



FACULTAD DE CIENCIAS EMPRESARIALES
CARRERA PROFESIONAL DE INGENIERÍA DE
SISTEMAS EMPRESARIALES

“LA FIRMA ELECTRÓNICA BASADO EN RECONOCIMIENTO
FACIAL Y EL RIESGO DE SUPLANTACIÓN DE IDENTIDAD EN EL
COLEGIO DE INGENIEROS DEL PERÚ, CONSEJO
DEPARTAMENTAL DE LIMA”

Tesis para optar el título profesional de:
Ingeniero de Sistemas Empresariales

Presentado por:

Raul Alejandro Cervantes Alejos (0000-0003-1376-2568)

Asesor:

Jose Luis Albites Sanabria (0000-0001-7688-6221)

Lima - Perú

2021

ACTA DE SUSTENTACIÓN DE TESIS

Lima, 4 de junio de 2021

Los integrantes del Jurado de tesis:

Presidente	Mg. Carlos Federico Díaz Sánchez.
Miembro 1	Mg. Luis Enrique Acosta Medina
Miembro 2	Dra. Regina de la Caridad Agramonte Rosell

Se reúnen para evaluar la tesis titulada:

"LA FIRMA ELECTRÓNICA BASADO EN RECONOCIMIENTO FACIAL Y EL RIESGO DE SUPLANTACIÓN DE IDENTIDAD EN EL COLEGIO DE INGENIEROS DEL PERÚ, CONSEJO DEPARTAMENTAL DE LIMA"

Presentado por el(la) bachiller.
CERVANTES ALEJOS RAUL ALEJANDRO

Para optar el Título Profesional de
Ingeniero de Sistemas Empresariales

Asesorado(a) por:
Jose Luis Albites Sanabria

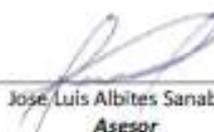
Luego de haber evaluado el informe final de tesis y evaluado el desempeño de(l) (los) estudiantes de la carrera de **Ingeniería de Sistemas Empresariales** en la sustentación, concluyen de manera unánime () por mayoría simple () calificar a:

Tesista:	CERVANTES ALEJOS RAUL ALEJANDRO		
Nota (en letras):	16		
Aprobado (<input type="checkbox"/>)	Aprobado - Muy buena (X)	Aprobado - Sobresaliente (<input type="checkbox"/>)	Desaprobado (<input type="checkbox"/>)

Los miembros del jurado firman en señal de conformidad.



Mg. Carlos Federico Díaz Sánchez
Presidente del Jurado



Jose Luis Albites Sanabria
Asesor



Mg. Luis Enrique Acosta Medina
Miembro 1



Dra. Regina de la Caridad Agramonte
Rosell
Miembro 2

Dedicatoria

Dedico este logro primeramente a nuestro Dios padre, que me da la fuerza y sabiduría en los momentos más difíciles, por darme su luz y entendimiento para la culminación de esta meta tan anhelada.

A mi amado padre que desde el cielo me ilumina día a día.

A mi amada madre por inculcarme buenos valores, constante perseverancia y excelentes consejos.

A mis hijos: Alejandra y Fabrizio, quienes son mi mayor inspiración en seguir adelante y cumplir mis objetivos profesionales y personales.

Agradecimiento

Un agradecimiento profundo hasta el cielo para mi asesor el Ing. Carlos Peralta Delgado por su experiencia, colaboración y disposición para realizar esta investigación. A los asesores y docentes que me apoyaron en este proyecto; y a mi familia y amigos, por su comprensión, apoyo y estímulo constante.

LA FIRMA ELECTRÓNICA BASADO EN RECONOCIMIENTO FACIAL Y EL RIESGO DE SUPLANTACIÓN DE IDENTIDAD EN EL COLEGIO DE INGENIEROS DEL PERÚ, CONSEJO DEPARTAMENTAL DE LIMA

Raúl Alejandro Cervantes Alejos ¹, José Luis Albites Sanabria ²

Resumen

La presente investigación tiene como objetivo determinar la relación entre la firma electrónica basado en reconocimiento facial y el riesgo de suplantación de identidad en el centro de peritaje del Colegio de Ingenieros del Perú, Club departa-mental de Lima. Se busca que el perito firme sus evidencias a través de la firma electrónica con validación facial. La tecnología facial se inicia con la detección facial, preprocesado de la imagen, extracción de los patrones faciales y verificación facial. Con la captura facial, se valida la identidad del Perito a través de una consulta con la base de datos de RENIEC.

El diseño de la investigación es experimental de tipo correlacional. La población fue de 475 peritos, tomando como muestra 60 peritos del Centro de Peritaje. La metodología empleada en el desarrollo del sistema informático fue Scrum y RUP (Rational Unified Process) mediante la herramienta StarUML para el análisis funcional, el sistema fue desarrollado con lenguaje de programación Java Web, framework Angular 9, con gestor de base de datos MYSQL. Los resultados mostraron que, en ca-da hipótesis planteada, existía una correlación directa entre las variables principales. Se concluye que los peritos están dispuestos a

¹ Ingeniería de Sistemas Empresariales, Facultad de Ciencias Empresariales, Universidad Científica del Sur. Lima, Perú. Email: 100085308@cientifica.edu.pe

² Magister en Ingeniería Biomédica de la Universidad de Brown. (Providence, RI, USA). Email: jalbites@cientifica.edu.pe

usar la firma electrónica como reemplazo a la firma manuscrita, reduciendo el riesgo de suplantación de identidad. Por lo cual, la firma electrónica favorece al perito en no tener que firmar volúmenes de hojas y que su identidad se encuentre validada en el informe pericial.

Palabras clave: Reconocimiento facial, Firma electrónica, Biometría facial.

Abstract

The objective of this research is to determine the relationship between the electronic signature based on facial recognition and the risk of identity theft in the expertise center of the College of Engineers of Peru, Departamental Club of Lima. It is intended that the expert sign their evidences through the electronic signature with facial validation. Facial technology starts with face detection, image pre-processing, extraction of facial patterns and facial verification. With the facial capture, the identity of the Expert is validated through a query with the RENIEC database.

The research design is experimental of the correlational type. The population was 475 experts, taking as a sample 60 experts from the Expertise Center. The methodology used in the development of the computer system was Scrum and RUP (Rational Unified Process) using the StarUML tool for functional analysis, the system was developed with the Java Web programming language, Angular 9 framework, with MYSQL database manager. The results showed that, in each hypothesis, there was a direct correlation between the main variables. It is concluded that the experts are willing to use the electronic signature as a replacement for the handwritten signature, reducing the risk of identity theft. Therefore, the electronic signature favors the expert in not having to sign volumes of sheets and that his identity is validated in the expert report.

Keywords: facial recognition, electronic signature, facial biometry.

1. Introducción

En la actualidad, la firma electrónica para firma de documentos, viene tomando más importancia. Sobre todo, si la firma es acompañada de la tecnología de reconocimiento facial para la validación de identidad del perito. Es cierto que la pandemia, la cual venimos atravesando, aceleró el uso de nuevas herramientas de firma remota. Sin embargo, en nuestra capital la masificación en el uso de esta tecnología aun trae muchas inseguridades, producto del alto índice de suplantación de identidad a través de la falsificación de documentos de identidad o reemplazo de la identidad a través de un medio digital.

El presente documento de investigación, tiene como objetivo general: Determinar la relación entre la firma electrónica basado en reconocimiento facial y el riesgo de suplantación de identidad en el CIP Lima. Conocer el funcionamiento de la herramienta de firma electrónica, el uso de la biometría facial con validación de identidad, el perito quien usa la herramienta, brindando seguridad y confidencialidad para agilizar la firma de documentos, informes, pericias, evitando la firma y el sellado innecesario de las hojas, ahorrando tiempo y costos administrativos en traslados para la entrega de documentos.

Esta investigación busca su difusión no solo a nivel de firma de documentos o informes de peritos, sino el de aplicarlo a otras actividades que requieran una firma remota, evitando el contacto físico y el cuidado del medio ambiente a través del ahorro en el consumo de papel.

1.1. Descripción de la Realidad problemática

El mundo viene sufriendo las consecuencias de una pandemia, generando un cambio en nuestra vida diaria, obligando a que el estado decrete un estado de emergencia para la detención de este virus. y esto no continúe con el aumento

de más pérdidas humanas, reduciendo el ritmo de todas las actividades. Obligándonos a un confinamiento social y a un trabajo remoto. Por lo cual, la tecnología debe ser aprovechada para la reactivación de las actividades.

Es por eso, que aun continuamos usando la firma manuscrita para suscribir contratos u otro tipo de documentos; y como consecuencia, generar derechos y obligaciones. Es así, que en tiempos de Covid-19, ya no estamos en la posibilidad de firmar documentos de manera presencial, surgiendo una necesidad inevitable de sustituir la firma manuscrita por otros mecanismos digitales como la firma electrónica con autenticación facial, para poder así continuar con las actividades administrativas dentro del territorio peruano.

