UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Sistema de autenticación biométrica de tecleo para mejorar la seguridad en un sistema web de una I.E.N. - Chiclayo

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

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

AUTOR:

Oyola Yarlaque, Hugo Hamilton (ORCID: 0000-0002-1369-1301)

ASESOR:

Dr. Pacheco Torres, Juan Francisco (ORCID: 0000-0002-8674-3782)

LÍNEA DE INVESTIGACIÓN:

Sistema de Información y Comunicaciones

TRUJILLO – PERÚ

2022

Dedicatoria

A mi esposa Shirley y a mis hijos Alexia Consuelo y Hugo David por su tolerancia, comprensión y paciencia, porque son el motivo de mi deseo de superación.

Con mucho cariño a mí queridos padres Consuelo, Hugo y Alejandrina sin su inmenso cariño y apoyo, no habría sido posible alcanzar mis metas.

Y en especial a mis segundos Padres Rosa Angélica Morí Gallegos y Federico Yarlaqué Córdova y a Lázaro Oyola quienes me iluminan desde el cielo y me siguen guiando en este trajinar de la vida.

A la Madre Santísima Virgen del Pilar, quien me ha dado la fe, salud y fortaleza para alcanzar mis metas.

Agradecimiento

A la “UNIVERSIDAD CÉSAR VALLEJO”, a la Escuela de Posgrado – Trujillo y a los docentes por brindarme la oportunidad de acogerme en sus aulas y permitirme cumplir esta meta propuesta.

A mis amigos de ahora y siempre, con quienes formé parte de grupos de trabajo, disfrutando de muy buenos momentos en el transcurso de la maestría y a quienes agradezco por haberlos conocido y por compartir conmigo sus experiencias y conocimientos.

EL AUTOR.

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

El presente trabajo de investigación titulado “Sistema de autenticación biométrica de tecleo para mejorar la seguridad en un sistema web en I.E.E. San José – Chiclayo”, se muestra la aplicación de un método biométrico de autenticación basado en la observación de la forma de teclear de los usuarios utilizando el patrón de tecleo o dinámica de tecleo del usuario. El tipo de indagación es aplicativa, con enfoque cuantitativo y diseño pre experimental. En el estudio participaron 30 trabajadores conformado por docentes, auxiliares de educación, personal administrativo, personal de servicio de la institución educativa, los cuales fueron elegidos en forma no probabilística por conveniencia y criterio del investigador. Fue validado por tres (03) expertos y sometido a la prueba de Alpha de Cronbach para obtener la confiabilidad de 0,914, indicando que el instrumento es altamente confiable. Se utilizó el instrumento cuestionario para recopilación de información. Los resultados mostraron el nivel que cuenta la institución educativa para implementar el sistema de autenticación biométrica de tecleo, conforme a los resultados recabados: dimensión seguridad el 60,0% lo considera bueno y un 43,3% indica es regular. En la medida en que logre implementarse, la autenticación biométrica de tecleo conllevaría que los procesos sean con total transparencia.

Palabras clave: autenticación biométrica, dinámica de tecleo, sistema web.

Abstract

The present research work entitled “Biometric Click Authentication System to Improve Security in a Web System at I.E.E. San José – Chiclayo”, shows the application of a biometric authentication method based on the observation of the user’s typing style using the user’s typing pattern or dynamics. The type of inquiry is applicable, with a quantitative approach and a pre-experimental design. The study involved 30 workers consisting of teachers, education assistants, administrative staff, and service staff of the educational institution, who were chosen in a non-probabilistic manner according to the convenience and criteria of the researcher. It was validated by three (03) experts and subjected to the Cronbach Alpha test to obtain the reliability of 0.914, indicating that the instrument is highly reliable. The questionnaire tool was used to collect information. The results showed the educational institution’s level of implementation of the biometric click authentication system, according to the results obtained: the security dimension 60.0% consider it good and 43.3% say it is regular. To the extent that it is implemented, biometric one-click authentication would mean that the processes are completely transparent.

Keywords: biometric authentication, click dynamics, web system.

I. INTRODUCCIÓN

A nivel internacional el mercado de las tecnologías biométricas crecerá en los próximos años y alcanzará los 55,420 millones de dólares para el año 2027. Además, se tiene que la compañía de Detección de Amenazas Informáticas, NordPass realizó un análisis en el cual detectó las contraseñas más frecuentes a nivel mundial. Considerándose que muchos usuarios, siguen usando sus mismas claves y ponen en peligro sus datos personales (Mena Roa, 2020).

NordPass detalla un ranking de 10 posiciones en las que se detallan las contraseñas más usadas a nivel mundial en el año 2020, se puede como primera posición tenemos la clásica contraseña 123456, pues miles de personas siguen utilizando los seis primeros dígitos en su password y no necesitan letras. Esta combinación ha sido hackeada 23 millones de veces al año. También se puede apreciar 123456789, que es parecida a la anterior, para aquellas webs que requieren más de 6 dígitos. Una contraseña se ha sido incorporada recientemente es picture1, es lo más común en plataformas de fotografía. La contraseña password, es la que jamás pasará de moda, ya que se debe mencionar que es un clásico de clásicos. El 12345678, es la favorita de los internautas y en este caso sin el número 9. El 111111, tiene más de 230,000 personas usan esta contraseña. Se considera también a la contraseña 123123, no es buena opción repetir 1, 2 y 3. El 12345, es menos común su uso, pero con una diferencia solo tiene 5 caracteres y es menos descubierta. Recordar que también es un clásico la contraseña 1234567890, puesto que es una consecución de números es también muy utilizada. Por último, tenemos a senha, es muy original, es una “contraseña” en portugués, está en el ranking debido a la cantidad de hablantes en esta lengua.

En Argentina (2020), la policía y otras fuerzas de seguridad implementaron el Sistema Federal de Identificación Biométrica (SIBIOS) el cual permite identificar personas con fines de investigación delincuencial.

Se debe tener en consideración que un municipio de la ciudad de Colombia (Guerrero, 2019), intentó implementar el reconocimiento facial en los servicios de transporte, este plan fue abortado por no existir datos a nivel nacional que hacía imposible las comparaciones.

Según Galindo (2018), en el que cita la frase de Robert Mueller “Hay dos tipos de empresa: las pirateadas y las que serán”, propone una nueva realidad digital sobre la seguridad en los actuales tiempos para acceder a cualquier sistema web o de escritorio, basado por contraseña ya sea redes públicas o privadas, pues están expuestas a sufrir diferentes tipos de ataques pasivos o activos, que vulneran sus infraestructuras.

En nuestro país las normativas que vienen regulando la utilización de la biometría ascienden al siglo XX y se concentra en crear registros y documentos para la validación del voto (libreta electoral) y facilitar el reclutamiento (libreta militar), actualmente no están en uso. A partir de 1993 se creó RENIEC, esta entidad estatal se ha encargado de definir y ejecutar la mayor parte de políticas públicas relacionadas a la biometría. En su inicio se utilizó esta tecnología para modernizar el sistema de registro de los ciudadanos como DNI y DNI electrónico. Por ello esta entidad utilizó los sistemas de biometría AFIS (Guerrero, 2019).

Se debe entender que el Perú ha sufrido los cambios respecto al incesante desarrollo tecnológico, acentuándose mucho en su mayoría por la epidemia del COVID-19 que ha afectado a la mayor parte del mundo y según las estadísticas policiales se tiene que entre enero y abril del 2021, existen 1,188 denuncias por casos que están relacionados a delitos informáticos y suplantación de identidad. (Peruano, 2021).

Asimismo, nuestro país cuenta con diversas normativas en materia de biometría, como la Ley N° 26497, Ley de Identidad Nacional y Registro Civil y sus modificaciones (1995) que otorgan al RENIEC implementar y mantener datos biométricos, la Ley N° 27269, La Ley y el Reglamento de Firmas y Certificados Digitales (2000) establece una representación de archivo de identidad y ordena el uso de verificación biométrica, el único proceso de este tipo a nivel subestatal. El caso es RENIEC, D. L. N° 1049 "Ordenanza Legal sobre Notario Público", modificado por D. L. N° 1232 (2015), que obliga a los notarios a utilizar la verificación biométrica para certificar principios, texto que prevé términos únicos de uso para servicios públicos de telecomunicaciones - OSIPTEL (2012) Los proveedores de servicios de telecomunicaciones utilizarán la verificación biométrica para identificar suscriptores y D. S. N° 023-2014-MTC (2014) Los transportistas y

distribuidores de tarjetas SIM o chips deben utilizar la verificación biométrica para verificar la identidad de una persona.

En el aspecto Nacional se tiene al Instituto Nacional de Estadística e Informática (INEI), no cuenta con información relevante debido a que nuestra legislación informática peruana está muy desfasada en el aspecto delictivo informático que se ha incrementado con nuevos ataques a la información. Asimismo, no se cuenta con información regional y menos del Departamento de Lambayeque, pues los ciudadanos de a pie no denuncian estos incidentes que ocurren a diario por los llamados ciberdelincuentes, quienes operar realizando ataques para dañar la información de instituciones, empresas y organizaciones, en las cuales aflora grandes pérdidas económicas y vulneran las barreras de protección, lo que queda es proteger las redes de comunicación. Se hace necesario el poder explorar nuevos modelos que se aproximen a una mayor seguridad de datos, modelos, sistemas y/o algoritmos.

La presente investigación está encaminada en la seguridad de la información, con la finalidad de brindar nuevos prototipos de aplicación es por ello que es importante la Implementación basada en patrones de tecleo para la detección de ataques en su sistema de esta institución educativa, el compromiso es elevar los niveles de exactitud en los sistemas de autenticación biométrica, para ello se recolectarán datos que se someterán a un proceso que implicaría diferentes etapas desde el pre procesamiento (ataques en redes de comunicación, diseño de mecanismos de detección de ataques) hasta su finalización.

Por otro lado, el volumen de datos en entidades públicas y privadas se ha incrementado rápidamente debido al trabajo remoto y aulas virtuales, evidencia de ello es el aumento de la vulnerabilidad, debido a la amplia propagación de amenazas, como ciberataques y altos costos de inversión en futuros sistemas de información; esto ha cambiado por completo estas instituciones, creando un gran desafío en la profesión de ingeniería de sistemas.

En definitiva, este trabajo tiene como objetivo demostrar el aporte a la seguridad de la información, dentro del marco de un sistema de autenticación biométrica basado en patrones de mecanografía, que permita a las instituciones educativas

públicas o privadas elegir un sistema, conocer sus ventajas o desventajas, y adaptarse a su entorno de trabajo asegurando seguridad en la información de las diferentes áreas de las que es responsable.

De estos hechos descritos en los párrafos anteriores nace el planteamiento del problema tal cual se aprecia en la siguiente pregunta: ¿De qué manera el sistema de autenticación biométrica de tecleo influirá en la seguridad de un sistema web de la I.E.E. San José de Chiclayo? Formulándose el siguiente Objetivo General, Mejorar la seguridad de un sistema web a través de un sistema de autenticación biométrica de tecleo de la I.E.E. San José de Chiclayo. Se precisan los Objetivos Específicos (a) Determinar en qué medida la implementación del sistema de autenticación biométrica de tecleo influye en el procedimiento de seguridad del sistema web de la I.E.E. San José de Chiclayo (b) Determinar en qué medida la implementación del sistema de autenticación biométrica de tecleo influye en los mecanismos de seguridad del sistema web de la I.E.E. San José de Chiclayo (c) Determinar en qué medida la implementación del sistema de autenticación biométrica de tecleo influye en la prevención de la seguridad del sistema web de la I.E.E. de Chiclayo (d) Determinar en qué medida la implementación del sistema de autenticación biométrica de tecleo influye en la validación de la seguridad del sistema web de la I.E.E. San José de Chiclayo.

II. MARCO TEÓRICO

Esta sección está estrechamente relacionada con el soporte de la teoría, ya que proporciona trabajos de investigación relacionados con las variables del sistema de autenticación biométrica y la seguridad del sistema web, incluida una presentación organizada de la teoría científica en la que se basa esta investigación.

En la indagación Jiamwei Li (2021), considera el problema de verificar la identidad del usuario en función de la dinámica de pulsación de teclas obtenida del texto libre. También se muestra que un modelo híbrido que consta de una CNN y una red neuronal recurrente (RNN) supera las investigaciones anteriores en este campo.

Entre los estudios internacionales, en España se encuentra Revilla (2017), que indica que un área de la autenticación biométrica que más ha recibido atención en los últimos años es la dinámica de tecleo, que examina diferentes técnicas de clasificación de usuarios con el fin de encontrar un sistema de autenticación alternativo para las contraseñas que se utilizan en la actualidad. Finalmente, sugiere hacer un estudio sobre diferentes técnicas de clasificación de usuarios por tipificación dinámica y poder implementar un sistema utilizando una de ellas.

Asimismo, Kołakowska y Landowska (2021) en su artículo analizan las pulsaciones de teclas cuando los colaboradores escriben en forma positiva y negativa. Realizando un semi experimento con 50 colaboradores. Mediante este estudio se confirma que si era viable examinar opiniones positivas y negativas de los patrones de pulsación de teclas con una exactitud predominante a la hipótesis aleatoria.

En su artículo los autores proponen teclados únicos asignados y utilizados soló por usuarios normales de teléfonos inteligentes para mejorar las capacidades de rendimiento de clasificación de usuarios de los teclados existentes. Los teclados propuestos están formados y basados en el algoritmo Mersenne Twister. (Choi, Shincheol , Minjae, & and Ji , 2021).

De manera similar, en su indagación Aubin (2019), tenemos un método para verificar personas basado en grafemas simples, dando un alto porcentaje de

respuestas correctas, y la combinación de letras también mejoró la verificación de 100% identidad.

Aguilera (2016) mostró en su artículo que recientemente, la demanda de la dinámica del ratón está aumentando y el enfoque de la investigación se ha vuelto interesante. Al igual que la dinámica de escritura, la dinámica de ratón se considera una alternativa a los sistemas de autenticación tradicionales y proporciona seguridad de red. Todos estos factores han hecho de la dinámica del ratón una herramienta atractiva para el mercado digital.

También tenemos Chile, en el artículo muestra que la identificación personal requiere que tengamos múltiples contraseñas, tokens, números o documentos de identificación personal, que son los más adecuados para estas actividades. La tecnología biométrica proporciona muchas formas diferentes de autenticación e identificación, pero a veces es insegura (Quintanilla, 2020).

