



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería Electrónica y Eléctrica

Escuela Académico Profesional de Ingeniería Electrónica

**Análisis comparativo de seguridad y experiencia
usuaria entre los lectores biométricos y la cámara del
celular contra huellas de polímero**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero Electrónico

AUTOR

Leandro Alonso DE LA CRUZ SOSA

ASESOR

Rafael BUSTAMANTE ALVAREZ

Lima, Perú

2021



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

De la Cruz, L. (2021). *Análisis comparativo de seguridad y experiencia usuaria entre los lectores biométricos y la cámara del celular contra huellas de polímero*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Académico Profesional de Ingeniería Electrónica]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Leandro Alonso De la Cruz Sosa
Tipo de documento de identidad	DNI
Número de documento de identidad	76219976
URL de ORCID	No aplica
Datos de asesor	
Nombres y apellidos	Rafael Bustamante Álvarez
Tipo de documento de identidad	DNI
Número de documento de identidad	09377230
URL de ORCID	https://orcid.org/0000-0003-3208-9356
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Teresa Nuñez Zuñiga
Tipo de documento	DNI
Número de documento de identidad	08006778
Miembro del jurado 1	
Nombres y apellidos	Rejis Renato Paredes Peñafiel
Tipo de documento	DNI
Número de documento de identidad	06758404
Miembro del jurado 2	
Nombres y apellidos	Wilbert Chavez Irazabal
Tipo de documento	DNI
Número de documento de identidad	08121733
Datos de investigación	

Línea de investigación	No aplica
Grupo de investigación	No aplica
Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	Edificio: Universidad Nacional Mayor de San Marcos País: Perú Departamento: Lima Provincia: Lima Distrito: Cercado de Lima Calle: Av. Carlos German Amenazaga 375 Latitud: -12.05636 Longitud: -77.08144
Año o rango de años en que se realizó la investigación	Diciembre 2019 - Diciembre 2020
URL de disciplinas OCDE	Ingeniería eléctrica, ingeniería electrónica https://purl.org/pe-repo/ocde/ford#2.02.01 Química inorgánica, Química nuclear https://purl.org/pe-repo/ocde/ford#2.07.04



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezaga 375 – Lima 1 – Perú



UNMSM

Firmado digitalmente por PAREDES
PENAFIEL Rejis Renato FAU
20148092282 hard
Motivo: Soy el autor del documento
Fecha: 29.12.2021 11:57:47 -05:00



ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL Nº 056/FIEE-EPIE/2021

Los suscritos Miembros del Jurado, nombrados por la Comisión Ejecutiva del Programa de Perfeccionamiento Profesional de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha, bajo La Presidencia De la **Dra. Nuñez Zuñiga, Teresa** integrado por **Mg. Paredes Peñafiel Rejis Renato** y **Mg. Chavez Irazabal Wilbert**.

Después de escuchar la Sustentación de Trabajo de Suficiencia Profesional del **Bach. DE LA CRUZ SOSA, LEANDRO ALONSO** con código N° **12190147** que para optar el Título Profesional de Ingeniero Electrónico sustentó su Trabajo de Suficiencia Profesional titulado **ANÁLISIS COMPARATIVO DE SEGURIDAD Y EXPERIENCIA USUARIA ENTRE LOS LECTORES BIOMÉTRICOS Y LA CÁMARA DEL CELULAR CONTRA HUELLAS DE POLÍMERO**.

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió **aprobar** otorgándole el calificativo de quince (15)

Ciudad Universitaria, 11 de diciembre del 2021

Dra. Nuñez Zuñiga, Teresa
Presidente de Jurado

Mg. Paredes Peñafiel, Rejis Renato
Miembro de Jurado

Mg. Chavez Irazabal Wilbert
Miembro Jurado

DEDICATORIA

Este trabajo está dedicado a mi familia que ha estado conmigo apoyándome en todo momento y principalmente por haberme inculcado los valores que me han llevado por el buen camino. Por eso les dedico este trabajo a ellos.

AGRADECIMIENTOS

Agradezco mucho a mis profesores y a mis compañeros que me han ayudado con su conocimiento, los cuales fueron fundamentales para la realización de este trabajo.

RESUMEN

En esta investigación se muestra el problema de fraude que afrontan las empresas de telecomunicaciones cuando realizan validaciones biométricas para la venta de servicios en las calles. También se describe los conceptos básicos sobre el funcionamiento de los lectores biométricos y qué tipos se usan para la validación en el entorno mencionado anteriormente para poder entender la importancia de estos equipos biométricos para la seguridad en las ventas y evitar las posibles sanciones por parte del MTC. Además, se detalla el proceso de testeo de lectores biométricos frente a ataques de presentación de huellas falsas, también se realizarán pruebas para asegurarse de que las huellas falsas sean de buena calidad y si presentan un riesgo para un sistema sin detección de huella falsa. Se realizarán los pasos del método test spoofing para determinar las métricas necesarias llamadas IAPMR y BPCER, estas métricas nos ayudarán a evaluar el nivel de seguridad y facilidad de uso de cada uno de los dispositivos testeados. Finalmente se usarán los datos obtenidos para compararlas entre los lectores biométricos y poder determinar cuál de todos los lectores biométricos usadas resulta el más adecuado para las empresas de telecomunicaciones dependiendo si le da prioridad a la seguridad o a la experiencia usuaria.

Palabras claves: Minucia, huella falsa, spoofing, lectores biométricos, tasas.

ABSTRACT

This research shows the fraud problem faced by telecommunications companies when they perform biometric validations for the sale of services on the streets. It also describes the basic concepts about the operation of biometric readers and what types are used for validation in the environment mentioned above in order to understand the importance of these biometric devices for security in sales and avoid possible sanctions by the MTC. In addition, the process of testing biometric readers against false fingerprint attacks is detailed, tests will also be carried out to ensure that the false fingerprints are of good quality and if they present a risk for a system without false fingerprint detection. The steps of the test spoofing method will be carried out to determine the necessary metrics called IAPMR and BPCER, these metrics will help us evaluate the level of security and ease of use of each of the tested devices. Finally, the data obtained will be used to compare them between the biometric readers and to be able to determine which of all the biometric readers used is the most suitable for telecommunications companies depending on whether it gives priority to security or user experience.

Keywords: Minute, false fingerprint, spoofing, biometric readers, rates

TABLA DE CONTENIDO

DEDICATORIA.....	ii
AGRADECIMIENTO	iii
RESUMEN.....	iv
ABSTRACT	v
TABLA DE CONTENIDO	vi
ÍNDICE DE FIGURAS.....	ix
ÍNDICE DE TABLAS.....	xi
CAPITULO I: INTRODUCCIÓN	1
1.1 Trayectoria profesional	4
CAPITULO II: CONTEXTO EN EL QUE SE DESARROLLA LA EXPERIENCIA.....	6
2.1 Empresa.....	6
2.2 Visión.....	6
2.3 Misión	6
2.4 Área, Cargo y Funciones Desempeñadas.....	6
2.5 Experiencia Profesional realizada en la organización.....	7
CAPITULO III: ACTIVIDADES DESARROLLADAS.....	8
3.1 Situación del Problema	8
3.1.1 Determinación del Problema.....	9

3.1.2 Formulación del Problema	10
3.2 Solución	11
3.2.1 Objetivos	12
3.2.2 Alcance.....	12
3.2.3 Metodología y Etapas.....	13
3.2.4 Fundamentos Utilizados.....	16
3.2.4.1 Biometría	16
3.2.4.2 Plantilla biométrica	19
3.2.4.3 Sensor biométrico.....	21
3.2.4.4 Sensor capacitivo	22
3.2.4.5 Sensor óptico	25
3.2.4.6 Reconocimiento de huella digital sin contacto.....	27
3.2.4.7 Requerimientos	31
3.2.5 Test Spoofing	33
3.2.5.1 Clonación de huella.....	33
3.2.5.2 Material	34
3.2.5.3 Fabricación de huella	34
3.2.6 Recolección y procesamiento de datos	35
3.2.6.1 Test de calidad.....	35
3.2.6.2 Tasas	36
3.3 Reflexión crítica de la experiencia	37
3.3.1 Etapa de Recolección	38

3.3.2 Clonación de huellas	39
3.3.3 Test de calidad.....	40
3.3.4 Test IAPMR	41
3.3.5 Test BPCER	43
CAPITULO IV: CONCLUSIONES.....	46
CAPITULO V: RECOMENDACIONES	47
CAPITULO VI: BIBLIOGRAFÍA.....	48
6.1 Fuentes de información.....	48
6.2 Glosario	52
ANEXOS	55

ÍNDICE DE FIGURAS

FIGURA 1: Tabla de Infracciones del MTC	1
FIGURA 2: Objetos incautados a falsificadores de huellas digitales.	9
FIGURA 3: Reconocimiento facial.	17
FIGURA 4: Conversión de coordenadas cartesianas a polares.	17
FIGURA 5: Extracción de patrones para reconocimiento de voz.	18
FIGURA 6: Tipos de huellas a nivel global.	20
FIGURA 7: Minucias biométricas.	20
FIGURA 8: Código de producto EikonTouch710.	23
FIGURA 9: Diagrama de bloques del sensor TCS1CM.	24
FIGURA 10: Lector biométrico EikonTouch710.	24
FIGURA 11: Sensor TCS1CM.	25
FIGURA 12: Sensor CBM E3.....	25
FIGURA 13: Funcionamiento del sensor óptico.....	26
FIGURA 14: Diagrama de bloques de CCD.	27
FIGURA 15: Diagrama de bloques de CMOS.	27
FIGURA 16: Selección de huella sugerida a capturar.....	28
FIGURA 17: Método de captura de huellas.....	29
FIGURA 18: Captura de huella exitosamente	30
FIGURA 19: Captura de huella fallida, huella falsa detectada.	30
FIGURA 20: Huella falsa.	35

FIGURA 21: Página web de Reniec para consultas de huellas sugeridas.....	39
FIGURA 22: Huella capturada y huella en negativo. (no pertenecen a una persona)	40
FIGURA 23: Huella falsa colocada sobre dedo índice.....	41
FIGURA 24: Ingreso de DNI y selección de huella.	42

ÍNDICE DE TABLAS

TABLA 1: Características principales de cada lector biométrico	31
TABLA 2: Requerimientos de cada lector biométrico.....	32
TABLA 3: Cuadro de actividades.....	37
TABLA 4: Resultados de test de calidad de huella.	41
TABLA 5: Resultados del test IAPMR.....	42
TABLA 6: Resultados del test BPCER.....	44

CAPÍTULO I: INTRODUCCIÓN

La suplantación de identidad es un problema que ha estado presente muchos años. En el Perú ha habido muchas quejas de personas que fueron suplantadas por delincuentes debido al bajo control de seguridad en la venta de líneas telefónicas ya que anteriormente no era obligatorio identificar al cliente, esto facilitaba realizar muchos delitos como fraude, suplantación de identidad, extorsión, etc.

A partir del Decreto Supremo N°023-2014-MTC de OSIPTEL [1], el cual obliga a las empresas de telecomunicaciones a verificar la identidad de sus clientes con su huella dactilar, se empezó a tomar más control de la venta de servicios de líneas telefónicas.

En una nota en línea de Perú21 [2], nos informan sobre la clonación de huellas dactilares, se creía que el uso de lectores biométricos evitaría las suplantaciones, pero recientes informes de la División de Investigación Criminal de Lima Sur de la Dirincri han puesto al descubierto a criminales que usaban huellas de polímero para poder vulnerar estos equipos y realizar compras de celulares de alta gama.

Es por eso que en esta investigación determinaremos cuál de los lectores biométricos resulta ser más recomendable para evitar las suplantaciones sin afectar la experiencia de uso de los usuarios. Además, se evitarán las sanciones impuestas por el Ministerio de transportes y comunicaciones al no cumplir con las normas de seguridad impuestas por OSIPTEL en la Ley N°27336[3].

Infracción	Multa mínima	Multa máxima
Leve	0.5 UIT	50 UIT
Grave	51 UIT	150 UIT
Muy grave	151 UIT	350 UIT

Figure 1. Tabla de Infracciones del MTC.

Uno de las primeras investigaciones que se encontró útil debido a su alta relación con la biometría dactilar pertenece a Ortiz (2010), a través de su tesis: “Mejora de imágenes de huellas digitales”, realiza una descripción detallada de aquellas características que se deben de tomar en cuenta para considerar de buena calidad a una huella dactilar. El estudio busca crear un algoritmo para poder realzar o aclarar estas características que se pueden perder al colocar mal la huella. La investigación fue experimental ya que tomó 53 muestras de huellas de baja calidad, logrando realzar el 87% de las muestras, el resto de huellas no pudo ser realzada porque tenían zonas demasiado borrosas debido al movimiento del dedo sobre el sensor. Se consideró importante esta tesis debido a que aquí se puede encontrar aquellas características de las huellas que pueden ser copiadas con mayor detalle para hacer una huella falsa de mayor calidad. Además, se llega a la conclusión de que la obtención de huellas de alta calidad no es fácil, ya que, si solo se cuenta con una porción de esta, entonces la huella será no recuperable y de baja calidad.

Un artículo relevante llamado “Reconocimiento de huella dactilar sin contacto” publicado en el Innovative Journal, el cual publica artículos sobre investigaciones tecnológicas, investigó sobre una nueva tecnología que usaba la cámara del celular para realizar la captura de huellas dactilares, los autores Shah & Poshiya (2013) presentaron diversos problemas que se solucionarían con este nuevo método de captura, tales como higiene, mantenimiento de equipos y huellas digitales latentes sobre el sensor. Después de mostrar el proceso por el que pasa la huella desde la captura hasta la verificación de la huella, se obtiene un 76% de similitud a la huella original, llegando a la conclusión que la captura es buena como para ser verificada fácilmente dependiendo de las condiciones de iluminación del entorno.

