FACULTAD DE INGENIERIA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

TESIS

Mecanismo de autenticación basado en puntos de referencia bidimensionales en imágenes digitales para mejorar la seguridad de aplicaciones web

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERA DE SISTEMAS

Autora

Cruz LLaguento Lucila del Carmen
ORCID https://orcid.org/0000-0003-1661-8879

Asesor

Mg. Arcila Diaz Juan Carlos
ORCID https://orcid.org/0000-0002-7788-951X

Línea de Investigación

Ciencias de la información como herramientas multidisciplinares y estratégicas en el contexto industrial y de organizaciones

Sublínea de Investigación

Informática y transformación digital en el contexto industrial y organizacional

Pimentel – Perú

2025

DECLARACIÓN JURADA DE ORIGINALIDAD

Quien suscribe la DECLARACIÓN JURADA, soy **Lucila del Carmen Cruz LLaguento** del Programa de Estudios de **Ingeniería de Sistemas** de la Universidad Señor de Sipán, declaro bajo juramento que soy autor del trabajo titulado:

MECANISMO DE AUTENTICACIÓN BASADO EN PUNTOS DE REFERENCIA BIDIMENSIONALES EN IMÁGENES DIGITALES PARA MEJORAR LA SEGURIDAD DE APLICACIONES WEB

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética de la Universidad Señor de Sipán, conforme a los principios y lineamientos detallados en dicho documento, en relación con las citas y referencias bibliográficas, respetando el derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y autentico.

En virtud de lo antes mencionado, firman:

Cruz LLaguento Lucila del Carmen	DNI: 76875154	

Pimentel, 15 de 12 del 2023

REPORTE DE SIMILITUD TURINITIN

Lucila del Carmen Cruz LLaguento

Mecanismo de autenticación basado en puntos de referencia bidimensionales en imágenes digitales para

Universidad Señor de Sipan

Detalles del documento

Identificador de la entrega
trn:oid:::26396:422679603

Fecha de entrega
22 ene 2025, 2:51 p.m. GMT-5

Fecha de descarga
22 ene 2025, 2:52 p.m. GMT-5

Nombre de archivo
turnitin cruz llaguento.docx

30 Páginas

8,607 Palabras

47,295 Caracteres

19% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto mencionado
- Coincidencias menores (menos de 8 palabras)

Fuentes principales

5% Fuentes de Internet
1% Publicaciones
17% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

MECANISMO DE AUTENTICACIÓN BASADO EN PUNTOS DE REFERENCIA BIDIMENSIONALES EN IMÁGENES DIGITALES PARA MEJORAR LA SEGURIDAD DE APLICACIONES WEB

Aprobación del jurado

MG. MEJIA CABRERA HEBER IVAN

Presidente del Jurado de Tesis

MG. ALVA ZAPATA JULIANA DEL PILAR

Secretario del Jurado de Tesis

MG. CELIS BRAVO PERCY JAVIER

Vocal del Jurado de Tesis

DEDICATORIA

A mis padres, Artidoro y Rosa, cuyo amor incondicional y sacrificios diarios me han permitido llegar hasta aquí. Su esfuerzo y dedicación me han dado la fortaleza para enfrentar cada reto, y su ejemplo ha sido la guía que me ha acompañado en cada paso de este camino académico. A mis hermanos, por su apoyo constante y por ser mi refugio en los momentos difíciles. A mis amigos, por su compañía, por celebrar conmigo los triunfos y por levantarme cuando las cosas no salían como esperaba. A todos ustedes, gracias por estar ahí, en los buenos y malos momentos.

La autora

AGRADECIMIENTO

A la Universidad Señor de Sipán – Chiclayo, por brindarme el apoyo invaluable y las herramientas académicas necesarias para alcanzar mis objetivos. Su compromiso con la formación de profesionales ha sido fundamental en mi desarrollo académico.

Al Mg. Arcila Diaz Juan Carlos y Mg. Fray Luis Becerra Suárez, por su constante asesoría y orientación a lo largo de este proceso de investigación. Su dedicación y compromiso han sido clave para el éxito de este trabajo

La autora

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El estudio tuvo como objetivo general desarrollar un mecanismo de autenticación basado en puntos de referencia bidimensionales en imágenes digitales para mejorar la seguridad en aplicaciones web. Para su implementación, se empleó un método con un enfoque dividido en dos etapas. En la primera parte, se establecieron tanto los requerimientos funcionales como los no funcionales, se crearon los prototipos necesarios y se llevó a cabo la implementación del sistema siguiendo el patrón de arquitectura modelo-vista-controlador (MVC). En la segunda fase, se evaluó el sistema con 25 participantes de distintos grupos etarios durante siete días, analizando los tiempos de autenticación, la capacidad de memorización y la usabilidad mediante el cuestionario QUIS.

Los hallazgos evidenciaron diferencias muy notables entre los grupos etarios en los periodos de autenticación y bloqueos. Los niños y adultos mayores tuvieron menores tasas de bloqueos y tiempos más reducidos, indicando mayor facilidad de uso, mientras que adolescentes y jóvenes presentaron tiempos más largos y más bloqueos. La capacidad de recordar el sistema fue alta en niños y adultos mayores, con una alta satisfacción según el cuestionario QUIS. El modelo demostró ser intuitivo y memorable, manteniendo su seguridad con resultados óptimos en las evaluaciones. En conclusión, se subraya la importancia de tener en cuenta la diversidad en las capacidades cognitivas al desarrollar mecanismos de autenticación. Este estudio aporta directrices valiosas para futuros desarrollos, destacando la relevancia de la usabilidad y la adaptabilidad a diferentes grupos poblacionales.

Palabras Clave: Autenticación con imagen, usabilidad, contraseñas gráficas, puntos bidimensionales.

ABSTRACT

The main objective of this study was to develop an authentication mechanism based on two-dimensional reference points in digital images to enhance security in web applications. For its implementation, a method with a two-stage approach was used. In the first stage, both functional and non-functional requirements were established, necessary prototypes were created, and the system was implemented following the model-view-controller (MVC) architectural pattern. In the second stage, the system was evaluated with 25 participants from different age groups over seven days, analyzing authentication times, memorization ability, and usability through the QUIS questionnaire.

The findings showed significant differences between age groups in authentication periods and lockouts. Children and older adults had lower lockout rates and shorter times, indicating greater ease of use, while adolescents and young adults showed longer times and more lockouts. The ability to recall the system was high among children and older adults, with high satisfaction according to the QUIS questionnaire. The model proved to be intuitive and memorable, maintaining its security with optimal results in the evaluations. In conclusion, the importance of considering cognitive diversity when developing authentication mechanisms is highlighted. This study provides valuable guidelines for future developments, emphasizing the relevance of usability and adaptability for different population groups.

Keywords: Authentication with image, usability, graphic passwords, two-dimensional dots.

I. INTRODUCCIÓN

Las plataformas web se han consolidado como herramientas esenciales debido a su facilidad de uso y accesibilidad, independientemente del dispositivo, sistema operativo o entorno de hardware, siempre que exista una conexión a internet. Esta versatilidad ha impulsado una notable transformación digital, abarcando sectores como el comercio electrónico, redes sociales y servicios financieros, todos orientados a optimizar y simplificar las actividades cotidianas de los usuarios [1], [2]. Dentro de este contexto, varios mecanismos de autenticación han sido implementados para autenticar la identidad de los usuarios y garantizar el acceso de forma segura a estas plataformas. Entre los más destacados se incluyen la autenticación mediante tokens, sistemas biométricos y la autenticación multifactor. No obstante, a pesar de su amplia adopción, estos mecanismos aún enfrentan desafíos significativos en cuanto a su facilidad de uso, los niveles de seguridad que ofrecen y el tiempo que requieren para completarse, lo que subraya la necesidad de continuar perfeccionando estos sistemas [3], [4]. El método más tradicional y ampliamente utilizado en la autenticación es el basado en contraseñas alfanuméricas, donde se valida la identidad del usuario comparando la clave ingresada con la previamente registrada. Sin embargo, a medida que las contraseñas requieren un mayor nivel de complejidad para garantizar seguridad, su memorización se vuelve considerablemente más difícil, especialmente cuando los usuarios necesitan gestionar contraseñas diferentes para múltiples servicios [1], [5]. Además, los esquemas de autenticación convencionales, como las claves con letras y números, han demostrado ser cada vez más susceptibles a vulnerabilidades, dado que pueden ser fácilmente comprometidos mediante ataques tales como el acceso indebido de credenciales y los intentos de fuerza bruta. Esta situación no solo expone la fragilidad de estas técnicas frente a amenazas externas, sino que también incrementa las dificultades para los usuarios al intentar recordar contraseñas más seguras, lo que termina afectando tanto la seguridad como la usabilidad del sistema.

En este contexto, se hizo imperativo formular la pregunta de investigación ¿Cómo se puede mejorar la seguridad en las aplicaciones web utilizando un mecanismo de autenticación

basado en puntos de referencia bidimensional en imágenes digitales? Ante esta interrogante se determinó la siguiente hipótesis, el uso de un mecanismo de autenticación basado en imágenes digitales puede mejorar la experiencia del usuario y mejorar la seguridad en las aplicaciones web. A partir de ello, el objetivo general de la investigación es desarrollar un mecanismo de autenticación basado en puntos de referencia bidimensionales en imágenes digitales para mejorar la seguridad en aplicaciones web; y como objetivos específicos: Definir los requerimientos funcionales del sistema de autenticación basado en puntos de referencia bidimensional en imágenes digitales, Implementar un prototipo funcional del mecanismo de autenticación basado en puntos de referencia bidimensional en imágenes digitales en una aplicación web, Realizar pruebas de usabilidad y la capacidad de ser recordada para evaluar la facilidad de uso del mecanismo de autenticación basado en puntos de referencia bidimensional en imágenes digitales en comparación con otros métodos de autenticación existentes, Realizar pruebas de seguridad para evaluar la resistencia del mecanismo de autenticación basado en puntos de referencia bidimensionales en imágenes digitales para los ataques a simple vista y ataques con cámara.

La presente investigación se justifica por la urgencia de aumentar la seguridad en plataformas web, que son fundamentales en la cotidianidad y en el funcionamiento de organizaciones, y que enfrentan amenazas cibernéticas cada vez más sofisticadas. Los enfoques convencionales de autenticación, como las claves de letras, números, y tokens, han demostrado vulnerabilidades significativas ante ataques como el hurto de credenciales y los ataques de fuerza bruta, además de plantear desafíos en cuanto a su complejidad y dificultad de recordar. En este contexto, la creación de un sistema de autenticación basado en puntos de referencias bidimensionales en imágenes digitales emerge como una propuesta novedosa que, además de aumentar la seguridad frente a ataques de ingeniería social y cámaras, también optimiza la satisfacción del usuario, erradicando la dependencia de retener contraseñas complejas en la memoria. Este enfoque responde a la creciente demanda de sistemas de autenticación más robustos y usables, contribuyendo al desarrollo de

aplicaciones web más seguras y alineadas con las expectativas de la comunidad tecnológica, promoviendo avances cruciales en la protección de datos sensibles en la era digital.

En respuesta a los desafíos mencionados, diversos investigadores a nivel nacional e internacional han explorado soluciones basadas en contraseñas gráficas como alternativa a los métodos tradicionales de autenticación. Un ejemplo notable es el trabajo de Zaman et al. [6], quienes propusieron un esquema innovador que combina elementos textuales y gráficos para mejorar la seguridad, la facilidad de memorización y la usabilidad. Este enfoque híbrido permite seleccionar diferentes modos de ingreso de contraseñas y emplea técnicas como drawmetric y autenticación en múltiples etapas, lo que refuerza la protección contra distintos tipos de ataques. Los resultados de su investigación evidencian que, con el tiempo y la práctica, los usuarios logran una mejora significativa en los tiempos de autenticación, lo que sugiere una adopción exitosa de este enfoque más intuitivo y seguro por parte de los usuarios. Así mismo, Hamdi et al. [7] propusieron un esquema innovador que utiliza esteganografía basada en diversas imágenes para reforzar la seguridad en sistemas de autenticación. La investigación aborda un problema crítico: la debilidad de los mecanismos de autenticación mediante gráficos frente a estrategias de ingeniería social maliciosa y técnicas de fuerza bruta. Para mitigar estos riesgos, el método desarrollado oculta los datos de verificación de identidad dentro de diversas imágenes mediante esteganografía, solicitando al usuario que elija la imagen adecuada como clave o contraseña. Este enfoque demostró ser significativamente más fiable y seguro, concluyendo que el esquema propuesto ofrece una mayor protección para la autenticación de usuarios en comparación con los métodos gráficos tradicionales. Por su parte, Damsgaard et al. [8] se enfocaron en analizar la facilidad de uso y efectividad de las contraseñas visuales en entornos infantiles, evaluando la capacidad de los niños para generar contraseñas seguras. Los resultados indicaron que, si bien la elección de imágenes resultó más sencilla de recordar y utilizar para los niños se identificó la necesidad de realizar mayores esfuerzos educativos para inculcar en ellos la relevancia de crear claves o contraseñas seguras. Estos hallazgos subrayan tanto el potencial de las contraseñas gráficas para mejorar la experiencia de usuario en poblaciones jóvenes, como la