En Argentina, Calot (2019), en su estudio describe que el impulso de la escritura permite identificar a las personas por su forma de escribir. Este trabajo analiza el poder de los algoritmos de frecuencia de pulsaciones de teclas contra el sesgo en los perfiles biométricos, utiliza un enfoque dimensional para modelar estados emocionales y realiza un experimento para capturar patrones de pulsaciones de teclas en diferentes estados emocionales.

A nivel nacional, Márquez (2018) en su investigación demostró un método biométrico basado en la escritura del usuario o el reconocimiento dinámico del teclado. Para este método se utilizaron 04 particularidades de escritura: código de tecla presionada, dos tipos de tiempo entre dos pulsaciones sucesivas y tiempo de permanencia de cada tecla, que desarrolló la tecnología en el sistema. La recepción es: código de tecla, tiempo de pulsación de tecla, empuje el tiempo, empuje el tiempo de liberación. Se realizaron 95 pruebas de validación con usuarios universitarios, y el desarrollo se desarrolló en dos etapas: el primer paso buscó capturar las pulsaciones de teclas del usuario y el segundo paso aplicó 4 valores umbral para el ajuste de tarifas, con el fin de determinar el mejor valor umbral aceptable y aplicando ajustes aproximados.

Encontramos a Mendoza & Vega (2019), cuyo objetivo en su investigación es proponer un plan de control para la detección de riesgos de ciberseguridad. Sugirió construir una hoja de ruta, en la que utilizó como repositorio principal un marco de información. Asimismo, describe la Norma ISO / IEC 33020-2015 (ISO 2015) con referencia a la evaluación de capacidad de los procesos y la guía COBIT 5 para gestión de riesgos (ISACA 2013), utilizada para la gestión y el control de riesgos asociados a la tecnología de la información. Esta investigación ha sido un desafío a la hora de aplicar una metodología muy nueva en el fenómeno de la ciberseguridad.

Se tiene en su indagación Díaz (2021), que las empresas de seguridad que utilizan sistemas de autenticación de un solo factor y de dos factores no son tan seguras y tienen problemas de seguridad en la implementación. Plantea la implementación del sistema de tipificación biométrica basado en biometría y aplicando RUP para mejorar la seguridad y autenticación de los empleados de la empresa.

Esta tesis se enmarca en el tema de los sistemas de autenticación mediante la autenticación biometría de tecleo, y en este contexto se indica la escasez de cultura investigadora en este campo de investigación tanto regional como local. Encontrándose artículos universitarios y trabajos de investigación que nos aportan las siguientes conclusiones:

Chinchay (2019), en sus resultados encontramos que se ha logrado disminuir el tiempo de absorbía en registrar asistencia y elaborar reportes, logrando la inserción de un sistema biométrico para huellas digitales, estableciendo una metodología que permite mantener un proceso de control de asistencias optimizado con respecto al desempeño de los colaboradores.

Los autores Díaz & Flores (2019), en sus resultados encontramos que el prototipo diseñado demostró el efecto de solución a los problemas, pues no generaba cola, ni retardos, no cuenta con personal para su supervisión, y no ha generado un gran volumen de papeles diariamente.

Entre las teorías que sustentan la investigación se encuentran:

Autenticación:

Para Fernández (2021), la autenticación es:

> *"El proceso de identificación de usuarios y verificación de su identidad. Esto evita que alguien ingrese a un sistema en particular o inicie sesión en cualquier plataforma de manera incorrecta, sin ser realmente un usuario legítimo autorizado para hacerlo".*

Según Guidott (2020), la autenticación

> *"solo intenta garantizar que la persona que firma la transacción sea la misma que la persona que registró al usuario. Si la identidad no se verifica durante el proceso de registro, no hay garantía sobre la identidad del usuario".*

Remarca, Guidott (2020) existen 5 factores de autenticación:

- Lo que solo tú sabes: información propia que el usuario proporciona al momento del registro. Lo más típico es el nombre de usuario / contraseña.
- Lo que tú tienes: Por ejemplo, recibir un código por SMS en el teléfono del usuario o acceder a un edificio a través de una tarjeta inteligente personal, o la autenticación de direcciones en su PC.
- Lo que tú eres: Normalmente se trata
- de una característica biométrica (por ejemplo, huella digital, iris, voz, cara…) que permite autenticar al usuario.
- Allá dónde estás: La ubicación del usuario (por ejemplo, dirección IP o coordenadas GPS). No se utiliza como único método, sino en combinación con otro método de autenticación.
- Lo que tú haces: autenticar a través del comportamiento del usuario (por ejemplo, la forma en que una persona sostiene su teléfono, el gesto de pulsación de tecla, los movimientos del mouse…).

Biometría:

> *"Es una forma de identificar a las personas en función de sus características fisiológicas o de comportamiento. Es un proceso similar al que normalmente*

atraviesan los humanos, donde identifican y reconocen a sus semejantes por su apariencia, voz, forma de caminar, etc." (INCIBE, 2016).

Clasificación de la biometría:

- Biometría Estática: Se caracteriza por la medición directa de las funciones del cuerpo humano. Las principales tesis se fundan en sistemas biométricos para huellas dactilares, geometría de manos, retina, córnea, iris y geometría facial. (Tolosa & Giz, 2019).
- Biometría Dinámica: Se encarga de estudiar las características y rasgos del comportamiento de la identidad humana. Por ejemplo, firma, reconocimiento de voz, dinámica de entrada, etc. (Tolosa & Giz, 2019)

Sistema de autenticación Biométrica:

Un sistema de identificación se define como un sistema biométrico que involucra la medición de una característica del cuerpo humano para determinar la identidad de un individuo (Faces, 2020).

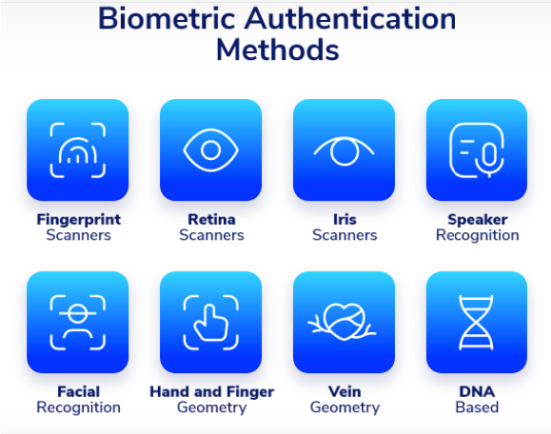
Para ello, debemos elegir una característica de gran diversidad o singularidad de un individuo a otro. Algunos de los principales métodos utilizados para identificar a las personas mediante la biometría incluyen (Din, 2021):

a) Reconocimiento por huellas dactilares: Una huella digital consta de una serie de líneas oscuras que simbolizan protuberancias llamadas vértices y una serie de áreas en blanco llamados valles.
b) Reconocimiento de firmas: Mediante un lector de firmas, la firma de una persona se analiza de dos formas: una es analizando la propia firma y la otra por escrito.
c) Mapa de la retina del ojo: Para identificar a una persona que usa este método, se hace pasar luz infrarroja a través de la pupila del ojo y se mide el patrón de las venas en la parte posterior del ojo.
d) Patrón del iris: Es un sistema biométrico más confiable porque el iris de una persona tiene 266 puntos únicos que permiten reconocerlo. Para escanear el iris, se debe usar un lector ocular para analizar los patrones de color de las ranuras en la parte coloreada del ojo.

e) Reconocimiento de la voz: Para reconocer a una persona por su voz, es necesario digitalizar los sonidos de diferentes palabras del individuo. Divida las palabras en sílabas con un timbre dominante tal vez 3 o 4, luego convertirlas a un formato digital y guárdelas en una tabla o espectro, llamado muestra de voz. (Voice Print).

Figura 1:

Método de autenticación Biométrica



Fuente: Tomado de ¿What Is Biometric Authentication?

Por otro lado, tenemos la encuesta 2016 ejecutada por Visa en Europa, determinó que dos tercios de europeos optaron por utilizar una autenticación biométrica para sus pagos o servicios a través de Internet y que la mitad de ellos creen que sus transacciones serán más sencillas y rápidas con esta tecnología (Barrios, 2017).

Patrones de tecleo:

> *"Se le conoce como dinámica de tecleo o dinámica dactilar o Keystroke Dynamics, en los cuales se ven los eventos de pulsar-soltar tecla, soltar-pulsar tecla y al tiempo en que transcurre estos dos eventos, es decir la velocidad del desplazamiento que transcurre entre tecla y tecla"* (Torres Jiménez & Acosta Escalante, 2019).

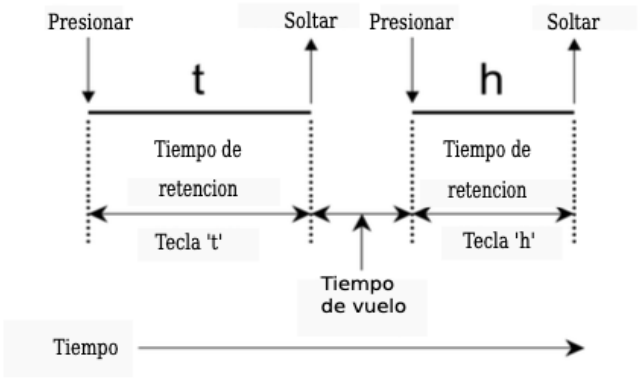
Warwick (2017) señala los rasgos más comunes:

1. Tiempo de vuelo: Este es el tiempo que transcurre desde que se suelta la tecla hasta que se pulsa la siguiente tecla repetidamente, como se muestra en la Figura 3. Este tiempo suele oscilar entre 50 y 800 milisegundos.

2. Tiempo de retención: Tiempo de retención de la clave (consulte la Figura 3), esta medida suele estar entre 60 y 140 ms.
3. Tecla: Esta es la tecla presionada, esta función proporciona información sobre el lado del teclado que se está utilizando. Esta función se utiliza para ajustar vuelos y tiempos de espera en contexto.

Figura 2:

Relación entre el tiempo de retención y latencia.



Fuente: Tomado de “Keystroke dynamics: Characteristics and opportunities”.

Características del tipo de escritura o tamaño de digitación:

Cuando el usuario ingresa su contraseña, se activan dos eventos de teclado, el evento KeyUp y el evento KeyDown. (Aguilar & Pérez, 2010).

Figura 3:

Evento Pulsar-Soltar.

- El tiempo transcurrido cuando el usuario presiona una tecla y suelta la misma tecla, llamaremos a este evento PRESS - RELEASE (KeyDown).

Fuente: Elaboración propia del autor.

Figura 4:

Evento Soltar-Pulsar

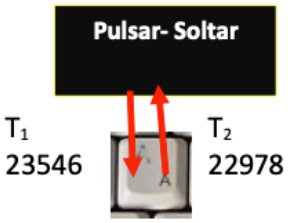
- La cantidad de tiempo que transcurre cuando el usuario suelta una tecla y presiona la siguiente tecla, llamaremos a este evento RELEASE - PRESS.

Fuente: Elaboración propia del autor.

Contador de tiempos de tecleo:

Figura 5:

Evento Soltar-Pulsar



$T_{transcurrido} = T_1 - T_2$

$T_{transcurrido} = 23546\text{-}22978$

$T_{transcurrido} = 568$

Esto indicará la cantidad de tiempo que ha transcurrido en cada evento de teclado.

Fuente: Elaboración propia del autor.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Fue aplicada el tipo de indagación, acorde Frascati (OCDE, 2015) citado en Cano (2019), son investigaciones únicas a fin de alcanzar nuevos conocimientos, desplegando ideas y transformándose en operativas; con enfoque cuantitativo.

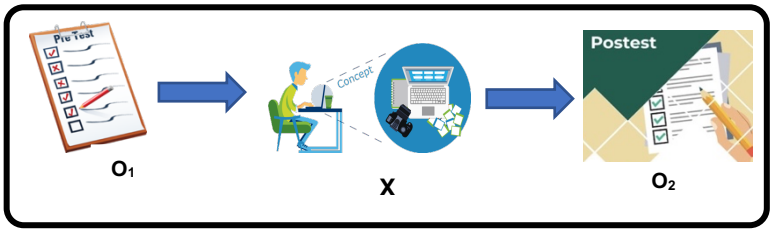
Es cuantitativa porque permite recopilar, analizar información de diversas fuentes, utilizando estadística y matemática con la intención de ponderar el problema de investigación (Hernández, Sampirie, & Mendoza, 2018).

Por otro lado, Hernández afirma que la investigación fue explicativa, ya que su objetivo es encontrar las razones o motivos de los hechos estudiados (Hernández, Sampirie, & Mendoza, 2018).

La investigación acoge diseño pre experimental, porque el investigador trata de acercarse a una investigación experimental no teniendo los medios de control suficiente que permitan la validez interna (Manzanares, 2018).

Figura 6:

Diseño de investigación



Fuente: Elaboración propia del autor.

Donde:

O1 : Seguridad en un sistema web antes de la implementación.

X : Sistema de autenticación biométrica de tecleo.

O2 : Seguridad en un sistema web después de la implementación.

3.2. Variables y operacionalización

3.2.1. Variable Independiente: *Sistema de autenticación biométrica de tecleo*

Definición conceptual:

La autenticación es una interfaz que sea capaz de recolectar los tiempos de tecleo de cada usuario al momento de autenticarse, así como también al crear sus plantillas de tecleo, esta interfaz debe proporcionarnos un conjunto de duración pertenecientes a una secuencia de caracteres escritos.

Definición Operacional:

Dependiendo del entorno de la aplicación un sistema biométrico puede ejecutarse en modo verificación o en modo identificación o reconocimiento. En el modo verificación la aplicación valida la identidad de dicha persona, En el modo identificación o reconocimiento, la aplicación compara los datos biométricos del usuario que está intentando acceder con los datos de muchos usuarios.

3.2.2. Variable Dependiente: *Seguridad en un sistema web*

Definición conceptual:

También conocido como «aplicaciones Web» son aquellos que no se instalan sobre un sistema operativo (Windows, Linux). Sino que se alojan en un servidor en la nube o sobre una intranet (red local). Su apariencia es similar a las páginas web que estamos acostumbrados a ver, pero de hecho los “sistemas web” tienen funcionalidades muy poderosas y en algunos casos brindan respuestas a casos particulares. Además, permiten adaptarse a cualquier dispositivo y de esta manera verlas desde dónde nos encontremos.