El segundo artículo enfocado en la captura de huella por cámara se llama “Reconocimiento de huella dactilar con cámaras incorporadas a teléfonos móviles” escrito por Derawi, Yang, & Busch (2012), este artículo se centraba en el alto progreso de las cámaras de los dispositivos móviles y como estos ayudarían a realizar el reconocimiento de captura de huellas dactilar entre otros rasgos biométricos. El objetivo principal es dar a conocer que esta tecnología puede reemplazar el uso de claves, token me, PINs, etc. Considerando el gran avance de la calidad de los celulares y el hecho de que cualquier persona tendría el acceso a la validación biométrica en sus manos, haría que esta tecnología mejore y se expanda rápidamente. Según los autores:

En un futuro de la computación verdaderamente generalizada, cuando se puede incrustar hardware pequeño y económico en varios objetos, este método también podría usarse para proteger valiosos objetos. Además, los dispositivos móviles autenticados de manera confiable también pueden servir como autenticación automatizada en relación con otros sistemas como el sistema de control de acceso o el inicio de sesión automático del sistema externo”. (Derawi, et al., 2012, p.11).

En el trabajo de Akhtar (2012) llamado “Seguridad de sistemas biométricos multimodales contra ataques de impostores” se explica las vulnerabilidades de distintos sistemas de biometría, entre ellas la biometría dactilar. También evalúa la seguridad de estos sistemas frente a ataques de suplantación de identidad. Akhtar llega a la conclusión de que aún están en una etapa temprana para el tratamiento en sistemas adversos, además menciona que el ataque directo realizado a los sensores llamado “Spoof Attack”, no necesita de técnicas avanzadas para realizarlas, por lo tanto, es la técnica más común que emplearía algún impostor para vulnerar esos equipos. En este experimento, hay que recalcar que el autor realizó las pruebas colocándose en el peor de los casos, ya que realizó huellas falsas de buena calidad con la autorización del propietario, lo cual no sucedería en un caso real.

La empresa Synaptics (2016) expone las formas de falsificar huellas digitales y como protegerse de ellas. En el White Paper “Protección contra suplantación de huellas dactilares en dispositivos móviles” se llega a la conclusión que la creciente dependencia de los dispositivos móviles para realizar compras y otras transacciones requieren de una autenticación segura, a la cual también debe darse una importancia creciente, es por eso que en mucho de los casos se suele usar hasta más de un tipo de método de seguridad.

CAPÍTULO II: CONTEXTO EN EL QUE SE DESARROLLÓ LA EXPERIENCIA

2.1 Empresa

In Solutions SAC es una empresa de servicios y tecnologías de la información que se dedica a cubrir las necesidades de seguridad tecnológica de las empresas a través de soluciones tecnológicas e innovadoras, ayudándolos a resolver los complejos problemas que enfrenta el negocio durante las transformaciones digitales.

2.2 Visión

La visión de negocio de la empresa es ser innovadores en el mercado local con soluciones que faciliten los procesos de los usuarios y les brinden seguridad, busca establecerse en los principales mercados del mundo para lo cual cuentan con alianzas con las principales empresas del mundo en el rubro de transformación digital que cambiarán fundamentalmente la forma en la que operan las empresas en el Perú, incrementando su valor y preparándolas para tiempos de constante cambio.

2.3 Misión

La misión de la empresa es cumplir con las exigencias del mercado y de los clientes en tiempos de transformación digital, integrando tecnología en las diferentes áreas de sus empresas y garantizando la protección de su información por medio del uso de la tecnología, biometría dactilar, biometría facial, firma digital acreditada ante

Indecopi, biometría sin contacto y desarrollo de software.

2.4 Área, Cargo y Funciones Desempeñadas

Área: Soporte

Cargo: Ingeniero de soporte

Funciones:

- Capacitación a clientes (empresas de telecomunicaciones, logística y mensajería) a nivel de usuario sobre el uso de aplicaciones de identificación biométrica.
- Soporte al cliente frente a dudas o incidencias con las aplicaciones y equipos.
- Mantenimiento de sensores de lectores biométricos EikonTouch710.
- Registro de fechas de habilitación de equipos y elaboración de la facturación mensual.
- Realizar pruebas de calidad de los equipos y aplicaciones.

2.5 Experiencia Profesional realizada en la organización

Ingeniero de soporte

Datos de la persona a cargo:

Jonmar Pérez Carrasco

Director de Tecnología

jonmar.perez@insolutions.pe

CAPÍTULO III: ACTIVIDADES DESARROLLADAS

3.1 Situación del Problema

La suplantación de identidad es un problema que ha estado presente muchos años. En otros países se ha implementado la tecnología biométrica dactilar para el reconocimiento de personas, principalmente para sistemas de seguridad de entidades públicas como la policía. Según Akhtar (2012), el ataque directo a un sensor por medio de una huella falsa es la forma más común de intentar vulnerar el equipo, ya que no necesita de técnicas avanzadas para lograrlo.

En el white paper titulado “Protección contra suplantación de huellas dactilares en dispositivos móviles” de la empresa Synaptics (2016), se indica que la capacidad de falsificar huellas dactilares se demostró después que Apple incorporase un lector de huellas en su celular y esta solución se volviera popular en los teléfonos inteligentes. Actualmente las huellas dactilares son la forma más común para realizar algunas transacciones y compras, además el uso de la biometría se ha ampliado a otros sectores.

En los últimos años ha habido muchas quejas de personas que fueron suplantadas por delincuentes debido al bajo control de seguridad en la venta de líneas telefónicas, esto facilitaba realizar muchos delitos como fraude, suplantación de identidad, extorsión, etc. Rafael Munte, el presidente del consejo directivo de Entel, declaró en una entrevista al diario La Reública (17 de junio del 2019) sobre la regulación del mercado de las telecomunicaciones; uno de los principales temas que se tocó fue el Decreto Supremo N°023-2014-MTC de OSIPTEL (2014), el cual obliga a las empresas de telecomunicaciones a verificar la identidad de sus clientes con su huella dactilar. En esta entrevista él menciona que estas normas están relacionadas a temas de seguridad, debido a que muchas personas descubrieron que tenían hasta 30 líneas a su nombre.

por las multas a las empresas de telecomunicaciones, ya que ellas son responsables del proceso de identificación y registro de sus clientes; además las empresas de telecomunicaciones podrían también ser víctimas de delincuentes que pueden realizar numerosas compras de equipos o utilizar sus servicios para cometer crímenes (extorsiones) desde el anonimato.

Así mismo, las personas suplantadas contraerían grandes deudas por compras que no hicieron y esto haría que la empresa reciba reclamos, generando problemas tanto al cliente como a la empresa. Esto claramente perjudica la imagen de la empresa al no ofrecer sus servicios y productos de manera confiable.

3.1.2 Formulación del Problema

Problema General

¿Cuál es el lector biométrico más seguro y práctico para las empresas de telecomunicaciones para la prevención de suplantación de identidades?

Problemas Específicos

¿Cuál es el procedimiento para realizar un test de anti-spoofing a un lector biométrico?

¿Qué consideraciones tomar en la elaboración de un molde de huella para poner a prueba los lectores biométricos?

¿Cuáles son los factores que nos ayudan en la medición y selección de un método de identificación biométrica?

3.2 Solución

La información obtenida al realizar las pruebas de ataques de huella falsa a los métodos de validación biométricas nos va a ayudar a elegir la mejor opción para utilizar en la venta de servicios. Por otro lado, teniendo en cuenta el problema de salud en el que se encuentra el mundo, esta investigación podría aportar información para tomar medidas en el sector salud evitando contagios, realizando mantenimientos adecuados y cumpliendo con las normas dictadas por el gobierno, las cuales veremos a continuación.

Se han realizado decretos supremos para acabar con los constantes delitos cometidos por personas que no se registran con su nombre y suplantan la identidad de otras, los cuales deberán ser acatados por las empresas que brindan servicios públicos móviles. El trabajo también brinda un beneficio social, ya que se evitará que personas inocentes sean acusadas por estafa, por culpa de personas que toman sus huellas dactilares para solicitar líneas de teléfono o equipos de alta gama.

Las empresas de telecomunicaciones podrán cumplir con el Decreto Supremo N°023-2014-MTC de OSIPTEL (2014) el cual menciona lo siguiente:

“Las empresas operadoras son responsables de todo el proceso de contratación de los servicios públicos de telecomunicaciones que provean, que comprende la identificación y el registro de los abonados que contratan sus servicios”. (p. 1)

Según el Decreto Supremo N°003-2016-MTC (2016, p. 23), el incumplimiento de la norma impone sanciones (Anexo 4) a la empresa de telecomunicaciones dependiendo de la gravedad de la infracción cometida. En el artículo 25 del título III de la Ley N°27336 (27 de julio del 2000), las multas no pueden exceder el 10% de los ingresos brutos y tienen un mínimo y máximo según la infracción cometida como se ve en la figura 1.

Estas normas buscan que el proceso de venta de los productos o servicios sea bien implementado y confiable. Al mejorar la seguridad, la empresa se evitará las multas y maximizará las ganancias, además ofrecerá un servicio de calidad a sus clientes. Se muestra en esta investigación los beneficios de cada una de las alternativas, para que, a juicio del usuario, se establezca lo conveniente según su criterio.

3.2.1 Objetivos

Objetivos General

Determinar el rendimiento de los lectores biométricos y la cámara del celular frente a ataques de impostores con huellas falsas.

Objetivos Específicos

Comparar los niveles de seguridad y uso de los lectores biométricos testeados.

Obtener las métricas necesarias para cuantificar el nivel de seguridad y de experiencia usuaria de los lectores biométricos usados.

Determinar cuáles son los lectores biométricos más recomendables y seguros.

3.2.2 Alcance

Población

La población son todas aquellas transacciones de personas que son identificadas biométricamente con los lectores biométricos antes mencionados capturando las huellas dactilares de los clientes para la venta de servicios móviles.

Muestra

Debido a que la cantidad de transacciones que se pueden hacer en el mercado es demasiada grande e indeterminada, se calculará la muestra de una población desconocida con la siguiente fórmula:

$$N = \frac{Z^2 \sigma^2}{E^2}$$

Donde:

- N = N° de pruebas
- Z = 2.58 (Factor de confianza para 99%, alfa=0.005)

- $\sigma = 5\%$ (desviación del resultado promedio, que tan cerca al resultado promedio de las comparaciones esperadas)
- $E = 3\%$ (Error esperado en las comparaciones)

Reemplazando valores y operando, nos da como resultado:

$$N = \frac{2.58^2(0.05)^2}{0.03^2}$$

$$N = 18.49$$

Redondeamos el valor de N a 20 porque el redondeo es a favor del estudio. Por lo tanto, el número de muestra que es tomará en cuenta para las pruebas será de 20 muestras.

3.2.3 Metodología y etapas

Descriptiva y tecnológica

Debido al alcance de esta investigación, es considerada del tipo descriptiva ya que presentamos las características de un grupo de métodos de identificación biométrica que nos proporcionan conocimientos para predecir resultados. Según Hernandez, Fernandez & Baptista (2014, p. 71), "Miden y evalúan diversos aspectos, dimensiones o componentes del fenómeno o fenómenos a investigar. Desde el punto de vista científico, describir es medir".

También es considerada tecnológica ya que estamos aprovechando los conocimientos teóricos que son producto de las investigaciones básicas para exponer las ventajas y desventajas de las alternativas de biometría y encontrar el método biométrico adecuado dependiendo de la situación.

Para el experimento tendremos las muestras genuinas y falsas correspondientes a los voluntarios, luego se ejecutará el siguiente proceso:

La huella falsa de cada usuario se crea a través de sus muestras de cada voluntario.

Se comparan las muestras de acceso de cada usuario con su muestra biométrica en Reniec.

Las muestras de huellas falsas se comparan con el modelo biométrico de los usuarios que están intentando suplantar, proporcionando una tabla de puntuaciones impostoras.

Las muestras de huellas reales se comparan con el modelo biométrico de los usuarios que están intentando suplantar, proporcionando una tabla de puntuaciones de huellas reales que fueron clasificadas como falsas incorrectamente.

Ambas tablas de puntuaciones servirán para obtener las tasas IAPMR y BPCER antes mencionadas. Para la comparación de los resultados de las pruebas entre sistemas biométricos usaremos el estándar ISO/IEC 30107-3. La norma ISO/IEC 30107-3 se refiere a la detección de ataques biométricos, donde usaremos los términos Tasa de coincidencia de presentación de ataque de impostor (IAPMR, por sus siglas en inglés) y Tasa de error de clasificación de presentación de buena fe (BPCER, por sus siglas en inglés). Estos valores son usados para medir la seguridad del sistema biométrico y la experiencia usuaria del cliente.

Método comparativo

El método usado en esta investigación es el método comparativo debido a las ventajas que nos brinda para determinar las ventajas y desventajas de cada lector biométrico, según Gómez y De León (2014, p. 229) “entre las ventajas que ofrece el método comparativo se cuentan el comprender cosas desconocidas a partir de las conocidas, la posibilidad de explicarlas e interpretarlas, perfilar nuevos conocimientos, destacar lo peculiar de fenómenos conocidos, sistematizar la información distinguiendo las diferencias con fenómenos o casos similares”.

En ese mismo documento nos explica las etapas del método comparativo, los cuales se tomarán en cuenta para esta investigación. En la primera etapa, se definirán las propiedades y características relevantes al experimento que se va a realizar. En este caso, se ha escogido la validación biométrica por huella dactilar y se ha tomado el tipo de sensor biométrico como característica principal para dividir a este grupo.

En la segunda etapa, definiremos los elementos que se escogerán según los criterios establecidos en la etapa anterior. Estos elementos son los 3 tipos de lectores biométricos usados por las empresas durante la venta de servicios de líneas telefónicas y el polímero como material usado para las pruebas de seguridad.

Finalmente se analizarán los datos obtenidos en los experimentos para luego determinar las conclusiones gracias a las etapas previas donde se recopiló datos y se evaluaron para obtener las diferencias y semejanzas de las variables. Los datos usados para el análisis son las tasas de coincidencia de presentación de ataque de impostor (IAPMR, por sus siglas en inglés) y de error de clasificación de presentación de buena fé (BPCER, por sus siglas en inglés).