Por esta razón, los peritos del colegio de ingenieros buscaron varias alternativas de solución, el cual facilite no solo la firma remota de documentos con autenticación de identidad, sino que se evite la exposición a un posible contagio por la labor diaria que ejercen.

Esta solución aporta a que los peritos no se sientan obligados en el traslado a sus instalaciones, o al traslado físico de documentos. Generando un beneficio económico, sobre todo por el periodo que venimos atravesando. Además, de ahorro de tiempo y gasto innecesario en papel. El software permite continuar con las actividades de autenticación y firma de documentos con la seguridad y confianza, por el uso de la firma electrónica de documentos.

Esta herramienta puede aplicarse también en diferentes actividades, tales como: Captación de talento humano, educación, banca, seguros, entre otros. Asimismo, podrá ser aplicado a diversos documentos como solicitudes, aprobaciones, contratos, escritos entre otros.

Por lo tanto, la pregunta de investigación es: ¿Cómo la firma electrónica basado en reconocimiento facial, se relaciona con el riesgo de suplantación de identidad en el Colegio de Ingenieros del Perú, Lima?

En función a la pregunta de investigación, se define el siguiente objetivo general: “Determinar la relación entre la firma electrónica basado en reconocimiento facial y el riesgo de suplantación de identidad en el Colegio de Ingenieros del Perú, Lima”.

De acuerdo con lo anterior se proponen las siguientes hipótesis:

HG: La Firma Electrónica basado en reconocimiento facial disminuye significativamente la suplantación de identidad de los peritos del Colegio de Ingenieros del Perú, Consejo Departamental de Lima.

HE1: La verificación de identidad influye significativamente en el riesgo de suplantación de identidad de los peritos del Colegio de Ingenieros del Perú, Lima.

HE2: El proceso de autenticación de identidad influye significativamente en el riesgo de suplantación de identidad de los peritos del Colegio de Ingenieros del Perú, Lima.

HE3: La trazabilidad de la identidad influye significativamente en el riesgo de suplantación de identidad de los peritos del Colegio de Ingenieros del Perú, Lima.

2. Materiales y Métodos

La investigación tiene como base un diseño Experimental, al tener control de las variables, podremos analizar su relación.

Un diseño experimental según (Hernández Sampieri, 2018) consiste en la manipulación intencional de la variable independiente, así como, contar con un

grupo antes y después del experimento; una condición adicional es trabajar con un grupo control para determinar las relaciones entre las variables. El método de análisis es hipotético-deductivo. El tipo de investigación aplicado fue correlacional, con un enfoque mixto.

La población fue finita, se contó con un número determinado de elementos.

La unidad analizada estuvo conformada por los peritos del Colegio de Ingenieros del Perú, Consejo Departamental de Lima.

La población está conformada por: 475 peritos.

Todos estos datos fueron recolectados con el apoyo del colegio de ingenieros del Perú.

El criterio de exclusión fueron todos los ingenieros colegiados, que no son peritos. El criterio de inclusión fueron todos los ingenieros Peritos hábiles.

La muestra es Probabilística. El tamaño de la muestra es calculado usando una fórmula con proporción de marco muestra, dando como resultado 60 personas.

En la siguiente tabla se muestra la propuesta operacional de variables.

Tabla 1. Operacionalización de Variables

Variable	Dimensión
Independiente: La firma electrónica basado en reconocimiento facial.	Verificación de Identidad
	Tecnología de Reconocimiento Facial
	Trazabilidad de la Identidad
Dependiente: Riesgo de suplantación de identidad	Riesgo de estafas

Fuente: Elaboración propia

En esta investigación para la medición de las variables de estudio, se aplicó la técnica de la encuesta. Preguntas dirigidas a los peritos para la indagación en el uso de la firma electrónica y la suplantación de identidad.

Tabla 2. *Ficha Técnica Variable Independiente*

Ficha técnica de la variable independiente

Variable	La firma electrónica basado en reconocimiento facial
Tipo de instrumento:	Encuesta
Unidad de estudio:	Peritos del Colegio de Ingenieros del Perú, Consejo Departamental de Lima.

Fuente: Elaboración propia

Tabla 3. *Ficha Técnica Variable Dependiente*

Ficha técnica de la variable dependiente

Variable	Riesgo de suplantación de identidad
Tipo de instrumento:	Encuesta
Unidad de estudio:	Peritos del Colegio de Ingenieros del Perú, Consejo Departamental de Lima.

Fuente: Elaboración propia

Para la **validación de instrumentos**, sometimos a consideración de juicio experto, para la validación de los ítems. Por lo cual, se necesitó del apoyo de profesionales, quienes a su vez cuentan con el dominio, el cual nos ayudaron con la medición de los ítems. Sobre su grado de experiencia nos brindaron su determinado criterio: si es aplicable o no es aplicable.

Para garantizar la fiabilidad de las variables de la tecnología de reconocimiento facial, se hizo uso del alfa de Cronbach. Posteriormente se PROCESARON los

datos haciendo uso del programa SPSS, considerando un 70% de confiabilidad como mínimo.

Tabla 4. Estadística de Fiabilidad

Estadísticos de fiabilidad	
Alfa de Cronbach	N de elementos
,795	17

Fuente: Elaboración propia

En la tabla 4. Se observa que el alfa de Cronbach calculado mediante el SPSS fue de 79.5%, con el instrumento diseñado de 17 preguntas.

En la siguiente tabla, se muestra la propuesta operacional de las variables.

Tabla 5. Definición operacional de las variables

Variab les	Dimensión	Indicador	Ítem	Escala
Variable Independiente La firma electrónica basado en reconocimiento facial	Dimensión 1: Verificación de Identidad	Nivel de Desempeño	¿Considera Ud. que ante un trámite y solicitud de captura biométrica las huellas son identificadas con facilidad?	1=Nunca; 2=Casi Nunca; 3=A veces; 4=Casi Siempre; 5=Siempre
			¿Cuál de los siguientes métodos biométricos ha utilizado Ud. con mayor frecuencia para la autenticación de identidad?	1=Dactilar; 2=Facial; 3=Iris; 4=Voz; 5=Palma de la Mano
		Nivel de Precisión	¿Cuál es el nivel de precisión que Ud. tiene conocimiento respecto a la captura dactilar?	1=No es preciso; 2=Casi nunca es preciso; 3=A veces es preciso; 4=Casi siempre es preciso; 5=Siempre es preciso
			¿Cuál es el nivel de precisión que Ud. tiene conocimiento respecto a la captura facial?	1=No es preciso; 2=Casi nunca es preciso; 3=A veces es preciso; 4=Casi siempre es preciso; 5=Siempre es preciso
		Nivel de Seguridad	¿Considera Ud. que la biometría dactilar para la validación de identidad es segura?	1=Nunca; 2=Casi Nunca; 3=A veces; 4=Casi Siempre; 5=Siempre
			¿Considera Ud. que la biometría facial para la validación de identidad es segura?	1=Nunca; 2=Casi Nunca; 3=A veces; 4=Casi Siempre; 5=Siempre

			¿Consideraría Ud. usar un método de validación de identidad sin contacto?	1=Nunca; 2=Casi Nunca; 3=A veces; 4=Casi Siempre; 5=Siempre
Dimensión 2: Tecnología de Reconocimiento Facial	Nivel de Confiabilidad		¿Considera Ud. que el nivel de confianza de la biometría facial es óptimo para la verificación de identidad?	1=No Considero; 2=No tengo información para opinar; 3=Es Probable; 4=Muy Probable; 5=Es Segura
		Nivel de Exactitud	¿Cuál es el nivel de exactitud que la plataforma con Reconocimiento Facial certifica su firma?	1=0%; 2= 1% - 25%; 3=26 - 50%; 4=51% - 75%; 5=76% - 100%
	Nivel de aceptación por parte del usuario		¿Considera firmar documentos a través de una plataforma con Reconocimiento Facial?	1=Nunca; 2=Casi Nunca; 3=A veces; 4=Casi Siempre; 5=Siempre
			¿Desearía Ud. instalar un componente en su computador para el Reconocimiento Facial?	1=Nunca; 2=Casi Nunca; 3=A veces; 4=Casi Siempre; 5=Siempre
			¿Considera importante hacer uso de una plataforma de firma electrónica con Biometría Facial en reemplazo de la firma tradicional?	1=Nunca; 2=Casi Nunca; 3=A veces; 4=Casi Siempre; 5=Siempre
Dimensión 3: Trazabilidad de la identidad	Trazabilidad de la Información		¿Considera Ud. saber dónde se encuentra el documento dentro de la plataforma luego de su firma?	1=La Plataforma no guarda documentos; 2=La Plataforma ocasionalmente guarda documentos; 3=La plataforma probablemente guarda documentos; 4=La plataforma debe guardar documentos; 5=La plataforma siempre guarda documentos
	Integridad de la Información		¿Cree Ud. que sus datos biométricos faciales puedan ser suplantados?	1=Nunca; 2=Casi nunca; 3=A veces; 4=Casi siempre; 5=Siempre
Variable Dependiente Riesgo de suplantación de identidad	Dimensión 1: Riesgo de Estafas	Cantidad de Estafas por tipo de suplantación	¿Cuál es el nivel de suplantación que Ud. tiene conocimiento sobre un documento nacional de Identidad (DNI)?	1=0%; 2=1% - 25%; 3=26% - 50%; 4=51% - 75%; 5=76% - 100%
		Nivel de Pérdida Económica	¿Ante una posible suplantación y clonación de identidad, cuanto cree que podría perder utilizando su nombre?	1=Menos de S/1,000; 2=De S/ 1,001 a S/3,000; 3=De S/3,001 a S/10,000; 4=De S/10,001 - S/50,000; 5=Más de S/50,000 3=De S/3,001 a S/10,000; 4=De S/10,001 - S/50,000; 5=Más de S/50,000 5=más de S/100,000