Definición Operacional:

El proceso de distribución, que es gestionado por más de una persona, debe asociarse a un negocio más dinámico. Es por eso que implementar un sistema informático o una aplicación web en la web es la mejor manera de solucionar este problema.

3.3. Población, muestra y muestreo

Población

Simbolizada por 203 trabajadores de la institución educativa emblemática San José de Chiclayo. Para Sánchez (2018), una población es un conjunto de elementos que tienen determinadas características habituales.

Tabla 1:

Población del estudio

CARGO	NÚMERO DE TRABAJADORES
DOCENTES	152
AUXILIARES DE EDUCACIÓN	18
PERSONAL ADMINISTRATIVO	26
PERSONAL DE SERVICIO	07
TOTAL	203

Fuente: Cuadro de Asignación de Personal (CAP) de la Institución Educativa Emblemática San José de Chiclayo.

Muestra

Fue de 30 trabajadores, según Sánchez (2018) es un subconjunto de la población que forma parte del objeto de estudio.

Muestreo

En el presente caso se utilizó un muestreo no probabilístico, y de acuerdo con Sánchez et al. (2018) por conveniencia del investigador, se consideró a los trabajadores: docentes, auxiliares de educación, administrativos y servicio, pues están realizando trabajo remoto ante la emergencia sanitaria ocasionada por el COVID-19 (Decreto Legislativo N° 1505, 2020).

3.4. Técnicas e instrumentos de recolección de datos

Técnica Encuesta:

Fue empleada la “encuesta online” basada en un cuestionario (Leal, 2018).

Instrumento:

Para recolectar datos se utilizó un cuestionario de 20 ítems, para los indicadores falta aceptación y falso rechazo y se consideró como respuestas la escala Likert.

Confiabilidad:

Para determinar esto, se utilizó el alfa de Cronbach. Detallándose en el anexo.

Estadística de Fiabilidad

Alfha de Cronbach	Nº de elementos
0,914	15

Validez:

Se utilizó la validación de tres expertos, que determinaron el nivel significativo del instrumento, por lo que existe afinidad entre los jueces. Según Robles y Rojas (2015), es un método muy usado, ampliamente empleado que radica en pedir a otros que den su juicio sobre la revisión de un instrumento.

3.5. Procedimientos

Se solicitó la carta de autorización para efectuar la investigación e ingresarla en mesa parte virtual de la I.E.E. Y finalmente, se efectuó el cuestionario online a los trabajadores que se hallaban efectuando trabajo remoto de la institución educativa.

3.6. Método de análisis de datos

El procesamiento de datos se realizó un pretest y postest, apoyándonos en Microsoft Excel y el software SPSS v25. Para el análisis descriptivo se utilizará tablas y figuras procediendo a la interpretación por indicador cuyos datos son del instrumento, permitiendo un entendimiento sencillo de los datos. Para el análisis inferencial se comprobó mediante la prueba de normalidad de Shapiro Wilk.

3.7. Aspectos éticos

Tabla 2:
Aspectos éticos

VALORACIÓN	PARTICULARIDADES
Medioambiente	La indagación no contamina el medio ambiente debido a que no realiza experimentos.
Objetividad	Total, y exhaustiva imparcialidad hacia los resultados de la investigación.
Privacidad	La información recopilada es confidencial, y está obligada a no brindarla a terceras personas.
Veracidad	Los datos son fácticos, obtenidos de la fuente original.

Fuente: Elaboración propia del autor.

IV. RESULTADOS

a) Resultados descriptivos del indicador Falsa aceptación.

Tabla 3:

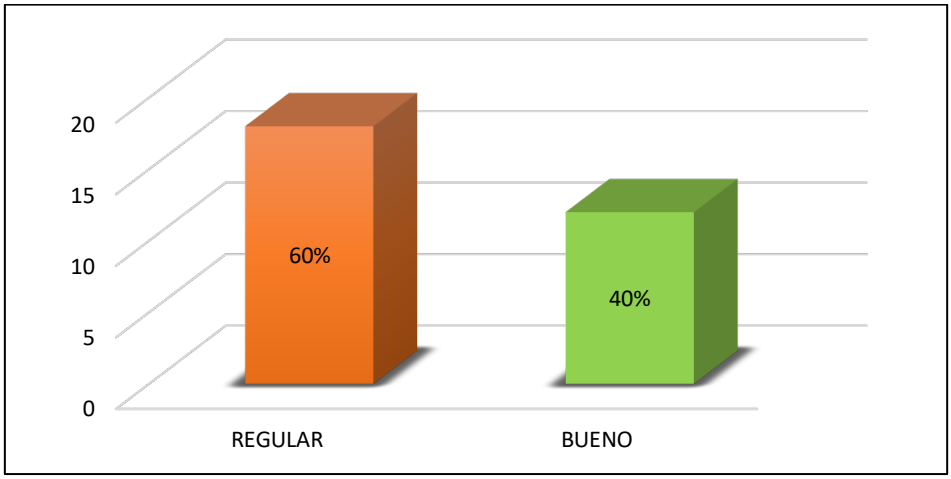
Falsa aceptación

		Frecuencia	Porcentaje
Válido	REGULAR	18	60,0
	BUENO	12	40,0
	Total	30	100,0

Fuente: Base de datos.

Figura 7:

Falsa aceptación



Nota: Resultados obtenidos de la tabla 3.

Se observa que los trabajadores en la figura 7 según los encuestados el 60% lo considera regular pues no conoce el uso del teclado, contraseñas, patrón de escritura, número de intentos, el estado de ánimo incide al momento de teclear y el 40% indica que es bueno porque considera que el método de autenticación biométrica es apropiado.

b) Resultados descriptivos del indicador Falso rechazo.

Tabla 4:

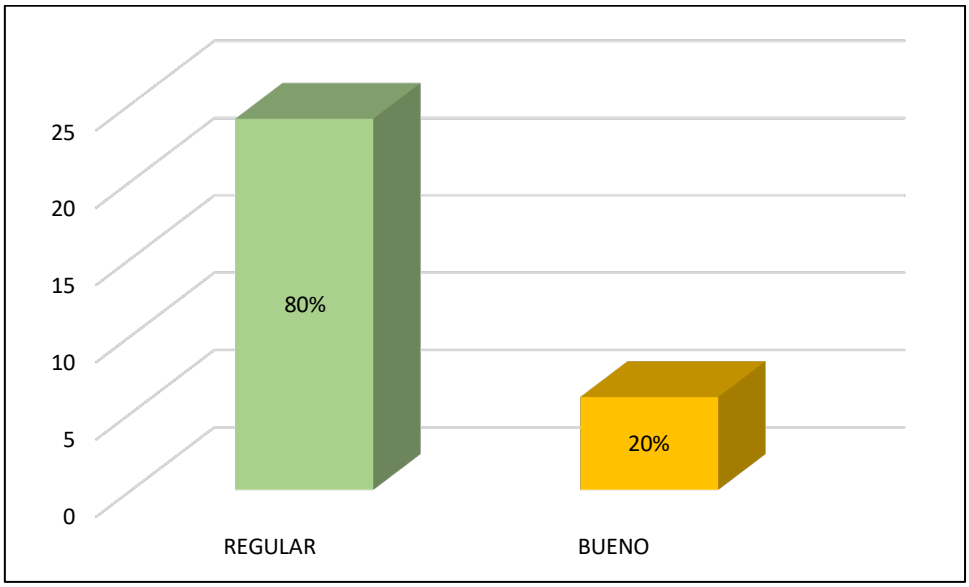
Falsa rechazo

		Frecuencia	Porcentaje
Válido	REGULAR	24	80,0
	BUENO	6	20,0
	Total	30	100,0

Fuente: Base de datos.

Figura 8:

Falso rechazo



Nota: Resultados obtenidos de la tabla 4.

De acuerdo a los resultados mostrados en la figura 8 se puede visualizar en la dimensión falso rechazo presenta un 80% indica que es regular, según estos resultados se puede inferir que los servidores consideran que para ingresar al sistema de la institución no solo basta con la contraseña para mantener un control en la seguridad del sistema, además un 20% indica que es bueno porque detecta a un usuario que no es titular y que ingresa al sistema con sus credenciales.

c) Resultados descriptivos de la variable Seguridad en un sistema web

A continuación, se presenta el resultado general obtenido de la aplicación del cuestionario sobre Seguridad en un sistema web en la I.E.E. San José – Chiclayo.

Tabla 5:

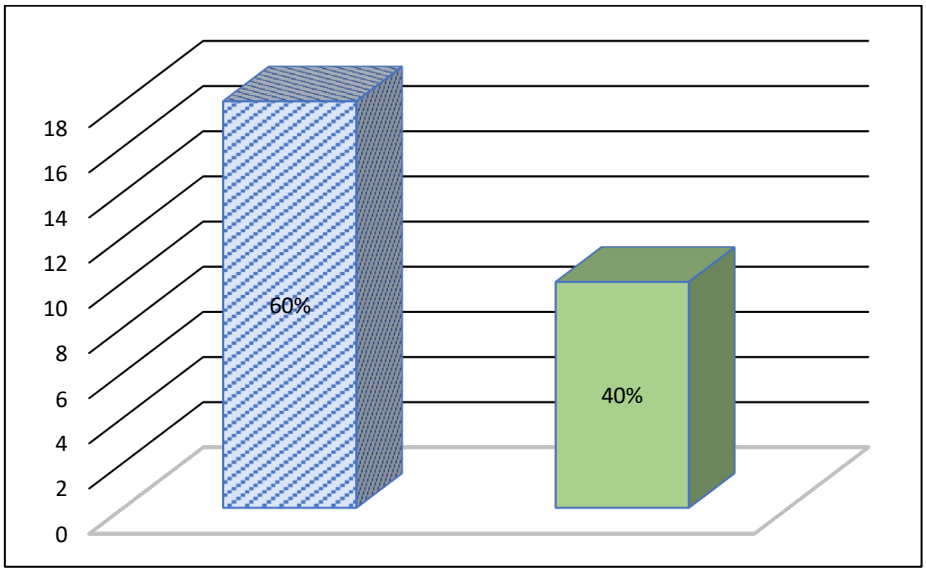
Variable General

		Frecuencia	Porcentaje
Válido	BUENO	18	60,0
	REGULAR	12	40,0
	Total	30	100,0

Fuente: Base de datos.

Figura 9:

Seguridad en un sistema web



Nota: Resultados obtenidos de la tabla 5.

Según la figura 9 muestra el análisis de la variable general donde un 60% considera que es bueno la seguridad de un sistema web, porque considera que la institución no viene aplicando un método de autenticación biométrica apropiado, sin embargo, un 40,0% sostiene la necesidad de evaluar las fallas del sistema web y generar estrategias para evitar malestares a los administrados.

Tabla 6:

Medidas descriptivas de la puntuación de pretest y postest.

Estadísticas de muestras emparejadas

		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	Falsa aceptación	17,8000	30	6,41335	1,17091
	Falso rechazo	26,4000	30	4,24751	0,77549

Fuente: Base de datos.

En la tabla observamos que en el pretest el promedio alcanzó 17,80 de ingresos de no autorizados de variabilidad de 6,41. En el post se obtuvo 26,40 no autorizados con variabilidad de 4,24 evidentemente existe una reducción.

Tabla 7:

Prueba de normalidad de Shapiro Wilk aplicado a seguridad en un sistema web.

	Shapiro-Wilk		
	Estadístico	**gl**	**Sig.**
Falsa aceptación	0,825	30	0,064
Falso rechazo	0,845	30	0,142

Fuente: Base de datos.

Los resultados obtenidos con la prueba Shapiro Wilk que muestra que existe evidencia estadística que los valores de significancia obtenidos son mayores a p=0,050, que permite concluir que estas puntuaciones tienen un comportamiento de una distribución normal.

Por lo tanto, aplicaremos estadística no paramétrica T de student de muestra relacionadas.

Tabla 8:

Prueba T aplicado a las puntuaciones del pretest y postest de los accesos no autorizados.

Prueba de muestras emparejadas

		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desv. estándar	Medida de estándar	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Falsa aceptación – Falso rechazo	8,60000	5,40498	,98681	-10,61825	-6,58175	-8,715	29	,000

Fuente: Base de datos.

Observamos en la prueba T de muestras relacionadas que el valor de significancia 0,000 es menor al valor p=0,05 que nos indica que existe evidencia estadística y existe una reducción de accesos no autorizados, es decir rechazamos la hipótesis nula.

d) Resultados de los indicadores de simulación de autenticación biométrica

El objetivo, es implementar y testear la autenticación biométrica y nos centramos en el siguiente análisis:

Figura 10:

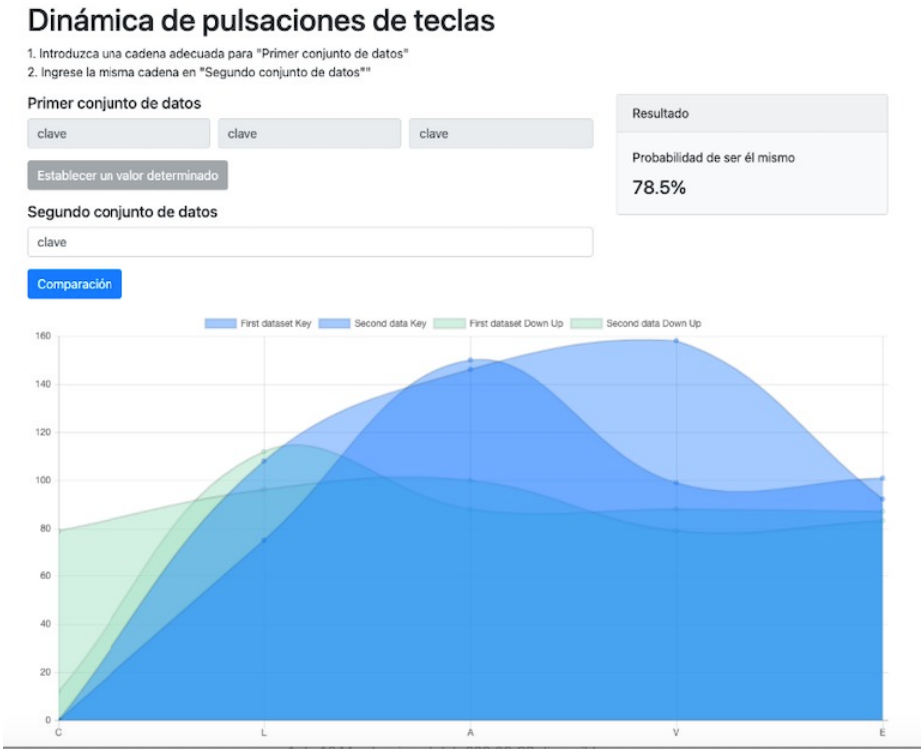
Diseño del ingreso al simulador de autenticación biométrica.