Diseño experimental

Para esta investigación se ha utilizado un diseño experimental, de acuerdo a Fleiss (2013), O'Brien (2009) y Green (2003) citado por Hernandez, Fernandez & Baptista (2014, p.129) en su libro "Metodología de la investigación" se menciona que "Una acepción particular de experimento, más armónica con un sentido científico del término, se refiere a un estudio en el que se manipulan intencionalmente una o más variables independientes (supuestas causas antecedentes), para analizar las consecuencias que la manipulación tiene sobre una o más variables dependientes (supuestos efectos consecuentes), dentro de una situación de control para el investigador".

Nuestras variables independientes que hemos manejado durante el experimento son los sistemas de detección de huellas de los lectores biométricos, los cuales son puestos a prueba y se les introducen huellas falsas de polímero por el sensor biométricos, estos son llamadas ataques de presentación. Los ataques de presentación fueron creados a partir de las plantillas biométricas de alta calidad obtenidas de voluntarios, los materiales, el método de clonación de huella y el procesamiento de la huella para mejorar su definición de las líneas de los valles y las crestas, todo esto detallado anteriormente en el marco teórico.

Todas estas variables introducidas generan una serie de resultados, los cuales se han anotado en las tablas 5 y 6 para obtener las métricas que nos ayudará a analizar y comparar el nivel de seguridad y experiencia usuaria de los sistemas de detección de huella falsa de los lectores biométricos y la cámara del celular. Estas métricas son los resultados de nuestras pruebas al haber introducido huellas falsas en cada sistema biométrico utilizado por las empresas de telecomunicaciones mencionados

anteriormente, por lo tanto, son las consecuencias de los experimentos realizados, es por eso que son consideradas nuestras variables dependientes

Las métricas usadas para medir los niveles de seguridad y experiencia de los sistemas de detección de huellas son los IAPMR y BPCER, estos 2 valores son los que describen las 2 características que buscamos comparar y nos ayuda a cumplir nuestro objetivo de comparar el comportamiento de los sistemas de detección de huellas falsas de los lectores biométricos frente a ataques de presentación de huellas de polímero.

3.2.4 Fundamentos utilizados

3.2.4.1 Biometría : Según la norma ISO/IEC2382:2015 (2015), define biometría como “Pertenece al uso de atributos específicos que reflejan características personales únicas, como una huella digital, una impresión del vaso sanguíneo del ojo o una impresión de voz, para validar la identidad de una persona.”

Existen muchos sistemas biométricos que nos permiten reconocer ciertas características únicas de una persona. Estos sistemas pueden ser divididos según las características extraídas para la identificación biométrica. A continuación, mencionaremos los principales sistemas biométricos.

Biometría facial

La biometría facial es el uso de características del rostro para identificar a una persona mediante la comparación con una imagen ya previamente capturada y guardada en una base de datos. El sistema detecta el rostro y extrae las principales características, como por ejemplo, la distancia entre los ojos, la anchura de la boca, la anchura de la nariz, la forma de los pómulos, etc. Un algoritmo se encargará de traducir estas medidas y convertirlas en una plantilla biométrica, la cual servirá para reconocer y verificar la identidad, comparando la imagen con otra plantilla de la base de datos. Este sistema es usualmente utilizado para identificar a personas en grandes ciudades.

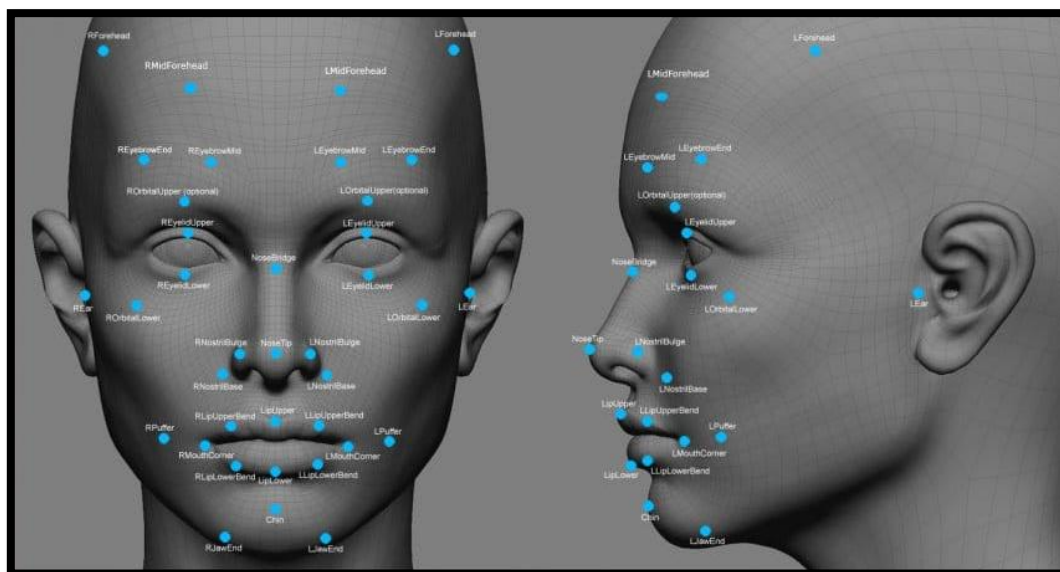


Figure 1. Reconocimiento facial. Recuperado de la página BaturaMobile.

Reconocimiento de iris

Es el método usado en los sistemas de biometría que capturan una imagen del patrón del iris con una cámara de iluminación infrarroja, a este patrón se le realiza una conversión de coordenadas cartesianas a coordenadas polares, de esta manera, la imagen pasa de una forma circular a una forma rectangular, para finalmente extraer la información necesaria para la identificación de la persona. En la actualidad se puede afirmar que es uno de los sistemas biométricos más eficientes debido a que la información ocupa muy poco espacio (256 bytes aproximadamente) y esto genera una alta velocidad de reconocimiento.

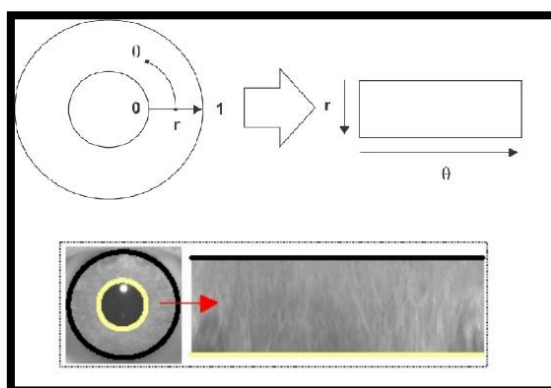


Figure 2. Conversión de coordenadas cartesianas a polares. Fuente Elaboración propia.

Reconocimiento de voz

El método de reconocimiento de voz consiste en la lectura de una o varias frases tomando en cuenta el timbre, la entonación, etc. La voz es comparada con los datos obtenidos anteriormente por parte del usuario enrolado en el momento de la validación. Este método está expuesto a ciertos factores externos que podrían afectar al resultado de la identificación, como por ejemplo el ruido, las enfermedades, el envejecimiento, entre otros.

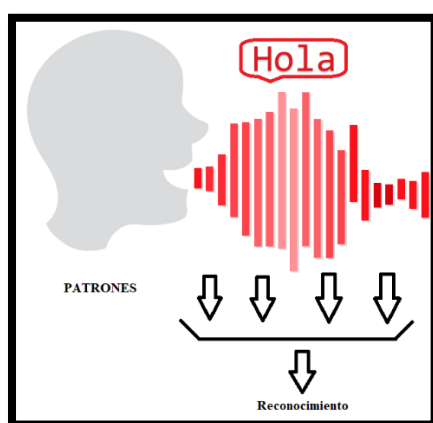


Figure 3. Extracción de patrones para reconocimiento de voz. Fuente Elaboración propia.

Biometría dactilar

La biometría dactilar es el método que utiliza las minucias biométricas del dedo, formadas por los valles y crestas, para identificar o validar la identidad de una persona. En la actualidad, es el método más común de los sistemas biométricos y cada vez se instalan más en distintas clases de dispositivos.

Al igual que las demás tecnologías, primero se debe obtener la huella para el proceso de enrolamiento de la persona y luego registrarlas en una base de datos, en este caso, la base de datos de RENIEC, la cual se encarga de organizar y mantener el Registro Único de Identificación de las Personas Naturales, lo que constituye el registro único y base de datos de identificación de todos los peruanos.

En el Perú todas las empresas de telecomunicaciones están obligadas a usar la verificación biométrica para verificar la identidad de aquellos clientes que deseen

contratar servicios de telefonía móvil, prepago, post pago, chips, recuperación de número y otros servicios complementarios. De esta manera, se evita realizar trámites engorrosos en donde el proveedor realiza una serie de preguntas, confirma los datos y pide algunos documentos, este tipo de biometría no solo genera facilidades a las empresas de telecomunicaciones sino también a otros sectores como notarías, bancos y couriers.

3.2.4.2 Plantilla biométrica: En el documento “Servicio de Verificación Biométrica” de RENIEC (2012) se detalla el servicio biométrico que brinda esta institución, además explica conceptos generales para comprender la biometría, señalando que “Las plantillas biométricas son la representación digital de una característica distintiva de un individuo, representan información extraída de una muestra biométrica.” (RENIEC, 2012, p. 69).

Las huellas dactilares proporcionan la información para la plantilla biométrica, las huellas son patrones generados por los valles y crestas de los dedos de las manos generando diversas configuraciones. La huella dactilar está presente en todas las personas del mundo y cada huella digital tiene un nivel muy alto de unicidad, es decir, no hay 2 personas con la misma huella. Estas no varían a través del tiempo y se regeneran cuando sufren lesiones leves, es por eso que la biometría dactilar es la más usada en el mercado.

Las huellas dactilares se pueden dividir en 2 grupos según las características analizadas a distintos niveles.

A nivel global

Los tipos de huellas dactilares en este nivel se pueden reconocer a simple vista. Este nivel de observación no nos ayuda mucho para la identificación biométrica ya que existen muchas personas que poseen el mismo tipo de huella a nivel global; pero sirve de ayuda para reconocer rápidamente cuando una persona no está colocando adecuadamente su huella. Los tipos de huellas son: Arco, lazo y remolino. Son nombrados de esta manera debido a su forma geométrica.



Figure 4. Tipos de huellas a nivel global. Fuente Elaboración propia.

A nivel local

La información que se extrae para la plantilla biométrica proviene de los detalles de las huellas dactilares, llamadas minucias. Estas minucias poseen la información necesaria para la validación e identificación biométrica, ya que las características de una minucia hacen que las huellas dactilares sean únicas. En la figura 7, veremos los tipos de minucias clasificadas por Reniec.

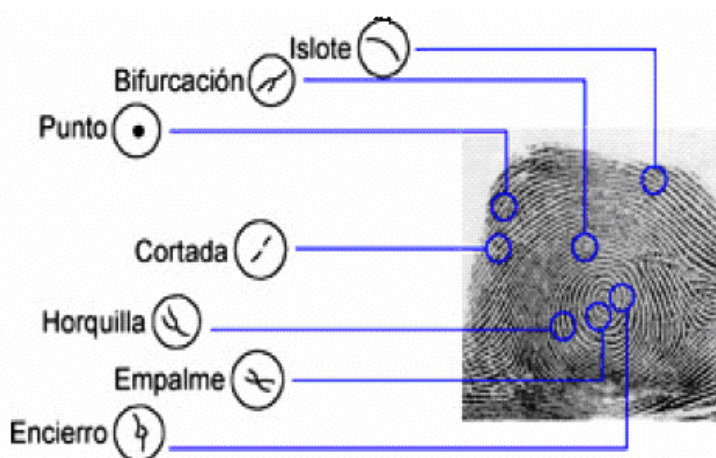


Figure 5. Minucias biométricas. Fuente Reniec.

- Islote: Es una cresta aislada sin bifurcación.
- Bifurcación: Es la cresta que viene del lado derecho de la huella dactilar y se divide en dos.
- Punto: Pequeño fragmento de cresta tan corto como ancho.

- Cortada: Es la discontinuidad de una cresta que presenta los extremos redondeados y cuya separación es aproximadamente del doble de la anchura de la cresta.
- Horquilla: Son dos crestas que vienen del lado izquierdo de la huella dactilar y se unen formando una sola.
- Empalme: Son dos crestas que unen en un punto y vuelven a dividirse para generar otra bifurcación.
- Encierro: Espacio formado por las dos ramas de una cresta bifurcada que vuelve a unirse.

Según Reniec (2012), existen cinco características de puntos de minucia, las cuales son tomadas en cuenta por el software encargado de la extracción de minucias:

“Crestas que finalizan y las crestas que crean bifurcaciones

Orientación: Cada punto de minucia se orienta en una dirección.

Frecuencia espacial: la frecuencia espacial se refiere a la densidad de las crestas en una superficie determinada.

Curvatura: Referente a la ratio de cambio de orientación de las crestas.

Posición: La posición de los puntos de minucia referentes a la localización en el plano x, y y también en concordancia a los puntos fijos”. (p. 69)

3.2.4.3 Sensor biométrico: Según la empresa Fingerprint (2019, p.17), define de la siguiente manera a los sensores biométricos: “un sensor de huellas digitales es un dispositivo electrónico utilizado para registrar una imagen digital del patrón de huellas digitales”.

Un sistema biométrico consta de un hardware y un software, en este caso, nos enfocaremos en la parte hardware del sistema ya que es ahí donde se realizan los ataques con huella falsa. Los lectores biométricos y la cámara del celular son parte del hardware del sistema biométrico, estos dispositivos son los encargados de capturar la data biométrica de la huella dactilar del individuo a verificar para que luego la minucia sea extraída y comparada con la almacenada en la base de datos.

