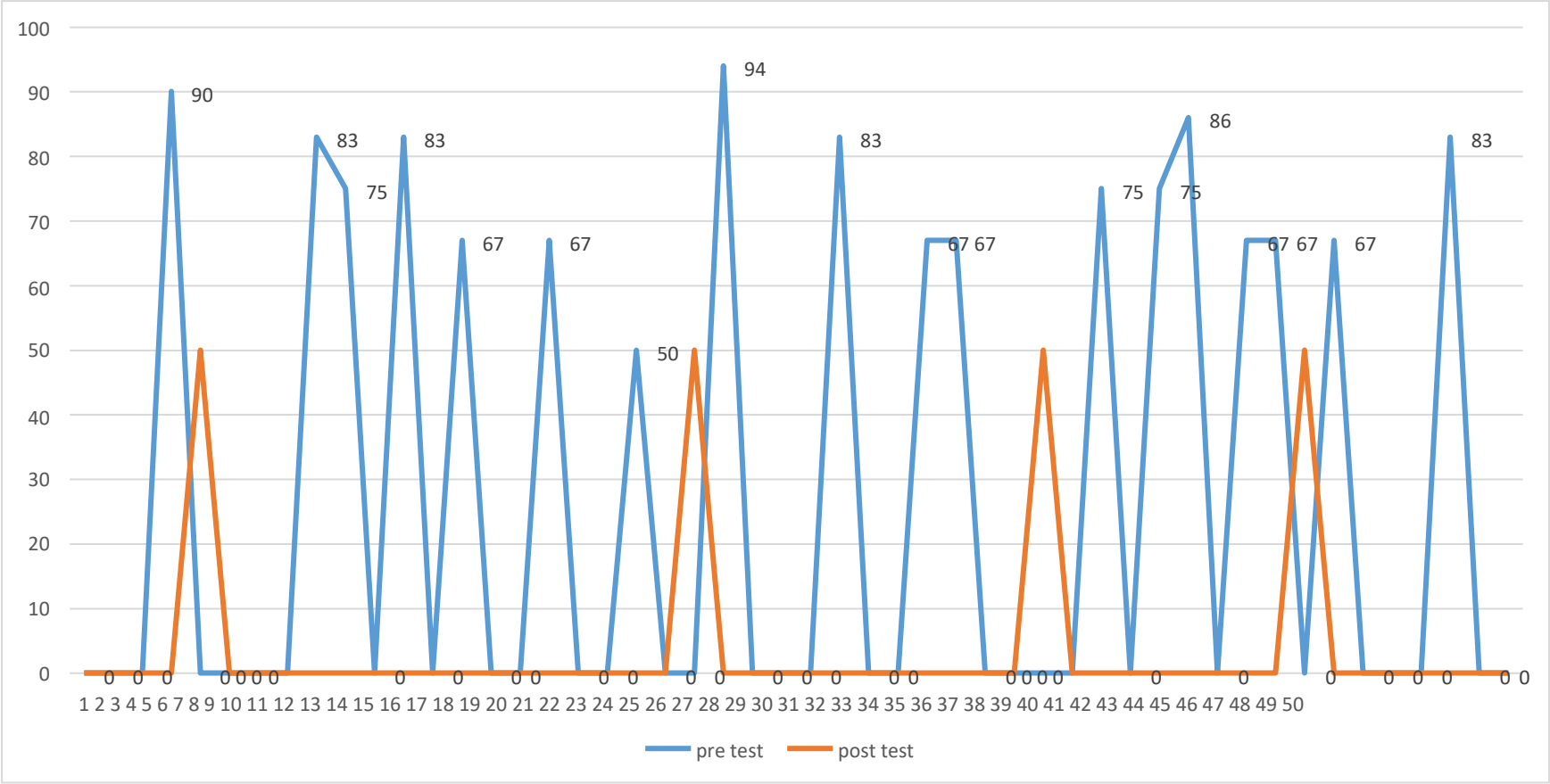
Anexo 5: Base de datos

	Indicador 1		Indicador 2		Indicador 3	
N	I1PreTest	I2PostTest	I1PreTest	I2PostTest	I1PreTest	I2PostTest
1	0	0	01:20	00:29	0.00	33.33
2	0	0	01:29	00:25	33.33	0.00
3	0	0	01:31	00:35	0.00	0.00
4	90	0	01:19	00:26	0.00	0.00
5	0	50	01:36	00:23	33.33	0.00
6	0	0	01:21	00:24	0.00	0.00
7	0	0	01:53	00:30	0.00	33.33
8	0	0	01:37	00:24	33.33	0.00
9	83	0	01:04	00:33	0.00	0.00
10	75	0	01:22	00:24	0.00	0.00
11	0	0	01:08	00:31	33.33	0.00
12	83	0	01:13	00:25	0.00	0.00
13	0	0	00:52	00:28	0.00	0.00
14	67	0	01:16	00:31	33.33	0.00
15	0	0	01:03	00:34	0.00	0.00
16	0	0	00:56	00:26	33.33	0.00
17	67	0	01:04	00:35	33.33	0.00
18	0	0	01:33	00:34	0.00	33.33
19	0	0	01:10	00:39	33.33	0.00
20	50	0	01:15	00:24	0.00	0.00
21	0	0	01:47	00:29	33.33	0.00
22	0	50	01:50	00:31	0.00	0.00
23	94	0	01:22	00:22	0.00	0.00
24	0	0	01:06	00:17	33.33	0.00
25	0	0	01:15	00:21	0.00	0.00
26	0	0	01:33	00:22	0.00	0.00
27	83	0	01:26	00:28	33.33	0.00
28	0	0	01:24	00:35	0.00	0.00
29	0	0	01:14	00:26	0.00	0.00
30	67	0	01:49	00:20	33.33	0.00
31	67	0	01:51	00:33	0.00	0.00
32	0	0	01:41	00:29	0.00	0.00
33	0	0	01:13	00:19	33.33	0.00
34	0	50	01:54	00:21	0.00	0.00
35	0	0	01:16	00:22	33.33	0.00
36	75	0	01:30	00:25	0.00	0.00
37	0	0	01:18	00:22	0.00	0.00