Nota: Aspecto del diseño del simulador de autenticación biométrica.

No se ha utilizado ningún framework, asimismo, el código ha sido desarrollado desde cero, mediante una página en HTML, CSS y JavaScript, los valores de tiempo que se han considerado entre ellos tenemos: código de tecla, pulsar soltar y soltar pulsar.

Figura 11:

Prueba de simulación de autenticación biométrica



Nota: Análisis de los datos obtenidos durante la simulación

Se visualiza que del grupo muestral de 30 trabajadores de la institución educativa que representa el 100%; el 78,5% se efectuaron pruebas de simulación de autenticación biométrica, cuyo objetivo fueron establecer la Falsa aceptación y Falso rechazo, se consideró el total de usuarios, esto indica que existe o la mayoría de los trabajadores tienen conocimiento alguno de la existencia de un sistema simulación de autenticación biométrica.

Los diversos datos que se obtuvieron en esta simulación la podremos encontrar en los anexos de la presente indagación.

V. DISCUSIÓN

En este apartado se muestra el resultado conseguido del cuestionario aplicado concerniente a la variable seguridad en la Institución Educativa Emblemática San José de Chiclayo, y se buscó detectar la suplantación de identidad a través del sistema de autenticación biométrica de tecleo, registrando los tiempos de latencia al pasar de una tecla a otra y los tiempos de mantener presionada una tecla. Lo detallamos empleando los contenidos y trabajos preconcebidos, los efectos mostrados concuerdan con la literatura precedente, si bien, concurren diversos puntos de vista que deben ser objetos de futuras investigaciones a fin de confirmar su eficacia.

A partir de los hallazgos encontrados, consentimos la hipótesis que sostiene que cada usuario ostenta un modelo determinado de digitación que puede ser almacenado y utilizado para detectar la suplantación de identidad en el sistema de la institución educativa emblemática San José de Chiclayo.

La finalidad de esta investigación es presentar el aporte a la seguridad de la información, dentro del marco de un sistema de autenticación biométrica basado en patrones de mecanografía, que permita, tanto a las instituciones educativas públicas o privadas elegir un sistema, conocer sus ventajas o desventajas, y adaptarse a su entorno de trabajo asegurando seguridad de la información en las distintas áreas de las que es responsable.

Análisis por Indicadores:

Tabla 3: El resultado obtenido referente a la seguridad en un sistema web de la institución educativa emblemática San José de Chiclayo, de acuerdo al estudio realizado se logró evidenciar que en cuanto al indicador falsa aceptación el 60,0% mencionan que es regular, pues no conoce el uso del teclado, contraseñas, patrón de escritura, número de intentos, el estado de ánimo incide al momento de teclear.

Asimismo, los resultados concuerdan con Torres Jiménez y Acosta Escalante (2019) quienes definen que los Patrones de Tecleo o conocido como dinámica de tecleo o dinámica dactilar o Keystroke Dynamics, ven los eventos de pulsar-soltar

tecla, soltar-pulsar tecla y al tiempo en que transcurre estos dos eventos, es decir la velocidad del desplazamiento que transcurre entre tecla y tecla.

Los resultados, encontrados se contrasta con los aportes de Kołakowska y Landowska (2021) mediante este estudio se confirma que si era viable examinar opiniones positivas y negativas de los patrones de pulsación de teclas con una exactitud predominante a la hipótesis aleatoria. Mencionan que a futuro se podrían incluir una combinación de patrones de pulsaciones de teclas con patrones de ratón o con señales fisiológicas.

El propósito de la seguridad de un sistema web ante la amenaza de ataques informáticos, requiere de esfuerzos en la totalidad del sitio web, a partir del uso de políticas para implantar y remozar contraseñas. Para ello las organizaciones deben manifestar un servicio muy oportuno y efectivo en la seguridad de sus recursos y datos que tienen, por ello se hace necesario el uso de estándares y normas en forma estructurada y coherente a fin de proceder ante las diversas situaciones que se presentan con la finalidad de prevenir, tomándose en cuenta que los individuos “hacen lo correcto si saben lo que es correcto”.

Tabla 4: En relación al indicador falso rechazo, Revilla (2017), indica que un área de la autenticación biométrica que más ha recibido atención en los últimos años es la dinámica de tecleo, que examina diferentes técnicas de clasificación de usuarios con el fin de encontrar un sistema de autenticación alternativo para las contraseñas que se utilizan en la actualidad. Asimismo, sugiere hacer un estudio sobre diferentes técnicas de clasificación de usuarios por tipificación dinámica y poder implementar un sistema utilizando una de ellas. Por ello en la Tabla 4 se puede visualizar que un 80,0% de los encuestados considera regular, además un 20,0% indica que es bueno. Estos resultados permiten coincidir con Faces (2020) un sistema de identificación se define como un sistema biométrico que involucra la medición de una característica del cuerpo humano para determinar la identidad de un individuo.

Aguilera (2016) indica que la demanda de la dinámica del ratón está aumentando y el enfoque de la investigación se ha vuelto interesante. Al igual que la dinámica de escritura, la dinámica de ratón se considera una alternativa a los

sistemas de autenticación tradicionales y proporciona seguridad de red. Todos estos factores han hecho de la dinámica del ratón una herramienta atractiva para el mercado digital.

Aubin (2019), y el método que utiliza para verificar personas basado en grafemas simples, dando un alto porcentaje de respuestas correctas, y la combinación de letras también mejoró la verificación de 100% identidad.

Tabla 5: En relación a la variable general en la Tabla 5 se evidencia que un 60,0% indica que es bueno, sin embargo, un 40,0% es regular. Estos resultados nos permiten tener en cuenta la teoría de la autenticación biométrica la cual hay una aceptación del método de autenticación biométrica, porque es clave en el proceso de identidad de un sujeto verificando que “tú eres tú”.

Por otro lado, Fernández (2021), ha definido que la autenticación es el proceso de identificación de usuarios y verificación de su identidad. Evitando que alguien ingrese a un sistema en particular o inicie sesión en cualquier plataforma de manera incorrecta, sin ser realmente un usuario legítimo autorizado para hacerlo. De esta manera no deja claro que en un futuro dejemos de usar contraseñas para dar paso a la autenticación biométrica y su aplicación a la vida práctica.

Igualmente, Guidott (2020), indica que la autenticación solo intenta garantizar que la persona que firma la transacción sea la misma que la persona que registró al usuario. Si la identidad no se verificó durante el proceso de registro, no hay garantía sobre la identidad del usuario.

Así tenemos, que Márquez (2018) en su investigación demostró un método biométrico basado en la escritura del usuario o el reconocimiento dinámico del teclado. Para este método se utilizaron cuatro características de escritura: código de tecla presionada, dos tipos de tiempo entre dos pulsaciones sucesivas y tiempo de permanencia de cada tecla, que desarrolló la tecnología en el sistema. La recepción es: código de tecla, tiempo de pulsación de tecla, empuje el tiempo, empuje el tiempo de liberación. Se realizaron 95 pruebas de validación con usuarios universitarios, y el desarrollo se desarrolló en dos etapas: el primer paso buscó capturar las pulsaciones de teclas del usuario y el segundo paso aplicó 4 valores

umbral para el ajuste de tarifas, con el fin de determinar el mejor valor umbral aceptable y aplicando ajustes aproximados.

Para la creación del sistema del sistema de autenticación biométrica no se ha utilizado ningún framework, indicar que el código ha sido desarrollado desde cero, creando una página en HTML, CSS y JavaScript en la cual se encontraba la estructura del simulador de autenticación biométrica, para ello se han detectado los patrones de digitación de cada uno de los usuarios del sistema, los valores de tiempo que se han considerado entre ellos tenemos: código de tecla, pulsar soltar y soltar pulsar. Comprobado la probabilidad de que los usuarios sean quien dicen ser, cabe resaltar que para realizar dichas pruebas se realizó con un teclado que se encontraba en buenas condiciones. En la Figura del anexo se muestra el diseño del ingreso al simulador de autenticación biométrica, que generaron estos datos de los tiempos de pulsar-pulsar.

Por ello, estos resultados permiten coincidir que un sistema biométrico el cual involucra las características del cuerpo humano y determina la identidad del individuo según lo manifestado por Faces (2020).

Se desarrollaron 143 pruebas de simulación de autenticación biométrica, local, cuyo objetivo residieron en establecer la Falsa aceptación (FA) y Falso rechazo (FR), se consideró el total de usuarios (100%), teniéndose como resultados el 38.5% para FA algunos usuarios no alcanzaron la probabilidad de ser quien dice ser, y un 61.5% para FR teniendo que algunos usuarios tuvieron errores al realizar la digitación, para lo cual se tomó en cuenta, un tiempo de demora prolongado y no adaptación al teclado, etc. En la tabla siguiente se muestran los datos obtenidos de la prueba.

Tabla 9

Porcentaje de falsa aceptación y falso rechazo obtenidos en las pruebas.

Grupo Prueba	Tipo	Pruebas	FA	FR
Usuarios	Local	143	38.5%	61.5%

Nota: Elaboración propia del autor.

Asimismo, se tiene un resultado para tiempos pulsación (pulsar - soltar), se tomó una muestra de 30 trabajadores de la institución educativa emblemática San José de Chiclayo, sobre la forma de teclear de cada uno de ellos. En la figura nos muestra el contador y el cálculo del corte del tiempo para el evento pulsar – soltar tecla, lo que se intenta mostrar es que de acuerdo a la rapidez con la que se incremente el contador será el número de cifras que logremos, en este caso como mínimo 3 cifras.

También tenemos el resultado de tiempos entre pulsaciones (soltar - pulsar), también conocida como dinámica de mecanografía, es el análisis sobre los hábitos de la escritura de un sujeto, es decir que los rasgos son únicos e irrepetibles para cada individuo. Así tenemos, que se ha podido verificar el tiempo que acontece cuando el usuario suelta una tecla y presione la tecla siguiente, a este evento se llama soltar - pulsar.

Por esta razón, y como se ha demostrado en los resultados obtenidos, las formas más simples de pulsaciones de teclas se han fundamentado en esta indagación en dos métricas simples: la cantidad de tiempo que se mantiene presionada una tecla (pulsar - soltar), es decir, el tiempo de permanencia, y la cantidad de tiempo que acontece entre soltar una tecla y presionar otra (soltar – pulsar), señalada como tiempo de vuelo.

Por último, se tiene en la figura del anexo el resultado final de la biometría practicada a los 30 trabajadores de la institución educativa emblemática San José de Chiclayo, teniendo en cuenta el tiempo de pulsación y el tiempo de pulsaciones en milisegundos.

Un elemento que se debe tener en cuenta durante todo el proceso, es que los trabajadores de la institución educativa emblemática San José de Chiclayo, fueron muy conscientes que en todo momento formaban parte del grupo de la presente indagación, es factible que los valores cambien si los trabajadores desconocen las plantillas de digitación de sus contraseñas las cuales estaban siendo demostradas y probadas, para de esta manera tener una validez de la comprobación de ser quien dice ser al sistema web de la institución.

Los factores como casos fortuitos, mala escritura, palabras complejas, estado de ánimo, sentimientos, emociones e incluso las más leves y otros no se han contemplado como elementos determinantes en la presente indagación,

Concluimos, que esta técnica simboliza una tecnología de autentificación de bajo costo, pues no demanda hardware adicional, interviniendo el teclado habitual como dispositivo biométrico.

VI. CONCLUSIONES

1. Se comprueba que, la creación e implementación de un sistema de autenticación biométrica basado en patrones de tecleo, mejorará significativamente el acceso de los trabajadores al sistema web de la institución educativa emblemática San José de Chiclayo, en los resultados finales de las 03 muestra obtenidas se obtuvo 85.67% de probabilidad de que la persona que estaba teclado es quien dice ser.

2. Un 60% de los trabajadores indica que es necesario un método de seguridad para el acceso al sistema ya que por diversos motivos algunos usuarios tienen sus contraseñas en hoja o papel, este método les ayudará, aunque tengan su contraseña no podrán imitar su forma de teclear, esto hace que disminuya considerablemente las suplantaciones de identidad de usuarios.

3. Se consigue apreciar que, la implementación de un sistema de autenticación biométrica aplicando la dinámica del tecleo, incrementó un 80.33% de exactitud de autenticación después de la implementación del post test.

4. En relación a la propuesta de autenticación biométrica basado en patrones de tecleo, después de haber sido elaborada en función al diagnóstico de la variable problema, los expertos decidieron que esta es sostenible y puede ser aplicada para contribuir en mejorar la seguridad del sistema web de la institución educativa emblemática San José de Chiclayo.

VII. RECOMENDACIONES

Al Director de la Institución Educativa Emblemática San José de Chiclayo se le recomienda considerar la propuesta de sistema de autenticación biométrica de tecleo, a fin de utilizar dicho sistema por no requerir de un hardware adicional, ser de bajo costo y no dañar el medio ambiente.

Al Director de la Institución Educativa Emblemática San José de Chiclayo se le recomienda implementar la infraestructura necesaria para el uso del sistema de autenticación biométrica de tecleo, con la finalidad de lograr que se evolucione de acuerdo a las nuevas necesidades tecnológicas la administración pública a nivel regional.

Al Gobernador Regional de Lambayeque y director de la Unidad de Gestión Educativa Local Chiclayo – UGEL, se les recomienda implementar y probar el sistema de autenticación biométrica de tecleo, en otras instituciones educativas nacionales en el ámbito regional.

A los trabajadores de la institución educativa que participen en los procesos de gestión del cambio para el uso del sistema de autenticación biométrica de tecleo, que aporten con sus sugerencias las cuales permitirán superar debilidades y tomar decisiones a fin de brindar un servicio con calidad en bien de los administrados.