La característica personal única que se usará será la huella dactilar y los dispositivos que evaluaremos serán las 3 herramientas de validación biométrica usadas para la venta de servicios móviles en las calles por las empresas de telecomunicaciones, los cuales son:

- EikonTouch710m (capacitivo)
- MSO 1300E3 (óptico)
- Veridium (cámara del celular)

El principal componente electrónico de los lectores biométricos es el sensor de huellas, el cual se encarga de capturar las características importantes de la huella dactilar. Los tipos de sensores se clasifican según su método de captura, cada persona o empresa decide qué tipo de sensor usar según sus necesidades y recursos disponibles, ya que algunos sensores pueden ser mucho más compactos, seguros o baratos.

3.2.4.4 Sensor capacitivo: Es uno de los tipos de sensores que se utiliza para la obtención de la huella dactilar, tal y como lo menciona la empresa Fingerprints (2019, p. 19) “un sensor capacitivo de huellas dactilares genera la imagen de la huella digital mediante el uso de una matriz que contiene miles de pequeñas placas de condensadores”. La superficie del dedo y los condensadores del sensor se comportan como placas paralelas de condensadores, ocasionando que se creen cargas eléctricas distintas debido a los valles y crestas del dedo.

Los lectores biométricos capacitivos usados en el Perú son los EikonTouch710, estos lectores poseen sensores TCS1CM. A continuación, veremos la información de estos sensores según su código de producto:

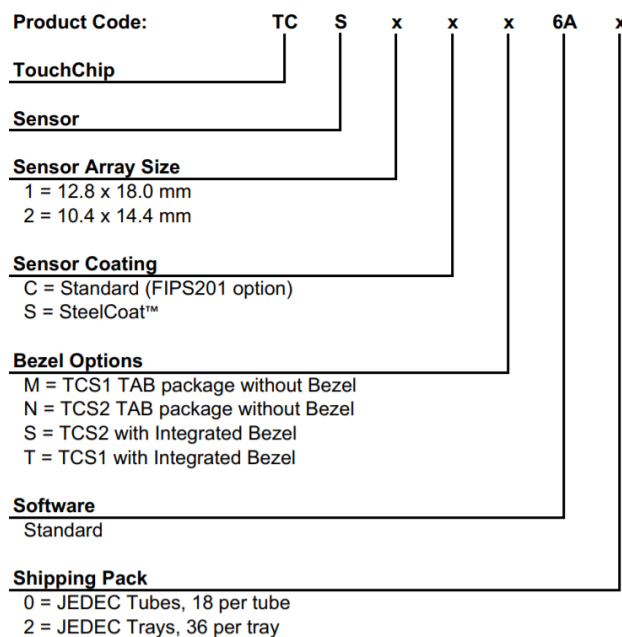


Figure 6. Código de producto EikonTouch710. Fuente In Solutions.

El diagrama de bloques de los sensores TCS1 y TCS2 posee un controlador de energía el cual evita picos de energía y permite que el dispositivo usa la energía eficientemente. También cuenta con un circuito que protege al dispositivo frente a descargas electrostáticas, esto es necesario ya que el sensor está en constante contacto con el usuario. La matriz de sensores capta las señales eléctricas generadas al colocar el dedo sobre el sensor y estas señales son convertidas a señales digitales y almacenadas a través de los conversores analógico/digital y los decodificadores respectivamente; de la misma manera, se envían señales digitales de vuelta para finalizar la captura de la huella.

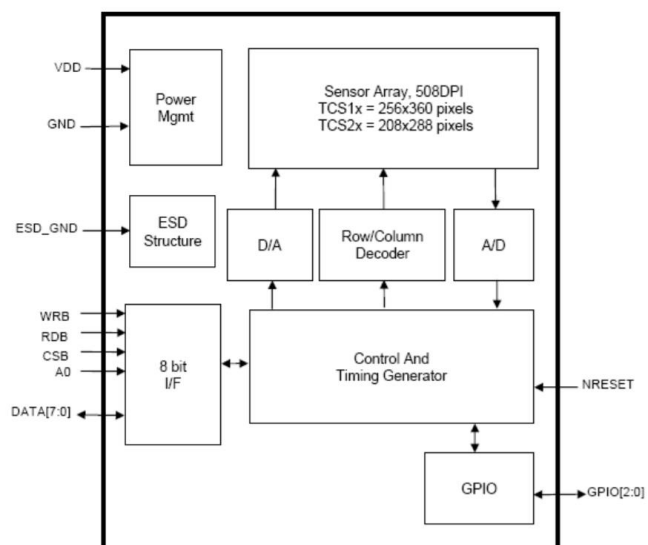


Figure 7. Diagrama de bloques del sensor TCS1CM. Fuente In Solutions.



Figure 8. Lector biométrico EikonTouch710. Fuente Elaboración Propia.



Figure 9. Sensor TCS1CM. Fuente In Solutions.

3.2.4.5 Sensor óptico: En la figura 11 vemos un sensor óptico CBM E3 el cual es del tipo óptico y son usados usado en los lectores MSO 1300 para la identificación de clientes en la venta de servicios móviles en la vía pública. La empresa Fingerprints (2019, p. 18) nos explica sobre el funcionamiento de este tipo de sensores, “Los sensores ópticos registran patrones de huellas digitales al capturar la luz visible y la convierten en señales eléctricas para crear la imagen de huella digital. Los sensores tienen conjuntos de fotodiodos o detectores de fototransistor que Convierta la energía en la luz que golpea el detector en carga eléctrica”.



Figure 10. Sensor CBM E3. Fuente In Solutions.

Estas es una de las tecnologías más populares y está basada en la reflexión total interna de la luz (FTIR, por sus siglas en inglés). Las crestas de los dedos entran en contacto con el vidrio, absorbiendo la luz; mientras que los valles de los dedos no entran en contacto con el vidrio, permitiendo que la luz sea reflejada y capturada por un dispositivo de carga acoplada (CCD, por sus siglas en inglés) o semiconductor

complementario de óxido metálico (CMOS, por sus siglas en inglés). Internamente una fuente de luz LED será la encargada de iluminar el otro lado del vidrio para que el detector pueda recibir y transformar las señales luminosas en señales eléctricas.

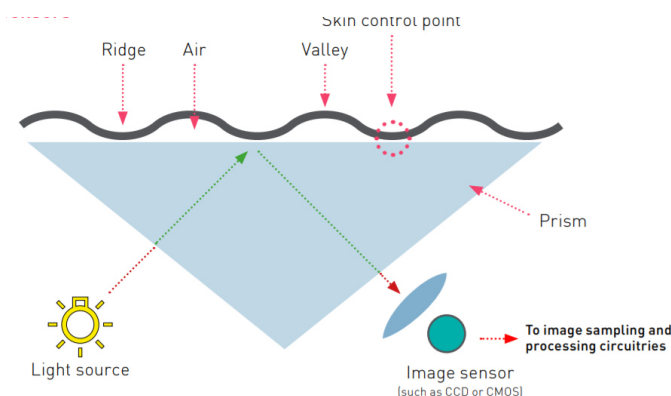


Figure 11. Funcionamiento del sensor óptico. Fuente Fingerprints.

Dispositivo de carga acoplada (CCD)

Los sensores realizan la conversión en del fotón a electrón en la celda, luego se desplaza a un registro horizontal donde sucesivamente se convertirán uno a uno el electrón a voltaje para finalmente aplicarle una ganancia y ser convertida a una señal analógica en un circuito. Este proceso produce necesita mucha energía y produce mucho calentamiento, por lo cual, no es usado actualmente en dispositivos ya que consume demasiada energía mientras está activo. Además, la temperatura ocasiona que se genere más ruido por lo que necesitará un circuito externo para atenuar el ruido y también para el proceso de conversión analógico digital.

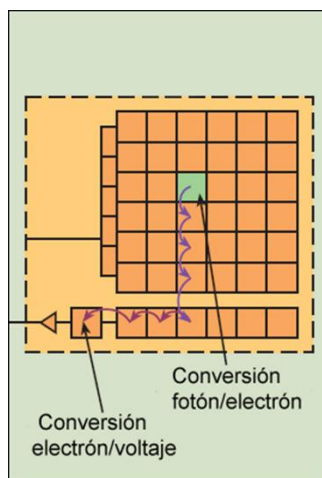


Figure 12. Diagrama de bloques de CCD. Recuperado de Decamaras.

Semiconductor complementario de óxido metálico (CMOS)

La energía del fotón obtenida en cada pixel es transformada en electrón y convertida a voltaje en la misma celda. Los voltajes obtenidos son amplificados y direccionados a través de un multiplexor al convertidor de analógico a digital. En este caso, el CMOS es mucho más compacto y posee convertidores A/D, circuitos temporizadores y amplificadores integrados en el mismo chip. Las ventajas de este dispositivo es que procesa la información captada mucho más rápido y sin consumir demasiada energía.

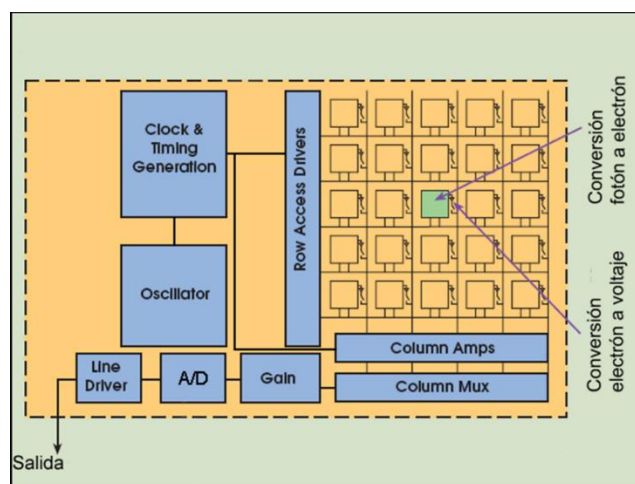


Figure 13. Diagrama de bloques de CMOS. Recuperado de Decamaras.

3.2.4.6 Reconocimiento de huella digital sin contacto: En el artículo “Reconocimiento de huella digital sin contacto” realizada por Shah & Poshia (2013,

p. 1) se define este reconocimiento de huella dactilar como: “La adquisición de huellas digitales sin contacto es una tecnología de detección remota para capturar el patrón de cresta-valle que proporciona información esencial para el reconocimiento”.

Según Derawi, Yang, & Busch (2012) autores del artículo “Reconocimiento de huella con la cámara embebida del celular”, el dispositivo que sustituirá al lector como instrumento para la captura de huella es la cámara del celular debido a su fácil acceso y su gran avance exponencial en los últimos años.

La tecnología de Veridium realiza la autenticación biométrica dactilar de la huella sin contacto, además es actualmente usada en el Perú por empresas del sector de telecomunicaciones para la venta de servicios públicos móviles. Esta es una solución biométrica dactilar también llamada sin contacto o 4-Fingers, que permite capturar los cuatros dedos o el pulgar en una sola toma mediante el uso de la cámara del teléfono sin requerir hardware adicional. La elección de captura de cuatro dedos o pulgar depende de las huellas sugeridas del cliente enviadas por el servicio de Reniec.

El proceso de captura inicia al momento de colocar el DNI del ciudadano. Posterior a ello se consultará el servicio web de mejores huellas de Reniec y el usuario tendrá la posibilidad de escoger qué huella tomar haciendo clic en una de las dos manos

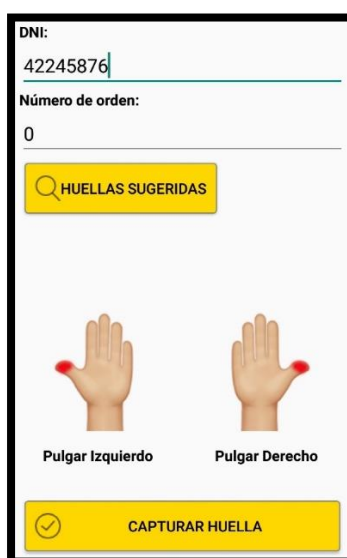


Figure 14. Selección de huella sugerida a capturar. Fuente Elaboración propia.

Después de ello, el sistema activará automáticamente la cámara posterior del celular y quedará a la espera de que se coloquen los cuatro dedos o el dedo pulgar seleccionado frente a la cámara del celular. Una vez que haya detectado los dedos de manera satisfactoria, cambiará el color del entorno de la huella de rojo a verde como se puede apreciar en las siguientes pantallas.

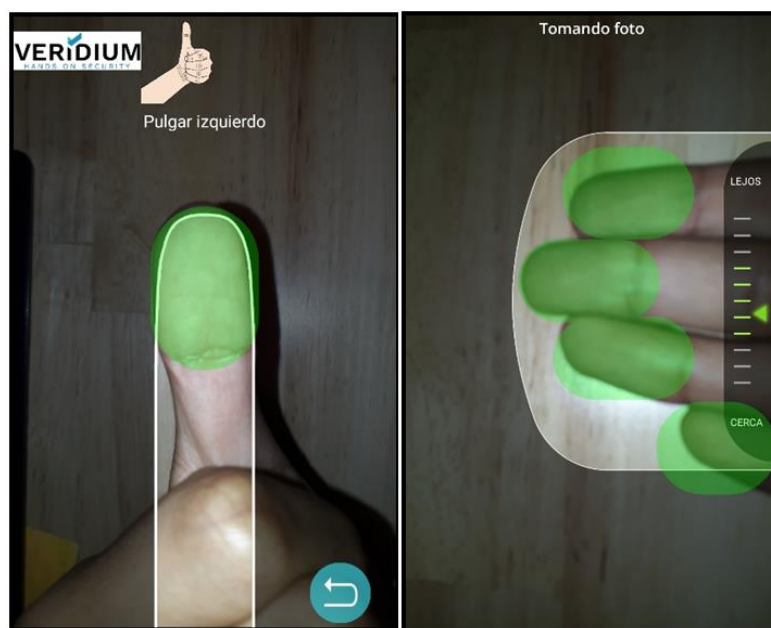


Figure 15. Método de captura de huellas. Fuente Elaboración propia.

Cuando el sistema haya detectado correctamente la mano y haya generado la minucia, lo indicará a través de un mensaje como el que se indica en la imagen del lado izquierdo; en caso haya detectado algún indicio de huella falsa, se mostrará un mensaje de reconocimiento fallido como se muestra en la imagen del lado derecho.