importancia de combinar este enfoque con estrategias educativas adecuadas para maximizar su efectividad en términos de seguridad. Wang et al. [9] introducen un novedoso enfoque para la autenticación mediante contraseñas o claves gráficas basadas en grafos etiquetados, con el objetivo de aumentar la seguridad en este tipo de métodos. Su propuesta incluye un algoritmo diseñado específicamente para crear y corroborar contraseñas o claves gráficas empleando grafos etiquetados elegantes-impares. Los hallazgos de su indagación llegan a concluir que la aplicación de este enfoque puede incrementar de manera sustancial la seguridad de las contraseñas gráficas, lo que representa una mejora significativa respecto a los sistemas convencionales. Por otro lado, Carter et al. [10] se enfocan en abordar los desafíos presentan las personas mayores al recordar sus claves de acceso alfanuméricas. Para ello, proponen un esquema de autenticación gráfica basado en imágenes de objetos cotidianos y relevantes para este grupo etario. Las pruebas se llevaron a cabo con participantes mayores de 65 años, quienes manifestaron que el uso de contraseñas gráficas resultaba más sencillo y menos frustrante que los métodos tradicionales. Como conclusión, los investigadores sugieren que la autenticación gráfica mediante imágenes de valor personal podría ofrecer una opción eficaz y fácil de usar para personas de edad avanzada que encuentran problemático el uso de contraseñas alfanuméricas. Este punto de vista no solo incrementa la experiencia de usuario, sino que también minimiza las barreras cognitivas relacionadas con la memorización de contraseñas complejas. Sun et al. [11] desarrollaron un sistema de autenticación mediante contraseñas basadas en imágenes diseñado específicamente para defenderse de incidentes de visualización sin permiso. Este sistema emplea señales de inicio de sesión de un solo uso que emplean barras en movimiento, tanto horizontales como verticales, para ocultar las imágenes de la contraseña, lo que complica significativamente la tarea de los atacantes, incluso si recurren a múltiples intentos utilizando cámaras. Los experimentos realizados para evaluar la memorabilidad y la usabilidad del sistema demostraron que ofrece una notable resistencia frente a estos ataques, sin afectar negativamente la facilidad de uso por parte de los usuarios. Además, Pulicherla et al. [12] propusieron una solución basada en software que permite al usuario capturar una imagen y,

posteriormente, seleccionar varios puntos específicos dentro de la misma para autenticarse. A fin de hacer el sistema más tolerante, los autores introdujeron un margen de error en la selección de los puntos, permitiendo que estos no tengan que ser exactos. Las pruebas realizadas mostraron que esta técnica alcanzó una precisión del 73.809%, lo que indica su potencial como un método de autenticación alternativo, aunque con margen para mejoras en su precisión y seguridad. Así mismo, Wen y Zi [24] desarrollan un novedoso sistema de autenticación que utiliza imágenes personalizadas junto con patrones gráficos complejos, con el objetivo de reforzar la seguridad en plataformas web. Este estudio se clasifica como aplicado, adoptando un enfoque cuantitativo y un diseño no experimental, con una muestra de 40 participantes de diversos grupos etarios, seleccionados por su accesibilidad. Se implementaron técnicas de evaluación observacional y un cuestionario estandarizado para medir la usabilidad, obteniendo un puntaje superior al 90%. Los hallazgos revelaron que el tiempo medio requerido para la autenticación fue de entre 28 y 50 segundos, mientras que la tasa de bloqueos durante 150 inicios de sesión en un período de prueba de siete días fue del 30%. Las conclusiones subrayan la eficacia del sistema frente a intentos de ataque visual, registrando una tasa de éxito inferior al 8% para los atacantes, lo que valida la solidez del mecanismo de autenticación propuesto. Esta investigación representa un avance significativo hacia el establecimiento de estándares elevados de seguridad digital al combinar requerimientos funcionales, de usabilidad y protección. De la misma manera, Kai et al, [25] presentan un enfoque innovador para la autenticación en aplicaciones móviles, utilizando biometría facial combinada con patrones de comportamiento del usuario. El objetivo de esta investigación es aumentar la seguridad y la accesibilidad en entornos digitales. Se trata de un estudio aplicado con un diseño experimental y un enfoque cuantitativo, donde se involucraron 30 participantes seleccionados aleatoriamente. Se aplicaron técnicas de análisis estadístico y encuestas para evaluar el grado de satisfacción del usuario, logrando un índice de satisfacción del 92%. Los resultados indicaron que el tiempo medio de autenticación fue de 25 a 38 segundos, con una tasa de éxito en la autenticación biométrica del 95% en condiciones óptimas. Las conclusiones destacan la alta efectividad del método propuesto,

que logró minimizar las tasas de fraude en comparación con métodos tradicionales, situando este sistema como una alternativa viable para la autenticación en dispositivos móviles. Este trabajo aporta al desarrollo de técnicas de autenticación más seguras y accesibles, alineándose con las necesidades actuales del mercado digital. Finalmente, Weitao et al, [26] investigan un sistema de autenticación basado en huellas dactilares que integra algoritmos de inteligencia artificial para detectar tendencias de comportamiento anómalos. El objetivo de esta investigación es incrementar la fiabilidad en los procesos de autenticación de usuarios en sistemas críticos. Este estudio es de tipo aplicada, con un enfoque cuantitativo y un diseño no experimental, analizando una población de 50 individuos elegidos mediante muestreo aleatorio. Se emplearon técnicas de análisis de datos y herramientas de software para evaluar la eficacia del sistema, alcanzando una precisión del 98% en la identificación de usuarios. Los resultados revelaron que el tiempo promedio de autenticación osciló entre 20 y 30 segundos, con una incidencia de intentos fallidos del 15% durante un mes de pruebas. Las conclusiones subrayan que el sistema es robusto ante intentos de suplantación, demostrando una resistencia del 85% a ataques simulados. Este estudio contribuye al avance en sistemas de autenticación seguros, proponiendo un modelo que mejora la seguridad en la gestión de información sensible.

II. Materiales y Método

2.1. Materiales

Para el desarrollo del mecanismo de autenticación basado en puntos de referencia bidimensionales en imágenes digitales se empleó un dispositivo portátil equipado con un procesador Intel Core i7-1165G7 con una frecuencia de 2.80 GHz, 8 GB de memoria RAM, bajo un entorno operativo Windows 11 de 64 bits, el detalle se puede apreciar en la tabla 1.

El sistema de autenticación, basado en contraseñas gráficas, se estructura en dos fases, considerando el desarrollo a nivel de front-end, cuyos wireframes fueron desarrollados mediante el sistema web Marvel App e implementados en HTML para la maquetación de la aplicación, CSS para la definición de estilos y JavaScript para la implementación dinámica de

la funcionalidad de la aplicación. En la otra fase, correspondiente al backend, se programó en el lenguaje de programación PHP 7.4, haciendo uso de la librería AJAX para gestionar el flujo de solicitudes y respuestas a través del protocolo HTTP. Además, se integró MySQL 5.6 para la gestión de las credenciales de acceso de los usuarios. Por último, se empleó un servicio de alojamiento compartido en un entorno operativo Linux, vinculado al dominio www.imagenlogin.com, donde se llevaron a cabo diversas pruebas de seguridad y usabilidad.

TABLA I: LISTA DE MATERIALES

COMPONENTE	DESCRIPCIÓN
Dispositivo de desarrollo	Procesador: Intel Core i7-1165G7 a 2.80 GHz, RAM: 8GB, Sistema Operativo: Windows 11 de 64 bits
Tecnologías de desarrollo	Nivel frontend: HMTL, CSS, JS, Bootstrap. Nivel backend: PHP 7.4, Ajax Gestor de base de datos: MySQL 5.6 Servidor local basado en XAMPP. Diseño de wireframes: Marbel APP.
Alojamiento web	Servido de alojamiento compartido basado en Linux, Dominio de pruebas: www.imagenlogin.com

Nota: Listado de materiales para la investigación. Elaboración propia

2.2. Método

El proceso metodológico comenzó considerando la entrada de una imagen sin considerar el tamaño o el formato de la imagen, en el sistema la imagen se adapta a un tamaño fijo de 300 x 280, la imagen subida se almacena en la carpeta del aplicativo y la url se guarda en la base de datos, una vez que el usuario tenga seleccionada la imagen procederá a marcar entre 4 a 6 puntos considerando el orden y la ubicación el cual es el patrón de autenticación. El registro de datos se almacena en una base de datos que tiene como tabla principal “persona” donde se almacena los datos del usuario nombres, apellidos, email, sexo, fecha de nacimiento y las coordenadas del patrón de autenticación en formato json. En la validación de datos se realiza la comparación del patrón ingresado al crear la

cuenta del usuario con el patrón ingresado al autenticarse, se validan tanto el orden de los puntos ingresados como la ubicación considerando un margen de error el cual se calcula por medio de la ecuación euclidiana además se desarrolló un aplicativo que nos permita evaluar el método, tal como se expone detalladamente en la Figura 1

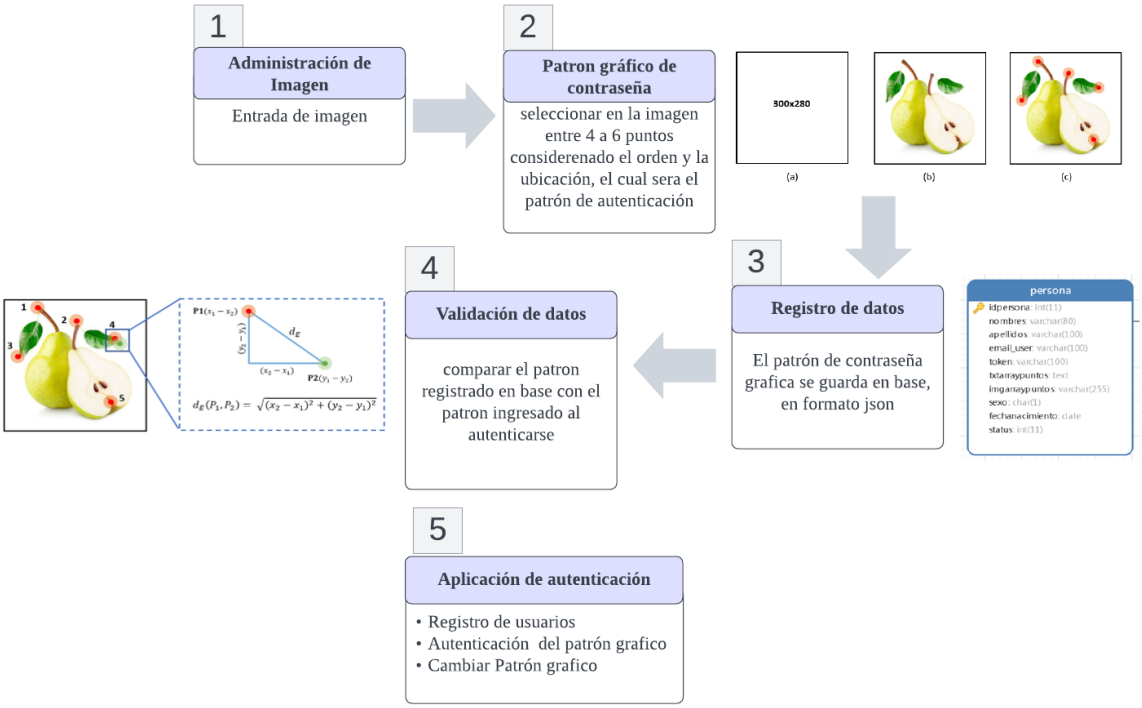


Fig. 1 Diagrama del método utilizado. Elaboración Propia

Inicialmente, se ha considerado que el usuario pueda subir la imagen de esta manera poder mejorar el nivel de recuperación de la información a largo plazo. En cuanto a la selección de la imagen, el usuario tiene la libertad de elegir cualquier imagen para cargar. Esta consideración se basa en estudios sobre memorabilidad [6],[18], que vincular una imagen, particularmente aquella que evoca un suceso personal de carácter histórico, puede potenciar significativamente la retención de la memoria. La imagen subida se guarda en la carpeta de imágenes del proyecto y la url de la imagen es almacenada en la base de datos. El tamaño establecido de la imagen es de width: 300px y de height: 280px sin embargo el usuario podrá seleccionar cualquier imagen y al momento de subir se adapta al tamaño correspondiente.

Una de las principales limitaciones cuando se trabaja con el lenguaje de programación

PHP es que no tiene un buen soporte para el tratamiento de imágenes, en comparación con otros lenguajes de programación como Python con su framework Flask. Para mitigar esta limitación, se utilizó CANVAS que está añadido en el estándar HTML5 como etiqueta <canvas>, el cual es soportado por los diferentes navegadores web.

El canvas implementado tiene una dimensión de 300x280 pixeles, en el cual se carga la imagen subida por el usuario. La imagen se redimensiona tanto en ancho como en alto según las dimensiones del canvas. A partir de ello, el usuario puede seleccionar entre 4 y 6 puntos de la imagen el cual es el patrón de autenticación. Todo este proceso es desarrollado mediante funciones de JavaScript, lo que permite al sistema tener un tiempo de respuesta muy rápido.

Fig. 2: Ejemplo de subir imagen y seleccionar los puntos. Elaboración Propia

Cada punto que el usuario ha establecido en la imagen es un par de valores X, Y. Estos valores son almacenados a nivel de frontend en un arreglo multidimensional en JavaScript, respetando el orden de selección de cada punto. Cuando el usuario ha seleccionado una cantidad de puntos cumpliendo la restricción establecida de entre 4 y 6 puntos, además de completar sus datos personales nombres, apellidos, correo, fecha de nacimiento y sexo. Estos datos son enviados al servidor mediante una solicitud HTTP de tipo POST. Las solicitudes son implementadas mediante funciones AJAX y código JSON, permitiendo de esta manera, una actualización del sistema parcial y asincrónica, obteniendo una fluidez muy natural en la interacción entre usuario y el sistema. Todos estos datos, son almacenados en la base de datos de Mysql.