Fuente: Elaboración propia

3. Resultados

Los resultados de las encuestas presentadas a continuación, ayudan a responder las hipótesis planteadas con anterioridad. Los resultados fueron obtenidos con el apoyo de la herramienta estadística SPSS. De acuerdo a las tabulaciones definidas en la herramienta nos permitió demostrar la aceptación o rechazo de las hipótesis planteadas en la investigación. De esta manera se comprueba que “La firma electrónica basado en reconocimiento facial se relaciona con el riesgo de suplantación de identidad en el Colegio de Ingenieros del Perú, Lima”.

Estadística Descriptiva:

Resultados de las encuestas

Pregunta No 1. ¿Considera Ud. que ante un trámite y solicitud de captura biométrica las huellas son identificadas con facilidad?

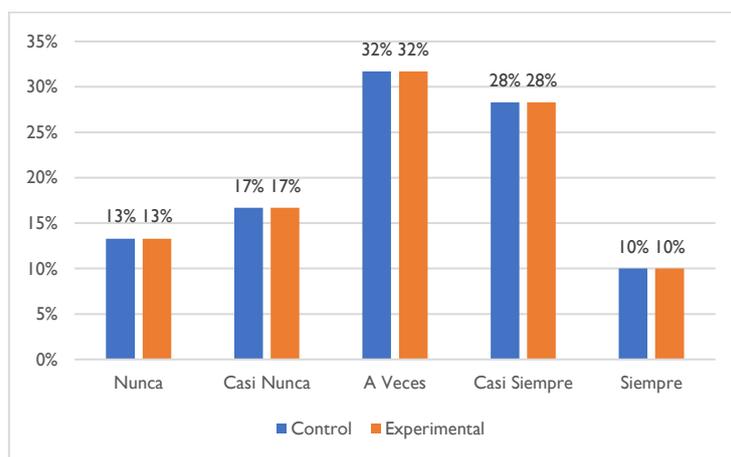


Figura 1. Trámite y solicitud de captura biométrica

De la Fig. 1 se aprecia que el 32% de los encuestados a veces sus huellas biométricas son identificadas con facilidad y el 28% casi siempre son identificadas. Sin embargo, El 13% manifiesta que sus huellas nunca son

identificadas y un 17% de casi nunca. Finalmente, los valores de ambos grupos son iguales, producto de que la pregunta no varía ante la prueba del aplicativo. Es decir, el encuestado mantiene su respuesta.

Pregunta No 2. ¿Cuál de los siguientes métodos biométricos ha utilizado Ud. con mayor frecuencia para la autenticación de identidad?

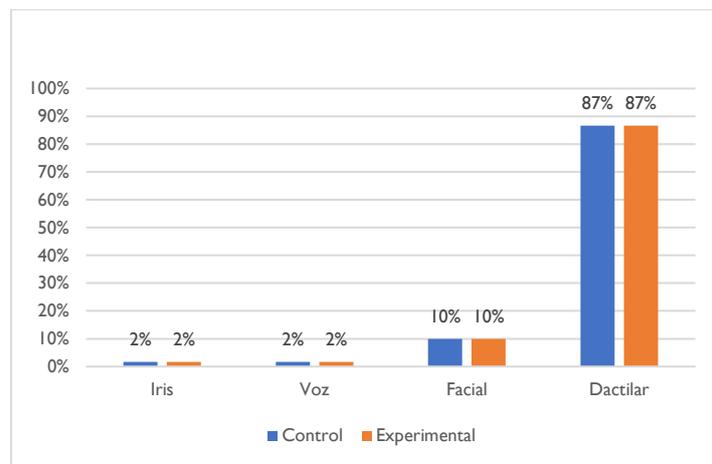


Figura 2. Métodos biométricos

De la Fig. 2 se aprecia que el 87% de los encuestados ha utilizado la biometría dactilar para autenticar su identidad. Sin embargo, solo el 10% ha utilizado la tecnología facial. Finalmente, los valores de ambos grupos son iguales, producto de que la pregunta no varía ante la prueba del aplicativo. Es decir, el encuestado mantiene su respuesta.

Pregunta No 3. ¿Cuál es el nivel de precisión que Ud. tiene conocimiento respecto a la captura dactilar?

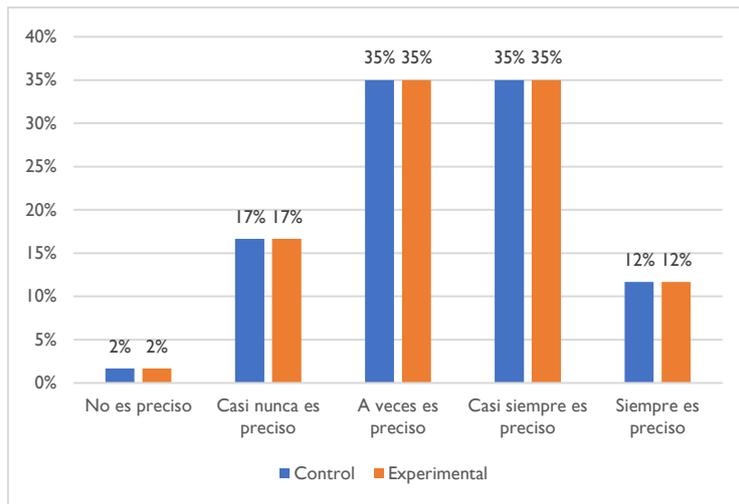


Figura 3. Nivel de Precisión captura dactilar

De la Fig. 3 se aprecia que el 70% de los encuestados considera que el nivel de presión respecto a la captura dactilar a veces es preciso y casi siempre es preciso. Sin embargo, el 17% manifiesta que casi nunca no es preciso. Finalmente, los valores de ambos grupos son iguales, producto de que la pregunta no varía ante la prueba del aplicativo. Es decir, el encuestado mantiene su respuesta.

Pregunta No 4. ¿Cuál es el nivel de precisión que Ud. tiene conocimiento respecto a la captura facial?

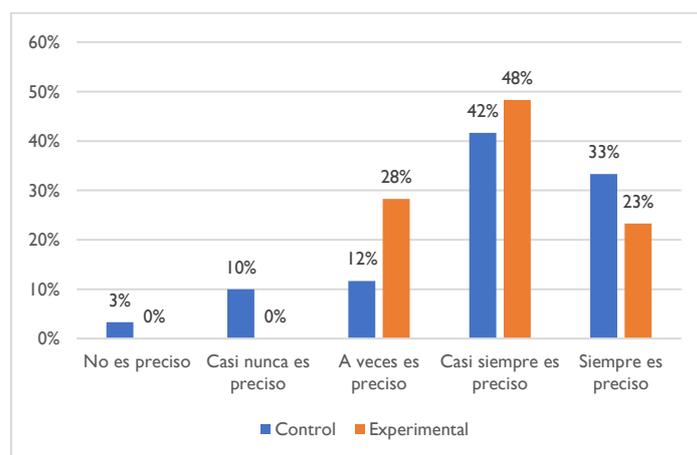


Figura 4. Nivel de Precisión captura facial

De la Fig. 4 se aprecia que del 100% de los encuestados, el 42% considera que el nivel de presión respecto a la captura facial casi siempre es preciso, el 33%

manifiesta que es preciso y el 10% manifiesta que casi nunca es preciso. Sin embargo, luego del uso del aplicativo, el 48% considera que casi siempre es preciso y el 23% indica que siempre es preciso.

Pregunta No 5. ¿Considera Ud. que el DNI es seguro para la validación de Identidad?

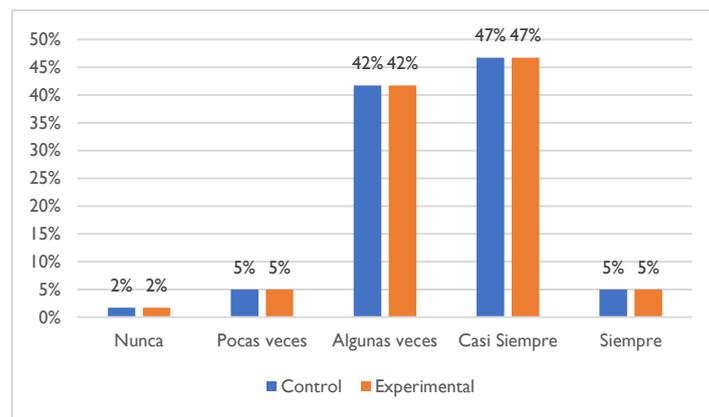


Figura 5. Seguridad del DNI

De la Fig. 5 se aprecia que el 47% de los encuestados considera que el DNI es seguro para la validación de identidad y el 42% señala que casi siempre es seguro. Sin embargo, el 5% manifiesta que pocas veces es seguro. Finalmente, los valores de ambos grupos son iguales, producto de que la pregunta no varía ante la prueba del aplicativo. Es decir, el encuestado mantiene su respuesta.