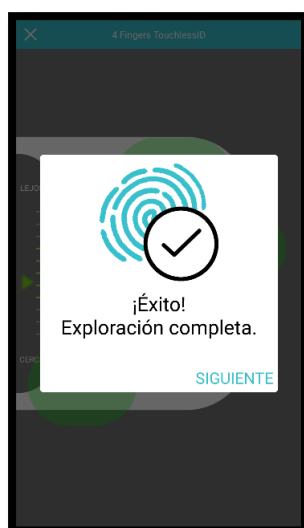


Figure 16. Captura de huella exitosamente. Fuente Elaboración propia.

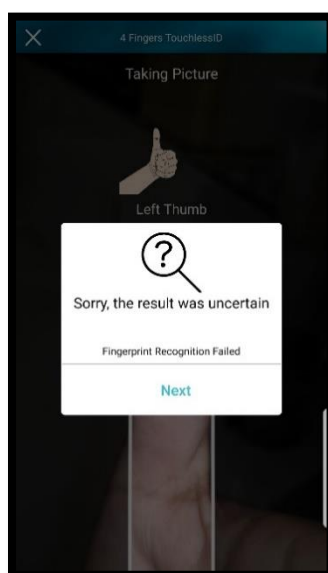


Figure 17. Captura de huella fallida, huella falsa detectada. Fuente Elaboración propia.

En la Tabla 1, presentamos las principales características de cada modelo de lector biométrico usado por las empresas de telecomunicaciones. Estos lectores biométricos cumplen con los formatos ISO/IEC 19794-2: 2011 e ISO/IEC 19794-4: 2011, los cuales son formatos de los datos para sistemas biométricos basados en minucias e imágenes de los dedos respectivamente.

Tabla 1

Características principales de cada lector biométrico.

	EikonTouch710m	MSO 1300 E3	4 Fingers Touchless
Marca	Crossmatch	Morpho	Veridium
Tipo de sensor	Capacitivo	Óptico	-
Tipo de lector	Monodactilar	Monodactilar	Monodactilar y 4 dedos
Peso	74 g	140 g	-
Resolución	508 dpi	500 dpi	500 dpi
Conectores	USB/microUSB/Tipo C	USB/microUSB	-
Formato de plantillas	ISO 19794-2, ANSI/INCITS 378. ISO 19794-4, imagen de compresión WSQ	ISO 19794-2, ANSI/INCITS 378 y formatos propietarios Morpho	WSQ e ISO/ANSI

Fuente: Elaboración propia.

3.2.4.7 Requerimientos: Según el Glosario estándar de IEEE de terminología de ingeniería de software (1990, p. 62) define a requerimiento como: “Una condición o capacidad que debe estar presente en un sistema o componentes de sistema para satisfacer un contrato, estándar, especificación u otro documento formal”.

USB OTG

Es una característica fundamental que convierte el puerto esclavo de un celular en un puerto host, permitiendo conectar otros dispositivos, en este caso, un lector biométrico. Keith (2005, p. 184) explica que “USB OTG aborda este deseo permitiendo que un dispositivo usb se comuniquen directamente con otro producto otg”.

Esta característica puede aprovecharse para transferir datos o conectar algún periférico al celular, en este caso, lo usaremos para conectar un lector biométrico el cual se alimentará de la batería del celular para poder capturar la huella. Es muy

importante esta característica, ya que los celulares que no tengan USB OTG no reconocerán al lector biométrico y en algunos casos, ni siquiera podrán energizarlo.

Cámara de celular

Derawi, Yang, & Busch (2012, p. 1), autores del artículo “Reconocimiento de huella con la cámara embebida del celular”, vieron el potencial que tenían los teléfonos móviles y predijeron que estos serían útiles para el procesamiento de varias tareas. “Incluso muchos de los celulares tienen reconocimiento de huella y se ha utilizado en muchas aplicaciones diferentes donde se requiere más seguridad. Se propone un enfoque de autenticación que aplica cámaras de teléfonos celulares que capturan imágenes de huellas digitales como rasgos biométricos”.

Sistema operativo

Según Wolf, Ruiz, Bergero, & Meza (2015, p. 17) en el libro “Fundamentos de sistemas operativos” menciona:” El sistema operativo es el principal programa que se ejecuta en toda computadora de propósito general (...). El sistema operativo es el único programa que interactúa directamente con el hardware de la computadora.”

En la Tabla 2 veremos los requerimientos de cada modelo de lector biométrico para poder implementarlo en los celulares de los usuarios.

Tabla 2

Requerimientos de cada lector biométrico.

	EikonTouch710m	MSO 1300 E3	Veridium
Cámara	No	No	Mínimo 5MP + Flash LED
Sistema operativo	Android 4.4-10	Android 4.4-10	Android 4.4-10
USB OTG	Sí	Sí	No
Puerto de entrada	USB/microUSB/Tipo C	USB/microUSB	No

Fuente: Elaboración Propia

3.2.5 Test Spoofing

Parthasaradhi, Derakhshani, Hornak, & Schuckers (2005, p. 1) define al test Spoofing como: “El proceso de derrotar un sistema biométrico mediante la introducción de una muestra biométrica falsa”.

El test spoofing sirve para evaluar el nivel de seguridad de los lectores biométricos y prevenir los intentos de suplantación de identidad por parte de los impostores. Existen muchas formas de vulnerar un sistema de seguridad, como por ejemplo hackeando los servidores de Reniec o del proveedor del sistema de biometría, pero esto significaría tomar un alto riesgo. La forma más fácil de vulnerar un sistema biométrico y con bajo riesgo es realizando un ataque de presentación con una muestra biométrica falsa.

Según la ISO/IEC 301073-3:2017, esta muestra biométrica falsa se denomina ataque de presentación. ISO/IEC 30107 contiene métricas para la evaluación de los mecanismos de detección de ataques de presentación (PAD, por sus siglas en inglés) de los sistemas biométricos.

ISO/IEC 301073-3:2017 menciona que “Los mecanismos PAD están sujetos a errores falsos positivos y falsos negativos. Los errores falsos positivos categorizan incorrectamente las presentaciones auténticas como presentaciones de ataque, lo que puede marcar o incomodar a los usuarios legítimos. Los errores falsos negativos categorizan erróneamente los ataques de presentación (también conocidos como presentaciones de ataque) como presentaciones auténticas, lo que puede resultar en una violación de seguridad”.

Para la detección de ataques de presentación es necesario la creación de una réplica de un objeto de características similares al original, en este caso, una huella falsa. Como se menciona en la definición de test spoofing, se debe de introducir esta muestra biométrica falsa por cada uno de los lectores biométricos a través de los sensores.

En la siguiente sección se explicará el proceso de clonación de huellas para poner a prueba la detección de ataques de presentación (PAD, por sus siglas en inglés) y principalmente se explicará las tasas que nos ayudará a medir los errores falsos positivos y errores falsos negativos.

3.2.5.1 Clonación de huella: La clonación de huella es la parte fundamental para realizar un test spoofing, ya que con las huellas falsas clonadas se realizarán los ataques de presentación a cada uno de los lectores biométricos que nos ayudarán a medir el nivel de seguridad. La clonación consiste en replicar la huella dactilar de una persona con el objetivo de obtener la minucia de la huella y poder usarla para vulnerar cualquier sistema biométrico. Maltoni, Maio, Jain, & Prabhakar (2009, p .382) mencionan que “un intruso podría usar una imagen de huella dactilar para crear una huella falsa (también conocida como dedo ficticio o dedo gomoso) que se puede aplicar en la superficie de imagen de un escáner de huella digital de escaneo en vivo”.

Realizaremos en esta etapa la obtención de la huella dactilar a clonar evitando el deterioramiento de la huella. Existen muchas maneras en la que los criminales pueden obtener una huella; en el informe de Perú21 (2019), nos explica que algunos de ellos eran ex trabajadores de empresas que tenían acceso a datos personales como la ficha original de Reniec donde aparecía la huella de la víctima. En otros casos obtenidos de un reportaje de América Noticias (2014), utilizaban las huellas colocadas en documentos para replicarlas en forma de sellos, como los que se encontraron en la sede de revista “Juez Justo” vinculada a la Red Orellana.

3.2.5.2 Material: Según Polimeni, Fabozzi, & Adelberg (1997, p.76): “Los materiales o suministros son los elementos básicos que se transforman en productos terminados a través del uso de la mano de obra y de los costos indirectos de fabricación en el proceso de producción”.

Los materiales que se usaron son de fácil acceso , esto hace que la clonación de huellas esté al alcance de cualquier persona, además el material del que elaboraremos el molde es el mismo que ha sido usado para delitos reportados por Perú21(2019) y América Noticias (2014) mencionados anteriormente. Existen muchos materiales que pueden servir como material para un molde de huella falsa debido a su apariencia y propiedades similares a las de un dedo real, aumentando así la probabilidad de poder burlar un sistema biométrico.

3.2.5.3 Fabricación de huella: El proceso de fabricación inicia una vez se haya definido todas las operaciones que se realizarán con los materiales escogidos para la producción de la huella falsa. Dichos materiales se transformarán en el producto final que necesitamos para poder poner a prueba los lectores biométricos. Para la obtención

de un producto de calidad, probablemente sea necesario ejecutar este proceso más de una vez, evaluaremos si es necesario realizar todo el proceso de fabricación nuevamente con un test de calidad, el cual es descrito en el siguiente paso.



Figure 18. Huella falsa.

3.2.6 Recolección y procesamiento de datos.

Recopilaremos todos los resultados de las pruebas realizadas con las huellas falsas y los colocaremos en tablas para su procesamiento, el objetivo es organizar los datos para que sean mucho más fáciles de entender y trabajar.

Según Arias (2012, p. 111) “En este punto se describen las distintas operaciones a las que serán sometidos los datos que se obtengan: clasificación, registro, tabulación y codificación si fuere el caso”. Al tabular la información, podremos obtener todas las tasas de porcentaje y, posteriormente, compararlas entre los resultados obtenidos de las pruebas de cada lector biométrico.

3.2.6.1 Test de calidad: Un test de calidad consiste en poner a prueba un producto para saber si este cumple las expectativas planteadas previamente. Después

de la creación de la huella falsa, se deberá probar que la calidad de la huella es lo suficientemente buena como para ir a Reniec y ser comparada con alguna de la base de datos.

El servicio de Reniec llamado “Verificación Biométrica de la identidad de las personas T33” (Anexo 1) se encargará de responder las solicitudes de verificación, dando como respuesta el nombre completo de la persona y un mensaje de validación conforme. Adicional a la verificación de la identidad de una persona, también devuelve otros mensajes cuya descripción los puede ver en el Anexo 2. Los códigos de respuesta 112 y 122 nos indica que la imagen dactilar WSQ es de baja calidad, ese mensaje nos ayudará a testear las huellas falsas elaboradas, ya que si estas no logran pasar el umbral de calidad, entonces las huellas que usamos para realizar las huella falsas no fueron capturadas correctamente o simplemente fueron mal fabricadas, en caso contrario, si las huellas falsas pasan el umbral, serán comparadas con la huella almacenada en la base de datos de Reniec y obtendremos una respuesta la cuál sería positiva (código de respuesta 70006) o negativa (código de respuesta 70007).

3.2.6.2 Tasas: Para la biometría usaremos las siguientes tasas para evaluar el funcionamiento a la hora de verificar la identidad de una persona. Según ISO/IEC 30107-3:2017 definen de la siguiente manera las tasas de medición que usaremos:

Tasa de coincidencia de presentación de ataque de impostor (IAPMR, por sus siglas en inglés): En la sección 3.2.6 de ISO/IEC 30107-3:2017 menciona que es la “Proporción de presentaciones de ataques de impostores que utilizan la misma especie de instrumento de ataque (PAI, por sus siglas en inglés) en la que la referencia objetivo coincide”.

Tasa de error de clasificación de presentación de buena fe (BPCER, por sus siglas en inglés): En la sección 3.2.2 de ISO/IEC 30107-3:2017 menciona que es la “Proporción de presentaciones auténticas clasificadas incorrectamente como ataques de presentación en un escenario específico”.

Si queremos evaluar y comparar la seguridad y el nivel de experiencia usuaria de algún sistema biométrico entonces estos valores son necesarios. Estas tasas nos ayudarán a medir la probabilidad de que una huella falsa nos genere una coincidencia positiva o con que probabilidad se rechazará una huella real.

El IAPMR y BPCER son inversamente proporcionales, por lo tanto, el aumento o disminución de una de las tasas significará lo contrario para la otra tasa. Esto se debe a que la variación de una de las tasas puede traer consecuencias graves en las aplicaciones en un sistema real. El aumento del IAPMR puede ocasionar el aumento de impostores debido a que el sistema se vuelve más vulnerable. En el caso contrario, el aumento del BPCER puede generar una mala experiencia de usuario, a pesar de que el usuario esté capacitado correctamente.

Nuestra investigación consiste en poner a prueba los métodos biométricos usados por los servicios de telecomunicaciones para la venta de líneas, es por eso que se realizará un set de pruebas a los sistemas biométricos antes mencionados. Con los valores IAPMR y BPCER lograremos ver el rendimiento que tienen estos métodos frente a ataques de huella falsa y poder compararlos. Las fórmulas que usaremos son las siguientes:

$$IAPMR = \frac{\text{Intentos exitosos de ataque}}{\text{Total de intentos de ataque}}$$

$$BPCER = \frac{\text{Intentos reales fallidos}}{\text{Total de intentos reales}}$$

3.3 Reflexión crítica de la experiencia

Se realizó exitosamente las pruebas con las huellas falsas a los lectores biométricos para comparar la eficacia, el nivel de seguridad y la experiencia usuaria de los distintos métodos biométricos, esto evitará las multas y maximizará las ganancias. Se muestra en esta investigación los beneficios de cada una de las alternativas, para que, a juicio del usuario, se establezca lo conveniente según su criterio.