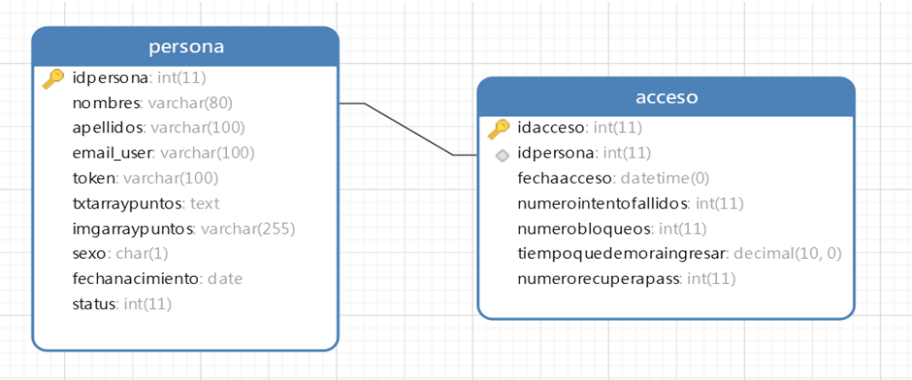


Fig. 3: Esquema Físico de la Base de Datos. Elaboración Propia

Durante el registro, se genera una clave gráfica personalizada a partir de la selección y ordenación de puntos en una imagen, esta clave compuesta por una secuencia de puntos, es utilizada posteriormente para verificar la identidad del usuario. Para realizar dicha validación, se mide la distancia exacta entre los puntos del patrón para confirmar su autenticidad, utilizando una fórmula matemática conocida como distancia euclidiana. Este método de cálculo, que se basa en el famoso teorema de Pitágoras, es fundamental en muchas áreas, desde las matemáticas hasta la ciencia de datos. En un plano, la distancia entre dos puntos se calcula usando una fórmula sencilla que involucra las coordenadas de esos puntos:

$$d_E(P_1, P_2) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

Fig. 4: Ecuación euclidiana utilizada como fórmula. Elaboración Propia

Esta fórmula, directamente relacionada con el famoso teorema de Pitágoras, nos permite medir la distancia más corta entre dos puntos, no solo en un plano, sino también en espacios más complejos. La Figura 5 muestra cómo aplicamos este principio para verificar la seguridad de nuestras contraseñas gráficas. Inicialmente, los puntos rojos numerados indican el orden en el que fueron registrados por el usuario durante la etapa de registro. Si el usuario, en el proceso de validación, selecciona un punto verde en la posición 4, el sistema compara este punto con el registrado previamente, utilizando la distancia euclidiana entre ambas posiciones. Este proceso es el mismo para todos los puntos del patrón.

Dado que es prácticamente imposible que un usuario seleccione exactamente el

mismo punto dos veces, se ha implementado un margen de error o tolerancia. Este margen, establecido en 10 píxeles, permite cierta variabilidad en la posición de los puntos seleccionados. En otras palabras, si el punto seleccionado por el usuario se encuentra dentro de un radio de 10 píxeles del punto registrado en la base de datos, se considera una coincidencia. Esta tolerancia es esencial para garantizar que el sistema pueda reconocer el patrón, incluso si existen pequeñas desviaciones en la selección de los puntos, lo que aumenta la usabilidad y la precisión del sistema de autenticación. Si al menos uno de los puntos seleccionados supera el rango de tolerancia, el sistema no valida el patrón, y el usuario recibe un mensaje de "ACCESO DENEGADO".

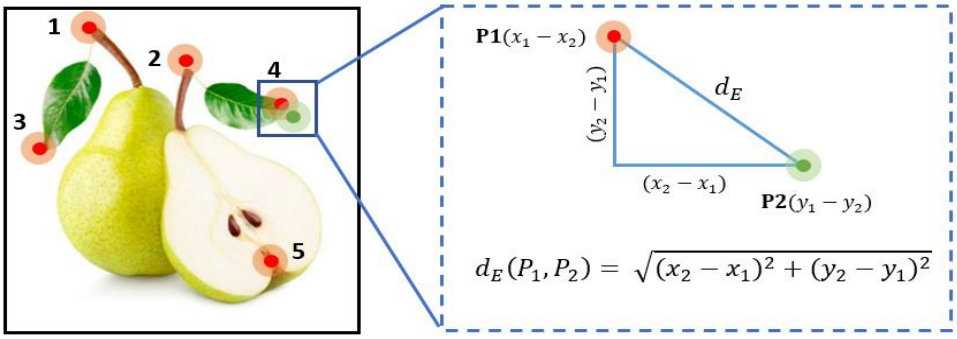


Fig. 5: Ejemplo de validación del patrón gráfico de contraseña utilizando la distancia euclidiana. Elaboración Propia

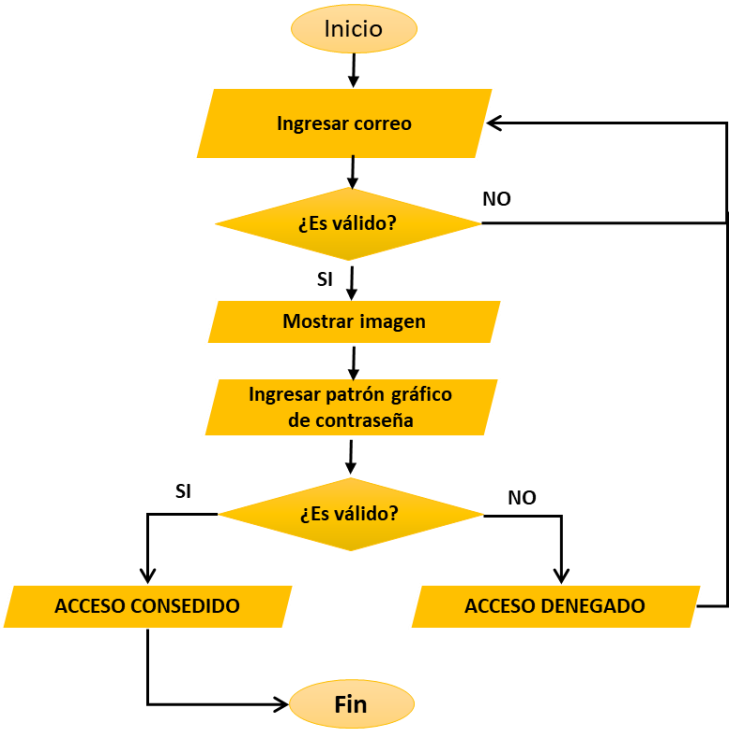


Fig. 6: Diagrama de flujo para el proceso de autenticación de usuarios. Elaboración Propia

El desarrollo del aplicativo de mecanismo de autenticación inicio con la identificación los requerimientos funcionales, así como los no funcionales son fundamentales para determinar tanto las capacidades operativas como las características de calidad que debe poseer un sistema informático [13]. Los requisitos funcionales especifican las funciones que el software debe llevar a cabo. En el caso del sistema desarrollado, estos comprenden la implementación del sistema de registro de usuarios, que abarca la recopilación de información básica tales como nombres, apellidos, dirección de correo electrónico, el género y fecha de nacimiento. Además, el usuario debe cargar una imagen en la cual seleccionará puntos específicos que servirán como su contraseña gráfica. El sistema también debe permitir la verificación de las credenciales de acceso, de modo que el usuario, al proporcionar su correo electrónico, pueda acceder a la imagen previamente registrada y seleccionar los puntos previamente designados para autenticar su identidad. Adicionalmente, el sistema debe ofrecer la posibilidad de cambiar la contraseña, utilizando un enlace que se envía directamente a la dirección de correo electrónico del usuario, proporcionando así un mecanismo seguro de recuperación de credenciales.

En cuanto a los requisitos no funcionales, estos están orientados a aspectos de calidad y rendimiento del sistema. La usabilidad se presenta como un componente clave, lo que implica que la interfaz del sistema debe ser intuitiva, fácil de comprender y manejar por usuarios de distintos niveles de experiencia. Asimismo, la seguridad de los datos es un aspecto crítico, ya que el sistema debe garantizar la protección y privacidad de los datos almacenados y transmitidos, protegiéndola contra accesos no autorizados y ataques. También se considera la disponibilidad del sistema, lo que asegura que los usuarios tengan la capacidad de acceder a la plataforma en cualquier instante, sin interrupciones, lo que es esencial para garantizar una experiencia de usuario sin interrupciones y de confianza. Estos requisitos no solo se enfocan en la funcionalidad del sistema, sino también en la satisfacción del usuario y la protección de la información sensible, lo que resulta crucial en el contexto de sistemas de autenticación avanzados.

TABLA II: REQUISITOS FUNCIONALES Y NO FUNCIONALES

TIPO DE REQUISITO	DESCRIPCIÓN
Requisitos funcionales	
Registro de nuevos usuarios	El sistema debe recopilar información personal del usuario, incluyendo la opción de cargar imágenes para crear un patrón gráfico que servirá como contraseña para acceder a la aplicación.
Autenticación de usuarios	Acceder a la validación del patrón gráfico de contraseña. Asimismo, se deben proporcionar alternativas para recuperar la contraseña y visualizar las opciones disponibles una vez que los datos hayan sido validados correctamente.
Gestión administrativa	Disponer de funcionalidades para llevar a cabo el mantenimiento de la aplicación, efectuar diversas configuraciones de ajustes, administrar la información de los usuarios y generar informes.
Requisitos no funcionales	
Usabilidad	Sistema de fácil utilización y comprensión.
Seguridad de datos	Garantizar la integridad y confidencialidad de los datos
Disponibilidad	Asegurar que el sistema esté accesible en cualquier momento.

Nota: Requisitos funcionales y no funcionales elaborado para la investigación

Una vez definidos y consolidados los requisitos funcionales, se procedió a elaborar el diagrama de casos de uso, que ilustra las interacciones y responsabilidades de los distintos actores del sistema. En este diagrama, se establece que el administrador asume la responsabilidad de mantener la aplicación, así como de gestionar las cuentas de los usuarios y supervisar el proceso de autenticación. Por otro lado, un nuevo usuario tiene la capacidad de gestionar la información de su perfil personal y llevar a cabo su autenticación

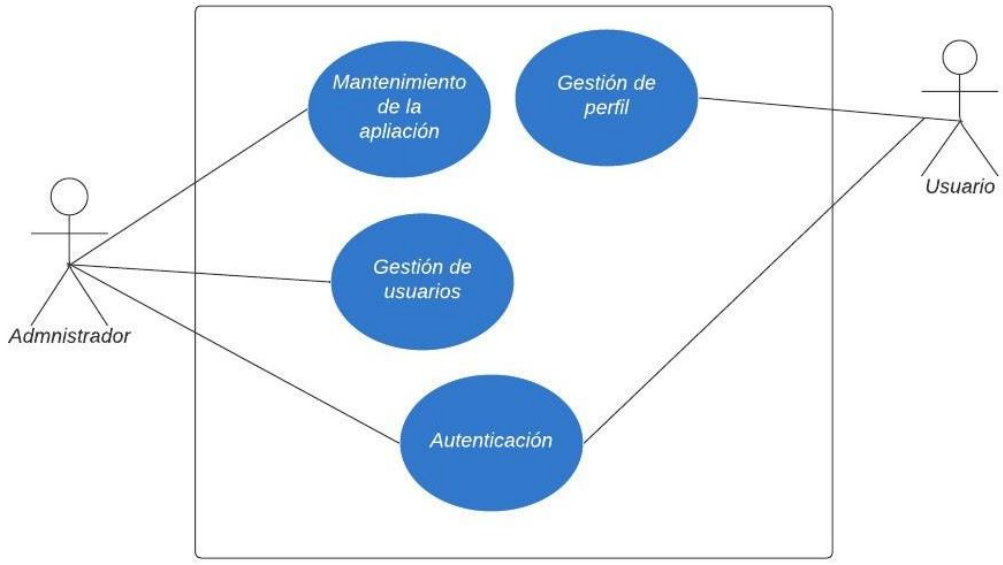


Fig. 7: Gráfico de casos de uso. Elaboración Propia

El diseño del prototipo inicialmente se refleja en un conjunto de wireframes que proporcionan una perspectiva temprana sobre la conceptualización del software, sin estar restringidos por el medio a través del cual se desarrollen [14]. Con base en los requisitos funcionales definidos anteriormente, se han creado los siguientes esquemas de interfaz. En la figura 8, se describen los wireframes diseñados para el proceso de creación de cuentas, los cuales están organizados de la siguiente forma: en el apartado (1), se muestra un formulario que da al usuario la posibilidad de ingresar la información requerida. A continuación, en el apartado (2), se ofrece al usuario la opción de elegir una imagen de su preferencia. Esta imagen elegida se utiliza en el apartado (3), donde el usuario puede establecer un patrón de contraseña gráfica mediante la selección de píxeles específicos de la imagen.

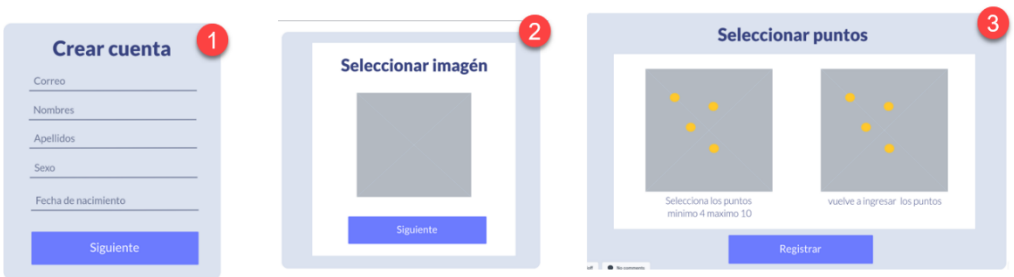


Fig. 8: Modelo de diseño de wireframes para añadir nuevos usuarios. Elaboración Propia

Este enfoque en el diseño de wireframes es fundamental, ya que proporciona un marco visual que facilita la comunicación de ideas y el entendimiento de la funcionalidad del software en sus etapas iniciales. Además, la integración de una imagen personalizable para el registro de la contraseña gráfica incrementa la protección y, al mismo tiempo, facilita una mejor interacción para el usuario. al permitir una mayor personalización en el proceso de autenticación. Al establecer un patrón de contraseña a partir de elementos visuales, se busca abordar la problemática de las contraseñas tradicionales al ofrecer un método de acceso que sea tanto memorable como seguro, alineándose con la necesidad de soluciones de autenticación más efectivas y accesibles.