Pregunta No 6. ¿Considera Ud. que la biometría dactilar para la validación de identidad es segura?

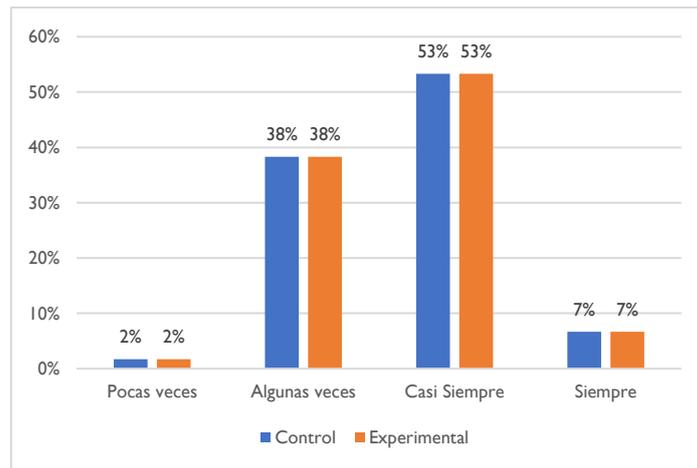


Figura 6. Seguridad de la biometría dactilar

De la Fig. 6 se aprecia que el 53% de los encuestados considera que casi siempre la biometría dactilar para la validación de identidad es segura y el 38% señala que algunas veces es segura. Sin embargo, el 7% considera que siempre es segura. Finalmente, los valores de ambos grupos son iguales, producto de que la pregunta no varía ante la prueba del aplicativo. Es decir, el encuestado mantiene su respuesta.

Pregunta No 7. ¿Considera Ud. que la biometría facial para la validación de identidad es segura?

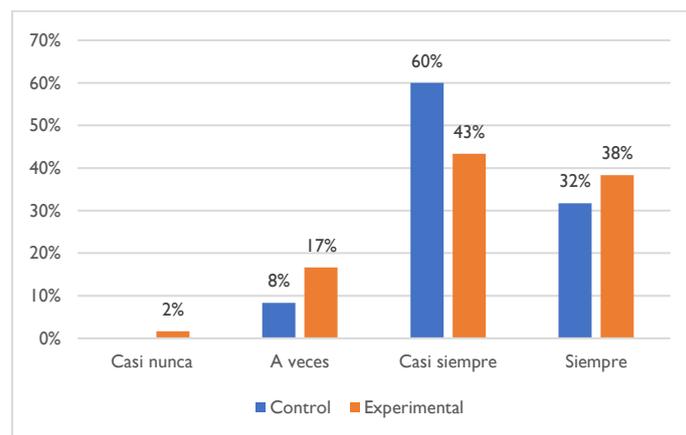


Figura 7. Seguridad de la biometría facial

De la Fig. 7 se aprecia que del 100% de los encuestados, el 60% considera que la biometría facial para la validación de identidad casi siempre es segura, el 32%

manifiesta que siempre es segura y el 8% manifiesta que casi a veces es segura. Sin embargo, luego del uso del aplicativo, el 43% considera que casi siempre es segura, el 38% indica que siempre es segura y el 17% considera que a veces es segura.

Pregunta No 8. ¿Consideraría Ud. usar un método de validación de identidad sin contacto?

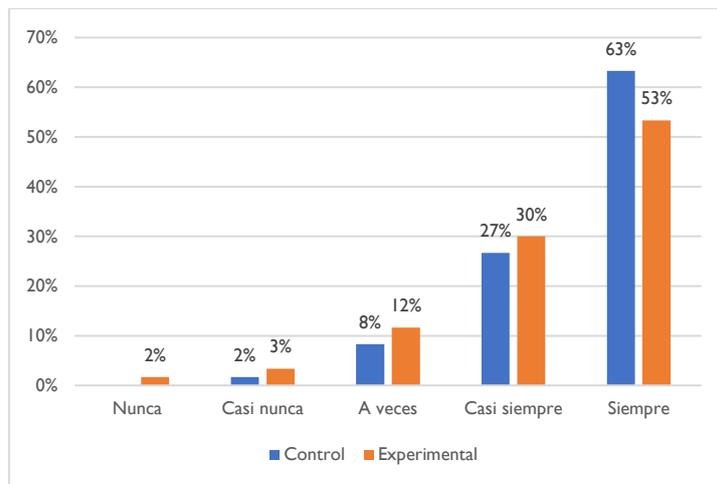


Figura 8. Método de identidad sin contacto

De la Fig. 8 se aprecia que del 100% de los encuestados, el 63% considera siempre usar un método de validación de identidad sin contacto, el 27% manifiesta que casi siempre lo usaría. Sin embargo, luego del uso del aplicativo, el 30% considera que lo usaría casi siempre y el 53% considera siempre usarlo.

Pregunta No 9. ¿Considera Ud. que el nivel de confianza de la biometría facial es óptimo para la verificación de identidad?

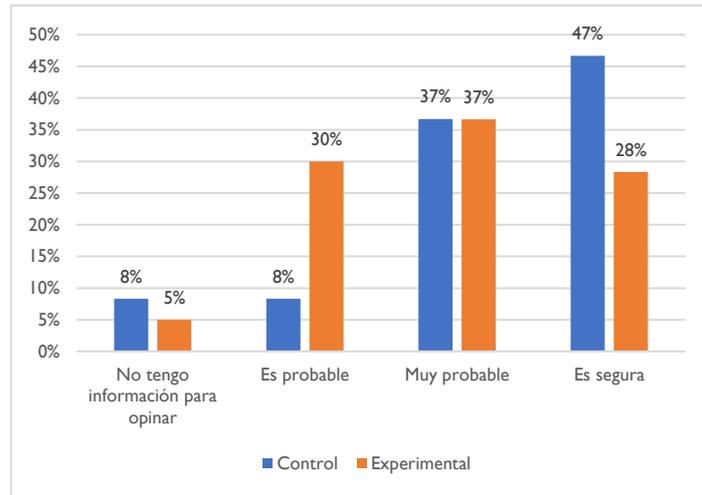


Figura 9. Nivel de exactitud de la plataforma

De la Fig. 9 se aprecia que del 100% de los encuestados, el 63% considera siempre usar un método de validación de identidad sin contacto, el 27% manifiesta que casi siempre lo usaría. Sin embargo, luego del uso del aplicativo, el 30% considera que lo usaría casi siempre y el 53% considera siempre usarlo

Pregunta No 10. ¿Cuál es el nivel de exactitud que la plataforma con Reconocimiento Facial certifica su firma?

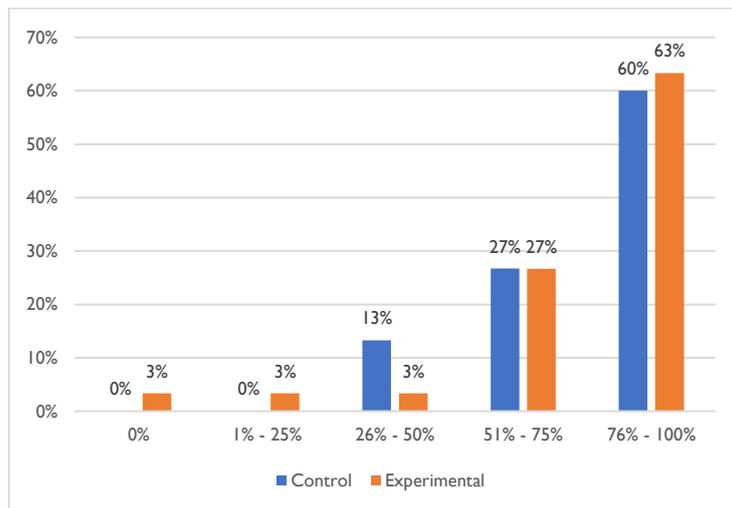


Figura 10. Nivel de exactitud de la plataforma

De la Fig. 10 se aprecia que del 100% de los encuestados, el 60% considera un nivel de exactitud de la plataforma de reconocimiento facial entre un 76%-100%, el 27% manifiesta una exactitud en un rango de 51%-75%. Sin embargo, luego

del uso del aplicativo, el 63% lo considera una exactitud entre un rango de 76%-100% y el 27% entre 51%-75%.

Pregunta No 11. ¿Considera firmar documentos a través de una plataforma con Reconocimiento Facial?