A continuación, se mostrará el plan de trabajo, el cual fue compartido con el asesor, para poder marcar las actividades paso a paso y en el orden correcto para evitar rehacer pasos innecesariamente.

Table 3

Cuadro de actividades.

Nombre de tarea
Etapas de Recolección

Recolectar los materiales para la clonación de huellas polímero
Recolectar las huellas de personas para el experimento.
Clonación de Huellas
Procesar la huella para impresión
Fabricación de huella
Test de calidad contra Reniec
Test IAPMR y BPCER
Test con Lector Capactivo
Test con Lector Optico
Test con Cámara
Análisis de datos de pruebas
Organizar los datos
Compararlos en gráficos y tablas
Resultados y conclusiones
Análisis de datos de costos
Organizar los datos
Compararlos en gráficos y tablas
Resultados y conclusiones
FIN DE PRUEBAS

Fuente: Elaboración Propia

A continuación, detallaremos cuales fueron las etapas que se tomó en cuenta para el experimento.

3.3.1 Etapa de Recolección

Esta es la primera etapa debido a que se tiene que reunir toda la información necesaria expuesta en el marco teórico. Se necesita 2 datos importante para la creación del molde, la elección del material y la búsqueda de voluntarios para la captura de sus huellas.

Se logró capturar las mejores huellas de 10 personas para obtener un total de 20 huellas dactilares. Solo se capturó 2 huellas por persona ya que Reniec solo te permite realizar la validación biométrica con un dedo de cada mano, estas huellas son llamadas “Huellas sugeridas”, incluso existe un servicio web de Reniec en donde se puede saber

cuáles son las huellas sugeridas de una persona solamente colocando su DNI y escribiendo un código de imagen.



Figure 191. Página web de Reniec para consultas de huellas sugeridas. Fuente: Reniec.

Además, se consiguió unos materiales de alta calidad y plantillas de huellas falsas de alta definición para generar un molde de buena calidad con valles y crestas iguales a una huella dactilar real.

3.3.2 Clonación de Huellas

El proceso consiste en escanear la huella del voluntario y obtener una imagen digital de ellas, este caso representaría el peor escenario para los sistemas biométricos ya que se cuenta con una imagen de alta calidad de la huella. No se detallará el proceso de realce de la imagen ni los pasos de la fabricación de la huella por seguridad, ya que el objetivo de esta investigación es aportar información beneficiosa para la seguridad biométrica.



Figure 202. Huella capturada y huella en negativo. (no pertenecen a una persona). Fuente:

Elaboración propia

3.3.3 Test de calidad

Para realizar el test de calidad se solicitó la desactivación momentánea de la detección de huella viva de Veridium, de esta manera, podremos enviar la huella falsa a Reniec y probar si esta logra pasar el umbral de calidad. Se realizó esta prueba a las 20 huellas falsas y el resultado se muestra en la tabla.

El resultado para todas las huellas falsas fabricadas fue exitoso, todas lograron pasar el umbral de calidad e incluso dieron como resultado HIT en el servicio biométrico de verificación dactilar. Esto demuestra la importancia de detener una huella falsa antes de que sea enviada a Reniec para evitar suplantaciones. También demostramos que las huellas falsas fabricadas son válidas para poder realizar nuestro test de spoofing a los métodos de identificación biométrica.

Tabla 4

Resultados de test de calidad de huella

Test de Calidad	
Huella 1	✓
Huella 2	✓
Huella 3	✓
Huella 4	✓
Huella 5	✓
Huella 6	✓

Huella 7	✓
Huella 8	✓
Huella 9	✓
Huella 10	✓
Huella 11	✓
Huella 12	✓
Huella 13	✓
Huella 14	✓
Huella 15	✓
Huella 16	✓
Huella 17	✓
Huella 18	✓
Huella 19	✓
Huella 20	✓

Fuente: Elaboración Propia

3.3.4 Test IAPMR

Debido a los resultados exitosos obtenidos en el test de calidad, se procede a realizar las pruebas de IAPMR de cada método biométrico. Como se puede ver en la figura 24, se ha colocado la huella falsa de polímero sobre el dedo que le corresponde, en este caso, es el dedo índice. La huella falsa fue hecha según la medida de dedo de cada voluntario, es por eso que cubre completamente la yema del dedo, a simple vista puede pasar desapercibido por su color similar al de la piel.



Figure 23. Huella falsa colocada sobre dedo índice. Fuente: Elaboración propia.

Luego se coloca en la aplicación el DNI del usuario al que le corresponde la huella falsa y se selecciona el dedo correspondiente. Es muy importante seleccionar y colocar el dedo que se intenta vulnerar, ya que si selecciona o se coloca otro dedo se estará haciendo mal la prueba.

Figure 214. Ingreso de DNI y selección de huella. Fuente: Elaboración propia.

Después de colocar la huella pueden suceder 2 escenarios:

Las huellas falsas son capturadas por el sistema biométrico y son enviadas a Reniec para ser comparadas con la huella almacenada del DNI ingresado, esto nos dará un HIT, el cual será representado con un “1”.

Por otro lado, si la huella falsa logra ser detectada entonces el sistema biométrico rechazará el envío de la huella, el cual será representado con un “0”.

Tabla 5

Resultados del test IAPMR

	EikonTouch710m	MSO 1300E3	Veridium
Huella 1	0	0	0

Huella 2	0	0	0
Huella 3	0	0	0
Huella 4	0	0	0
Huella 5	0	0	0
Huella 6	0	0	0
Huella 7	0	0	0
Huella 8	0	0	0
Huella 9	0	1	1
Huella 10	0	0	0
Huella 11	0	0	0
Huella 12	0	0	0
Huella 13	0	1	0
Huella 14	0	1	1
Huella 15	0	0	0
Huella 16	0	0	0
Huella 17	0	0	0
Huella 18	0	0	0
Huella 19	0	0	0
Huella 20	0	0	0

Fuente: Elaboración Propia

Según los datos de la tabla 6, se procederá a calcular el IAPMR de cada método biométrico. Para esto usaremos la fórmula definida anteriormente:

$$IAPMR = \frac{\text{Intentos exitosos de ataque}}{\text{Total de intentos de ataque}}$$

$$IAPMR_{\text{reikon}} = \frac{0}{20} = 0$$

$$IAPMR_{\text{mso}} = \frac{3}{20} = 0.15$$

$$IAPMR_{\text{veridium}} = \frac{2}{20} = 0.1$$

3.3.5 Test BPCER

En este escenario se realizarán las mismas pruebas hechas en el test anterior, pero en este caso, se utilizarán las huellas genuinas de cada usuario, ya que el objetivo es obtener el valor BPCER que nos ayudará a mediar la tasa de pruebas realizadas con una huella genuina que fueron clasificadas incorrectamente como huellas falsas por el sistema biométrico. Este valor nos servirá para medir el nivel de experiencia usuaria que tendrá un cliente real al usar el sistema biométrico.

Primero se coloca el DNI del usuario y se selecciona la huella a capturar, después de colocar la huella correspondiente pueden suceder 2 escenarios:

Las huellas genuinas capturadas son detectadas como huellas falsas por el sistema biométrico y no son enviadas a Reniec para ser comparadas con la huella almacenada del DNI ingresado, llamaremos a esto un NO HIT y será representado con un “0”.

Por otro lado, si la huella genuina logra pasar el sistema biométrico entonces la huella será comparada con la que se encuentra almacenada en Reniec y nos dará un HIT el cual será representado con un “1”.

Tabla 6.

Resultados del test BPCER.

	EikonTouch710m	MSO 1300E3	Veridium
Huella 1	1	1	1
Huella 2	1	1	1
Huella 3	1	1	1
Huella 4	1	1	0
Huella 5	1	1	1
Huella 6	1	1	1
Huella 7	1	1	0
Huella 8	1	1	1
Huella 9	1	1	1
Huella 10	1	1	1
Huella 11	1	1	1
Huella 12	1	1	0
Huella 13	1	1	1
Huella 14	1	1	1
Huella 15	1	1	1
Huella 16	1	1	1
Huella 17	1	1	1
Huella 18	1	1	1
Huella 19	1	1	1
Huella 20	1	1	1

Fuente: Elaboración Propia

Según los datos de la tabla 7, se procederá a calcular el BPCER de cada método biométrico. Para esto usaremos la fórmula definida anteriormente:

$$BPCER = \frac{\text{Intentos reales fallidos}}{\text{Total de intentos reales}}$$

$$BPCER_{eikon} = \frac{0}{20} = 0$$

$$BPCER_{mso} = \frac{0}{20} = 0$$

$$BPCER_{veridium} = \frac{3}{20} = 0.15$$

De los resultados de la Tabla 6 y 7, se puede observar que el lector EikonTouch710 tiene el valor más bajo en IAPMR y BPCER, por lo tanto, posee el nivel de seguridad y experiencia usuaria más alto, esto lo vuelve ideal para la venta de líneas y servicios, la única desventaja sería que estos lectores son del tipo capacitivo, su sensor está expuesto y lo hace vulnerable a daños físicos por mal uso y accidentes.

Veridium tiene un nivel de seguridad bastante alto pero su usabilidad es regular y la más baja de los tres sistemas biométricos. Cabe mencionar que los voluntarios no conocían esta tecnología y estaban más familiarizados con los lectores convencionales, sin embargo, consideraron bastante seguro el hecho de que no tenían que entrar en contacto con ningún dispositivo que fue usado por otras personas.

CAPÍTULO IV: CONCLUSIONES

Los datos obtenidos de la investigación realizada nos ayudan a medir el nivel de seguridad por medio de la métrica IAPMR y la usabilidad y experiencia usuaria de cada uno de los lectores comparando los valores de las métricas BPCER. De estos valores podemos concluir que los lectores biométricos EikonTouch170, los cuales utilizan sensores capacitivos, tienen un mejor balance de seguridad y experiencia a diferencia de los que utilizan un método óptico debido a sus bajos valores de BPCER e IAPMR.

El lector MSO1300E3 tiene el BPCER más bajo posible, ocasionando que su usabilidad y durabilidad sean sus mayores ventajas, ya que, al utilizar un sensor óptico colocado internamente en la carcasa del lector, evita daños directos ocasionados por factores externos. A diferencia de los lectores capacitivos que si reciben daños quedarían inservibles, estos daños solo bajarían la calidad de la imagen capturada más no ocasionarían un daño grave, prolongando de esta manera su tiempo de vida útil.

El alto valor de BPCER de Veridium significa que el usuario tendrá que realizar varios intentos de captura para poder validarse. Esto lo vuelve poco amigable para operaciones rápidas como la venta de servicios en la vía pública, donde hay mucha competencia y otras empresas pueden ofrecer y finalizar la venta mucho más rápido con alguno de los otros 2 lectores biométricos.

CAPÍTULO V: RECOMENDACIONES

Se recomienda utilizar los lectores biométricos EikonTouch710 debido a que los buenos resultados obtenidos con este lector biométrico garantizan un alto nivel de seguridad y facilidad de uso.

El lector MSO1300E3 tiene el IAPMR más alto de todos, lo que hace vulnerable a ataques con huellas falsas. Esto no lo hace recomendable para sistemas de alta seguridad o venta de equipos de alto valor, ya que podría ser fácilmente vulnerado y generar pérdidas por estafa.

CAPÍTULO VI: BIBLIOGRAFÍA

6.1 Fuentes de Información

- a) Akhtar Zahid (2012). *Seguridad de biométrico multimodal, sistema contra la suplantación de identidad*. Recuperado de:
https://pralab.diee.unica.it/sites/default/files/Akhtar_PhD2012.pdf
- b) América Noticias (14 de setiembre del 2014). *Cuarto Poder: Sellos en forma de huellas digitales encontraron en sede de revista 'Juez Justo'*. Recuperado de:
https://www.youtube.com/watch?v=phvepvH6b_A&feature=emb_title
- c) Arias Odón Fidias (2012). *El proyecto de investigación*. Recuperado de:
https://trabajosocialudocpno.files.wordpress.com/2017/07/fidias_g-_arias-_el_proyecto_de_investigacic3a3c2b3n_6ta-_edicic3a3c2b3n1.pdf
- d) AuthenTec (2011). *TCS1/TCS2-TCD58E TouchChip Chipset Datasheet*. Recuperado de:
<http://m.sztlink.com/uploads/201809/5b91de4db2eee.pdf>
- e) Batura (2020). *Procesamiento de Imagen II: Reconocimiento facial en Apps*. Recuperado de:
<https://baturamobile.com/eu/blog/procesamiento-de-imagen-ii-reconocimiento-facial-en-apps/>
- f) Derawi Mohammad, Yang Bian; Busch Christoph (2012). *Fingerprint recognition with embedded cameras on mobiles phones*. Recuperado de:
<https://www.christoph-busch.de/files/Derawi-FingerCamera-secdoc-2012.pdf>
- g) Ebel F. y Nestel S. (1993). *Sensores para la técnica de procesos y manipulación*. Recuperado de:
https://www.festodidactic.com/ov3/media/customers/1100/094342_leseprobe_es.pdf
- h) El Comercio (08 de julio del 2019). *Telefónica: Osiptel confirma multa por no*