La Figura 9 ilustra un ejemplo de los wireframes asociados al procedimiento de verificación de datos de acceso. En el apartado (1), se muestra el wireframe diseñado para la entrada del correo electrónico del usuario. Si la validación del correo electrónico se realiza con éxito, se activa el apartado (2), en la que se le brinda al usuario la posibilidad de escoger cualquier punto dentro de la imagen presentada. Finalmente, en la sección (3), se exhibe la interfaz central que el usuario observará tras haber completado de forma satisfactoria la validación de sus credenciales.

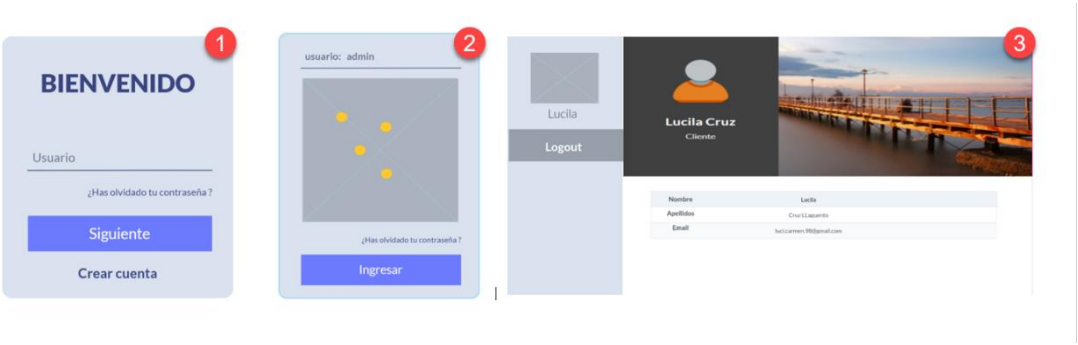


Fig. 9: Modelo de wireframes para la validación de datos de acceso. Elaboración Propia

Este proceso de validación es crucial para asegurar la protección y la integridad del sistema, al permitir únicamente el acceso a aquellos usuarios cuyas credenciales han sido verificadas. Al incorporar un método visual para la autenticación, se busca mejorar la experiencia del usuario, haciendo el proceso de acceso no solo más seguro, sino también más interactivo y personalizable. La estructura de los wireframes facilita la comprensión del

flujo del sistema y permite identificar posibles mejoras antes de la implementación final del software, asegurando que se cumplan los requisitos funcionales y se minimicen las vulnerabilidades en el mecanismo de autenticación.

La Figura 10 ilustra los wireframes diseñados para el proceso de restablecimiento del patrón de datos de acceso. En el apartado (1), se muestra un formulario donde el usuario debe proporcionar su cuenta de correo electrónico personal. A continuación, en el apartado (2), se presenta un mensaje personalizado que valida la remisión de un enlace destinado a la recuperación del patrón de contraseña, enviado a la cuenta de correo que el usuario indicó, según lo detallado en el apartado (3). Finalmente, en el apartado (4), se le brinda al usuario la opción de crear un nuevo patrón de acceso.

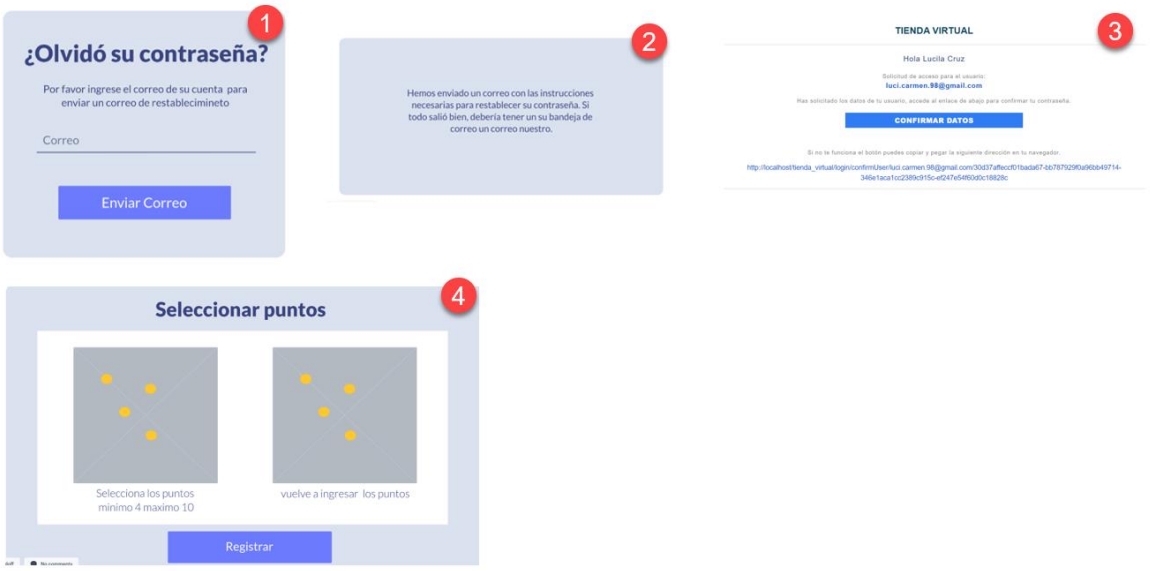


Fig. 10: Modelo de diseño para la restauración del patrón de seguridad. Elaboración Propia

Este proceso de restablecimiento es fundamental para la gestión de la seguridad, ya que permite a los usuarios recuperar el acceso a su cuenta de manera segura en caso de olvidar su patrón de autenticación. La implementación de un sistema que envía un enlace de restablecimiento al correo electrónico del usuario no solo mejora la experiencia de usuario al proporcionar una solución accesible, sino que también refuerza la seguridad del sistema al requerir la verificación de una cuenta de correo electrónico registrada. Estos wireframes son una representación clave en el desarrollo del software, ya que ayudan a visualizar el flujo de la interfaz y aseguran que se cumplan los estándares de usabilidad y funcionalidad

requeridos.

La implementación del sistema comenzó con la adopción de la arquitectura de MVC(Modelo-Vista-Controlador), que segmenta la aplicación en tres capas distintas. La capa de presentación se ocupa de mostrar la información al usuario, mientras que la capa de modelo maneja la lógica y los datos de la aplicación, la capa de controlador, por su parte, actúa como un intermediario, gestionando las interacciones entre la vista y el modelo, y actualizando la vista según las acciones del usuario [15]. Esta elección arquitectónica se fundamenta en la clara distribución de funciones entre las capas, lo que contribuye a facilitar el mantenimiento, la escalabilidad, la adaptabilidad y la flexibilidad del software [16]. Este enfoque es ampliamente empleado en el desarrollo de aplicaciones web en diversos sectores, como la enseñanza, la sanidad y la agricultura, entre otros [17].

El sistema integra dos algoritmos fundamentales para llevar a cabo las actividades que el usuario puede realizar, específicamente el registro y la autenticación, los cuales se detallan a continuación.

El primer algoritmo inicia con la captura de datos biográficos esenciales, tales como: dirección de correo electrónico, nombres propios, apellidos, género, fecha de nacimiento y una fotografía digital. La dirección de correo electrónico funge como un identificador único que el usuario utilizará para autenticarse en el sistema. En cuanto a la selección de la imagen, el usuario tiene la libertad de elegir cualquier imagen para cargar.

Una vez capturada la información inicial, se procede a generar un patrón de desbloqueo gráfico. El usuario selecciona entre cuatro y seis puntos sobre una imagen de referencia, estableciendo así una secuencia de interacción única. Tanto la cantidad como el orden de los puntos seleccionados conforman la clave de acceso al sistema. Este patrón se verifica y almacena en la base de datos.

El segundo algoritmo ejecutado se encarga de la etapa de autenticación, cuyo objetivo primordial es validar la identidad de un usuario que solicita acceso a la aplicación. Como resultado de este algoritmo, se genera una salida que puede ser "ACCESO AUTORIZADO" o "ACCESO NO AUTORIZADO". El diagrama de flujo que ilustra este proceso se encuentra

en la Figura 11.

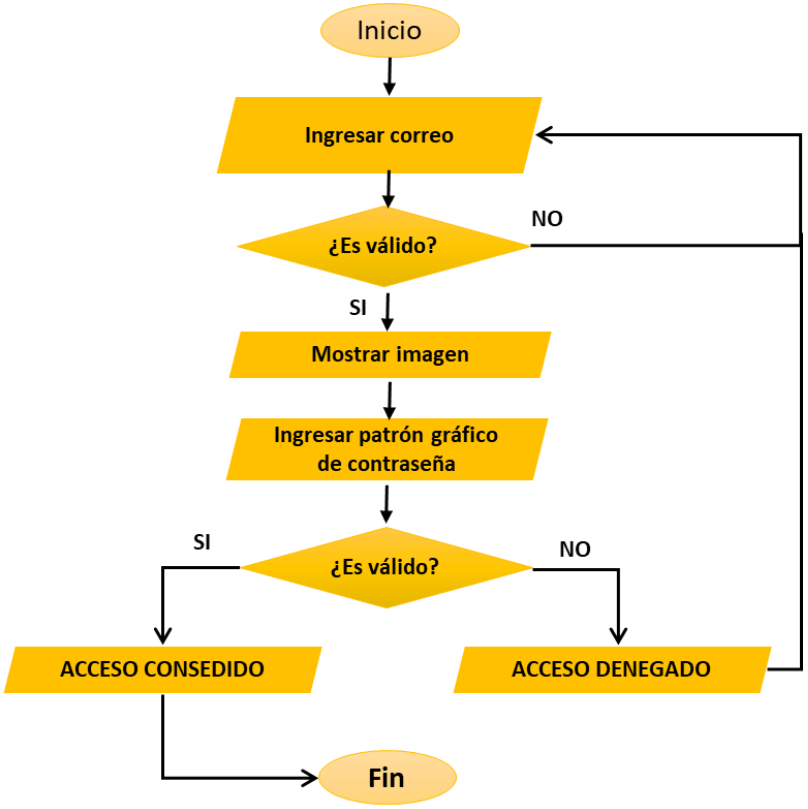


Fig. 11: Diagrama de flujo para el proceso de autenticación de usuarios. Elaboración Propia

La plataforma ha sido implementada en el dominio https://imagenlogin.com/, donde puede ser utilizada conforme a lo detallado en las etapas de registro y autenticación de usuarios. En la Figura 12, se presenta una descripción del proceso correspondiente a la fase de registro. De igual manera, en la Figura 13 se ilustra el mecanismo de validación de credenciales, mientras que en la Figura 14 se expone el procedimiento para la recuperación de la contraseña.

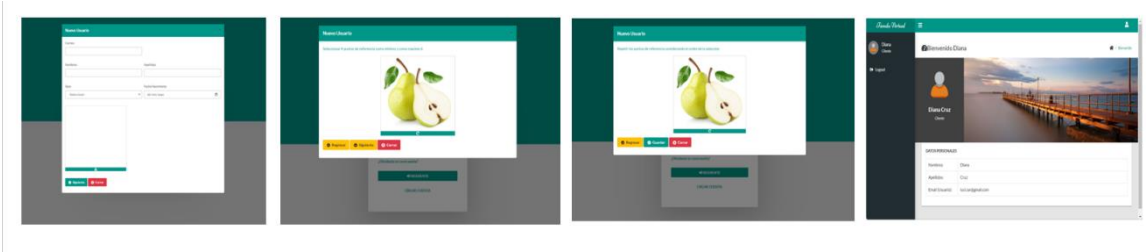


Fig. 12: Implementación de wireframes del proceso de creación de usuario. Elaboración Propia

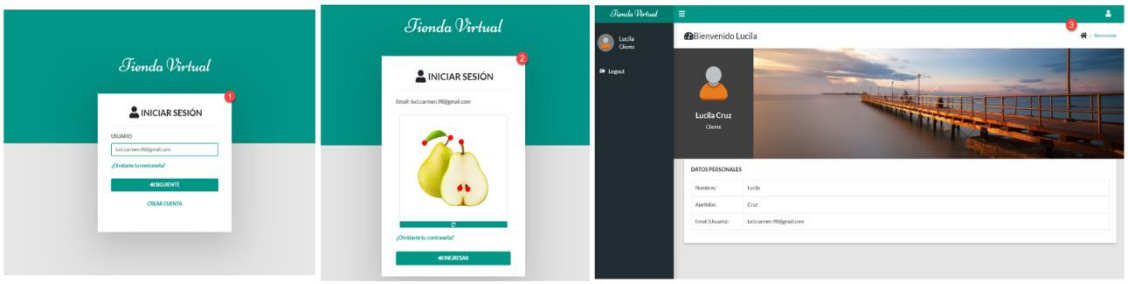


Fig. 13: Implementación de wireframes del proceso de validación de credenciales. Elaboración Propia