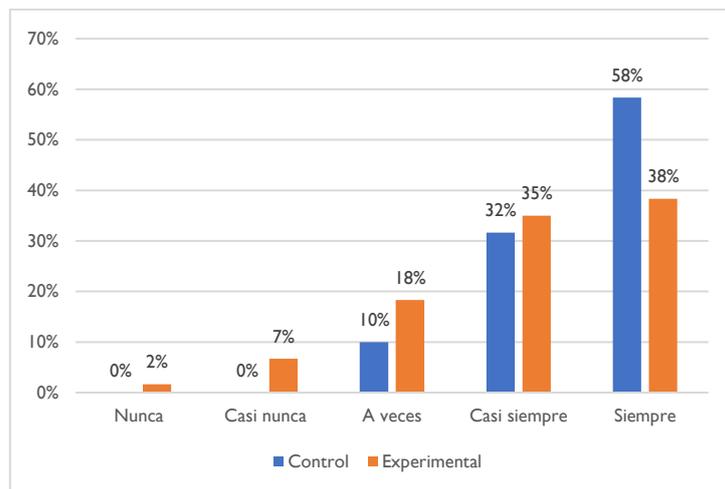


Figura 11. Firmar con plataforma facial

De la Fig. 11 se aprecia que del 100% de los encuestados, el 58% considera siempre firmar documentos a través de una plataforma con Reconocimiento Facial, el 32% considera firmar casi siempre. Sin embargo, luego del uso del aplicativo, el 38% considera que siempre lo usaría y el 35% considera firmar casi siempre.

Pregunta No 12. ¿Desearía Ud. no instalar un componente en su computador para el Reconocimiento Facial?

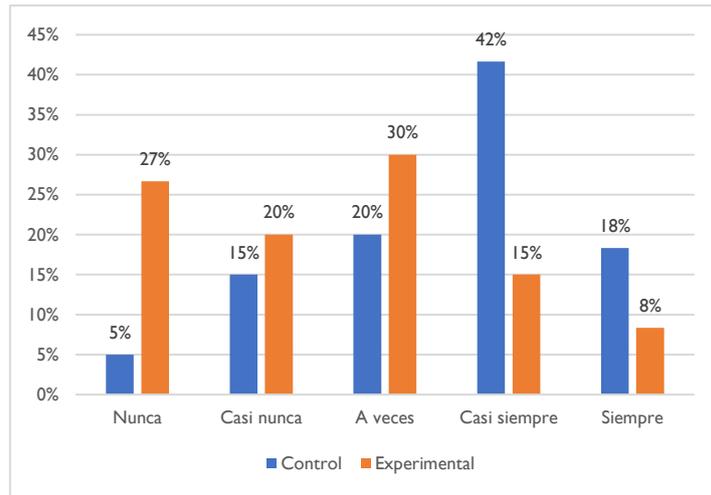


Figura 12. Instalación de componente facial

De la Fig. 12 se aprecia que del 100% de los encuestados, el 42% considera no instalar un componente en su computador para el Reconocimiento Facial, el 20% considera a veces no instalar. Sin embargo, luego del uso del aplicativo, el 30% considera a veces no instalar el componente y el 27% considera instalar el componente.

Pregunta No 13. ¿Considera importante hacer uso de una plataforma de firma electrónica con Biometría Facial en reemplazo de la firma tradicional?

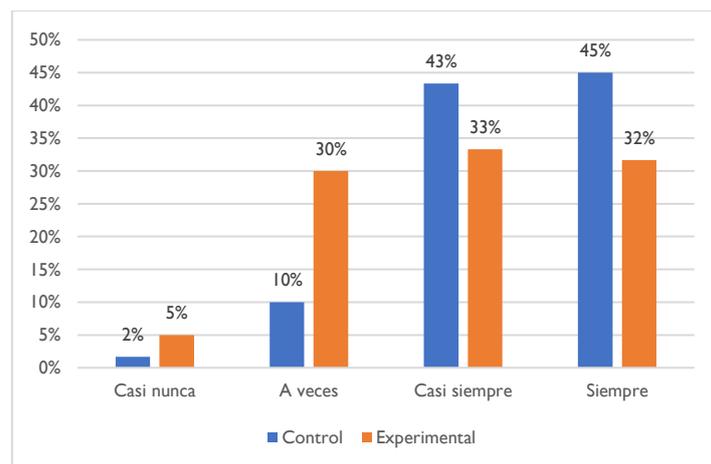


Figura 13. Reemplazo de la firma tradicional

De la Fig. 13 se aprecia que del 100% de los encuestados, el 45% considera siempre importante hacer uso de una plataforma de firma electrónica con Biometría Facial en reemplazo de la firma tradicional, el 43% considera casi

siempre hacer uso de la plataforma y el 10% casi nunca. Sin embargo, luego del uso del aplicativo, el 32% considera siempre hacer uso de la plataforma, 33% casi siempre y el 30% a veces.

Pregunta No 14. ¿Considera Ud. saber dónde se encuentra el documento dentro de la plataforma luego de su firma?

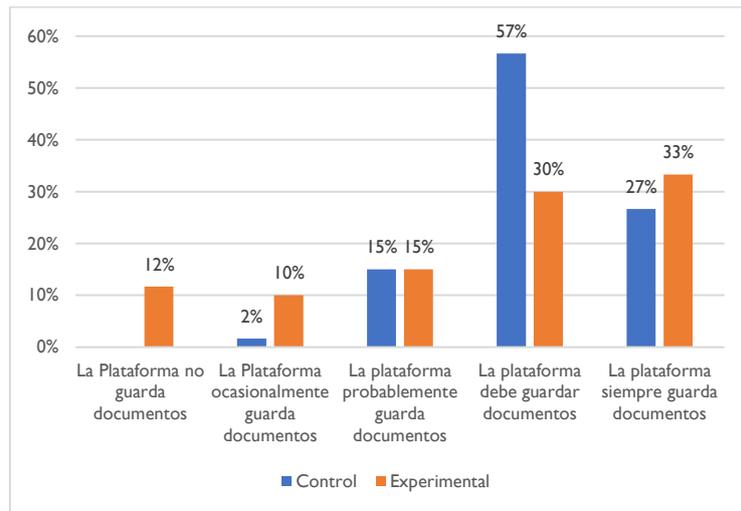


Figura 14. Trazabilidad de la firma

De la Fig. 14 se aprecia que del 100% de los encuestados, el 57% considera que la plataforma de guardar documentos, el 27% considera que la plataforma siempre debe guardar documentos. Sin embargo, luego del uso del aplicativo, el 33% considera que la plataforma siempre debe guardar documentos y el 30% debe guardar documentos.

Pregunta No 15. ¿Cree Ud. que sus datos biométricos faciales puedan ser suplantados?

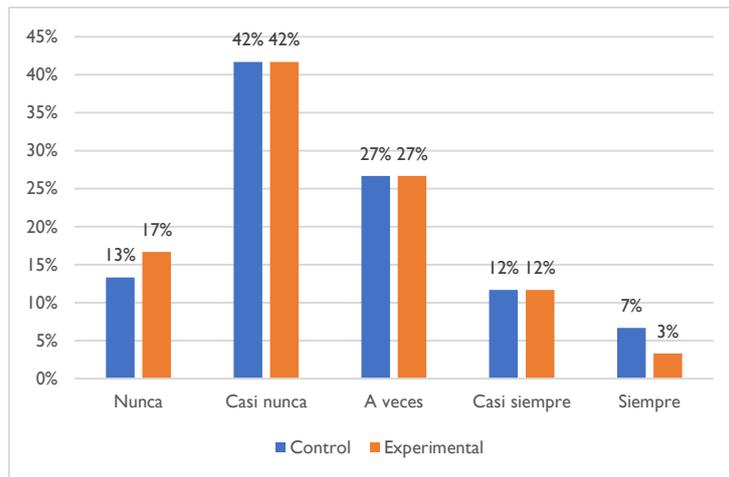


Figura 15. Suplantación de datos biométricos faciales

De la Fig. 15 se aprecia que del 100% de los encuestados, el 42% considera casi nunca que sus datos biométricos faciales puedan ser suplantados, el 27% considera a veces pueda haber suplantación y el 13% considera nunca habrá suplantación. Sin embargo, luego del uso del aplicativo, el 42% considera casi siempre habrá suplantación, 27% a veces y el 17% nunca.

Pregunta No 16. ¿Cuál es el nivel de suplantación que Ud. tiene conocimiento sobre un documento nacional de Identidad (DNI)?