- validar huellas en venta de líneas*. Recuperado de:
<https://elcomercio.pe/economia/negocios/osiptel-confirman-multa-telefonica-s-626-650-validar-huellas-venta-lineas-noticia-nndc-653381-noticia/?ref=ecr>
- i) El Peruano (31 de octubre del 2016). *Normas legales*. Recuperado de:
<https://busquedas.elperuano.pe/download/full/DXR VHglOKx2BjQ27Gt0eno>
- j) Fingerprints (2019). *Biometric Technologies*. Recuperado de:
https://www.fingerprints.com/uploads/2019/10/fpc_white_paper_digital.pdf
- k) García Santiago (2012). *Ingeniería de mantenimiento*. Recuperado de:
<http://www.renovetec.com/ingenieria-del-mantenimiento.pdf>
- l) Gestión (20 de setiembre del 2019). *Confirman multa a Claro de S/ 1.4 millones por activar líneas sin verificar identidad de usuarios*. Recuperado de:
<https://gestion.pe/economia/confirman-multa-claro-s-1-4-millones-verificar-identidad-clientes-nndc-276409-noticia/?ref=gesr>
- m) Gestión (17 de diciembre del 2018). *Osipitel confirma multas por S/ 1.85 millones para vietnamita Bitel*. Recuperado de:
<https://gestion.pe/economia/empresas/osiptel-confirma-multas-s-1-85-millones-vietnamita-bitel-253053-noticia/>
- n) Gomez Días Carlos y De León De la Galarza Elda (2014). *Método Comparativo*. Recuperado de:
<http://eprints.uanl.mx/9802/1/Estudio%20Comparado.pdf>
- o) Hernandez Roberto, Fernandez Carlos y Baptista Pilar (2014). *Metodología de la investigación*. Recuperado de:
https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf
- p) IEEE (1990). *Glosario estándar de IEEE de terminología de ingeniería de software*. Recuperado de:
http://www.mit.jyu.fi/ope/kurssit/TIES462/Materiaalit/IEEE_SoftwareEngGlossary.pdf
- q) ISO, IEC (2015). *ISO/IEC 2382:2015: Information technology - Vocabulary*. Recuperado de:
<https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en>
- r) ISO, IEC (2017). *ISO/IEC 30107-3:2017: Information technology – Biometric presentation attack detection – part 3: Testing and reporting*. Recuperado de:
<https://www.iso.org/obp/ui/#iso:std:iso-iec:30107:-3:ed-1:v1:en>

- s) Keith Jack (2005). *A handbook for the digital engineer*. Recuperado de:
https://books.google.com.pe/books?id=Kp5J7G8kXN4C&pg=PA184&lpg=PA184&dq=usb+on+the+go+ieee&source=bl&ots=8M8S6mkCUc&sig=ACfU3U2RHQTZz-sTK_hoS_CmhUMOVJqNvQ&hl=es419&sa=X&ved=2ahUKEwiIjurT3MrmAhU9K7kGHYVTBWkQ6AEwEHoECAgQAQ#v=onepage&q=usb%20on%20the%20go&f=false
- t) La República (17 de junio del 2019). *Rafael Muelle: “Las operadoras deben ser eficientes y en eso la regulación no pone freno*. Recuperado de:
<https://sociedadtelecom.pe/2019/06/17/rafael-muelle-las-operadoras-deben-ser-eficientes-y-en-eso-la-regulacion-no-pone-freno/>
- u) La República (17 de febrero del 2020). *Osipitel confirma multas a Bitel y a Entel por más de tres millones de soles*. Recuperado de:
<https://larepublica.pe/economia/2020/02/17/osipitel-confirma-multas-a-bitel-y-a-entel-por-mas-de-tres-millones-de-soles/>
- v) Maltoni Davide, Maio Dario, Jain Anil y Prabhakar Salil (2009). *Handbook of fingerprint recognition*. Recuperado de:
<https://books.google.com.pe/books?id=1Wpx25D8qOwC&pg=PA388&lpg=PA388&dq=fake+finges+author&source=bl&ots=9yR20Skwb6&sig=ACfU3U1IIWE-njtPf5l2BFn6HfLGwFf9HA&hl=es419&sa=X&ved=2ahUKEwih7YK10MrmAhhVUHRkGHRoLBmYQ6AEwAHoECAkQAQ#v=onepage&q=fake%20fingerprint&f=false>
- w) Naresh K. Malhotra; David F. Birks; Peter Wills (2019). *Marketing Research*. Recuperado de:
<https://www.studocu.com/en/document/universidad-argentina-de-la-empresa/investigacion-de-mercado/summaries/resumen-del-libro-11-y-12/2955238/view>
- x) Ortiz Lozada (2010). *Mejora de imágenes de huellas digitales*. Recuperado de:
http://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/540/ORTIZ_ALFREDO_MEJORA_IMAGENES_HUELLAS_DIGITALES.pdf?sequence=1&isAllowed=y
- y) Osipitel (2014). *Decreto Supremo N°023-2014-MTC*. Recuperado de:
http://transparencia.mtc.gob.pe/idm_docs/normas_legales/1_0_4718.pdf

- z) Osiptel (17 de julio del 2000). *Ley N° 27336*. Recuperado de:
http://transparencia.mtc.gob.pe/idm_docs/normas_legales/1_0_126.pdf
- aa) Parthasaradhi Sujana, Derakhshani Reza, Hornak Lawrence y Schuckers Stephanie (2005). *Time series detection of perspiration as a liveness test in fingerprint devices*. Recuperado de:
https://www.researchgate.net/publication/3421630_TimeSeries_Detection_of_Perspiration_as_a_Liveness_Test_in_Fingerprint_Devices
- bb) Perú21 (17 de marzo del 2019). *Alerta sobre clonación de huellas dactilares*. Recuperado de:
<https://peru21.pe/lima/alerta-clonacion-huellas-dactilares-466129-noticia/?foto=2>
- cc) Polimeni, Fabozzi y Adelberg (1997). *Contabilidad de costos*. Recuperado de:
<http://fullseguridad.net/wp-content/uploads/2017/01/Contabilidad-de-costos-3ra-Edici%C3%B3n-Ralph-S.-Polimeni.pdf>
- dd) RENIEC (2012). *Servicio de verificación biométrica – SVB*. Recuperado de:
http://www.reniec.gob.pe/portal/pdf/05_svb.pdf
- ee) Shah Jainam, Poshia Ujash (2013). *Touchless fingerprint recognition*. Recuperado de:
<http://innovativejournal.in/index.php/ajcsit/article/view/363/348>
- ff) Synaptics (2016). *Protección contra suplantación de huellas dactilares en dispositivos móviles*. Recuperado de:
<https://www.synaptics.com/sites/default/files/sentrypoint-anti-spoofing-wp.pdf>
- gg) Wolf Gunnar, Ruiz Esteban, Bergero Federico y Meza Erwin (2015). *Fundamentos de sistemas operativos*. Recuperado de:
https://sistop.org/pdf/sistemas_operativos.pdf

6.2 Glosario

C

Cuantificación Escalar de Ondículas (WSQ, por sus siglas en inglés)

Es un método de compresión de imágenes de huella digital en escala de grises diseñado por el FBI con el fin de reducir el tamaño de las imágenes de huella digital evitando la pérdida de información o de calidad durante la compresión.

Conversores Digital-Analógico (D/A) y Analógico-Digital (A/D)

Dispositivos electrónicos encargados de convertir la señal analógica a digital o viceversa.

Controlador de energía

Permite controlar la cantidad de energía eléctrica consumida por un dispositivo, con un impacto mínimo en el rendimiento.

Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés)

Realiza estándares internacionales para todas las tecnologías eléctricas, electrónicas y relacionadas.

Comité Internacional de Estándares de Tecnología de la Información (INCITS, por sus siglas en inglés)

Encargado de los estándares relacionados a la tecnología y opera bajo las reglas del ANSI.

D

Decodificador de columna y fila

Estos decodificadores se usarán para almacenar y organizar la información capturada por la matriz de sensores.

E

Entradas y salidas de propósito general (GPIO, por sus siglas en inglés)

Son pines de entrada y salida los cuales no están dedicados a algún proceso en especial, sino están diseñados para que se les den un propósito.

Estructura de descarga electrostática (ESD, por sus siglas en inglés)

Una estructura de protección ESD protege un circuito de una descarga electrostática, para evitar un mal funcionamiento o avería de un dispositivo electrónico.

G

Generador de control y temporización

El generador de temporización proporciona todos los relojes necesarios para la sincronización y las señales para controlar todas las operaciones.

H

HIT

Es el resultado que da el servicio de biométrica cuando la huella capturada coincide con la huella de la base de datos, por lo tanto, la verificación logra ser exitosa.

I

Instituto Nacional Estadounidense de Estándares (ANSI, por sus siglas en inglés)

Organismo que supervisa los estándares de todos los productos, procesos o servicios de Estados Unidos.

M

Matriz de sensores

Conjunto de sensores que convierte la energía en una respuesta eléctrica que luego puede representarse utilizando algoritmos de procesamiento de señales digitales.

O**Organización Internacional de Normalización o Estandarización (ISO, por sus siglas en inglés)**

Crea normas o estándares de calidad, eficiencia y seguridad para diversos productos, servicios y tecnologías.

U**Unidad Impositiva Tributaria (UIT)**

Valor de referencia que se utiliza en las normas tributarias como en multas. Su valor actual es de 4300 soles.

ANEXOS

Anexo 1: Tabla de costo por consulta según el tipo de servicio

RENIEC
REGISTRO NACIONAL DE IDENTIFICACION Y VOTACION

TEXTO UNICO DE PROCEDIMIENTOS ADMINISTRATIVOS - TUPA AÑO 2017
Decreto Supremo No. 353-2016-EF (UIT = S/ 4,050.00)
R.J. No. 156-2017/JNAC/RENIEC y modificatorias

Código RN	Código BCP (vía)	Código PVM Efectivo	No Procedimiento	Concepto	Tasa % UIT 4050	Monto S/	ANTES
			031	SERVICIOS INTERNET			
				CONSULTAS EN LINEA VIA INTERNET			
				a. Consultas en Línea Via Internet - NIVEL 1	0.02%	0.90	1.60
				b. Consultas en Línea Via Internet - NIVEL 2	0.03%	1.20	2.00
				c. Consultas en Línea Via Internet - NIVEL 3	0.04%	1.60	2.50
				CONSULTAS EN LINEA VIA LINEA DEDICADA			
			032	0 - 400,000	0.01%	0.60	0.90
				400,001 - 800,000	0.01%	0.40	0.68
				800,001 - 1'200,000	0.01%	0.26	0.48
				1'200,001 - 1'600,000	0.00%	0.17	0.31
				1'600,001 - A MÁS	0.00%	0.11	0.19
			033	VERIFICACION BIOMETRICA DE LA IDENTIDAD DE LAS PERSONAS			
				0 - 30,000	0.04%	1.50	1.90
				30,001 - 120,000	0.02%	0.98	1.33
				120,001 - 390,000	0.01%	0.59	0.86
				390,001 - 1'200,000	0.01%	0.32	0.52
				1'200,001 - A MÁS	0.00%	0.14	0.29
			034	VERIFICACION BIOMETRICA DE CONSULTA INTEGRADA			
				0 - 5,000	0.11%	2.00	4.20
				5,001 - 10,000	0.08%	1.60	2.94
				10,001 - 15,000	0.05%	1.20	1.91
				15,001 - 20,000	0.03%	0.84	1.15
				20,001 - a más	0.02%	0.55	0.63
			035	WEB SERVICE BIOMETRICO DACTILAR	0.02%	0.70	
			036	WEB SERVICE DE DATOS	0.01%	0.40	
			037	WEB SERVICE BIOMETRICO FACIAL	0.02%	0.70	
			030	COTEJO MASIVO DE DATOS			
				0 - 90,000	0.00%	0.20	0.50
				90,001 - 360,000	0.00%	0.19	0.35
				360,001 - 720,000	0.00%	0.18	0.23
				720,001 - 1'080,000	0.00%	0.17	0.14
				1'080,001 - A MÁS	0.00%	0.16	0.08

FORMA DE PAGO		
TRIBUTO	SERVICIO	BANCO
1031	COTEJO MASIVO	BANCO DE LA NACION
1023	CONSULTAS EN LINEA VIA INTERNET PRE PAGO (INDICANDO RUC DE LA EMPRESA)	BANCO DE LA NACION
	EL CODIGO DE LOS DEMAS SERVICIOS SE LES ASIGNA A LAS EMPRESAS EN EL MOMENTO DE REGISTRARLAS AL SISTEMA	BCP

Anexo 2: Tabla de mensajes de respuesta de Reniec

Código de respuesta	Mensaje RENIEC
70006	Validación conforme
70007	No coincide con el DNI ingresado
2	El usuario no existe
3	Entidad no se encuentra registrada y/o no tiene convenios con RENIEC
4	Entidad no cuenta con este servicio
5	El convenio de la entidad con RENIEC se encuentra deshabilitado
6	El servicio se encuentra deshabilitado para esta entidad
7	El servicio no está vigente para esta entidad
8	El usuario se encuentra deshabilitado para este servicio de la entidad
9	El usuario se encuentra cancelado en el convenio
10	El usuario está eliminado
11	El usuario no se encuentra registrado en el convenio
12	RUC de la entidad se encuentra inactivo por deuda
13	RUC de la entidad está cancelado
14	Usuario cancelado en RENIEC
15	Error en el Sistema de Convenios.
100	Objeto enviado para la consulta biométrica es nulo.
101	Se ha encontrado datos nulos en el objeto enviado para la consulta biométrica.
102	Se ha encontrado datos no válidos en el objeto enviado para la consulta biométrica.
109	Se generó una excepción en el proceso de comparación biométrica de las plantillas biométricas.
110	Error en las imágenes dactilares WSQ enviados para la consulta biométrica.
111	No se logró obtener las plantillas biométricas del ciudadano desde las imágenes WSQ
112	Las imágenes dactilares WSQ enviados para la consulta biométrica son de baja calidad.
120	Error en la imagen dactilar WSQ enviados para la consulta biométrica.
121	No se logró obtener la plantilla biométrica del ciudadano desde la imagen WSQ.
122	La imagen dactilar WSQ enviado para la consulta biométrica es de baja calidad.