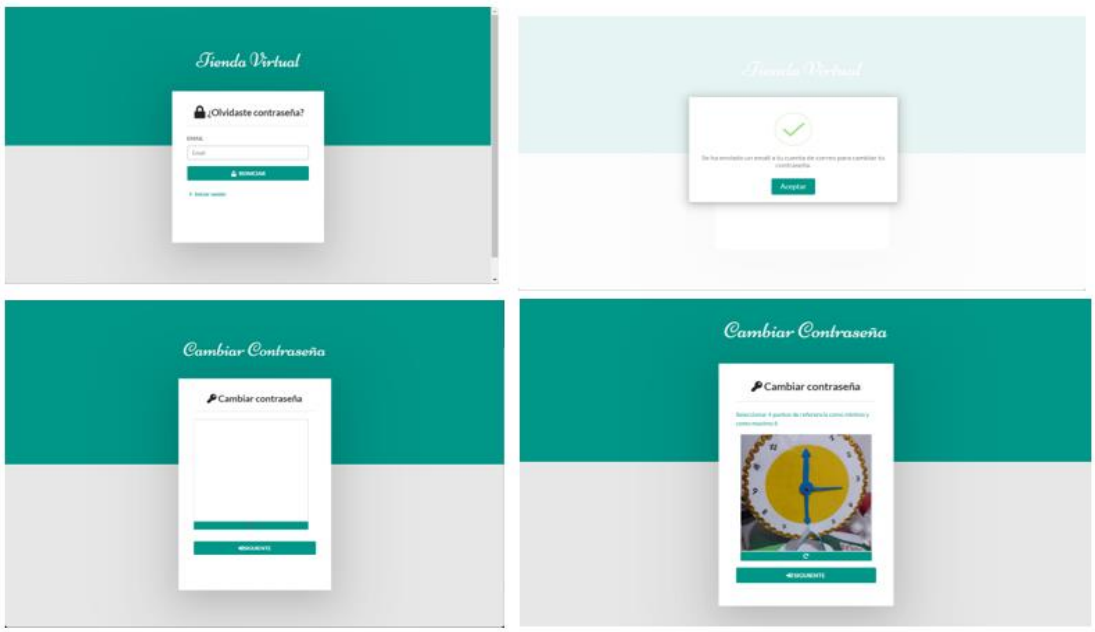


Fig. 14: Implementación de wireframes del proceso de restauración del patrón de credenciales. Elaboración Propia

III. RESULTADOS Y DISCUSIÓN

3.1. Resultados

Para garantizar una evaluación exhaustiva del sistema de autenticación por patrón gráfico, se conformó una muestra diversa de 25 participantes, representando un amplio espectro de edades. La muestra se estructuró en cinco grupos etarios: niños, adolescentes, jóvenes, adultos y adultos mayores, con cinco individuos en cada grupo el listado de los participantes se encuentra detallado en el anexo 3. Esta distribución permitió evaluar el desempeño del sistema en diferentes poblaciones, considerando las posibles variaciones en la habilidad motora, la familiaridad con la tecnología y otros factores cognitivos asociados a la edad. La selección de los participantes se basó en criterios de accesibilidad y conveniencia,

y en el caso de los menores de edad, se obtuvo el consentimiento informado de sus tutores legales.

TABLA III: DEMOGRÁFICA DE LA MUESTRA DE ESTUDIO.

Grupo	Rango Edad	Cantidad	% de Usuarios Masculinos	% de Usuarios Femeninos
Niños	06 - 12	5	60%	40%
Adolescentes	13 - 18	5	40%	60%
Jóvenes	19 - 30	5	40%	60%
Adultos	31 - 59	5	60%	40%
Adulto mayor	60 a más	5	40%	60%

NOTA: Elaboración propia

Para evaluar la usabilidad y efectividad de la aplicación, se llevó a cabo un estudio de campo de una semana de duración con 25 participantes. En la primera sesión, cada usuario configuró su perfil de autenticación siguiendo un protocolo detallado. Posteriormente, con el objetivo de familiarizarse con el sistema y evaluar su desempeño a lo largo del tiempo, los participantes utilizaron la aplicación de manera regular, al menos una vez al día. Este diseño experimental permitió analizar la curva de aprendizaje de los usuarios y la adaptabilidad del sistema a diferentes patrones de uso. Durante esta fase, se recopilaron datos sobre las posibles dificultades que los participantes enfrentaron al intentar autenticarse tras períodos prolongados de inactividad, el detalle de la recopilación de datos se encuentra especificado en el anexo 3.

Al analizar los datos de tiempo de autenticación por grupos de edad, se observaron patrones interesantes. Si bien el tiempo promedio de autenticación para cada grupo fue relativamente cercano, se detectaron variaciones significativas entre los individuos de cada grupo. Los niños, en general, demostraron una mayor rapidez y consistencia en el proceso de autenticación, con un tiempo promedio de 34 segundos. Los adolescentes, por su parte, presentaron una variabilidad ligeramente mayor, con un tiempo promedio de 39 segundos. El grupo de jóvenes exhibió el tiempo promedio más elevado, aunque con una dispersión considerable en los datos individuales. Sorprendentemente, los adultos mayores se ubicaron cercanos a los niños en términos de tiempo promedio de autenticación, lo que sugiere una

adaptación efectiva al sistema.

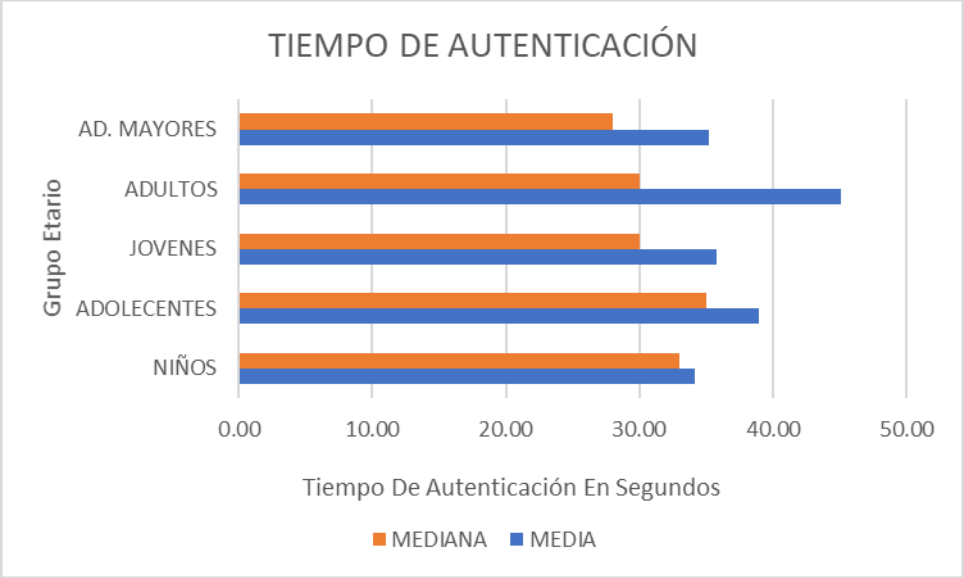


Fig. 15: Tiempo de autenticación para cada grupo de estudio en función de la media y mediana.

Los resultados presentados en la Figura 15 fueron analizados de la bitácora de tiempos de autenticación detallado en el anexo 3, esta figura muestra que los tiempos de autenticación promedio para los niños, adolescentes, jóvenes y adultos mayores son similares, con valores aproximados de 34, 39 y 35 segundos, respectivamente. No obstante, se observa una notable variabilidad, especialmente en el grupo de adultos, donde la media se ve afectada por algunos tiempos de autenticación extremadamente elevados. La mediana, al ser menos influenciada por valores extremos, refleja que la mayoría de los participantes, sin importar su grupo etario, logran autenticarse en tiempos cercanos a los valores centrales. Estos resultados subrayan la relevancia de considerar la variabilidad al analizar los tiempos de autenticación en función de las diferentes edades.

La memorabilidad se refiere a la habilidad para almacenar información en la memoria a largo plazo. En el ámbito de la seguridad informática, este concepto está relacionado con la facilidad con la que los usuarios pueden recordar y utilizar contraseñas o mecanismos de autenticación. Un sistema se considera más memorable si permite a los usuarios recordar la información sin dificultad, manteniendo altos niveles de seguridad [19].

Esta característica es fundamental para el método de autenticación propuesto en el presente estudio. Con el objetivo de evaluar su eficacia, se ha realizado un análisis del número de bloqueos generados en función de cada grupo etario. La Tabla 2 presenta un resumen del total de bloqueos registrados al utilizar el método de autenticación basado en

patrones gráficos de contraseña, la bitácora de bloqueos se encuentra detallado en el anexo 3.

TABLA IV: TOTAL, DE BLOQUEOS POR CADA GRUPO ETARIO.

Grupo	Cantidad de bloqueos de cuenta
Niños	2
Adolescentes	14
Jóvenes	16
Adultos	4
Adultos mayores	8

Nota: Elaboración propia

Según los datos expuestos en la Tabla 4, el grupo de niños presenta el menor número de bloqueos, lo que podría sugerir que este método de autenticación les resulta más fácil de recordar o más memorable, provocando menos errores y, por ende, menos bloqueos. En contraste, los adolescentes y jóvenes muestran una cantidad significativamente mayor de bloqueos, lo cual podría indicar que, a pesar de su familiaridad con la tecnología, enfrentan desafíos para recordar los patrones de autenticación, lo que incrementa los fallos. En el caso de los adultos mayores, a pesar de pertenecer a un grupo que se podría asumir tiene más dificultades con tecnologías más recientes, registran menos bloqueos que los adolescentes y jóvenes. Esto sugiere que encuentran el uso de patrones gráficos más fácil de memorizar o utilizar que otras alternativas de autenticación.

En cuanto a la usabilidad del software, esta se refiere a la facilidad con la que puede ser comprendido y utilizado por el usuario final, lo que incrementa su atractivo bajo ciertas condiciones [20]. Para evaluar este aspecto en la presente investigación, se utilizó el "Cuestionario para la satisfacción de la interfaz de usuario (QUIS)", una herramienta estandarizada ampliamente reconocida y aplicada en diversos estudios [21],[22],[2],[23]. Este cuestionario está estructurado en 5 categorías, abarcando un total de 27 ítems, cada uno de los cuales se evalúa en una escala del 0 al 9.

Al concluir el periodo de prueba de siete días, se pidió a todos los participantes que completaran el cuestionario QUIS, resultados detallados de la respuesta de los participantes

se encuentran en el anexo 4. Cada ítem, como se detalla en la Tabla 3, representa un criterio que los usuarios evaluaron, expresando su percepción de satisfacción en una escala que va de 0 (lo más negativo) a 9 (lo más positivo). La media indica la puntuación promedio que se otorgó a cada ítem, superando los 8 puntos y con un promedio general que se sitúa entre 8.25 y 8.95 por cada pregunta. La desviación estándar (Std. Dev) sirve como un indicador de dispersión que refleja cuánto se desvían los valores individuales de la media en el conjunto de datos. En este contexto, para cada ítem analizado (como “terrible-maravilloso”, “difícil-fácil”, entre otros), la desviación estándar revela el grado de variabilidad o dispersión en las respuestas de los usuarios respecto a la puntuación media.

Por ejemplo, una desviación estándar baja, como en el caso del ítem “rígido-flexible” con un valor de 0.41, sugiere que las respuestas de los participantes están muy alineadas con la puntuación media de 8.80, lo que indica un amplio acuerdo entre los usuarios sobre esta evaluación. En contraste, un ítem con una desviación estándar mayor, como “aburrido-estimulante” con 0.89, señala que las respuestas de los usuarios muestran una dispersión más amplia en torno a la media de 8.55, evidenciando una mayor diversidad en las opiniones respecto a ese aspecto particular de la aplicación analizada.

TABLA V: RESULTADOS DE USABILIDAD OBTENIDOS MEDIANTE LA HERRAMIENTA QUIS.

CAT1: OVERALL REACTION TO THE SOFTWARE		**[0-5]**	**6**	**7**	**8**	**9**	**Mean**	**Std. Dev**
P01	terrible - wonderful	-	-	2	6	12	8.50	0.69
P02	difficult-easy	-	-	1	1	18	8.85	0.49
P03	frustrating-satisfying	-	-	1	4	15	8.70	0.57
P04	inadequate power-adequate power	-	1	1	4	14	8.55	0.83
P05	dull-stimulating	-	1	2	2	15	8.55	0.89
P06	rigid-flexible	-	-	-	4	16	8.80	0.41
CAT2: SCREEN								
P07	Reading characters on the screen	-	-	-	2	18	8.90	0.31
P08	Highlighting simplifies task	-	-	-	6	14	8.70	0.47
P09	Organization of information	-	-	-	3	17	8.85	0.37
P10	Sequence of screens	-	-	-	2	18	8.90	0.31
CAT3: TERMINOLOGY AND SYSTEM INFORMATION								
P11	Use of terms throughout system	-	-	1	5	14	8.65	0.59
P12	Terminology related to task	-	-	4	6	10	8.30	0.80
P13	Position of messages on screen	-	-	1	7	12	8.55	0.60
P14	Prompts for input	-	1	1	3	15	8.60	0.82
P15	Computer informs about its progress	-	-	1	4	15	8.70	0.57
P16	Error messages	-	-	-	7	13	8.65	0.49
CAT4: LEARNING								

P17	Learning to operate the system	-	-	1	2	17	8.80	0.52
P18	Exploring new features by trial and error	-	-	-	2	18	8.90	0.31
P19	Remembering names and use of commands	-	-	1	4	15	8.70	0.57
P20	Performing tasks is straightforward	-	1	4	4	11	8.25	0.97
P21	Help messages on the screen	-	-	3	3	14	8.55	0.76
P22	Supplemental reference materials	-	-	2	5	13	8.55	0.69
CAT5: SYSTEM CAPABILITIES								
P23	system speed	-	-	-	1	19	8.95	0.22
P24	system reliability	-	-	-	3	17	8.85	0.37
P25	system tends to be	-	-	-	5	15	8.75	0.44
P26	Correcting your mistakes	-	-	1	3	16	8.75	0.55
P27	Designed for all levels of users	-	-	-	1	19	8.95	0.22

Nota: Elaboración propia

En relación a las distintas categorías analizadas, las puntuaciones promedio son notablemente elevadas en cada una de ellas. Este resultado sugiere que los usuarios experimentan un alto nivel de satisfacción con la interfaz de usuario en su conjunto. Las calificaciones se sitúan entre el 95.3% y el 98.3%, lo que evidencia una percepción favorable en aspectos como la usabilidad, el diseño, la funcionalidad y otros elementos evaluados a través de las diversas categorías del cuestionario QUIS (ver Figura 15).