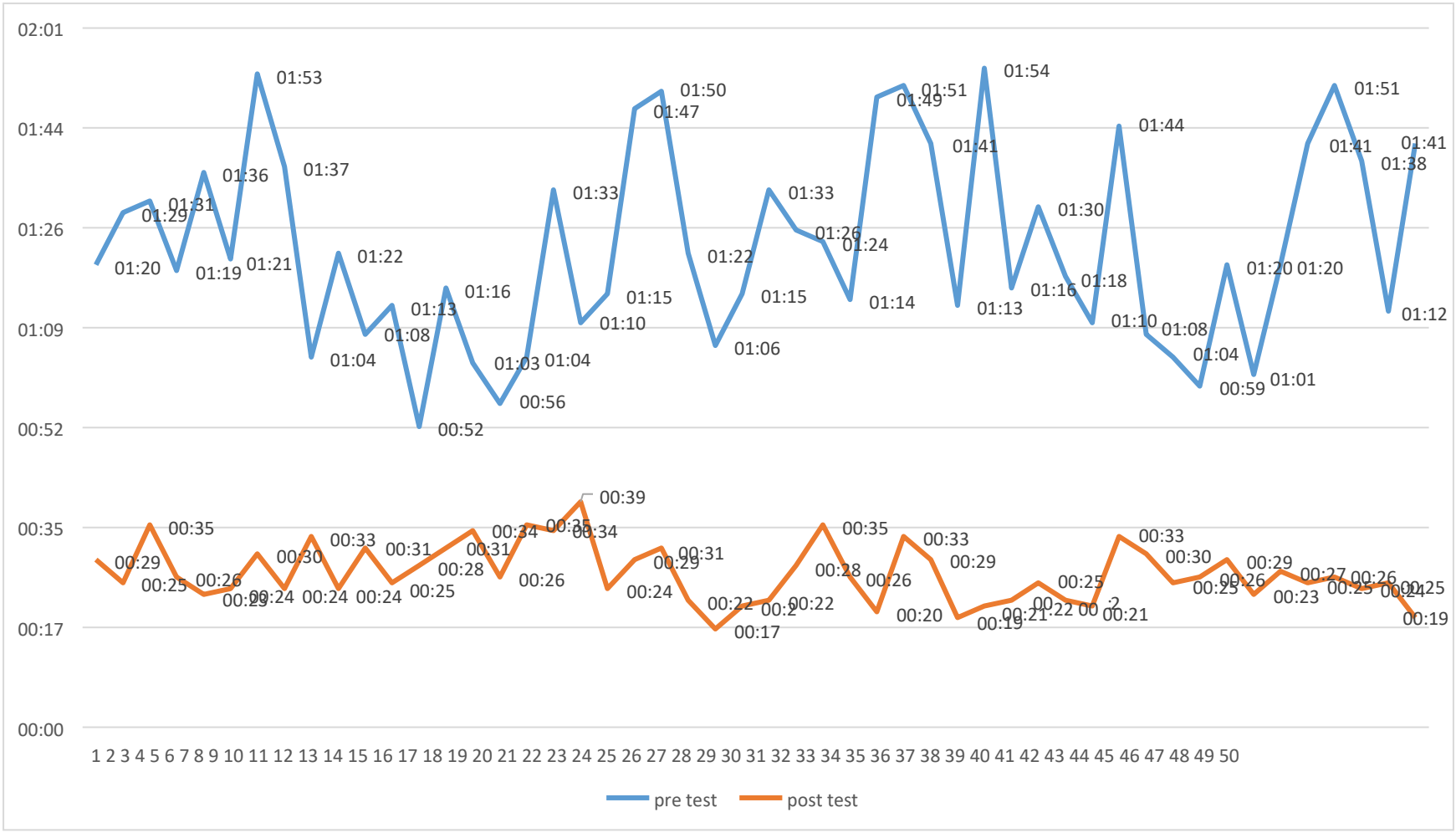
38	75	0	01:10	00:21	33.33	0.00
39	86	0	01:44	00:33	0.00	0.00
40	0	0	01:08	00:30	0.00	0.00
41	67	0	01:04	00:25	0.00	0.00
42	67	0	00:59	00:26	33.33	0.00
43	0	50	01:20	00:29	0.00	33.33
44	67	0	01:01	00:23	0.00	0.00
45	0	0	01:20	00:27	0.00	0.00
46	0	0	01:41	00:25	0.00	0.00
47	0	0	01:51	00:26	0.00	0.00
48	83	0	01:38	00:24	0.00	0.00
49	0	0	01:12	00:25	33.33	0.00
50	0	0	01:41	00:19	0.00	0.00