REFERENCIAS

Aguilar, H., & Pérez, L. (2010). *Autenticación de usuarios a través de biometría de tecleo*. Recuperado el 3 de setiembre de 2021, de CIINDET 2010: http://b-dig.iie.org.mx/BibDig2/P11-0498/p318.pdf

Aguilera, B. (2016). *Mejora de sistemas de autenticación de personas basados en dinámica de ratón*. Recuperado el 3 de setiembre de 2021, de https://repositorio.uam.es/bitstream/handle/10486/673337/Merida_Aguilera_Belen_tfg.pdf?sequence=1&isAllowed=y

Alina, R. (2020). Seguridad y biometría en cuestión: el sistema federal de identificación biométrica (SIBIOS) en Argentina. *Revista de ciencias sociales*(87), 16.

Aubin, V. (2019). *Verificación de la identidad de personas en base a trazos manuscritos simples*. Recuperado el 3 de setiembre de 2021, de https://eprints.ucm.es/id/eprint/56034/1/T41187.pdf

Barrios, M. (2017). Las ventajas de la biometría en el mundo financiero. *Portafolio*.

Calot, E. (2019). *Robustez de las métricas de clasificación de cadencia de tecleo frente a variaciones emocionales*. Recuperado el 03 de setiembre de 2021, de http://sedici.unlp.edu.ar/bitstream/handle/10915/104357/Documento_completo.pdf?sequence=1&isAllowed=y

Cano, C. (2019). Dos visiones diferentes de entender la investigación, para la formación en educación superior. *Revista Atlante: Cuadernos de Educación y Desarrollo*. Recuperado el 18 de Mayo de 2020, de https://www.eumed.net/rev/atlante/2019/07/investigacion-educacion-superior.html

Chinchay, I. (2019). *Implementación de un sistema de gestión de RR. HH, incluyendo un dispositivo biométrico de huellas digitales, para optimizar el proceso de control de asistencia y evaluar el desempeño laboral, en una estación de servicios ubicada en lambayeque*. Recuperado el 3 de setiembre

de 2021, de file:///Users/hugo/Downloads/TL_ChinchayFarro%C3%B1ayIgor%20(1).pdf.

Choi, M., Shincheol , L., Minjae, J., & and Ji , S. (2021). Keystroke Dynamics-Based Authentication Using Unique Keypad. *Sensors, 21*(2242), 19.

Cuesta-Quintero, F. R., Coronel Rojas, L. A., Rico Bautista, D., Barrientos Advendaño, E., Montaño Vergel, O. J., & Páez Noriega, C. M. (2019). *Sistema de detección de intrusos a través de una red Honeynet para entornos de red cableada sobre IPV6*. Recuperado el 07 de Setiembre de 2021, de https://www.semanticscholar.org/paper/SISTEMA-DE-DETECCI%C3%93N-DE-INTRUSOS-A-TRAV%C3%89S-DE-UNA-DE-Quintero-Rojas/2a061eaa70f9cd06e1eafd21f20b4d4c4f622487#:~:text=10.24054/16927257.V33.N33.2019.3328: DOI: 10.24054/16927257.V33. N33.2019.3328

Decreto Legislativo N° 1505. (2020). *Decreto Legislativo que establece medidas temporales excepcionales en materia de gestión de recursos humanos en el sector público ante la emergencia sanitaria ocasionada por el COVID-19.* Lima: Normas Legales - El Peruano. Recuperado el 20 de mayo de 2020, de https://busquedas.elperuano.pe/download/url/decreto-legislativo-que-establece-medidas-temporales-excepci-decreto-legislativo-n-1505-1866220-6

Díaz Collantes, J. A., & Flores Soraluz, G. I. (2019). *Diseño e implementación de prototipo de un sistema biométrico para mejorar el control de asistencia del personal docente en la FACFYM*. Recuperado el 3 de setiembre de 2021, de https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/4907/BC-TES-3742%20DIAZ%20COLLANTES%20-%20FLORES%20SORALUZ.pdf?sequence=1&isAllowed=y

Díaz, J. (2021). *Sistema basado en biometría de la dinámica de tecleo, aplicando rup, para la autenticación de personal en la empresa severox Perú S.A.C*. Recuperado el 3 de setiembre de 2021, de http://repositorio.autonoma.edu.pe/bitstream/AUTONOMA/1253/1/Diaz%20Diaz%2c%20Jordan.pdf

Din, A. (2021). *What Is Biometric Authentication? A Complete Overview*. Recuperado el setiembre de 03 de 2021, de Heimdal Security: https://heimdalsecurity.com/blog/biometric-authentication/

Faces, R. (2020). *Tipos de sistemas biométricos: la guía completa*. Recuperado el 3 de setiembre de 2021, de Blog de Biometría: https://recfaces.com/es/articles/tipos-de-identificacion-biometrica#1

Fernández, L. (2021). *Qué significa autenticación y la autorización*. Recuperado el 03 de setiembre de 2021, de RZ, Redes Ozone: https://www.redeszone.net/tutoriales/seguridad/diferencias-autenticacion-autorizacion/

Galindo, J. S. (2018). La escuela de la ciberseguridad de IBM. *El Economista*, pág. 1.

Guerrero, C. (2019). *Hiperderecho*. Recuperado el 03 de setiembre de 2021, de Identificación biométrica obligatoria: https://hiperderecho.org/2019/06/identificacion-biometrica-obligatoria/

Guidotti, A. (2020). La identificación y la autenticación, elementos esenciales para tele trabajar con total seguridad en plena crisis del Covid-19. *Revista Transformación Digital*. Recuperado el 03 de setiembre de 2021, de https://www.revistatransformaciondigital.com/2020/04/30/la-identificacion-y-la-autenticacion-elementos-esenciales-para-teletrabajar-con-total-seguridad-en-plena-crisis-del-covid-19/

Hernández, R., Sampirie, R., & Mendoza, C. (2018). *Metodología de la Investigación. Las Rutas cuantitativas, cualitativa y mixta.* México: Editorial Mc Graw Hill Education.

INCIBE. (2016). Tecnologías biométricas aplicadas a la Ciberseguridad. *Una guía de aproximación para el empresario, 1*, 32. Recuperado el 03 de setiembre de 2021, de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

Jianwei Li, H.-C. C. (2021). *Free-Text Keystroke Dynamics for User Authentication*. Recuperado el 3 de setiembre de 2021, de https://arxiv.org/pdf/2107.07009.pdf

Kolakowska, A., & Landowska, A. (2021). "Keystroke Dynamics Patterns While Writing Positive and Negative Opinions". (17: 5963). doi: https://doi.org/10.3390/s21175963

Leal, J. P. (2018). Recuperado el 22 de mayo de 2020, de ¿Qué son las encuestas en línea o encuestas online?: https://www.blogger.com/profile/02400758696425848385

Legales, N. (2000). *Ley Nº 27629 - Ley de Firmas y certificados digitales*. Obtenido de El Peruano: https://diariooficial.elperuano.pe/pdf/0030/ley-27269.pdf

Legales, N. (2014). *D.S. Nº 023-2014-MTC - Decreto Supremo que modifica el Decreto Supremo N° 024-2010-MTC que aprueba el procedimiento para la subsanación de la información consignada en el Registro de Abonados Pre Pago*. Obtenido de http://transparencia.mtc.gob.pe/idm_docs/normas_legales/1_0_4718.pdf

Manzanares, M. (2018). *Metodología para la evaluación de la Calidad de Servicios*. Obtenido de Gestión de calidad: https://riubu.ubu.es/bitstream/handle/10259/4889/Tema_3_metodologia_para_la_evaluacion.pdf?sequence=7&isAllowed=y

Márquez, P. (2018). *Patrones de digitación para evitar la suplantación de identidad en el sistema transaccional de una universidad privada*. Recuperado el 3 de setiembre de 2021, de https://repositorio.uncp.edu.pe/bitstream/handle/20.500.12894/5111/Marquez%20Solis.pdf?sequence=1&isAllowed=y

Mena Roa, M. (2020). *Statista*. Recuperado el 03 de setiembre de 2021, de '123456', la contraseña más usada este año: https://es.statista.com/grafico/23636/contrasenas-mas-usadas-en-el-mundo/

Mendoza Silva, L. F., & Vega Gallegos, G. (2019). *Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la empresa SICS*. Recuperado el 03 de setiembre de 2021, de https://repositorio.up.edu.pe/bitstream/handle/11354/2250/Luis_Tesis_Maestria_2019.pdf?sequence=1&isAllowed=y

MINJUS. (2015). *D.L. Nº 1049 - Decreto Legislativo del Notariado*. Obtenido de https://www.minjus.gob.pe/wp-content/uploads/2017/04/Decreto-Legislativo-N%C2%BA-1049.pdf

OCDE. (2015). *Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development, The Measurement of Scientific, Technological and Innovation Activities.* (OCDE, Ed.) Paris, Francia. DOI: http://dx.doi.org/10.1787/9789264239012-en

OSIPTEL. (2012). *R.C.D. Nº 138-2012 - TUO de las condiciones de uso de los servicios públicos de las telecomunicaciones*. Obtenido de https://www.osiptel.gob.pe/media/3onb5qj2/resolucion138-2012-cd-osiptel_tuo-condiciones.pdf

Peruano. (2021). Ciberdelitos en el Perú: Se elevan denuncias de fraude informático y suplantación de identidad. *Diario Oficial El Peruano*, pág. 01.

Quintanilla, G. (2020). Legislación, riesgos y retos de los sistemas biométricos. *Revista chilena de derecho y tecnología, 09*(1). Recuperado el 03 de setiembre de 2021, de Scielo: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000100063&lang=pt

Quintero, A. C. (2019). *Sistema de detección de intrusos a través de una Honeynet para entornos de una red cableada sobre IPV6*. (Universidad de Pamplona I.I.T.D.A) Recuperado el 07 de Setiembre de 2021, de 10.24054/16927257.V33.N33.2019.3328: emanticscholar.org/paper/SISTEMA-DE-DETECCIÓN-DE-INTRUSOS-A-TRAVÉS-DE-UNA-DE-Quintero-Rojas/2a061eaa70f9cd06e1eafd21f20b4d4c4f622487

Revilla, F. (2017). *Autenticación y verificación de usuarios mediante dinámica del tecleo*. Recuperado el 03 de setiembre de 2021, de https://eprints.ucm.es/id/eprint/44424/1/MemoriaTFG-AutenticacionYVerificacionDeUsuariosPorDinamicaDelTecleo.pdf

Robles Garrote, P., & Rojas, M. d. (2015). La validación por juicio de expertos: dos investigaciones cualitativas en Lingüística aplicada. *Revista Nebrija de Lingüística Aplicada*, 2 -16. Recuperado el 18 de mayo de 2020, de https://www.nebrija.com/revista-linguistica/files/articulosPDF/articulo_55002aca89c37.pdf

Sánchez, H., Reyes, C., & Mejía, K. (2018). *Manual de términos en investigación científica, tecnológica y humanística* (Primera ed.). Lima, Perú: Bussiness Support Aneth S.R.L.

SPIJ. (1995). *Ley Nº 26497 - Ley Orgánica del registro nacional de identificación y estado civil.* Obtenido de https://cdn.www.gob.pe/uploads/document/file/1501058/Ley_N%C2%B0_26497.pdf.pdf

Tolosa, C., & Giz, A. (2019). *Sistemas Biométricos.* Recuperado el setiembre de 2021, de si.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

Torres Jiménez, A., & Acosta Escalante, F. (2019). *Sistema de Protección de Datos usando Dinámica de Tecleo.* Recuperado el 3 de setiembre de 2021, de https://www.google.com/search?q=Sistema+de+Protecci%C3%B3n+de+Datos+usando+Din%C3%A1mica+de+Tecleo.+Alejandra+Lil%C3%AD+Torres+Jim%C3%A9nez1%2C+Dr.Francisco+Diego+Acosta+Escalante&rlz=1C5CHFA_enPE966PE966&oq=Sistema+de+Protecci%C3%B3n+de+Datos+usando+Din%

Warwick R., A. (2017). High-accuracy detection of early Parkinson's Disease using multiple characteristics of finger movement while typing. *Plos One*, 20.

ANEXO

INSTITUCIÓN EDUCATIVA EMBLEMÁTICA

Colegio Nacional De San José

"AÑO DEL BICENTENARIO DEL PERÚ: 200 AÑOS DE INDEPENDENCIA"

Chiclayo, 16 de diciembre del 2021.

OFICIO N°0236/2021/UGEL.CH/I.E."SJ"-D

SEÑOR : *MBA HUGO HAMILTON OYOLA YARLAQUE.*
MAESTRANTE DE LA ESCUELA DE POSGRADO.

ASUNTO : *AUTORIZA APLICAR INSTRUMENTOS PARA TESIS.*

Tengo a bien dirigirme a su digna persona para saludarlo muy cordialmente a nombre de la Institución Educativa Emblemática "San José" de Chiclayo y, a la vez comunica a su despacho:

Que, habiéndose recepcionado el expediente N° 2015-TM de fecha 19 de noviembre del presente año, el cual nos solicita la respectiva Autorización para aplicar instrumentos para el desarrollo de tesis, los mismos que le servirán para su trabajo de investigación denominado "Sistema de autenticación biométrica de tecleo para mejorar la seguridad del sistema web de la Institución Educativa Emblemática "San José" de Chiclayo".

Por este motivo y con mi visto bueno, se le **AUTORIZA APLICAR LOS INSTRUMENTOS PARA EL DESARROLLO DE SU TESIS;** asimismo le brindaremos las facilidades que el caso amerita ya que nos resulta de gran interés conocer sus opiniones, vivencias y experiencias sobre el trabajo de investigación.

Sin otro particular; aprovecho la ocasión para expresarle los sentimientos de mi especial consideración y estima personal.

Atentamente.

INSTITUCIÓN EDUCATIVA EMBLEMÁTICA C.N. DE "SAN JOSÉ" DIRECCIÓN CHICLAYO

MG. MARCO ALEXIS BARRETO ARELLANO
DIRECTOR

MABA/DIRECT.
Rgv/Técn. Adtva.

San José Ayer, Hoy y Siempre

Av. Elvira García y García N° 285 - Chiclayo

"AÑO DEL BICENTENARIO DEL PERÚ: 200 AÑOS DE INDEPENDENCIA"

Chiclayo, 22 de diciembre del 2021.

OFICIO N°0245/2021/UGEL.CH/I.E."SJ"-D

SEÑOR : *MBA HUGO HAMITON OYOLA YARLAQUE.*
MAESTRANTE DE LA ESCUELA DE POGRADO.

ASUNTO : *CONFORMIDAD E IMPLEMENTACIÓN DE LA INVESTIGACIÓN.*

Tengo a bien dirigirme a su digna persona para saludarlo muy cordialmente a nombre de la Institución Educativa Emblemática "San José" de Chiclayo y,a la vez comunicó a Usted.