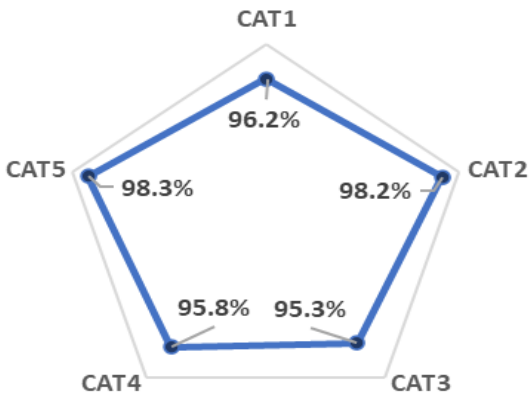


Fig. 16: Porcentaje de aceptación en la evaluación de usabilidad por categoría.

Así mismo, para cumplir con el cuarto objetivo específico, se han realizado pruebas de seguridad orientadas a evaluar la capacidad de resistencia del mecanismo de autenticación basado en puntos de referencia bidimensionales en imágenes digitales frente a ataques a simple vista y ataques con cámara. Ambos tipos de ataques son comunes en entornos donde un usuario malintencionado puede observar el proceso de autenticación o grabarlo con el fin de obtener acceso sin la autorización del usuario legítimo. Las pruebas se

llevaron a cabo en un entorno controlado y con la misma muestra inicial de 25 participantes divididos en cinco grupos etarios: niños, adolescentes, jóvenes, adultos y adultos mayores.

La evaluación se estructuró en dos fases: una fase de ataque a simple vista y una fase de ataque con cámara, cada una realizada con tres iteraciones por participante. El atacante intentaba replicar los patrones de autenticación observados para acceder a la cuenta del usuario, midiendo así la tasa de éxito de los ataques bajo condiciones reales.

En la fase de ataques a simple vista, un atacante malintencionado se ubicó cerca del participante durante el proceso de autenticación, intentando observar visualmente la selección de los puntos de referencia. Posteriormente, el atacante intentaba reproducir el patrón observado en la misma imagen para obtener acceso. Los resultados muestran que el ataque a simple vista tiene una tasa de éxito extremadamente baja, ver tabla 6. La naturaleza visualmente compleja del mecanismo, que se basa en la selección de puntos específicos dentro de una imagen, hace difícil para un atacante recordar y reproducir el patrón correctamente. A continuación, se presentan los datos por grupo etario.

TABLA VI: RESULTADOS DE PRUEBA – ATAQUE A SIMPLE VISTA

Grupo Etario	Intentos Totales	Éxito del ataque (%)	Fallo del Ataque (%)
Niños (6-12 años)	15	6.67%	93.33%
Adolescentes (13-18 años)	15	6.67%	93.33%
Jóvenes (19-30 años)	15	0.00%	100.00%
Adultos (31-59 años)	15	0.00%	100.00%
Adultos mayores (60+ años)	15	6.67%	93.33%

Nota: Elaboración propia

En promedio, la tasa de éxito de los ataques a simple vista fue del 4.00%, mientras que la tasa de fallos fue del 96.00%. Este resultado evidencia que el mecanismo de autenticación es altamente resistente a este tipo de ataques, especialmente en grupos de jóvenes y adultos, que no presentaron ningún éxito por parte del atacante.

En la fase de ataques con cámara, el atacante grabó el proceso de autenticación utilizando una cámara de alta resolución para capturar el momento exacto en el que el usuario seleccionaba los puntos de referencia en la imagen. Luego, el atacante intentaba reproducir el patrón observando el video. Los resultados de los atacantes con cámara mostraron una tasa de éxito aún más baja en comparación con los atacantes a simple vista, ver tabla 7. A pesar de la grabación detallada del proceso de autenticación, los atacantes encontraron difícil reproducir con precisión los puntos de referencia seleccionados, debido a la complejidad de los patrones gráficos y la precisión requerida. Los resultados se detallan a continuación.

TABLA VII: RESULTADOS DE PRUEBA – ATAQUE CON CÁMARA

Grupo Etario	Intentos Totales	Éxito del ataque (%)	Fallo del Ataque (%)
Niños (6-12 años)	15	6.67%	93.33%
Adolescentes (13-18 años)	15	0.00%	100.00%
Jóvenes (19-30 años)	15	0.00%	100.00%
Adultos (31-59 años)	15	0.00%	100.00%
Adultos mayores (60+ años)	15	0.00%	100.00%

Nota: Elaboración propia

El promedio de éxito en los ataques con cámara fue de solo un 1.33%, mientras que la tasa de fallos fue del 98.67%. Este resultado indica que el uso de cámaras, aunque proporciona información visual adicional, no es suficiente para comprometer el sistema de autenticación, debido a la dificultad de seleccionar los puntos correctos con la precisión necesaria.

3.2. Discusión

La selección de muestra para la evaluación del mecanismo de autenticación basado en patrón gráfico de contraseña involucró a 25 participantes, seleccionados por su accesibilidad y conveniencia. Se categorizó a los participantes según su grupo etario, y se obtuvieron datos demográficos detallados en la Tabla 1. Durante siete días, cada participante

probó la aplicación, configurando su perfil de autenticación y llevando a cabo autenticaciones diarias, registrando las dificultades encontradas tras periodos prolongados.

Los resultados mostraron que los tiempos de autenticación variaron según el grupo etario. Los niños mostraron un promedio de 34 segundos, mientras que los adolescentes promediaron 39 segundos. Los adultos presentaron tiempos promedio de 45.11 segundos y los adultos mayores 35.20 segundos. La dispersión de los datos indicó que, aunque los promedios eran similares para niños, adolescentes y adultos mayores, los jóvenes mostraron una mayor variabilidad en los tiempos de autenticación. Estos resultados resaltan la importancia de considerar la variabilidad en los tiempos de autenticación en diferentes grupos de edad.

En el trabajo de [6] evaluó el tiempo de autenticación con 30 usuarios obteniendo que un tiempo promedio para registro e inicio de sesión de 31.31 y 37.11 segundos respectivamente

mientras que en el trabajo de [6], se evaluó el tiempo de autenticación de una contraseña híbrida entre contraseña gráficas y contraseña textual, Se realizó el análisis con un total de 160 participantes y en un periodo de tiempo de dos semanas obteniendo resultados de entre los 20 y 40 segundos. De estos resultados se puede observar que en comparación con el tiempo de autenticación del sistema propuesto se obtiene entre 34 y 45 segundos en promedio. Si bien es cierto se muestra un ligero incremento en el tiempo de autenticación, se debe a que en la presente investigación se estableció grupos etarios considerando desde niños hasta adultos mayores.

En cuanto a la memorabilidad del método de autenticación, se evaluó la cantidad de bloqueos generados por grupo etario. Los niños mostraron la menor cantidad de bloqueos, seguidos por los adultos y los adultos mayores, mientras que adolescentes y jóvenes presentaron mayores incidencias de bloqueos. Estos hallazgos sugieren que la memorabilidad del método podría variar según la edad, con los niños y adultos mayores mostrando mayor facilidad para recordar los patrones.

En la investigación de [24], se obtuvo un tiempo medio de autenticación de 28 a 50

segundos, similar a los tiempos registrados en este estudio, lo que sugiere que, aunque existe una ligera variabilidad, el enfoque propuesto mantiene un rendimiento competitivo. Además, los resultados sobre la memorabilidad, donde los niños y adultos mayores mostraron menos bloqueos en comparación con adolescentes y jóvenes, reflejan una tendencia observada en la investigación de [25]., que también destacó la importancia del diseño centrado en el usuario para diferentes grupos etarios. Esto respalda la conclusión de que la usabilidad es crucial, ya que el uso del "Cuestionario para la satisfacción de la interfaz de usuario (QUIS)" arrojó resultados positivos, reforzando las afirmaciones de [26], quienes reportaron una precisión del 98% en sus sistemas. La combinación de estas métricas de tiempo, memorabilidad y satisfacción del usuario subraya que el sistema de autenticación propuesto no solo mejora la seguridad, sino que también ofrece una experiencia de usuario accesible y satisfactoria, lo cual es fundamental en el desarrollo de soluciones tecnológicas efectivas en el ámbito digital actual.

Para complementar la evaluación de usabilidad, se empleó el "Cuestionario para la satisfacción de la interfaz de usuario (QUIS)", obteniendo altas puntuaciones promedio en todas las categorías evaluadas. Las puntuaciones reflejan una percepción positiva en términos de usabilidad, diseño y funcionalidad de la interfaz de usuario. Estos resultados resaltan la satisfacción general de los usuarios con la aplicación evaluada.

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Durante el proceso de desarrollo de software, uno de los pasos clave es la identificación de los requisitos funcionales y no funcionales. En este contexto, se han establecido un total de seis requisitos, de los cuales tres son funcionales, enfocados en la gestión administrativa, el proceso de registro y la autenticación. Los otros tres requisitos son no funcionales y se relacionan con aspectos de seguridad, usabilidad y disponibilidad. Para representar estos requisitos, se elaboró un diagrama de casos de uso que modela el comportamiento de la

aplicación.

El desarrollo de la aplicación se llevó a cabo mediante la integración de diversas tecnologías que respaldan tanto el back-end como el front-end, en función de los casos de uso previamente establecidos. Durante la etapa de registro, el usuario ingresa datos personales y crea un patrón gráfico de contraseña, que luego se emplea en la fase de autenticación; en este caso, se ha aplicado la técnica de distancias euclidianas para calcular el margen de error. Todo este procedimiento se implementó en un servidor Linux bajo el dominio www.imagenlogin.com, lo que facilita la realización de pruebas para evaluar la usabilidad, la memorabilidad y la seguridad de la aplicación.

En relación con los resultados, se evaluaron diversos indicadores, incluyendo el tiempo de autenticación, que promedió entre 34 y 45 segundos. Asimismo, se consideró la memorabilidad, reflejada en una tasa de bloqueos del 25% sobre un total de 190 inicios de sesión efectuados en un periodo de siete días por 25 participantes, distribuidos en cinco grupos etarios. Para medir la usabilidad, se empleó un cuestionario estandarizado denominado QUIZ, el cual arrojó una puntuación superior al 95%, evidenciando una percepción favorable del aplicativo por parte de los usuarios.

Las pruebas de seguridad realizadas demuestran que el mecanismo de autenticación basado en puntos de referencia bidimensionales en imágenes digitales es altamente resistente frente a ataques a simple vista y con cámara. La tasa de éxito de los atacantes fue menor al 10%, lo que indica que el sistema ofrece una seguridad significativamente superior a los métodos convencionales de autenticación, como las contraseñas alfanuméricas. Estos resultados confirman que el uso de imágenes personalizadas y patrones gráficos complejos constituye una barrera efectiva contra la observación malintencionada, cumpliendo con los objetivos de mejorar la seguridad en aplicaciones web.

4.2. Recomendaciones

Basándonos en los hallazgos de la evaluación del mecanismo de autenticación y la experiencia del usuario, se ofrecen recomendaciones específicas para mejorar la usabilidad y la eficiencia de los métodos de autenticación en aplicaciones web, considerando las diferencias entre grupos etarios.

Primero, se sugiere la implementación de opciones de autenticación personalizadas según la edad del usuario. Esto implica adaptar la complejidad del método de autenticación para hacerlo más intuitivo y fácilmente recordable, especialmente para adolescentes y jóvenes, quienes demostraron mayores dificultades en la memorabilidad del patrón gráfico.

Otra recomendación es realizar pruebas continuas con usuarios de diferentes grupos etarios para evaluar la eficacia y la usabilidad del método de autenticación. Los comentarios y datos recopilados de estas pruebas deben utilizarse para ajustar y mejorar iterativamente el diseño del sistema de autenticación.

Adicionalmente, se propone llevar a cabo investigaciones adicionales para comprender más a fondo las preferencias y las capacidades de los diferentes grupos demográficos en relación con los métodos de autenticación. Este enfoque permitirá desarrollar soluciones más efectivas y adaptadas a las necesidades específicas de cada grupo.

Por último, se subraya la importancia de priorizar la seguridad de los métodos de autenticación sin comprometer su usabilidad. Buscar un equilibrio entre la facilidad de uso y la robustez del sistema de autenticación es crucial para garantizar una experiencia segura y satisfactoria para todos los usuarios. Estas recomendaciones pretenden mejorar la experiencia del usuario, promoviendo la usabilidad y la eficacia de los mecanismos de autenticación en aplicaciones móviles, reconociendo las diferencias en las habilidades y preferencias de distintos grupos etarios.

REFERENCIAS

[1] X. Wang, Z. Yan, R. Zhang, and P. Zhang, “Attacks and defenses in user authentication systems: A survey,” *Journal of Network and Computer Applications*, vol. 188, p. 103080, Aug. 2021, doi: 10.1016/J.JNCA.2021.103080.

[2] F. L. Becerra-Suarez, D. Villanueva-Ruiz, V. A. Tuesta-Monteza, and H. I. Mejia-Cabrera, “Usability Evaluation of Mobile Application Software Mockups,” *Lecture Notes in Networks and Systems*, vol. 506 LNNS, pp. 321–331, 2022, doi: 10.1007/978-3-031-10461-9_22/COVER.

[3] N. Çevik, S. Akleylek, and K. Y. Koç, “Keystroke Dynamics Based Authentication System,” *Proceedings - 6th International Conference on Computer Science and Engineering, UBMK 2021*, pp. 644–649, 2021, doi: 10.1109/UBMK52708.2021.9559008.