200	No se cargó la librería DLL para el servicio de consulta biométrica en el MOO.
202	No se encontró registros del número de DNI en el AFIS.
203	No se encontró plantillas biométricas del número de DNI en el AFIS.
206	Formato de plantilla biométrica declarada en el objeto no es válido.
207	Se ha encontrado más de un registro de plantillas biométricas activas para el número de DNI en el AFIS.
208	Identificador en el AFIS para el número de DNI es nulo o vacío.
209	El registro correspondiente al número de DNI en el AFIS no contiene las plantillas biométricas, se encontró valores nulos.
210	El registro correspondiente al número de DNI en el AFIS no contiene una plantilla biométrica, se encontró una de las plantillas con valor nulo.
212	No se ha obtenido ninguna imagen dactilar WSQ desde el cliente para la consulta biométrica.
213	Se generó una excepción a nivel de la comunicación con el componente MOO.
301	DNI del <Usuario/Ciudadano>:<Número_DNI> no existe en la base de datos del RENIEC
302	El DNI del <Usuario/Ciudadano>:<Número_DNI> corresponde a un menor de edad
303	DNI del <Usuario/Ciudadano>:<Número_DNI> está cancelado
304	Ciudadano con DNI:<Número_DNI> no registra impresiones dactilares en el sistema de RENIEC
306	Número de RUC no es válido
307	DNI de usuario no es válido
308	DNI del ciudadano no es válido
309	Dirección IP del cliente no es válido
310	Dirección MAC del cliente no es válido
312	DNI <nu_dni> sin registro de huellas de mejor calidad.
313	DNI <nu_dni>sin registro en la BD AFIS - RENIEC
316	OK
999	No se encuentra información para mostrar, revisar la configuración de parámetros
70019	Error de servicio!

Anexo 3: Principales mensajes del estado del DNI a respuesta a una consulta biométrica

AUTENTICACIÓN E IDENTIFICACIÓN BIOMÉTRICA DE LA IDENTIDAD

MU-368-GT/5GIS/164

	(también es para consulta facial)	
" CORRESPONDE "	Cuando las impresiones dactilares enviadas al Servicio de Verificación Biométrica corresponden con las de la Base de Datos Biométrica del RENIEC. Cuando la Imagen CORRESPONDE al ciudadano	El servicio confirma que el ciudadano es la persona quien dice ser.
" NO CORRESPONDE "	Cuando el Servicio de Verificación Biométrica determina que las impresiones dactilares enviadas no corresponden a las almacenadas en la Base de Datos Biométrica del RENIEC. Cuando la Imagen NO CORRESPONDE al ciudadano	Si se ha tomado adecuadamente las impresiones dactilares, es probable que estén muy dañadas, por lo tanto, deberán efectuar lo siguiente: 1. Se debe usar otros medios alternos (como la consulta integrada, Consultas en Línea) para CONFIRMAR que la persona ES quien dice ser, conforme lo venían haciendo antes del presente servicio.
" BAJA CALIDAD "	Cuando las impresiones dactilares no han sido capturadas de manera correcta y/o realmente son de baja calidad	2. Adicionalmente sugerir al ciudadano realizar un trámite de renovación de imágenes con captura en vivo, para esto debe de indicar al ciudadano que debe consultar a nuestra línea gratuita a nivel nacional 0800-11040 opción 5, ingrese su No. de DNI, validaran su número, le derivaran a una operadora y le deberán consultar sobre cuál oficina es la más cercana a su actual domicilio registrado y que cuente con esta modalidad de registro (Captura en Vivo). y si es desde un móvil marcar

		013154000 anexo 1900 opción 5. 3. Para la consulta facial NO CORRESPONDE, el servicio nos indica que no es el ciudadano
--	--	--

Principales mensajes como resultado de la comparación biométrica.

Esto se menciona como casuística para la captura de las impresiones dactilares (posición de la impresión dactilar al momento de la captura) a enviar al servicio biométrico.

INPUT: CAPTURA DE IMPRESION DACTILAR		OUTPUT: RESPUESTA DE LA CONSULTA	
PRIMERA IMPRESIÓN DACTILAR	SEGUNDA IMPRESIÓN DACTILAR	RESPUESTA	RESULTADO DE LA CONSULTA
Huella derecha del ciudadano	Sin huellas	CORRESPONDE	La impresión dactilar capturada corresponde al DNI consultado.
Sin huellas	Huella izquierda del ciudadano	CORRESPONDE	La impresión dactilar capturada corresponde al DNI consultado.
huella derecha del ciudadano	huella izquierda del ciudadano	CORRESPONDE	La primera impresión dactilar capturada corresponde al DNI consultado. La segunda impresión dactilar capturada corresponde al DNI consultado
huella derecha del ciudadano	huella derecha del ciudadano	CORRESPONDE	Al menos una impresión dactilar capturada (primera impresión dactilar) corresponde al DNI consultado
huella derecha del ciudadano	huella de otro ciudadano		
huella derecha del ciudadano	Mancha, Mala Captura		
huella izquierda del ciudadano	huella izquierda del ciudadano	CORRESPONDE	Al menos una impresión dactilar capturada (segunda impresión dactilar) corresponde al DNI consultado
huella de otro ciudadano	huella izquierda del ciudadano		

Mancha, Mala Captura	huella izquierda del ciudadano		
huella izquierda del ciudadano	huella derecha del ciudadano	CORRESPONDE	La primera impresión dactilar capturada corresponde al DNI consultado y la segunda impresión dactilar capturada corresponde al DNI consultado, pero las posiciones están intercambiadas.
huella izquierda del ciudadano	huella de otro ciudadano	CORRESPONDE	Al menos una impresión dactilar capturada (primera impresión dactilar) corresponde al DNI consultado, pero su posición esta intercambiada
huella izquierda del ciudadano	Mancha, Mala Captura		
huella de otro ciudadano	huella derecha del ciudadano	CORRESPONDE	Al menos una impresión dactilar capturada (segunda impresión dactilar) corresponde al DNI consultado, pero su posición esta intercambiada
Mancha, Mala Captura	huella derecha del ciudadano		
huella de otro ciudadano	Sin huellas	NO CORRESPONDE	La impresión dactilar capturada no corresponde al DNI consultado.
Sin huellas	huella de otro ciudadano		
huella de otro ciudadano	huella de otro ciudadano	NO CORRESPONDE	Ninguna de las impresiones dactilares capturadas corresponde al DNI consultado.
huella de otro ciudadano	Mancha, Mala Captura		
Mancha, Mala Captura	huella de otro ciudadano		
Mancha, Mala Captura	Mancha, Mala Captura	BAJA CALIDAD	El ciudadano debe realizar su actualización de huellas en las oficinas registrales del RENIEC donde se encuentra operativo ver constancia en PDF

Anexo 4: Regimen de Infracciones y sanciones aplicable al decreto supremo N°003-2016-MTC que modifica el decreto supremo N°023-2014-MTC

ÍTEM	INFRACCIÓN	REFERENCIA NORMATIVA	SANCIÓN
1	La empresa operadora que en el periodo establecido no cumpla con informar o informe parcialmente (a través de llamadas telefónicas, locuciones grabadas y envío de SMS), a los abonados prepago que tengan la condición de persona natural con más de cinco (05) pero con menos de once (11) líneas registradas a su nombre, acerca de: (a) la necesidad de validar sus datos mediante el Sistema de Verificación Biométrica de Huella Dactilar y (b) la fecha de suspensión parcial de servicio de no realizarse la referida validación, de acuerdo al contenido, cantidad y frecuencia comunicados por el OSIPTEL, incurrirá en INFRACCIÓN GRAVE.	Literal I.1) de la Primera Disposición Complementaria Final del Decreto Supremo N° 023-2014-MTC. Primer párrafo de la Primera Disposición Complementaria DEL Decreto Supremo N° 003-2016-MTC.	GRAVE
2	La empresa operadora que en el plazo establecido no proceda a suspender parcialmente el servicio, o no mantenga la referida suspensión por el periodo establecido según corresponda, a los abonados prepago: (i) cuyo registro presente situaciones de no correspondencia con la información que obra en el RENIEC y/o (ii) que tengan la condición de persona natural con más de cinco (05) pero con menos de once (11) líneas registradas a su nombre, y estos abonados no hayan procedido a la validación de sus datos mediante el Sistema de Verificación Biométrica de Huella Dactilar, incurrirá en INFRACCIÓN GRAVE.	Literales g) y I.2) de la Primera Disposición Complementaria Final del Decreto Supremo N° 023-2014-MTC.	GRAVE
3	La empresa operadora que durante el periodo de suspensión parcial del servicio a los abonados prepago (i) cuyo registro presente situaciones de no correspondencia con la información que obra en el RENIEC, (ii) que tengan la condición de personas naturales con más de diez (10) líneas registradas a su nombre, y/o (iii) que tengan la condición de persona natural con más de cinco (05) pero con menos de once (11) líneas registradas a su nombre, no permita a estos abonados recibir llamadas, mensajes de texto, utilizar los servicios de información y asistencia y tener acceso a los números de emergencia, incurrirá en INFRACCIÓN LEVE.	(Literales g), k.2 y I.2) de la Primera Disposición Complementaria Final del Decreto Supremo N° 023-2014-MTC).	LEVE
4	La empresa operadora que no informe o informe parcialmente a través de una locución grabada, cuando se intente realizar una llamada, desde las líneas suspendidas por falta de validación de los abonados prepago (i) cuyo registro presente situaciones de no correspondencia con la información que obra en el RENIEC, y/o (ii) que tengan la condición de persona natural con más de cinco (05) pero con menos de once (11) líneas registradas a su nombre, que: (a) el servicio se encuentra suspendido hasta que los abonados cumplan con la validación y/o regularización de sus datos mediante el Sistema de Verificación Biométrica de Huella Dactilar (b) la fecha de la suspensión total del servicio, y (c) el número telefónico al que los abonados se comunicarán sin costo, para obtener información sobre el procedimiento para realizar la validación y/o regularización, incurrirá en INFRACCIÓN LEVE.	Literales g), y I.2) de la Primera Disposición Complementaria Final del Decreto Supremo N° 023-2014-MTC.	LEVE
5	La empresa operadora que en el plazo establecido no proceda a suspender totalmente el servicio, o no mantenga la referida suspensión por el periodo establecido según corresponda, a los abonados prepago: (i) cuyo registro presente situaciones de no correspondencia con la información que obra en el RENIEC, y/o (ii) que tengan la condición de persona natural con más de cinco (05) pero con menos de once (11) líneas registradas a su nombre, y estos abonados no hayan procedido con la validación de sus datos mediante el Sistema de Verificación Biométrica de Huella Dactilar, incurrirá en INFRACCIÓN GRAVE.	Literales h) y I.3) de la Primera Disposición Complementaria Final del Decreto Supremo N° 023-2014-MTC.	GRAVE
6	La empresa operadora que durante el periodo de suspensión total del servicio a los abonados prepago: (i) cuyo registro presente situaciones de no correspondencia con la información que obra en el RENIEC, y/o (ii) que tengan la condición de persona natural con más de cinco (05) pero con menos de once (11) líneas registradas a su nombre, no permita a estos abonados utilizar los servicios de información y asistencia, y tener acceso a los números de emergencia, incurrirá en INFRACCIÓN LEVE.	Literales h) y I.3) de la Primera Disposición Complementaria Final del Decreto Supremo N° 023-2014-MTC.	LEVE
7	La empresa operadora que no proceda a dar de baja el servicio a los abonados prepago (i) cuyo registro presente situaciones de no correspondencia con la información que obra en el RENIEC, y/o (ii) que tengan la condición de persona natural con más de cinco (05) pero con menos de once (11) líneas registradas a su nombre, y estos abonados no hayan efectuado la validación de sus datos mediante el Sistema de Verificación Biométrica de Huella Dactilar, incurrirá en INFRACCIÓN GRAVE.	Literales i) y I.4) de la Primera Disposición Complementaria Final del Decreto Supremo N° 023-2014-MTC.	GRAVE

ÍTEM	INFRACCIÓN	REFERENCIA NORMATIVA	SANCIÓN
8	En los casos de desconocimiento de titularidad de los servicios contratados bajo la modalidad prepago, la empresa operadora que no cumpla con realizar el cambio de titularidad correspondiente, en favor de aquellos usuarios que vienen utilizando el servicio, a través del Sistema de Verificación Biométrica de Huella Dactilar, incurrirá en INFRACCIÓN MUY GRAVE.	Último párrafo de la Primera Disposición Complementaria Final del Decreto Supremo N° 023-2014-MTC.	MUY GRAVE
9	La empresa operadora que no cumpla con el envío de los SMS preestablecidos en la Segunda Disposición Complementaria Final del Decreto Supremo N° 003-2016-MTC, en la cantidad y frecuencia comunicados por el OSIPTEL, incurrirá en INFRACCIÓN LEVE.	Tercer y último párrafo de la Segunda Disposición Complementaria Final del Decreto Supremo N° 003-2016-MTC.	LEVE
10	La empresa operadora que no cumplan con la pauta publicitaria y el contenido de los mensajes aprobados por el OSIPTEL para el desarrollo de la campaña de difusión masiva en televisión y radio, incurrirá en INFRACCIÓN LEVE.	Tercera Disposición Complementaria Final del Decreto Supremo N° 003-2016-MTC.	LEVE
11	La empresa operadora móvil que no realice la validación y/o regularización de los datos personales de sus abonados mediante el Sistema de Verificación Biométrica de Huella Dactilar, respecto a aquellos abonados prepago (i) cuyo registro presente situaciones de no correspondencia con la información que obra en el RENIEC (ii) que tengan la condición de personas naturales con más de diez (10) líneas móviles registradas a su nombre, y/o (iii) que tengan la condición de personas naturales con más de cinco (5) pero con menos de once (11) líneas móviles registradas a su nombre, incurrirá en INFRACCIÓN MUY GRAVE.	Penúltimo párrafo de la Primera Disposición Complementaria Final del Decreto Supremo N° 023-2014-MTC y Única Disposición Complementaria Final de la presente Resolución.	MUY GRAVE
12	El Operador Móvil Virtual y el Operador Móvil con Red que inicie operaciones comerciales con posterioridad a la fecha de entrada en vigencia del Decreto Supremo N° 003-2016-MTC, y que luego de transcurrido el plazo de doce (12) meses, no haya implementado en forma obligatoria el Sistema de Verificación Biométrica de Huella Dactilar, en todas las oficinas o centros de atención y puntos de venta, incurrirán en INFRACCIÓN GRAVE.	Cuarta Disposición Complementaria Final del Decreto Supremo N° 003-2016-MTC.	GRAVE