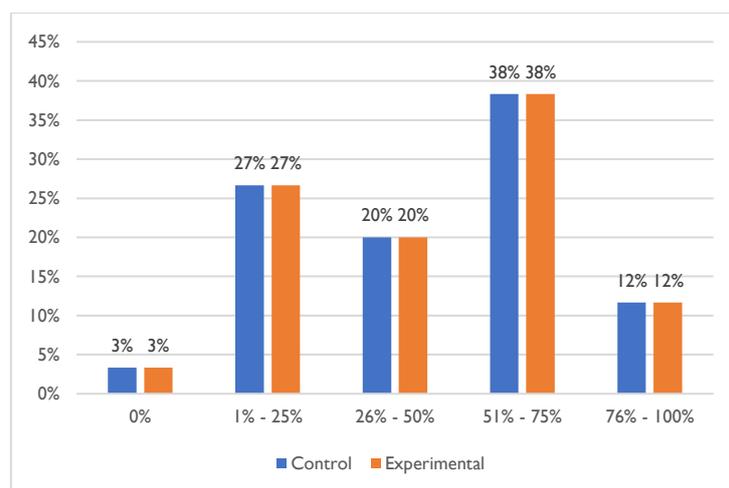


Figura 16. Nivel de suplantación del DNI

De la Fig. 16 se aprecia que del 100% de los encuestados, el 38% considera un rango 51%-75%, como nivel de suplantación del DNI, el 27% considera un rango de 1%-25% como nivel de suplantación y el 20% considera un rango de 26%-

50%. Finalmente, los valores de ambos grupos son iguales, producto de que la pregunta no varía ante la prueba del aplicativo. Es decir, el encuestado mantiene su respuesta.

Pregunta No 17. ¿Ante una posible suplantación y clonación de identidad, cuanto cree que podría perder utilizando su nombre?

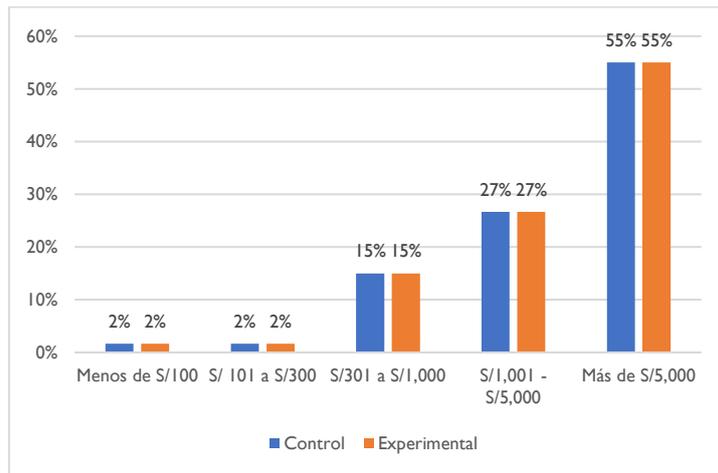


Figura 17. Perdida ante una posible clonación

De la Fig. 17 se aprecia que del 100% de los encuestados, el 55% considera que podría perder más de S/5,000 ante una posible suplantación y clonación de identidad, el 27% considera perder en un rango de S/1,001 - S/5,00 y el 13% considera perder en un rango de S/3001 – S/1,000. Finalmente, los valores de ambos grupos son iguales, producto de que la pregunta no varía ante la prueba del aplicativo. Es decir, el encuestado mantiene su respuesta.

Estadística Inferencial:

En base a los resultados obtenidos de las encuestas, se hizo uso del alfa de Cronbach para medir la confiabilidad del instrumento utilizado. Los cuales demostraron los siguientes resultados.

Prueba de Normalidad

1. Hipótesis

Se plantean las hipótesis para la normalidad

Ho = Los datos tienen una distribución normal

HI = Los datos difieren de una distribución normal

2. Nivel de Significancia

$$\alpha = 0.05$$

3. Valor de Prueba

Kolmogorov-Smirnov (Muestra mayor a 50)

4. Comparación de p y α

$$P\text{Valor} < \alpha = 0.05$$

5. Decisión

Se rechaza la Ho

6. Conclusión.

En la tabla 6 se puede observar que las variables tienen un pvalor de 0.000, el cual es menor a 0.05 que es nuestro nivel de comparación. Por lo cual, se rechaza la Ho, es decir que todas las variables difieren del comportamiento normal.

Tabla 6. Prueba de Normalidad

	Pruebas de normalidad		
	Kolmogorov-Smirnov ^a		
	Estadístico	gl	Sig.
P1	.183	60	.000
P2	.490	60	.000
P3	.207	60	.000
P4	.244	60	.000

P5	.272	60	.000
P6	.310	60	.000
P7	.239	60	.000
P8	.308	60	.000
P9	.202	60	.000
P10	.355	60	.000
P11	.227	60	.000
P12	.162	60	.000
P13	.200	60	.000
P14	.240	60	.000
P15	.249	60	.000
P16	.244	60	.000
P17	.323	60	.000

a. Corrección de la significación de Lilliefors

Fuente: Elaboración propia

Por lo tanto, para establecer la relación entre las variables utilizamos la prueba de Spearman, que es una prueba no paramétrica.

Tabla 7. Coeficiente de correlación

			Correlaciones				
			D1	D2	D3	V1	
			Verificación de identidad	Tecnología de reconocimiento facial	Trazabilidad de la identidad	La firma electrónica basado en reconocimiento facial	
Rho de Spearman	D4	Riesgo de estafa	Coeficiente de correlación	,276*	,347**	-,272*	,278*
			Sig. (bilateral)	Relación baja	Relación baja	Relación baja	Relación baja
	V2	Riesgo de suplantación de identidad	Coeficiente de correlación	,276*	,347**	-,272*	,278*
			Sig. (bilateral)	Relación baja	Relación baja	Relación baja	Relación baja

Fuente: Elaboración propia

En la tabla 7 podemos observar las siguientes relaciones:

Existe una relación baja entre la verificación de Identidad y el riesgo de estafa en los peritos del Colegio de Ingenieros del Perú, Consejo Departamental de Lima.

Existe una relación baja entre la tecnología de reconocimiento facial y el riesgo de estafa en los peritos del Colegio de Ingenieros del Perú, Consejo Departamental de Lima.

Existe una relación negativa baja entre la trazabilidad de la identidad y el riesgo de estafa en los peritos del Colegio de Ingenieros del Perú, Consejo Departamental de Lima.

Existe una relación baja entre la firma electrónica basado en reconocimiento facial y el Riesgo de estafa en los peritos del Colegio de Ingenieros del Perú, Consejo Departamental de Lima.

Existe una relación baja entre la verificación de Identidad y la variable Riesgo de suplantación de identidad en los peritos del Colegio de Ingenieros del Perú, Consejo Departamental de Lima.

Existe una relación baja entre la tecnología de reconocimiento facial y el riesgo de suplantación de identidad en los peritos del Colegio de Ingenieros del Perú, Consejo Departamental de Lima.

Existe una relación negativa baja entre la trazabilidad de la identidad y el riesgo de suplantación de identidad en los peritos del Colegio de Ingenieros del Perú, Consejo Departamental de Lima.

Existe una relación baja entre la firma electrónica basado en reconocimiento facial y el riesgo de suplantación de identidad en los peritos del Colegio de Ingenieros del Perú, Consejo Departamental de Lima.

3.1. Contraste de Hipótesis

Para corroborar la veracidad de la hipótesis planteada, se optó por hacer uso de una prueba de correlación basado en los siguientes elementos:

Variable 1. La firma electrónica basado en reconocimiento facial

Variable 2. Riesgo de suplantación de identidad

Dimensión 1. Verificación de Identidad

Dimensión 2. Tecnología de reconocimiento facial

Dimensión 3. Trazabilidad de la identidad

Dimensión 4. Riesgo de Estafas

Debido a que los elementos en estudio no tuvieron comportamiento normal, se determinó realizar la prueba con el coeficiente de correlación de Spearman.

Prueba de hipótesis general de la investigación.

Tabla 8. Resultado de la prueba de correlación entre la variable “La firma electrónica basado en reconocimiento facial y el Riesgo de suplantación de identidad”

Correlaciones			Riesgo de suplantación de identidad
Rho de Spearman	La firma electrónica basado en reconocimiento facial	Coeficiente de correlación	,278*
		Sig. (bilateral)	.032
		N	60

Fuente: Elaboración propia

De acuerdo con la Tabla 5, el valor de significancia entre las variables: “La firma electrónica basado en reconocimiento facial y el Riesgo de suplantación de identidad” (0.032) ha sido menor al planteado (0.05). Por lo tanto, se acepta H_1 , del mismo modo, el coeficiente de correlación calculado (0.278) comprueba que la correlación es positiva baja. Se concluye que: La Firma Electrónica basado en reconocimiento facial disminuye significativamente la suplantación de identidad de los peritos del Colegio de Ingenieros del Perú, Consejo Departamental de Lima.

Tabla 9. Resultado de la prueba de correlación entre la dimensión Verificación de identidad y la variable Riesgo de suplantación de identidad

Correlaciones			Riesgo de suplantación de identidad
Rho de Spearman	Verificación de identidad	Coeficiente de correlación	,276*
		Sig. (bilateral)	.033
		N	60

Fuente: Elaboración propia

De acuerdo con la Tabla 6, el valor de significancia entre la dimensión “Verificación de identidad y la variable Riesgo de suplantación de identidad” (0.033) ha sido menor al planteado (0.05). Por lo tanto, se acepta H_1 , del mismo modo, el coeficiente de correlación calculado (0.276) comprueba que la correlación es positiva baja. Se concluye que: Existe una relación directa entre la verificación de identidad y el riesgo de suplantación de identidad en el Colegio de Ingenieros del Perú, Lima.