[4] A. F. Al-Aboosi, M. Broner, and F. Y. Al-Aboosi, “Bingo: A Semi-Centralized Password Storage System,” *Journal of Cybersecurity and Privacy 2022, Vol. 2, Pages 444-465*, vol. 2, no. 3, pp. 444–465, Jun. 2022, doi: 10.3390/JCP2030023.

[5] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, “PassPoints: Design and longitudinal evaluation of a graphical password system,” *Int J Hum Comput Stud*, vol. 63, no. 1–2, pp. 102–127, Jul. 2005, doi: 10.1016/J.IJHCS.2005.04.010.

[6] S. Z. Nizamani, S. R. Hassan, R. A. Shaikh, E. A. Abozinadah, and R. Mehmood, “A novel hybrid textual-graphical authentication scheme with better security, memorability, and usability,” *IEEE Access*, vol. 9, pp. 51294–51312, 2021, doi: 10.1109/ACCESS.2021.3069164.

[7] K. Hamdi and A. Al-Shqeerat, “An Enhanced Graphical Authentication Scheme Using Multiple-Image Steganography”, doi: 10.32604/csse.2023.028975.

[8] H. Assal, A. Imran, and S. Chiasson, “An exploration of graphical password authentication for children,” *Int J Child Comput Interact*, vol. 18, pp. 37–46, Nov. 2018, doi: 10.1016/J.IJCCI.2018.06.003.

[9] H. Wang, J. Xu, M. Ma, and H. Zhang, “A New Type of Graphical Passwords Based on Odd-Elegant Labelled Graphs,” *Security and Communication Networks*, vol. 2018, 2018, doi: 10.1155/2018/9482345.

[10] N. Carter, C. Li, Q. Li, J. A. Stevens, E. Novak, and Z. Qin, “Graphical passwords for older computer users,” *International Journal of Security and Networks*, vol. 13, no. 4, pp. 211–227, 2018, doi: 10.1504/IJSN.2018.095170.

[11] H.-M. Sun, S.-T. Chen, J.-H. Yeh, and C.-Y. Cheng, “A Shoulder Surfing Resistant Graphical Authentication System,” *IEEE Trans Dependable Secure Comput*, vol. 15, no. 2, pp. 180–193, 2018, doi: 10.1109/TDSC.2016.2539942.

[12] P. Pulicherla and S. R. Baddam, “Image map: Alternative for password based authentication,” *International Journal of Recent Technology and Engineering*, vol. 8, no. 3, pp. 2055–2057, 2019, doi: 10.35940/ijrte.C4540.098319.

[13] J. E. Otalora-Luna, M. Callejas-Cuervo, and A. C. Alarcon-Aldana, *Metamodelo de medicion de esfuerzo en proyectos de desarrollo de software*. Editorial UPTC, 2018. [Online]. Available: https://elibro.net/es/lc/bibsipan/titulos/132832

[14] Ó. S. Ramón, J. S. Cuadrado, J. G. Molina, and J. Vanderdonckt, “A layout inference algorithm for Graphical User Interfaces,” *Inf Softw Technol*, vol. 70, pp. 155–175, Feb. 2016, doi: 10.1016/J.INFSOF.2015.10.005.

[15] F. A. Masoud, D. H. Halabi, and D. H. Halabi, “ASP.NET and JSP frameworks in model view controller implementation,” *Proceedings - 2006 International Conference on Information and Communication Technologies: From Theory to Applications, ICTTA 2006*, vol. 2, pp. 3593–3598, 2006, doi: 10.1109/ICTTA.2006.1684998.

[16] M. Jailia, A. Kumar, M. Agarwal, and I. Sinha, “Behavior of MVC (Model View Controller) based Web Application developed in PHP and.NET framework,” *Proceedings of 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG 2016*, Apr. 2017, doi: 10.1109/ICTBIG.2016.7892651.

[17] M. Aniche, G. Bavota, C. Treude, A. Van Deursen, and M. A. Gerosa, “A validated set of smells in model-view-controller architectures,” *Proceedings - 2016 IEEE International Conference on Software Maintenance and Evolution, ICSME 2016*, pp. 233–243, Jan. 2017, doi: 10.1109/ICSME.2016.12.

[18] X. Dazhan, W. Xiaoyu, and S. Guoquan, “Image Memorability Prediction Based on Machine

Learning," *2020 IEEE 3rd International Conference on Computer and Communication Engineering Technology, CCET 2020*, pp. 91–94, Aug. 2020, doi: 10.1109/CCET50901.2020.9213119.

[19] Z. Parish, A. Salehi-Abari, and J. Thorpe, "A study on priming methods for graphical passwords," *Journal of Information Security and Applications*, vol. 62, p. 102913, Nov. 2021, doi: 10.1016/J.JISA.2021.102913.

[20] "Usability testing for early-stage software prototypes | Opensource.com." Accessed: Dec. 09, 2023. [Online]. Available: https://opensource.com/article/17/9/paper-based-usability-testing

[21] J. Sauro and J. R. Lewis, "Standardized usability questionnaires," *Quantifying the User Experience*, pp. 185–248, Jan. 2016, doi: 10.1016/B978-0-12-802308-2.00008-4.

[22] J. P. Chin, V. A. Diehl, and K. L. Norman, "Development of an instrument measuring user satisfaction of the human-computer interface," *Conference on Human Factors in Computing Systems - Proceedings*, vol. Part F130202, pp. 213–218, May 1988, doi: 10.1145/57167.57203.

[23] S. Hasanpour-Heidari *et al.*, "Development of an online cancer data collection and processing tool for population-based cancer registries in a low-resource setting: The CanDCap experience from Golestan, Iran," *Int J Med Inform*, vol. 166, p. 104846, Oct. 2022, doi: 10.1016/J.IJMEDINF.2022.104846.

[24] W. Wen Chuan y L. Zi Wei , SVD-Based Self-Embedding Image Authentication Scheme Using Quick Response Code Features, Taiwan: VISUAL Comunicación y IMAGE Representation, 2020.

[25] Kai Gao, HWEI HORNG y C. CHEN CHANG, A Novel (2, 3) Reversible Secret Image Sharing Based on Fractal Matrix, Taiwan: IEEAccess, 2020.

[26] Weitao Song, Qijia Cheng, Yue Liu, Yuanjin Zheng, Zhiping Lin y Yongtian Wang, Three-dimensional image authentication using binarized images in double random phase integral imaging, Beijing, China: CHINESE OPTICS LETTERS, 2019.

ANEXOS:

Anexo 1: Acta de revisión de similitud de la investigación

Universidad Señor de Sipán

ANEXO 01: ACTA DE REVISIÓN DE SIMILITUD DE LA INVESTIGACIÓN

Yo **Victor Alexis Tuesta Monteza** docente del curso de **Investigación II** del Programa de Estudios de **Ingeniería de Sistemas** y revisor de la investigación del (los) estudiante(s), **Lucila del Carmen Cruz LLaguento** titulada:

MECANISMO DE AUTENTICACIÓN BASADO EN PUNTOS DE REFERENCIA BIDIMENSIONALES EN IMÁGENES DIGITALES PARA MEJORAR LA SEGURIDAD DE APLICACIONES WEB

Se deja constancia que la investigación antes indicada tiene un índice de similitud del **12%**, verificable en el reporte final del análisis de originalidad mediante el software de similitud TURNITIN. Por lo que se concluye que cada una de las coincidencias detectadas no constituyen plagio y cumple con lo establecido en la Directiva sobre índice de similitud de los productos académicos y de investigación en la Universidad Señor de Sipán S.A.C., aprobada mediante Resolución de Directorio N° 145-2022/PD-USS.

En virtud de lo antes mencionado, firma:

Victor Alexis Tuesta Monteza	DNI: 42722929	

Pimentel, 26 de 12 de 2023.

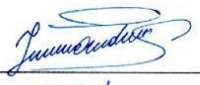
Anexo 2: Acta de aprobación del asesor

Universidad Señor de Sipán

ACTA DE APROBACIÓN DEL ASESOR

Yo **Juan Carlos Arcila Diaz**. quien suscribe como asesor designado mediante Resolución de Facultad N° **1509 - 2023**, del proyecto de investigación titulado **mecanismo de autenticación basado en puntos de referencia bidimensionales en imágenes digitales para mejorar la seguridad de aplicaciones web**, desarrollado por el(los) estudiante(s): **Lucila del Carmen Cruz LLaguento**, del programa de estudios de **Ingeniería de sistemas**, acredito haber revisado, realizado observaciones y recomendaciones pertinentes, encontrándose expedito para su revisión por parte del docente del curso.

En virtud de lo antes mencionado, firman:

Arcila Diaz Juan Carlos **(Asesor)**	DNI: 47715777	
Cruz LLaguento Lucila del Carmen **(Autor)**	DNI: 76875154	

Pimentel, 19 de 12 de 2023

Anexo 3: Carta o correo de recepción del manuscrito remitido por la revista

USS Transforma tu mundo

LUCILA DEL CARMEN CRUZ LLAGUENTO <cllaguentolucil@uss.edu.pe>

[IyU] Envio recibido por el sistema (38319)
1 mensaje

Ing. Rafael Andrés González Rivera, PhD <revistas.javeriana22@gmail.com> 27 de diciembre de 2023, 23:37
Para: Lucila Cruz LLaguento <cllaguentolucil@uss.edu.pe>

Apreciado Lucila Cruz LLaguento:

En la revista Ingenieria y Universidad hemos recibido su aplicación.
Favor remitir el número de su artículo en consultas y respuestas:38319

Gracias al sistema de gestión de revistas online, podrá seguir su progreso a través de esta plataforma.

URL del manuscrito: https://revistas.javeriana.edu.co/index.php/iyu/authorDashboard/submission/38319
Nombre de usuaria/o: cllaguentolucil

Agradecemos su colaboración, con gusto atenderemos sus comentarios y sugerencias acerca del funcionamiento de esta plataforma para la gestión de la revista.

Cordialmente,

Diego Alejandro Patiño Guevara, M.Sc., Ph.D.
Editor in Chief
Ingeniería y Universidad: *Engineering for development*
School of Engineering
Pontificia Universidad Javeriana
Bogotá, Colombia
reving@javeriana.edu.co
Facebook - Twitter - LinkedIn - Academia.edu - Mendeley - Google Scholar

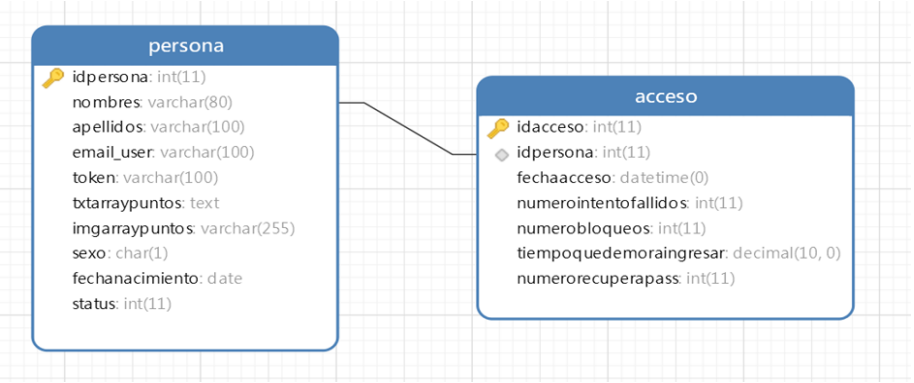
Anexo 4: Bitácora de resultados de cantidad de bloqueos.

Título: Acceso al sistema	
Fecha: 26/11/2023 al 02/12/2023	
Escenario	El aplicativo fue alojado en un hosting compartido en un entorno Linux, vinculado al dominio www.imagenlogin.com, con un espacio en disco de 1GB, versión de apache 2.4.62 y versión de MYSQL 10.6.20-MariaDB-cll-lve
Prerrequisitos	- El usuario primeramente debe tener el link para acceder al sistema de autenticación. - El usuario debe crear su cuenta que le permita autenticarse.
Insumos	- Lista de Participantes

TIPO	EDAD	NOMBRE	CORREO	SEXO
NIÑOS	6-12 AÑOS	Runny Andoni Tapia Palacios	runnyandonitapia@gmail.com	M
		Luciana Quispe Exebio	yvictoriae15@gmail.com	F
		Cristhian Fabian Becerra Quiroz	cfabianbecerra1@gmail.com	M
		Shantall Torres Plasencia	shantalltp@gmail.com	F
		Fabio Aurich Koo	kellykoo140313@gmail.com	M
ADOLECENTES	13-18 AÑOS	Herlinda Cruz	herlindacruzllaguento@gmail.com	F
		Anyeline Chilon Mundaca	anyelinemundaca@gmail.com	F
		Analy Uceda Liñan	analyucedalinan@gmail.com	F
		Daniel Huaman Perez	daniel.13@gmail.com	M
		Junior Diaz Tapia	tapiaj@gmail.com	M
JOVENES	19 - 30 AÑOS	Joel Alexander Guevara Cueva	gcuevajoel310195@gmail.com	M
		Lile Díaz Tapia	dtapialile@crece.uss.edu.pe	F
		Bersy Díaz Tapia	bersydt02@gmail.com	F
		Yhilver Isiadro Cruz Llaguento	yhilvercruzllaguento31@gmail.com	M
		Faby Cruz Llaguento	fabycruzyaguento@gmail.com	F
ADULTOS	31-59 AÑOS	Abel Augusto Guevara Cueva	abel.20.80@gmail.com	M
		Antonio Fuentes Alcantara	fuentes.antonioj@gmail.com	M
		Rosa Fuentes Alcantara	rozyfuentes10@gmail.com	F
		Susana Fuentes Alcantara	susi_fuentes@hotmail.com	F
		Victor Ramírez Lora	viarlo19@hotmail.com	M
ADULTOS MAYOR	MAYORES DE 60 AÑOS	Marco Antonio Fuentes Espinoza	m.antonio.fuentes.espinoza@gmail.com	M
		Carmen Rosa Alcantara Flores	rosa.alcantara.fores@gmail.com	F
		Maria Manuel Farro Sampén	dfarrojavierman@uss.edu.pe	F
		Luz Cueva Choquehuanca	luzamer_22@hotmail.com	F
		Manuel Ronaldo Delgado Samamé	delgadojavier238@gmail.com	M

<table>
<tr><td></td><td>

- Estructura de la tabla acceso en la base de datos



</td></tr>
<tr><td>Indicadores aceptación</td><td>

- **Tasa de bloqueos:** se evaluó la cantidad de bloqueos generados por grupo etario, cuando el usuario realizaba tres intentos fallidos de autenticación se realiza un registro en la base de datos y el usuario puede volver a intentar autenticarse después de 2 segundos.
- **Tiempo de Autenticación:** se evaluó el tiempo que demora el usuario en autenticarse desde ingresa su correo hasta autenticarse con éxito.