Que, habiéndose recepcionado el expediente N° 2015-TM de fecha 19 de noviembre del presente año, el cual nos solicita la respectiva Autorización para aplicar instrumentos para el desarrollo de tesis, los mismos que le servirán para su trabajo de investigación denominado "Sistema de autenticación biométrica de tecleo para mejorar la seguridad del sistema web de la Institución Educativa Emblemática "San José" de Chiclayo".

Por este motivo y con mi visto bueno, se le da la **CONFORMIDAD Y ACEPTACIÓN DE IMPLEMENTAR SU INVESTIGACIÓN**; asimismo le agradecemos por haber desarrollado su investigación en base a nuestra Institución Educativa Emblemática, puesto que nos resulta de gran ayuda el conocer nuevas tecnologías que nos mantengan a la vanguardía del ámbito regional.

Sin otro particular; aprovecho la ocasión para expresarle los sentimientos de mi especial consideración y estima personal.

Atentamente.

INSTITUCIÓN EDUCATIVA EMBLEMATICA C.N. DE "SAN JOSE" DIRECCIÓN CHICLAYO

MG. MARCO ALEXIS BARRETO ARELLANO
DIRECTOR

MABA/DIRECT.
Rgv/Técn. Adtva.

ENCUESTA DE SEGURIDAD EN UN SISTEMA WEB

ENCUESTA DE SEGURIDAD EN UN SISTEMA WEB

Estimado(a) trabajador(a):

Los siguientes Ítems se formulan como parte de un trabajo de investigación para medir la **Seguridad en un sistema web** de nuestra Institución. Por lo que le pedimos su colaboración leyendo y respondiendo a lo solicitado.

DATOS GENERALES:

Edad ☐ años Sexo ☐ Femenino ☐ Masculino

INSTRUCCIONES: Por favor, lea cuidadosamente cada frase y marca con un aspa (X) la valoración que mejor describa su forma de actuar teniendo en cuenta las siguientes calificaciones:

Totalmente en desacuerdo	En desacuerdo	Indeciso	De acuerdo	Totalmente de acuerdo
1	2	3	4	5

DIMENSIÓN: FALSA ACEPTACIÓN	CALIFICACIÓN				
1. Conoce usted el uso de los teclados.	1	2	3	4	5
2. Usted se adapta a cualquier tipo de teclado a usar.	1	2	3	4	5
3. Usted al presionar una tecla y otra lo realiza con mucha fuerza.	1	2	3	4	5
4. Considera usted que es necesario tener un patrón de escritura al utilizar el teclado.	1	2	3	4	5
5. Considera que se debe tener un número de intentos para acceder al sistema.	1	2	3	4	5
6. Considera que el método de autenticación biometrica es apropiado.	1	2	3	4	5
7. Usted tiene un método de seguridad al ingresar su contraseña mediante el teclado.	1	2	3	4	5
8. Cree usted que el sistema debe aceptar a cualquier usuario solo teniendo la contraseña personal.	1	2	3	4	5
9. Considera que la probabilidad para teclear su contraseña es siempre la misma.	1	2	3	4	5
10. Cree usted que su estado de animo (triste, alegre, deprimido, molesto) guarda relación con su forma de teclear.	1	2	3	4	5
DIMENSIÓN: FALSO RECHAZO					

1. Cree Usted que para ingresar al sistema de la institución solo basta con la contraseña para mantener un control en la seguridad del sistema.	**1**	**2**	**3**	**4**	**5**
2. Considera que se debe implementar un método de autenticación biométrica para el acceso al sistema de la institución.	**1**	**2**	**3**	**4**	**5**
3. Usted suele compartir su contraseña con personas desconocidas	**1**	**2**	**3**	**4**	**5**
4. Considera que para ingresar al sistema se debe tener un número de intentos permitidos.	**1**	**2**	**3**	**4**	**5**
5. Usted suele compartir su contraseña con personas desconocidas.	**1**	**2**	**3**	**4**	**5**
6. Sus compañeros de trabajos conocen su contraseña de acceso al sistema.	**1**	**2**	**3**	**4**	**5**
7. Usted considera que se debe detectarse cuando un usuario que no es usted, ingresa al sistema de la institución con sus credenciales.	**1**	**2**	**3**	**4**	**5**
8. Su contraseña es fácil de suplantar.	**1**	**2**	**3**	**4**	**5**
9. Las contraseñas que utiliza para acceder al sistema son las misma o similares a las utiliza para su correo personal o redes sociales.	**1**	**2**	**3**	**4**	**5**
10. Usted considera recordar su contraseña en su computadora o en hoja y papel.	1	2	3	**4**	**5**

Muchas gracias por su colaboración.

VALIDACIÓN DE INSTRUMENTOS

UNIVERSIDAD CÉSAR VALLEJO

INFORME SOBRE JUICIO DE EXPERTOS PARA VALIDAR INSTRUMENTOS DE RECOLECCIÓN DE DATOS

I. DATOS INFORMATIVOS:

1.1. Apellidos y Nombres del experto: SERQUEN BRAVO SHIRLEY
1.2. Grado académico que ostenta : Maestría en Administración de Negocios - MBA
1.3. Institución donde trabaja : Área de Recursos Humanos - UGEL - Chiclayo
1.4. Experiencia laboral (años) :…05……
1.5. Título de la tesis: **"Sistema de autenticación biométrica de tecleo para mejorar la seguridad en un sistema web de una I.E.N. - Chiclayo"**
1.6. Nombre del autor de la tesis : Hugo Hamilton Oyola Yarlaque.
1.7. Nombre del instrumento a validar: Cuestionario.

II. ASPECTOS A VALIDAR:

CRITERIO	INDICADORES	DEFICIENTE				BAJA				REGULAR				BUENA				MUY BUENA			
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Está redactado (a) con lenguaje apropiado.																		X		
2. OBJETIVIDAD	Describe ideas relacionadas con la realidad a solucionar.																		X		
3. ACTUALIZACIÓN	Sustentado en aspectos teóricos científicos de actualidad.																				X
4. ORGANIZACIÓN	El instrumento contiene organización lógica.																				X
5. SUFICIENCIA	El instrumento contiene aspectos en cantidad y calidad.																				X
6. INTENCIONALIDAD	Adecuado (a) para mejorar la gestión pública.																			X	
7. CONSISTENCIA	Basado (a) en aspectos teóricos científicos.																				X
8. COHERENCIA	Entre las variables, indicadores y el instrumento.																			X	
9. METODOLOGÍA	El instrumento responde al propósito del diagnóstico																				X
10. PERTINENCIA	Útil y adecuado (a) para la investigación																				X
TOTAL:																			180	190	600

III. OPINIÓN DE APLICABILIDAD:

El instrumento de recojo de datos pertinente su aplicabilidad.

IV. PROMEDIO DE VALORACIÓN: 970

Lugar y fecha: Chiclayo, 12 de octubre del 2021.

FIRMA DEL EXPERTO
DNI: 45498435

UNIVERSIDAD CÉSAR VALLEJO

INFORME SOBRE JUICIO DE EXPERTOS PARA VALIDAR INSTRUMENTOS DE RECOLECCIÓN DE DATOS

I. DATOS INFORMATIVOS:

1.1. Apellidos y nombres del experto: Oyola Cortez, Hugo Milton
1.2. Grado académico que ostenta : Doctor en Gestión Pública y Gobernabilidad
1.3. Institución donde trabaja : Universidad "César Vallejo" Campus Chiclayo
1.4. Experiencia laboral (años) :…07……
1.5. Título de la tesis: **"Sistema de autenticación biométrica de tecleo para mejorar la seguridad en un sistema web de una I.E.N. - Chiclayo"**
1.6. Nombre del autor de la tesis : Hugo Hamilton Oyola Yarlaque.
1.7. Nombre del instrumento a validar: Cuestionario.

II. ASPECTOS A VALIDAR:

CRITERIO	INDICADORES	DEFICIENTE				BAJA				REGULAR				BUENA				MUY BUENA			
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Está redactado (a) con lenguaje apropiado.																				X
2. OBJETIVIDAD	Describe ideas relacionadas con la realidad a solucionar.																			X	
3. ACTUALIZACIÓN	Sustentado en aspectos teóricos científicos de actualidad.																			X	
4. ORGANIZACIÓN	El instrumento contiene organización lógica.																				X
5. SUFICIENCIA	El instrumento contiene aspectos en cantidad y calidad.																			X	
6. INTENCIONALIDAD	Adecuado (a) para mejorar la gestión pública.																				X
7. CONSISTENCIA	Basado (a) en aspectos teóricos científicos.																				X
8. COHERENCIA	Entre las variables, indicadores y el instrumento.																				X
9. METODOLOGÍA	El instrumento responde al propósito del diagnóstico																				X
10. PERTINENCIA	Útil y adecuado (a) para la investigación																				X
TOTAL:																				285	700

III. OPINIÓN DE APLICABILIDAD:

El instrumento de recojo de datos resulta pertinente para el fin que se espera alcanzar.

IV. PROMEDIO DE VALORACIÓN: 985

Lugar y fecha: Chiclayo, 12 de octubre del 2021.

Hugo Milton Oyola Cortez
ABOGADO
REG. C.A.L. 0000

FIRMA DEL EXPERTO
DNI: 16408554

UNIVERSIDAD CÉSAR VALLEJO

INFORME SOBRE JUICIO DE EXPERTOS PARA VALIDAR INSTRUMENTOS DE RECOLECCIÓN DE DATOS

I. DATOS INFORMATIVOS:

1.1. Apellidos y nombres del experto: Contreras Orellana Jessica Gladys
1.2. Grado académico que ostenta : Magister Ingeniero de Sistemas – Tecnologia de la Información
1.3. Institución donde trabaja : Coordinadora Universidad Católica Los Ángeles de Chimbote
1.4. Experiencia laboral (años) :…09……
1.5. Título de la tesis: **"Sistema de autenticación biométrica de tecleo para mejorar la seguridad en un sistema web de una I.E.N. - Chiclayo"**
1.6. Nombre del autor de la tesis : Hugo Hamilton Oyola Yarlaque.
1.7. Nombre del instrumento a validar: Cuestionario.

II. ASPECTOS A VALIDAR:

CRITERIO	INDICADORES	DEFICIENTE				BAJA				REGULAR				BUENA				MUY BUENA			
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Está redactado (a) con lenguaje apropiado.																				X
2. OBJETIVIDAD	Describe ideas relacionadas con la realidad a solucionar.																			X	
3. ACTUALIZACIÓN	Sustentado en aspectos teóricos científicos de actualidad.																			X	
4. ORGANIZACIÓN	El instrumento contiene organización lógica.																				X
5. SUFICIENCIA	El instrumento contiene aspectos en cantidad y calidad.																			X	
6. INTENCIONALIDAD	Adecuado (a) para mejorar la gestión pública.																				X
7. CONSISTENCIA	Basado (a) en aspectos teóricos científicos.																				X
8. COHERENCIA	Entre las variables, indicadores y el instrumento.																				X
9. METODOLOGÍA	El instrumento responde al propósito del diagnóstico																				X
10. PERTINENCIA	Útil y adecuado (a) para la investigación																				X
TOTAL:																				285	700

III. OPINIÓN DE APLICABILIDAD:

El instrumento cumple con los requisitos para su aplicación.

IV. PROMEDIO DE VALORACIÓN: 985

Lugar y fecha: Chiclayo, 12 de octubre del 2021.

JESSICA GLADYS CONTRERAS ORELLANA
INGENIERA DE SISTEMAS

FIRMA DEL EXPERTO
DNI: 41350063

MATRIZ DE EVALUACIÓN DE EXPERTOS

MATRIZ DE EVALUACIÓN DE EXPERTOS

Título de la investigación:	Sistema de autenticación biométrica de tecleo para mejorar la seguridad en un sistema web de una I.E.N. – Chiclayo.
Línea de investigación:	Auditoria de Sistemas y Seguridad de la información
El instrumento de medición pertenece a las variables:	VI: SISTEMA DE AUTENTICACIÓN BIOMÉTRICA VD: SEGURIDAD EN UN SISTEMA WEB

Mediante la matriz de evaluación de expertos. Ud. Tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio

Ítems	Preguntas	Aprecia		Observaciones
		SÍ	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	X		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	X		
3	¿El instrumento de recolección de datos se mencionan las variables de investigación?	X		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	X		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	X		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	X		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición?	X		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	X		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	X		

Sugerencias:

Nombre completo: Hugo Milton Oyola Cortez
DNI: 16408554
Grado: Doctor en Gestión Pública y Gobernabilidad

Hugo Milton Oyola Cortez
Firma del Experto

MATRIZ DE EVALUACIÓN DE EXPERTOS

Título de la investigación:	Sistema de autenticación biométrica de tecleo para mejorar la seguridad en un sistema web de una I.E.N. – Chiclayo.
Línea de investigación:	Auditoria de Sistemas y Seguridad de la información
El instrumento de medición pertenece a las variables:	VI: SISTEMA DE AUTENTICACIÓN BIOMÉTRICA VD: SEGURIDAD EN UN SISTEMA WEB

Mediante la matriz de evaluación de expertos. Ud. Tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio

Ítems	Preguntas	Aprecia		Observaciones
		SÍ	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	X		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	X		
3	¿El instrumento de recolección de datos se mencionan las variables de investigación?	X		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	X		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	X		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	X		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición?	X		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	X		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	X		

Sugerencias:

Nombre completo: SHIRLEY SERQUEN BRAVO
DNI: 45498435
Grado: MAESTRÍA EN ADMINISTRACIÓN DE NEGOCIOS - MBA

Firma del Experto

MATRIZ DE EVALUACIÓN DE EXPERTOS

Título de la investigación:	Sistema de autenticación biométrica de tecleo para mejorar la seguridad en un sistema web de una I.E.N. – Chiclayo.
Línea de investigación:	Auditoria de Sistemas y Seguridad de la información
El instrumento de medición pertenece a las variables:	VI: SISTEMA DE AUTENTICACIÓN BIOMÉTRICA VD: SEGURIDAD EN UN SISTEMA WEB

Mediante la matriz de evaluación de expertos. Ud. Tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio

Ítems	Preguntas	Aprecia		Observaciones
		SÍ	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	X		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	X		
3	¿El instrumento de recolección de datos se mencionan las variables de investigación?	X		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	X		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	X		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	X		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición?	X		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	X		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	X		

Sugerencias:

Nombre completo: Jessica Gladys Contrera Arellano
DNI: 41350063
Grado: Magister Ingeniero de Sistemas
Reg. CIP: 126517

Firma del Experto

OPERACIONALIZACIÓN DE VARIABLES

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICIÓN	INSTRUMENTOS
Independiente: Sistema de autenticación biométrica de tecleo	La autenticación es una interfaz capaz de recopilar el recuento de tiempos de tecleo de un usuario al autenticarse, así como al crear su imagen de tecleo, que debe proporcionarnos un conjunto de marcas de tiempo para una cadena de caracteres escritos.	Dependiendo del contexto de la aplicación, el sistema de autenticación biométrica puede operar de dos modos, el modo verificación o el modo de identificación o reconocimiento.	Pulsación de Tecleo	Código de la Tecla	De razón	Encuesta
				Tiempos Pulsación *(pulsar - soltar)*		
				Tiempos entre Pulsaciones *(soltar – pulsar)*		
Dependiente: Seguridad en un sistema web	También conocido como «aplicaciones Web» son aquellos que no se instalan sobre un sistema operativo (Windows, Linux). Sino que se alojan en un servidor en la nube o sobre una intranet (red local). Su apariencia es similar a las páginas web que estamos acostumbrados a ver, pero de hecho los "sistemas web" tienen funcionalidades muy poderosas y en algunos casos brindan respuestas a casos particulares. Además, permiten adaptarse a cualquier dispositivo y de esta manera verlas desde dónde nos encontremos.	El proceso de distribución, que es gestionado por más de una persona, debe asociarse a un negocio más dinámico. Es por eso que implementar un sistema informático o una aplicación web en la web es la mejor manera de solucionar este problema.	Seguridad	Falsa Aceptación		
				Falso Rechazo		

Fuente: Elaboración propia del autor.