Tabla 10. Resultado de la prueba de correlación entre la dimensión Tecnología de reconocimiento facial y la variable Riesgo de suplantación de identidad

Correlaciones			Riesgo de suplantación de identidad
Rho de Spearman	Tecnología de reconocimiento facial	Coefficiente de correlación	,347**
		Sig. (bilateral)	.007
		N	60

Fuente: Elaboración propia

De acuerdo con la Tabla 7, el valor de significancia entre la dimensión Tecnología de reconocimiento facial y la variable Riesgo de suplantación de identidad” (0.007) ha sido menor al planteado (0.05). Por lo tanto, se acepta H_1 , del mismo modo, el coeficiente de correlación calculado (0.347) comprueba que la correlación es positiva baja. Se concluye que: La Tecnología de reconocimiento facial influye significativamente en la suplantación de identidad en el Colegio de Ingenieros del Perú, Lima.

Tabla 11. Resultado de la prueba de correlación entre la dimensión Trazabilidad de la identidad y la variable Riesgo de suplantación de identidad

Correlaciones			Riesgo de suplantación de identidad
Rho de Spearman	Trazabilidad de la identidad	Coefficiente de correlación	-,272*
		Sig. (bilateral)	.036
		N	60

Fuente: Elaboración propia

De acuerdo con la Tabla 8, el valor de significancia entre la dimensión Trazabilidad de la identidad y la variable Riesgo de suplantación de identidad”

(0.036) ha sido menor al planteado (0.05). Por lo tanto, se acepta H_1 , del mismo modo, el coeficiente de correlación calculado (-0.272) comprueba que la correlación es negativa baja. Es decir, a mayor trazabilidad de la identidad habrá menos riesgo de suplantación. Se concluye que: La trazabilidad de la identidad influye significativamente en el riesgo de suplantación de identidad en el Colegio de Ingenieros del Perú, Lima.

4. Discusión

En base a la Hipótesis general planteada “La Firma Electrónica basado en reconocimiento facial disminuye significativamente la suplantación de identidad de los peritos del Colegio de Ingenieros del Perú, Consejo Departamental de Lima”. Se puede evidenciar que existe una relación directa. A mayor uso de la firma electrónica, esto generará una baja en la suplantación de identidad.

Ayala Goyes (2018) en su tesis, el problema manifestado fue que los docentes y personal administrativo usaban un capturador de huella biométrico con código de acceso, el cual generaba no solo atrasos, sino que había indicios de suplantación, y lentitud en el mercado de asistencia.

Se propuso una solución de biometría facial a través de algoritmo propios para la optimización de tiempos en captura facial y validación de identidad; y obtener reportes en tiempos correctos.

En base a la hipótesis específica “La verificación de identidad influye significativamente en el riesgo de suplantación de identidad en el Colegio de Ingenieros del Perú, Lima”. Se puede evidenciar que existe una relación directa. A mayor uso de la verificación de identidad, esto generará una baja en la suplantación de identidad.

Arroyo, Alonso, Rivera, & Humberto (2019), en su tesis de investigación, ante la existencia de pacientes que llegaban a emergencia sin documento de identidad o simplemente se hacían pasar por otra persona. Se diseñó un modelo biométrico a través de la tecnología de reconocimiento facial bajo plataforma Cloud para la identificación de pacientes y bajar el nivel de suplantación. Se utilizó el algoritmo LBPH (Histograma local de patrones binarios) el cual hace comparativas a la par dando una similitud del 95%. El piloto funcionó, pero recomendaron subir más fotos de la persona para el entrenamiento y poder tener más exactitud de la persona.

En base a la hipótesis específica “La Tecnología de reconocimiento facial influye significativamente en la suplantación de identidad en el Colegio de Ingenieros del Perú, Lima”. Se puede evidenciar que existe una relación directa. A mayor uso de la Tecnología de reconocimiento facial, esto generará una baja en la suplantación de identidad.

Coronel Zegarra, (2020) en su tesis manifiesta que el problema es que, para clasificar y reconocer rostros, se requiere la extracción de patrones de rasgos faciales a partir de los pixeles que contiene la imagen. Dicho estudio concluye en que los métodos de preprocesamiento facial se llegaron a relacionar con el sistema de manera directa y efectiva. Se confirmó que en una captura de rostro los métodos de alineamiento facial llegan a ser efectivos. Además, dependiendo de la aplicación de una combinación de los factores como por ejemplo el modelo de validación facial, la fuente de información para comparar los rostros y el método de detección facial puede influenciar de manera positiva o negativa.

En base a la hipótesis específica “La trazabilidad de la identidad influye significativamente en el riesgo de suplantación de identidad en el Colegio de Ingenieros del Perú, Lima.” Se puede evidenciar que existe una relación inversa. A mayor trazabilidad de identidad, esto generará una baja en el riesgo de suplantación de identidad.

Basantes Verdugo (2018) en su tesis el problema era identificar al supuesto padre o apoderado, existiendo una probabilidad de suplantación de identidad. Se propuso implementar una herramienta de reconocimiento facial, en el cual se empezó a enrolar los patrones faciales a todos los alumnos, padres y/o apoderados. Los alumnos antes de dejar la institución eran comparados por la herramienta de comparación facial alumno-padre o alumno apoderado con la base de datos de capturas faciales. Cuando la comparativa era satisfactoria se enviaba un mensaje al móvil del padre sobre el recojo del alumno, dejando una trazabilidad de la persona que había venido a recogerlo. Generando seguridad y confiabilidad a los padres de familia frente a una posible suplantación. Este proyecto tuvo su justificación en la inseguridad ciudadana en la que se vive y en salvaguardar la integridad del alumno. Se inició un piloto con una muestra pequeña de maestros y alumnos.

Contribución de autoría

Raúl Cervantes Alejos. Conceptualización, Análisis formal, Investigación

Carlos Peralta Delgado. Conceptualización, Metodología, Validación

Conflicto de Interés

No existe interés común, ni relación alguna con la entidad de estudio, el cual afecte al trabajo de investigación.

Referencias bibliográficas

- Arroyo, L. M., Alonso, D., Rivera, B., & Humberto, M. (1 de Diciembre de 2019). *Modelo Tecnológico de Reconocimiento Facial para la Identificación de Pacientes en el Sector Salud TESIS*. Obtenido de Universidad Peruana de Ciencias Aplicadas (UPC): <https://repositorioacademico.upc.edu.pe/handle/10757/648832>
- Ayala Goyes, M. (Julio de 2018). *Sistema biometrico de reconocimiento facial para el control de asistencia del personal docente y administrativo de la Uniandes Tulcán*. Obtenido de Repositorio Institucional UNIANDES: <http://dspace.uniandes.edu.ec/handle/123456789/8694>
- Basantes Verdugo, N. (2018). *Desarrollo de una Plataforma Tecnológica para la Gestión de Seguridad en una Institución Educativa de Grado Inicial mediante el uso de Sistemas Móviles, Reconocimiento Facial y Sistemas de Alertas*. Obtenido de Repositorio Institucional de la Universidad de Guayaquil: <http://repositorio.ug.edu.ec/handle/redug/32717>
- Coronel Zegarra, B. (2020). *Impacto del preprocesamiento de imágenes en la efectividad de la verificación facial empleando visión computacional*. Obtenido de Universidad ESAN: <https://repositorio.esan.edu.pe/handle/20.500.12640/2111>
- EL PERUANO. (15 de 03 de 2020). *Plataforma Digital del Estado Peruano*. Obtenido de <https://www.gob.pe/institucion/pcm/normas-legales/460472-044-2020-pcm>
- Hernandez Sampieri, R. (2018). *Metodología de la investigación - Sexta Edición*. México: Mc Graw Hill.

ANEXOS

Anexo 1. Sustento de envío para publicación.

RV: [Ing.Investig] Envío recibido - Ingeniería e Investigación

Raul Alejandro Cervantes Alejos <100085308@cientifica.edu.pe>
 To: "carlosperaltad@gmail.com" <carlosperaltad@gmail.com>
 Cc: "alejandro.cervantes@acj.pe" <alejandro.cervantes@acj.pe>

Thu, Apr 15, 2021 at 12:29 AM

Estimado Profesor:

Buenas noches, acabo de enviar el paper para su publicación a la revista UNAL.
 Quedo atento ante cualquier duda o consulta.

ISSN 2248-8723

Saludos Cordiales
 Alejandro

De: Andrés Pavas <revii_bog@unal.edu.co>

Enviado: jueves, 15 de abril de 2021 0:25

Para: Raul Alejandro Cervantes Alejos <100085308@cientifica.edu.pe>

Asunto: [Ing.Investig] Envío recibido - Ingeniería e Investigación

Raul Alejandro Cervantes Alejos:

Respetado autor, reciba un cordial saludo. Hemos recibido su manuscrito "La firma electrónica basado en reconocimiento facial y el riesgo de suplantación de identidad en el colegio de ingenieros del Perú, Consejo Departamental de Lima". Gracias al sistema en línea de gestión de revistas que usamos, podrá seguir su progreso a través del proceso editorial identificándose en el sitio web de la revista:

URL del manuscrito: <https://revistas.unal.edu.co/index.php/ingeinvt/authorDashboard/submission/95090>

Nombre de usuario/a: 100085308

Si tiene cualquier pregunta no dude en contactar con nosotros/as.