</td></tr>
<tr><td>Resultados</td><td>

- **Bitácora de bloqueos**

CANTIDAD DE BLOQUEOS					
#	NIÑOS	ADOLECENTES	JOVENES	ADULTOS	ADULTOS MAYORES
26/11/2023	0	1	0	0	0
26/11/2023	0	0	0	1	0
26/11/2023	0	2	0	0	0

</td></tr>
</table>

		26/11/2023	0	0	1	0	0	
		26/11/2023	0	1	1	0	3	
		27/11/2023	0	0	1	0	3	
		27/11/2023	0	1	0	1	0	
		27/11/2023	0	0	1	0	0	
		27/11/2023	0	0	0	0	0	
		27/11/2023	2	0	0	0	0	
		28/11/2023	0	0	0	0	0	
		28/11/2023	0	0	1	0	1	
		28/11/2023	0	0	0	0	1	
		28/11/2023	0	1	4	1	0	
		28/11/2023	0	4	1	0	0	
		29/11/2023	0	1	0	0	0	
		29/11/2023	0	0	0	0	0	
		29/11/2023	0	0	0	0	0	
		29/11/2023	0	0	0	0	0	
		29/11/2023	0	0	0	0	0	
		30/11/2023	0	0	0	0	0	
		30/11/2023	0	0	0	0	0	
		30/11/2023	0	1	2	0	0	
		30/11/2023	0	0	0	0	0	
		30/11/2023	0	1	0	0	0	
		1/12/2023	0	1	0	0	0	
		1/12/2023	0	0	0	0	0	
		1/12/2023	0	0	0	0	0	
		1/12/2023	0	0	0	0	0	
		1/12/2023	0	0	3	0	0	
		2/12/2023	0	0	0	0	0	
		2/12/2023	0	0	0	0	0	
		2/12/2023	0	0	0	0	0	

2/12/2023	0	0	0	0	0
2/12/2023	0	0	1	1	0

- **Bitácora de tiempo de autenticación**

TIEMPO DE AUTENTICACIÓN EN SEGUNDOS					
FECHA	**NIÑOS**	**ADOLECENTES**	**JOVENES**	**ADULTOS**	**ADULTOS MAYORES**
26/11/2023	69	48	52	34	25
26/11/2023	22	26	35	35	36
26/11/2023	15	35	35	26	25
26/11/2023	45	31	29	30	55
26/11/2023	20	50	30	29	52
27/11/2023	20	26	39	30	28
27/11/2023	46	16	77	61	35
27/11/2023	41	35	25	60	35
27/11/2023	20	35	43	38	36
27/11/2023	17	21	20	25	21
28/11/2023	35	72	88	16	84
28/11/2023	35	17	16	35	60
28/11/2023	76	25	16	21	45
28/11/2023	57	35	36	21	16
28/11/2023	14	52	51	32	14
29/11/2023	26	60	12	27	25
29/11/2023	39	55	51	28	74
29/11/2023	16	45	25	24	26
29/11/2023	48	37	11	24	18
29/11/2023	14	66	93	29	16
30/11/2023	33	25	15	20	22
30/11/2023	37	55	21	20	60

		30/11/2023	12	78	28	27	37	
		30/11/2023	33	55	48	54	22	
		30/11/2023	18	37	25	30	27	
		1/12/2023	21	16	29	63	18	
		1/12/2023	57	35	33	44	28	
		1/12/2023	51	36	16	30	105	
		1/12/2023	82	35	63	37	22	
		1/12/2023	12	47	22	14	10	
		2/12/2023	23	43	17	71	55	
		2/12/2023	36	37	31	96	19	
		2/12/2023	25	25	20	199	29	
		2/12/2023	47	25	38	23	28	
		2/12/2023	34	26	62	226	24	

Anexo 5: Ficha de prueba de facilidad de uso

Título: Prueba de facilidad de uso	
Fecha: 4/12/2023	
Escenario	El cuestionario tiene como propósito recoger opiniones sobre la experiencia de uso del sistema, después de haber interactuado con él durante los últimos 7 días, para evaluar experiencia de usabilidad, rendimiento del sistema, y percepción de utilidad.
Prerrequisitos	Haber participado de los 7 días pruebas de acceso al sistema.
Insumos	- Tener acceso al cuestionario QUIZ
Indicadores	- El cuestionario QUIZ costa de 27 ítems segmentado en 5 categorías OVERALL REACTION TO THE SOFTWARE, SCREEN, TERMINOLOGY AND SYSTEM INFORMATION y LEARNING, SYSTEM CAPABILITIES. - El usuario puede evaluar cada ítem según su percepción de satisfacción en una escala que va de 0 (lo más negativo) a 9 (lo más positivo)

Resultados

	OVERALL REACTION TO THE SOFTWARE	US1	US2	US3	US4	US5	US6	US7	US8	US9	US10	US11	US12	US13	US14	US15	US16	US17	US18	US19	US20	US21	US22	US23	US24
P01	terrible - wonderful	9	9	7	7	9	9	9	8	9	8	9	9	9	8	8	9	8	9	8	9	8	9	9	8
P02	difficult-easy	9	9	9	9	7	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9
P03	frustrating-satisfying	9	9	9	8	9	8	9	9	9	9	9	8	9	9	9	8	9	9	9	9	9	9	9	9
P04	inadequate power-adequate power	9	8	9	7	9	9	8	9	9	9	8	6	9	9	9	8	9	9	9	8	9	9	9	8
P05	dull-stimulating	9	8	7	6	9	9	9	9	9	9	9	9	9	9	9	9	9	8	7	7	9	8	9	9
P06	rigid-flexible	8	9	8	9	9	9	9	9	9	9	9	9	8	9	9	9	9	9	8	8	7	7	8	9
	SCREEN																								
P07	Reading characters on the screen	8	9	9	9	8	9	9	9	9	9	9	9	9	9	9	9	9	9	9	7	9	9	9	8
P08	Highlighting simplifies task	9	9	9	9	9	9	9	9	9	9	8	8	9	9	8	9	9	8	8	8	9	9	9	9
P09	Organization of information	9	9	9	9	9	9	8	9	9	9	8	9	9	9	9	9	9	9	9	9	8	9	7	9
P10	Sequence of screens	9	9	8	9	9	9	9	9	9	9	9	9	9	9	9	9	9	8	9	9	9	9	9	9
	TERMINOLOGY AND SYSTEM INFORMATION																								
P11	Use of terms throughout system	9	9	8	8	7	9	9	9	9	8	9	9	9	8	9	9	9	8	9	9	9	8	9	8
P12	Terminology related to task	9	9	9	9	8	8	8	7	7	8	9	7	9	8	8	9	9	9	9	9	8	7	8	9
P13	Position of messages on screen	9	8	9	8	9	9	9	8	8	9	9	9	8	9	8	9	9	8	9	9	9	9	9	8
P14	Prompts for input	9	9	9	7	9	9	8	8	9	9	9	6	8	9	9	9	9	9	9	8	9	9	8	9
P15	Computer informs about its progress	9	9	8	8	9	8	9	9	9	8	9	9	9	9	9	9	9	7	9	8	9	9	9	9
P16	Error messages	8	8	8	9	9	9	9	9	9	9	8	8	9	9	9	9	9	9	8	8	9	8	9	9
	LEARNING																								
P17	Learning to operate the system	9	9	9	9	9	9	9	9	9	9	9	9	9	9	8	9	7	9	9	9	9	9	9	8
P18	Exploring new features by trial and error	9	9	9	9	9	9	8	9	9	9	9	9	9	9	8	9	9	9	9	9	8	9	9	9
P19	Remembering names and use of commands	8	9	9	8	9	9	9	8	7	9	8	9	9	9	9	9	9	9	9	8	9	9	9	8
P20	Performing tasks is straightforward	8	8	9	7	9	7	9	9	6	9	7	9	9	8	8	7	9	9	9	8	9	8	9	9
P21	Help messages on the screen	9	9	9	7	9	9	9	9	8	9	9	9	9	8	7	8	9	9	9	9	8	7	9	9
P22	Supplemental reference materials	9	7	9	9	9	9	8	9	9	9	8	9	9	8	9	9	8	9	8	9	9	9	8	7
	SYSTEM CAPABILITIES																								
P23	system speed	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9
P24	system reliability	9	9	8	9	8	9	9	9	9	9	9	9	8	9	9	9	9	9	9	9	8	8	9	7
P25	system tends to be	8	9	9	9	9	9	9	9	9	9	9	9	9	9	8	8	9	9	8	9	9	9	9	8
P26	Correcting your mistakes	8	9	9	9	7	9	9	9	9	8	9	9	9	9	9	9	9	9	8	9	9	9	8	9
P27	Designed for all levels of users	9	9	9	9	9	9	8	9	9	9	9	9	9	9	9	9	9	9	9	8	8	7	9	9

Anexo 6: Matriz de consistencia

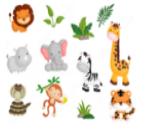
MATRÍZ DE CONSISTENCIA LÓGICA DE TRABAJO DE INVESTIGACIÓN

Enfoque metodológico

Titulo	Mecanismo de autenticación basado en puntos de referencia bidimensional en imágenes digitales para mejorar la seguridad de aplicaciones web				
Problema	**Hipótesis**	**Objetivo General**	**Objetivo Especifico**	**Tipo de Investigación**	**Diseño de Investigación**
¿Cómo se puede mejorar la seguridad en las aplicaciones web utilizando un mecanismo de autenticación basado en puntos de referencia bidimensional en imágenes digitales en comparación con otros métodos de autenticación existentes?	El uso de un mecanismo de autenticación basado en puntos bidimensionales en imágenes digitales mejorará significativamente la seguridad en las aplicaciones web en comparación con otros métodos de autenticación existentes	Desarrollar un mecanismo de autenticación basado en puntos de referencia bidimensional en imagenes digitales para mejorar la seguridad en aplicaciones web	Definir los requerimientos funciones y no funcionales del sistema de autenticación basado en puntos de referencia bidimensional en imagenes digitales. Implementar un prototipo funcional del mecanismo de autenticación basado en puntos de referencia bidimensional en imagenes digitales en una aplicación web. Realizar pruebas de usabilidad y la capacidad de ser recordada para evaluar la facilidad de uso del mecanismo de autenticación basado en puntos de referencia bidimensional en imagenes digitales en comparación con otros métodos de autenticación existentes. Realizar pruebas de seguridad para evaluar la resistencia del mecanismo de autenticación basado en puntos de referencia bidimesionales en imagenes digitales para los ataques de surf del hombro (ataques a simple vista y ataques con cámara)	Tecnologica aplicada	cuasi-experimental

Metodología

Administración de Imágenes



El usuario tendrá la posibilidad de subir o seleccionar una imagen

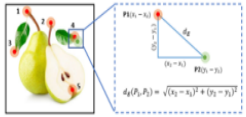
Registro de datos

Se guarda los datos en la base de datos

Patrón gráfico de contraseña

El usuario selecciona los puntos de referencia que serán guardados en la base de datos considerando el orden de selección

Validación de datos



Distancia euclideana
Ecu. Cuadráticas diafontinas
Cont. Árbol topográfico.

Para acceder se considera un marguen de error de los puntos seleccionador

Anexo 7: Operacionalización de las variables

Variable de estudio	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Ítems	Instrumento	Valores finales	Tipo de variable	Escala de medición
Mecanismo de autenticación grafica con puntos de referencia.	Un mecanismo de autenticación es un proceso utilizado para verificar la identidad de un usuario o entidad que intenta acceder a un sistema o servicio.	Para medir el tiempo de autenticación consideraremos un registro desde que el usuario intenta iniciar hasta que logra ingresar a la aplicación. Se llevará un control si el usuario intenta ingresar más de tres veces colocando la clave incorrecta se desactivará la web por unos momentos. Los usuarios responderán el cuestionario que luego que analizara.	No aplica	Tiempo de autenticación = TF-TI	No aplica	observación bitácora de resultados	Segundos	Cuantitativas Numérica	Razón
				Tasa de bloqueos de cuentas	No aplica	observación bitácora de resultados	Numero de cuentas		
				Facilidad de uso	corresponde a 27 enunciados del cuestionario QUIZ para evaluar la facilidad de uso	Cuestionario	Porcentaje		

Seguridad de aplicaciones web.	la seguridad en aplicaciones web un tema muy importante debido a la creciente dependencia de aplicaciones web para realizar transacciones, compartir información y almacenar datos confidenciales.	Se simularán una cierta cantidad de ataques de hombro derecho donde se busca obtener una tasa de ataques que tuvieron éxito.	No aplica	capacidad de resistencia a ataques de hombro derecho	No aplica	Observación bitácora de resultados	Porcentaje		