VALIDEZ Y CONFIABILIDAD DE INSTRUMENTO DE RECOLECCIÓN DE DATOS

Base de datos de la Prueba Piloto

											ALFA DE CRONBACH									
SUJETOS	I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	I11	I12	I13	I14	I15	I16	I17	I18	I19	I20	TOTAL
1	2	5	2	2	2	2	4	4	2	2	4	4	2	2	2	2	2	2	5	2	54
2	4	4	2	4	2	2	2	4	1	2	2	2	3	2	4	4	2	4	5	4	59
3	2	3	3	2	1	3	2	3	2	3	2	1	2	3	1	2	2	2	4	2	45
4	1	2	1	1	2	1	2	2	2	1	2	1	1	1	1	1	1	1	5	1	30
5	2	4	2	2	2	2	2	4	1	2	2	4	2	2	1	2	2	2	5	2	47
6	4	4	2	4	2	2	2	4	2	2	2	2	3	2	4	4	2	4	5	4	60
7	2	5	3	2	2	3	2	5	2	3	2	2	2	3	2	2	3	2	4	2	53
8	2	1	1	2	2	1	1	1	1	1	1	1	2	1	1	2	2	2	5	2	32
9	2	4	2	2	2	2	2	4	2	2	2	2	2	2	1	2	2	2	4	2	45
10	2	5	3	2	2	3	4	2	2	3	4	4	2	3	2	2	2	2	5	2	56
11	1	2	1	1	2	1	2	2	2	1	2	1	1	1	1	1	1	1	5	1	30
12	2	4	2	2	2	2	2	4	1	2	2	4	2	2	1	2	2	2	5	2	47
13	4	4	2	4	2	2	2	4	2	2	2	2	3	2	4	4	2	4	5	4	60
14	2	5	3	2	2	3	2	5	2	3	2	2	2	3	2	2	3	2	4	2	53
15	2	1	1	2	2	1	1	1	1	1	1	1	2	1	1	2	2	2	5	2	32
VARIANZA	0.86	1.849	0.533	0.862	0.062	0.53	0.649	1.662	0.222	0.533	0.649	1.36	0.329	0.533	1.32	0.862	0.267	0.8622	0.196	0.862	

α (ALFA) =	0.9148526
K (NUMERO DE ITEMS) =	20
∑Vi (VARIANZA DE CADA ITEM)=	15
Vt (VARIANZA TOTAL) =	114.6

$$a = \frac{k}{k-1}\left(1 - \frac{\sum v_i}{vt}\right)$$

Confiabilidad de la variable seguridad en un sistema web

Estadística de Fiabilidad

Alfha de Cronbach	Nº de elementos
0,914	15

N=15

Aplicado una prueba piloto a 15 sujetos (trabajadores de la Institución educativa) se determinó a través de la prueba de Alfa de Conbrach que el instrumento tiene una alta confiabilidad (0,91**)

BASE DE DATOS DE LA VARIABLE SEGURIDAD EN UN SISTEMA WEB

		DATOS DE BASE DE LA VARIABLE : SEGURIDAD EN UN SISTEMA WEB																						
		D1: FALSA ACEPTACIÓN										D2: FALSO RECHAZO												
SUJETOS	SEXO	I 1	I 2	I 3	I 4	I 5	I 6	I 7	I 8	I 9	I 10	I 11	I 12	I 13	I 14	I 15	I 16	I 17	I 18	I 19	I 20	D1	D2	TOTAL
1		1	1	1	1	1	1	2	1	1	1	2	5	3	5	1	2	3	1	2	1	11	25	36
2		2	2	2	2	1	1	1	1	2	1	1	5	1	4	3	2	5	2	2	2	15	27	42
3		1	1	1	1	2	2	2	1	1	1	3	2	2	2	1	1	2	2	3	2	13	20	33
4		3	1	1	3	2	2	1	4	2	3	1	5	2	4	1	2	4	4	5	5	22	33	55
5		1	1	2	4	4	4	2	2	4	4	1	5	1	4	3	2	5	2	2	2	28	27	55
6		1	1	1	1	1	1	2	1	1	1	2	5	3	5	1	2	3	1	2	1	11	25	36
7		2	2	2	2	1	1	1	1	2	1	1	5	1	4	3	2	5	2	2	2	15	27	42
8		1	1	1	1	2	2	2	1	1	1	3	2	2	2	1	1	2	2	3	2	13	20	33
9		3	1	1	3	2	2	1	4	2	3	1	5	2	4	1	2	4	4	5	5	22	33	55
10		1	1	2	4	4	4	2	2	4	4	1	5	1	4	3	2	5	2	2	2	28	27	55
11		1	1	1	1	1	1	2	1	1	1	2	5	3	5	1	2	3	1	2	1	11	25	36
12		2	2	2	2	1	1	1	1	2	1	1	5	1	4	3	2	5	2	2	2	15	27	42
13		1	1	1	1	2	2	2	1	1	1	3	2	2	2	1	1	2	2	3	2	13	20	33
14		3	1	1	3	2	2	1	4	2	3	1	5	2	4	1	2	4	4	5	5	22	33	55
15		1	1	2	4	4	4	2	2	4	4	1	5	1	4	3	2	5	2	2	2	28	27	55
16		1	1	1	1	1	1	2	1	1	1	2	5	3	5	1	2	3	1	2	1	11	25	36
17		2	2	2	2	1	1	1	1	2	1	1	5	1	4	3	2	5	2	2	2	15	27	42
18		1	1	1	1	2	2	2	1	1	1	3	2	2	2	1	1	2	2	3	2	13	20	33
19		3	1	1	3	2	2	1	4	2	3	1	5	2	4	1	2	4	4	5	5	22	33	55
20		1	1	2	4	4	4	2	2	4	4	1	5	1	4	3	2	5	2	2	2	28	27	55
21		1	1	1	1	1	1	2	1	1	1	2	5	3	5	1	2	3	1	2	1	11	25	36
22		2	2	2	2	1	1	1	1	2	1	1	5	1	4	3	2	5	2	2	2	15	27	42
23		1	1	1	1	2	2	2	1	1	1	3	2	2	2	1	1	2	2	3	2	13	20	33
24		3	1	1	3	2	2	1	4	2	3	1	5	2	4	1	2	4	4	5	5	22	33	55
25		1	1	2	4	4	4	2	2	4	4	1	5	1	4	3	2	5	2	2	2	28	27	55
26		1	1	1	1	1	1	2	1	1	1	2	5	3	5	1	2	3	1	2	1	11	25	36
27		2	2	2	2	1	1	1	1	2	1	1	5	1	4	3	2	5	2	2	2	15	27	42
28		1	1	1	1	2	2	2	1	1	1	3	2	2	2	1	1	2	2	3	2	13	20	33
29		3	1	1	3	2	2	1	4	2	3	1	5	2	4	1	2	4	4	5	5	22	33	55
30		1	1	2	4	4	4	2	2	4	4	1	5	1	4	3	2	5	2	2	2	28	27	55
																					Items	10	10	20
																					Mínimo	0	0	0
																					Máximo	20	40	80
																					Rango	20	40	80
																					Categori	3	3	3
																					Amplitu	6.6666667	13.333333	26.666667
																					BAJO	6	13	26
																					REGULA	13	27	53
																					BUENO	20	40	60

CÓDIGO DE TECLAS

Código ASCII de teclas en un teclado:

Caracteres ASCII de control		
00	NULL	(carácter nulo)
01	SOH	(inicio encabezado)
02	STX	(inicio texto)
03	ETX	(fin de texto)
04	EOT	(fin transmisión)
05	ENQ	(consulta)
06	ACK	(reconocimiento)
07	BEL	(timbre)
08	BS	(retroceso)
09	HT	(tab horizontal)
10	LF	(nueva línea)
11	VT	(tab vertical)
12	FF	(nueva página)
13	CR	(retorno de carro)
14	SO	(desplaza afuera)
15	SI	(desplaza adentro)
16	DLE	(esc.vínculo datos)
17	DC1	(control disp. 1)
18	DC2	(control disp. 2)
19	DC3	(control disp. 3)
20	DC4	(control disp. 4)
21	NAK	(conf. negativa)
22	SYN	(inactividad sínc)
23	ETB	(fin bloque trans)
24	CAN	(cancelar)
25	EM	(fin del medio)
26	SUB	(sustitución)
27	ESC	(escape)
28	FS	(sep. archivos)
29	GS	(sep. grupos)
30	RS	(sep. registros)
31	US	(sep. unidades)
127	DEL	(suprimir)

Caracteres ASCII imprimibles					
32	espacio	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

ASCII extendido (Página de código 437)							
128	Ç	160	á	192	└	224	Ó
129	ü	161	í	193	┴	225	ß
130	é	162	ó	194	┬	226	Ô
131	â	163	ú	195	├	227	Ò
132	ä	164	ñ	196	─	228	õ
133	à	165	Ñ	197	┼	229	Õ
134	å	166	ª	198	ã	230	µ
135	ç	167	º	199	Ã	231	þ
136	ê	168	¿	200	╚	232	Þ
137	ë	169	®	201	╔	233	Ú
138	è	170	¬	202	╩	234	Û
139	ï	171	½	203	╦	235	Ù
140	î	172	¼	204	╠	236	ý
141	ì	173	¡	205	═	237	Ý
142	Ä	174	«	206	╬	238	¯
143	Å	175	»	207	¤	239	´
144	É	176	░	208	ð	240	≡
145	æ	177	▒	209	Ð	241	±
146	Æ	178	▓	210	Ê	242	‗
147	ô	179	│	211	Ë	243	¾
148	ö	180	┤	212	È	244	¶
149	ò	181	Á	213	ı	245	§
150	û	182	Â	214	Í	246	÷
151	ù	183	À	215	Î	247	¸
152	ÿ	184	©	216	Ï	248	°
153	Ö	185	╣	217	┘	249	¨
154	Ü	186	║	218	┌	250	·
155	ø	187	╗	219	█	251	¹
156	£	188	╝	220	▄	252	³
157	Ø	189	¢	221	¦	253	²
158	×	190	¥	222	Ì	254	■
159	ƒ	191	┐	223	▀	255	nbsp

de uso frecuente (idioma español)	
ñ	alt + 164
Ñ	alt + 165
@	alt + 64
¿	alt + 168
?	alt + 63
¡	alt + 173
!	alt + 33
:	alt + 58
/	alt + 47
\	alt + 92

vocales con acento (acento agudo español)	
á	alt + 160
é	alt + 130
í	alt + 161
ó	alt + 162
ú	alt + 163
Á	alt + 181
É	alt + 144
Í	alt + 214
Ó	alt + 224
Ú	alt + 233

vocales con diéresis	
ä	alt + 132
ë	alt + 137
ï	alt + 139
ö	alt + 148
ü	alt + 129
Ä	alt + 142
Ë	alt + 211
Ï	alt + 216
Ö	alt + 153
Ü	alt + 154

símbolos matemáticos	
½	alt + 171
¼	alt + 172
¾	alt + 243
¹	alt + 251
³	alt + 252
²	alt + 253
ƒ	alt + 159
±	alt + 241
×	alt + 158
÷	alt + 246

símbolos comerciales	
$	alt + 36
£	alt + 156
¥	alt + 190
¢	alt + 189
¤	alt + 207
®	alt + 169
©	alt + 184
ª	alt + 166
º	alt + 167
°	alt + 248

comillas, llaves paréntesis	
"	alt + 34
'	alt + 39
(	alt + 40
)	alt + 41
[	alt + 91
]	alt + 93
{	alt + 123
}	alt + 125
«	alt + 174
»	alt + 175

RESULTADO DE DESCRIPTIVOS DEL INDICADOR:

TIEMPOS PULSACIÓN (PULSAR - SOLTAR)

Para establecer el evento pulsar – soltar tecla, se determinó mediante la fórmula, que se encuentra reflejada en la figura siguiente:

Tiempos Pulsación (pulsar - soltar)

$$\boldsymbol{ps_i = t_{i.soltar} - t_{i.pulsar}}\ ,\ \ donde\ i = 1,2,\dots,n$$

N°	USUARIO	TIEMPOS PULSACIÓN
1	USUARIO 01	21,19,19,11,15,15
2	USUARIO 02	21,19,19,7,19,11
3	USUARIO 03	17,19,15,15,15,19
4	USUARIO 04	17,19,23,7,15,15
5	USUARIO 05	18,19,15,3,19,15
6	USUARIO 06	21,15,19,11,23,19
7	USUARIO 07	21,15,19,11,23,19
8	USUARIO 08	21,15,19,11,23,19
9	USUARIO 09	17,15,15,15,15,15
10	USUARIO 10	18,19,19,15,11,15
11	USUARIO 11	18,23,23,23,23,15
12	USUARIO 12	15,47,39,39,39,31
13	USUARIO 13	22,19,31,27,27,19
14	USUARIO 14	18,19,23,27,23,23
15	USUARIO 15	15,39,47,31,31,31

N°	USUARIO	TIEMPOS PULSACIÓN
16	USUARIO 16	18,11,15,11,16,11
17	USUARIO 17	22,19,19,11,15,11
18	USUARIO 18	18,19,19,19,19,15
19	USUARIO 19	18,23,23,35,27,39
20	USUARIO 20	15,15,39,31,39,23
21	USUARIO 21	22,15,23,23,15,19
22	USUARIO 22	18,23,27,7,15,23
23	USUARIO 23	22,19,23,11,11,11
24	USUARIO 24	22,11,15,11,15,15
25	USUARIO 25	22,15,19,19,15,15
26	USUARIO 26	17,19,23,7,15,15
27	USUARIO 27	18,19,15,3,19,15
28	USUARIO 28	21,15,19,11,23,19
29	USUARIO 29	21,19,19,11,15,15
30	USUARIO 30	21,19,19,7,19,11

Nota: Resultado de tiempo de pulsaciones pulsar – soltar de 30 usuarios.