Anexo 6: Comportamiento de las medidas descriptivas

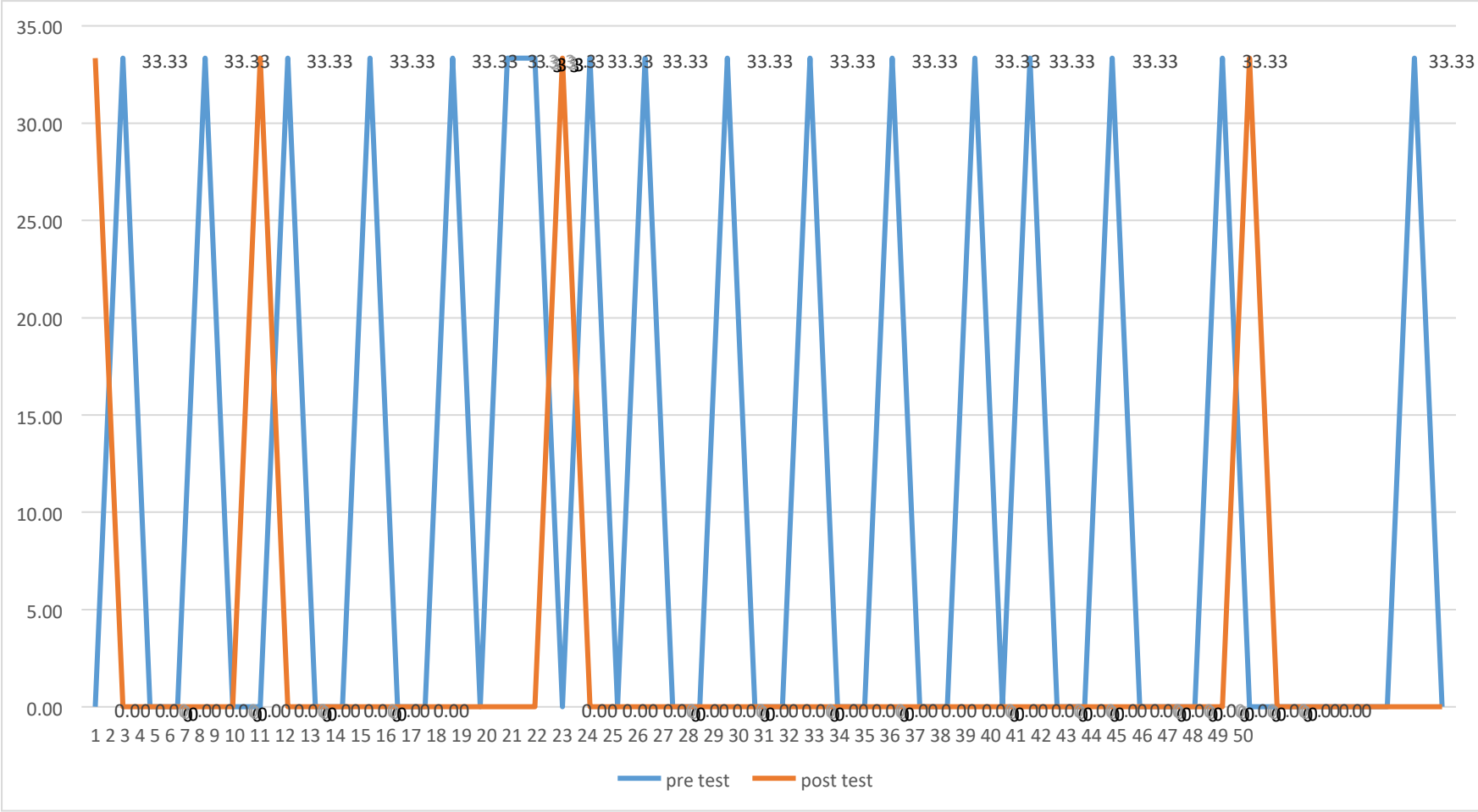
Indicador 1: Comportamiento de las medidas descriptivas del indicador porcentaje de validaciones con errores, antes y después de la implementación de la biometría facial.



Indicador 2: Comportamiento de las medidas descriptivas del indicador tiempo de consulta, antes y después de la implementación de la biometría facial.



Indicador 3: Comportamiento de las medidas descriptivas del indicador Porcentaje de riesgo de fallas, antes y después de la implementación de la biometría facial.



UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Autenticidad del Asesor

Yo, VISURRAGA AGUERO JOEL MARTIN, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Biometría Facial en la mejora del Proceso de Autenticación del Usuario en una Notaría Pública, Lima 2022", cuyo autor es ESPINOZA BERAMENDI JUAN ROYER, constato que la investigación tiene un índice de similitud de 21.00%, 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, 07 de Enero del 2023

Apellidos y Nombres del Asesor:	**Firma**
VISURRAGA AGUERO JOEL MARTIN **DNI:** 10192325 **ORCID:** 0000-0002-0024-668X	Firmado electrónicamente por: JMVISURRAGA el 11-01-2023 20:53:33

Código documento Trilce: TRI - 0513092

INVESTIGA UCV