Próximamente estaremos comunicándonos con ustedes sobre el proceso de evaluación. Gracias por confiar en Ingeniería e Investigación para la divulgación de sus productos.

Andrés Pavas

Ingeniería e Investigación <https://revistas.unal.edu.co/index.php/ingeinvt>

Tel.: (57-1) 318 5000 Ext. 13374 Universidad Nacional de Colombia, Bogotá, Colombia

La información contenida en este correo es para uso exclusivo del destinatario y puede ser confidencial. En caso de recibir este correo por error, por favor no imprima, copie, reenvíe o divulgue de manera total o parcial este mensaje. Borre este correo y todas las copias y avise al remitente. Gracias.

Anexo 2. Matrix de Consistencia.

Título: La firma electrónica basado en reconocimiento facial y el riesgo de suplantación de identidad en el Colegio de Ingenieros del Perú, Consejo Departamental de Lima

Problema general	Objetivo general	Hipótesis general	Variables/Dimensiones	Definición conceptual	Definición operacional
¿Cómo la firma electrónica basado en reconocimiento facial, se relaciona con el riesgo de suplantación de identidad en el CIP Lima?	Determinar la relación entre la firma electrónica basado en reconocimiento facial y el riesgo de suplantación de identidad en el CIP Lima.	La Firma Electrónica basado en reconocimiento facial disminuye significativamente e la suplantación de identidad de los peritos del Colegio de Ingenieros del Perú, Consejo Departamental de Lima.	<p>Variable independiente:</p> <p>X= La firma electrónica basado en reconocimiento facial</p> <p>Dimensiones:</p> <p>Verificación de Identidad Tecnología de Reconocimiento Facial Trazabilidad de la identidad</p>	Según (Gimeno Hernández, 2010) el sistema de reconocimiento facial es una aplicación dirigida por ordenador que identifica automáticamente e a una persona en una imagen digital. Esto es posible mediante un análisis de las características faciales del sujeto extraídas de la imagen para su posterior comparación con una base de imágenes.	Mediante el uso del smartphone se podrá recibir documentos para la firma, previa validación y validar la identidad.
¿Cómo influirá la verificación de identidad en el riesgo de suplantación de identidad en el CIP Lima?	Demostrar si la verificación de identidad influye en el riesgo de suplantación de identidad en el CIP Lima.	La verificación de identidad influye significativamente e en el riesgo de suplantación de identidad en el CIP Lima.			
¿Cómo influirá la Tecnología de Reconocimiento Facial en el riesgo de suplantación de identidad en el Colegio de Ingenieros del Perú, Lima?	Demostrar si la Tecnología de reconocimiento facial influye en el riesgo de suplantación de identidad en el Colegio de Ingenieros del Perú, Lima.	La Tecnología de reconocimiento facial influye significativamente e en la suplantación de identidad en el Colegio de Ingenieros del Perú, Lima.	<p>Variable dependiente:</p> <p>Y= Riesgo de suplantación de identidad</p> <p>Dimensiones:</p> <p>Riesgo de estafas</p>	Según (Borghello & Temperini, 2017) La identidad, conjunto de patrones y características detalladas el cual hacen única en la identificación de la persona en Internet. Es una forma única en la identidad de cada persona, bajo su rasgo dinámico y sobre todo en un aspecto social, moral y psicológico.	Es la capacidad de validar la identidad facial de un ciudadano ante la base de datos de RENIEC. Para evitar la suplantación se realizará una prueba de vida.
¿De qué manera la trazabilidad de la identidad influye en el riesgo de suplantación de identidad en el Colegio de Ingenieros del Perú, Lima?	Demostrar si la trazabilidad de la identidad influye en el riesgo de suplantación de identidad en el Colegio de Ingenieros del Perú, Lima.	La trazabilidad de la identidad influye significativamente e en el riesgo de suplantación de identidad en el Colegio de Ingenieros del Perú, Lima.			

Anexo 3. Matriz de Operacionalización

Variab les	Dimensión	Indicador	Ítem	Escala	Instrumento	
Variable Independiente La firma electrónica basado en reconocimiento facial	Dimensión 1: Verificación de Identidad	Nivel de Desempeño	¿Considera Ud. que ante un trámite y solicitud de captura biométrica las huellas son identificadas con facilidad?	1=Nunca; 2=Casi Nunca; 3=A veces; 4=Casi Siempre; 5=Siempre	Encuesta	
			¿Cuál de los siguientes métodos biométricos ha utilizado Ud. con mayor frecuencia para la autenticación de identidad?	1=Dactilar; 2=Facial; 3=Iris; 4=Voz; 5=Palma de la Mano	Encuesta	
		Nivel de Precisión	¿Cuál es el nivel de precisión que Ud. tiene conocimiento respecto a la captura dactilar?	1=No es preciso; 2=Casi nunca es preciso; 3=A veces es preciso; 4=Casi siempre es preciso; 5=Siempre es preciso	Encuesta	
			¿Cuál es el nivel de precisión que Ud. tiene conocimiento respecto a la captura facial?	1=No es preciso; 2=Casi nunca es preciso; 3=A veces es preciso; 4=Casi siempre es preciso; 5=Siempre es preciso	Encuesta	
			Nivel de Seguridad	¿Considera Ud. que la biometría dactilar para la validación de identidad es segura?	1=Nunca; 2=Casi Nunca; 3=A veces; 4=Casi Siempre; 5=Siempre	Encuesta
		¿Considera Ud. que la biometría facial para la validación de identidad es segura?		1=Nunca; 2=Casi Nunca; 3=A veces; 4=Casi Siempre; 5=Siempre	Encuesta	
		¿Consideraría Ud. usar un método de validación de identidad sin contacto?		1=Nunca; 2=Casi Nunca; 3=A veces; 4=Casi Siempre; 5=Siempre	Encuesta	
		Dimensión 2: Tecnología de Reconocimiento Facial	Nivel de Confiabilidad	¿Considera Ud. que el nivel de confianza de la biometría facial es óptimo para la verificación de identidad?	1=No Considero; 2=No tengo información para opinar; 3=Es Probable; 4=Muy Probable; 5=Es Segura	Encuesta
			Nivel de Exactitud	¿Cuál es el nivel de exactitud que la plataforma con Reconocimiento Facial certifica su firma?	1=0%; 2= 1% - 25%; 3=26 - 50%; 4=51% - 75%; 5=76% - 100%	Encuesta
	Nivel de aceptación por parte del usuario		¿Considera firmar documentos a través de una plataforma con Reconocimiento Facial?	1=Nunca; 2=Casi Nunca; 3=A veces; 4=Casi Siempre; 5=Siempre	Encuesta	
			¿Desearía Ud. instalar un componente en su computador para el Reconocimiento Facial?	1=Nunca; 2=Casi Nunca; 3=A veces; 4=Casi Siempre; 5=Siempre	Encuesta	
			¿Considera importante hacer uso de una plataforma de firma electrónica con Biometría Facial en	1=Nunca; 2=Casi Nunca; 3=A veces; 4=Casi Siempre; 5=Siempre	Encuesta	

			reemplazo de la firma tradicional?		
	Dimensión 3: Trazabilidad de la identidad	Trazabilidad de la Información	¿Considera Ud. saber dónde se encuentra el documento dentro de la plataforma luego de su firma?	1=La Plataforma no guarda documentos; 2=La Plataforma ocasionalmente guarda documentos; 3=La plataforma probablemente guarda documentos; 4=La plataforma debe guardar documentos; 5=La plataforma siempre guarda documentos	Encuesta
		Integridad de la Información	¿Cree Ud. que sus datos biométricos faciales puedan ser suplantados?	1=Nunca; 2=Casi nunca; 3=A veces; 4=Casi siempre; 5=Siempre	
Variable Dependiente Riesgo de suplantación de identidad	Dimensión 1: Riesgo de Estafas	Cantidad de Estafas por tipo de suplantación	¿Cuál es el nivel de suplantación que Ud. tiene conocimiento sobre un documento nacional de Identidad (DNI)?	1=0%; 2=1% - 25%; 3=26% - 50%; 4=51% - 75%; 5=76% - 100%	Encuesta
		Nivel de Pérdida Económica	¿Ante una posible suplantación y clonación de identidad, cuanto cree que podría perder utilizando su nombre?	1=Menos de S/1,000; 2=De S/ 1,001 a S/3,000; 3=De S/3,001 a S/10,000; 4=De S/10,001 - S/50,000; 5=Más de S/50,000 3=De S/3,001 a S/10,000; 4=De S/10,001 - S/50,000; 5=Más de S/50,000 5=más de S/100,000	