En la siguiente figura se puede apreciar que se tomó una muestra de 30 usuario - trabajadores de la institución educativa emblemática San José de Chiclayo sobre su forma de teclear. Aquí nos muestra la implementación de un contador y el cálculo del corte del tiempo para el evento pulsar – soltar tecla, lo que se intenta mostrar es que de acuerdo a la rapidez con la que se incremente el contador será el número de cifras que logremos, en este caso como mínimo 3 cifras.

RESULTADO DE DESCRIPTIVOS DEL INDICADOR:

TIEMPOS ENTRE PULSACIONES (SOLTAR - PULSAR)

Para establecer el evento soltar – pulsar tecla, se determinó mediante la fórmula, que se encuentra reflejada en la figura:

Tiempos entre Pulsaciones (soltar - pulsar)

$$sp_i = t_{i+1.pulsar} - t_{i+1.soltar}$$

N°	USUARIO	TIEMPOS ENTRE PULSACIONES
1	USUARIO 01	19,11,11,15,8
2	USUARIO 02	19,15,11,11,11
3	USUARIO 03	31,7,11,15,7,19
4	USUARIO 04	15,3,7,11,7,15
5	USUARIO 05	27,35,135,19,55
6	USUARIO 06	27,11,11,15,7,15
7	USUARIO 07	27,11,11,15,7,15
8	USUARIO 08	27,11,11,15,7,15
9	USUARIO 09	0,27,11,11,3
10	USUARIO 10	0,23,11,11,7
11	USUARIO 11	23,27,19,15,23
12	USUARIO 12	271,39,47,191
13	USUARIO 13	147,51,59,55,67
14	USUARIO 14	163,80,43,24,27
15	USUARIO 15	31,39,7,15

N°	USUARIO	TIEMPOS ENTRE PULSACIONES
16	USUARIO 16	0,27,11,11,11
17	USUARIO 17	0,23,19,11,11
18	USUARIO 18	119,187,31,15,43
19	USUARIO 19	183,35,71,76,151
20	USUARIO 20	47,15,7,15
21	USUARIO 21	7,27,19,27,47
22	USUARIO 22	135,23,31,35,27
23	USUARIO 23	11,23,27,11,15
24	USUARIO 24	0,27,19,11,7
25	USUARIO 25	0,27,23,19,35
26	USUARIO 26	15,3,7,11,7,15
27	USUARIO 27	27,35,135,19,55
28	USUARIO 28	27,11,11,15,7,15
29	USUARIO 29	19,11,11,15,8
30	USUARIO 30	19,15,11,11,11

Nota: Resultado de tiempo de pulsaciones soltar – pulsar de 30 usuarios.

En la presente figura se puede verificar el tiempo que acontece cuando el usuario suelta una tecla y presione la tecla siguiente, a este evento se llamará soltar - pulsar.

RESULTADO FINAL DE LA BIOMETRÍA DE LOS 30 USUARIOS

Para obtener el siguiente resultado se tuvo en cuenta tanto el tiempo de pulsación como el tiempo entre pulsaciones en milisegundos.

Resultado de biometría a 30 usuarios

N°	USUARIOS	USUARIO	MUESTRA 1	MUESTRA 2	MUESTRA 3
1	USUARIO 1	ABAUTISTAL	0.098685457	0.938600241	0.633982398
2	USUARIO 4	EABARCAL	0.66567699	0.389525285	0.169138778
3	USUARIO 6	AMARRUFOR	0.858952847	0.820932056	0.648989196
4	USUARIO 9	ADANAQUESJ	0.97189688	0.446242414	0.439583507
5	USUARIO 15	AGUINAGAVSJ	0.03868725	0.568515767	0.105854034
6	USUARIO 19	ADIAZDS	0.166583704	0.560821035	0.289334619
7	USUARIO 31	AÑIQUENCC	0.348921454	0.061089981	0.676463841
8	USUARIO 37	ALEONAT	0.327300355	0.545048497	0.790521225
9	USUARIO 38	ACHECAM	0.398875185	0.986897094	0.136250191
10	USUARIO 39	AGALLARDOHP	0.24413356	0.744318036	0.527176735
11	USUARIO 46	CARBULU	0.158341072	0.079078469	0.433295676
12	USUARIO 49	ABECERRAJP	0.974620829	0.715966544	0.328827359
13	USUARIO 57	AMANAYAYC	0.361199098	0.753647404	0.095754759
14	USUARIO 60	BDEORTIZM	0.900485203	0.193170433	0.973825224
15	USUARIO 61	BGOICOCHEAJA	0.409369043	0.098503838	0.042838841
16	USUARIO 63	BOSCATEGUILM	0.268069571	0.423971348	0.689223829
17	USUARIO 64	MABALLADARESMAN	0.062790465	0.006730914	0.251406578
18	USUARIO 65	BTUÑOQUEM	0.830743518	0.136553743	0.07172026
19	USUARIO 75	BARJESUS	0.750095113	0.730625954	0.700198248
20	USUARIO 78	BPAREDESFC	0.767262073	0.364603958	0.869202375
21	USUARIO 84	SEBENAVIDESCI	0.223497354	0.171610111	0.816202534
22	USUARIO 85	BSOSAM	0.276502523	0.795094872	0.556246192
23	USUARIO 89	JBENITESCE	0.688306126	0.3974126	0.353128715
24	USUARIO 92	NEBERNACHI	0.346839708	0.840882286	0.856614378
25	USUARIO 103	BFERNANDEZGA	0.516224999	0.674936114	0.247193732
26	USUARIO 104	JLBUSTAMANTEL	0.389578428	0.481557237	0.074470078
27	USUARIO 108	CVASQUEZJA	0.364493966	0.865206926	0.86834032
28	USUARIO 115	CALARCONM	0.088074245	0.334244362	0.930664947
29	USUARIO 118	CUGAZWA	0.362919604	0.997139	0.286522908
30	USUARIO 119	CVILLALOBOSR	0.517831908	0.183019884	0.382633277

Nota: Resultado de tiempo de pulsación entre pulsaciones en milisegundos.

PROPUESTA: SISTEMA DE AUTENTICACIÓN BIOMÉTRICA

1. INTRODUCCIÓN

La presente propuesta se centra en la utilización de herramientas y técnicas adecuadas con la finalidad de aplicarlas correctamente, y de esta forma optimizar la autenticación biométrica de tecleo, procurando identificar si el usuario que está tecleando es quien dice ser, con el objetivo claro de disminuir y solucionar los conflictos que se presenten para tomar decisiones acerca de los recursos de seguridad podemos emplear en nuestro sistema y del grado de cautela que deberemos adoptar.

Seguidamente, se puntualiza en el proceso de desarrollo del procedimiento. Se explica el diseño del sistema y las herramientas a utilizar para su desarrollo, detallando además cada componente del sistema.

2. METODOLOGÍA

De acuerdo a la revisión bibliográfica, investigaciones recopiladas se decidió utilizar los siguientes métodos en esta investigación: **Dinámica de Tecleo o Keystroke Dynamics**

1. Generar el Vector

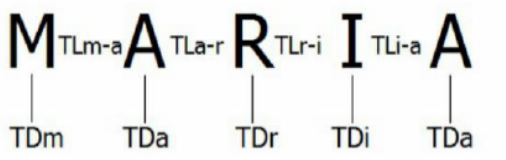
Lo primero es generar el patrón para cada usuario. Elegimos como modelo, la palabra **MARIA**, para la dinámica de tecleo y hay que tomar las subsiguientes muestras:

Visualizando el Vector en Duración y Latencia

Donde:

D = Duración

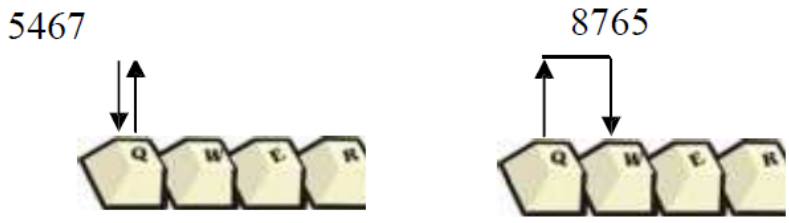
L= Latencia



De acuerdo a este comportamiento único nos ofrece las bases para desplegar un diseño de autenticación, sobre las características que nos interesan para el análisis del comportamiento las cuales están relacionadas con eventos de las pulsaciones de las teclas, y son: Tiempos Pulsación y Tiempos entre Pulsaciones.

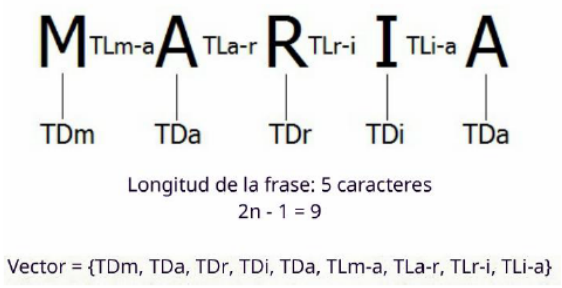
Los Tiempos Pulsación es el tiempo que transcurre desde que se presiona una tecla hasta que se libera. Los Tiempos entre Pulsaciones corresponde al tiempo que pasa desde que se suelta una tecla hasta que se presiona la siguiente.

Medición de tiempo Pulsar – Soltar y Soltar - Pulsar



2. Medición de Vectores de Tiempo

Se realiza el proceso de medición del vector con la muestra para el tiempo de pulsación de cada letra y el tiempo entre pulsaciones. Para crear nuestro patrón tomaremos N muestras de la expresión clave **MARIA** escritas por nuestro usuario, cada una de las muestras tendrá 2*n-1 posiciones siendo n el número de caracteres de la palabra. En este caso cada muestra o vector que recogimos obtendrá 9 posiciones:



3. Código de la Tecla.

Viene hacer el valor que está coligado en la tabla ASCII para una tecla. Para las claves que tienen letras mayúsculas, estas pueden ser logradas presionando las teclas "Shift" o "Caps Lock", dando como resultado diversos posibles conjuntos de códigos.

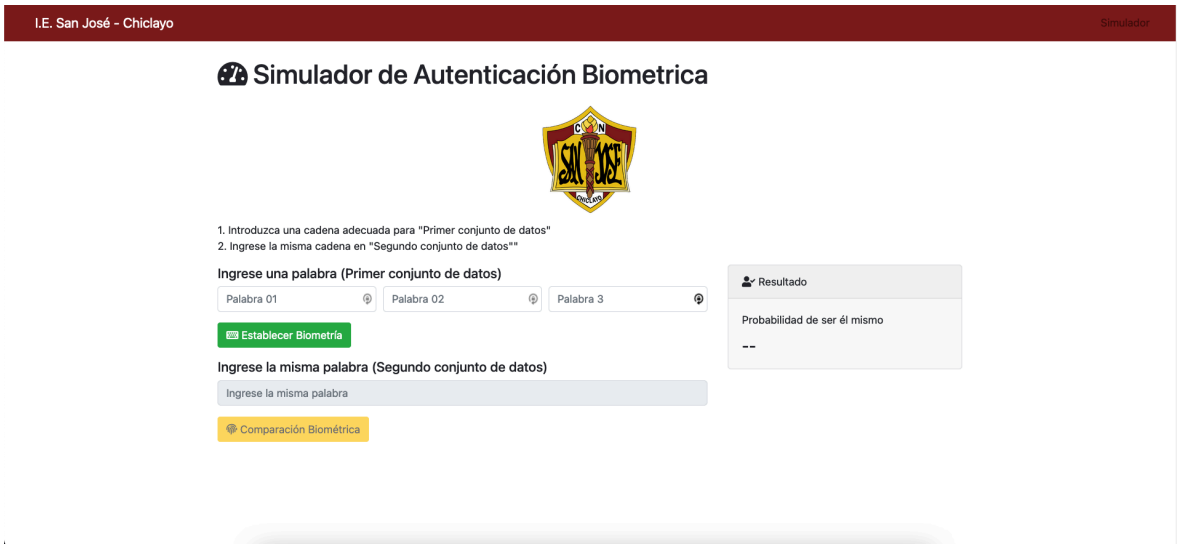
4. Consideraciones

- Velocidad de tecleo: Rápido – Lento
- Modalidad: Para las mayúsculas se usa right-shift o left-shift
- Pausa entre letras
- Errores.

Las peculiaridades son computadas en tiempo real manipulando los datos obtenidos en el instante que los usuarios teclean su clave. Las claves con m caracteres dan como resultado n pulsaciones de teclas, donde $m \leq n$, pues existen caracteres que necesitan más de una tecla para que esta pueda ser representada, como las letras mayúsculas o acentuadas.

5. Diseño del Sistema

El sistema ha sido desarrollado en HTML y CSS, además de utilizar Bootstrap 5. El JavaScript está realizado desde 0, en el cual se deben ingresar una palabra o conjunto de datos dentro de 03 input para ir calculando: Código de Tecla, Pulsar – Soltar y Soltar Pulsar de las teclas presionadas.



Posteriormente a ello debe ingresar la misma palabra en el último input y darle clic en el botón de comparación biométrica para que el sistema realice la comparación del Usuario.