ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

COMPARATIVA DE LAS PRINCIPALES TÉCNICAS BIOMÉTRICAS PARA DISMINUIR LAS VULNERABILIDADES A LA CONFIDENCIALIDAD EN DISPOSITIVOS MÓVILES

RENE HUMBERTO ALVARADO ALVARADO

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA – ECUADOR

MAYO – 2021

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DEL TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado: **DISEÑO E IMPLEMENTACIÓN DE UN MODELO BIOMÉTRICO PARA REDUCIR LAS VULNERABILIDADES A LA CONFIDENCIALIDAD EN DISPOSITIVOS MÓVILES,** de responsabilidad del Ing. Rene Humberto Alvarado Alvarado, ha sido minuciosamente revisado por los miembros del Tribunal del Trabajo de Titulación, quedando autorizada su presentación.

Tribunal:

ING. LUIS EDUARDO HIDALGO ALMEIDA PhD. **PRESIDENTE**	LUIS EDUARDO HIDALGO ALMEIDA Firmado digitalmente por LUIS EDUARDO HIDALGO ALMEIDA Nombre de reconocimiento (DN): c=EC, o=BANCO CENTRAL DEL ECUADOR, ou=ENTIDAD DE CERTIFICACION DE INFORMACION-ECIBCE, l=QUITO, serialNumber=0000445780, cn=LUIS EDUARDO HIDALGO ALMEIDA Fecha: 2021.05.26 01:03:32 -05'00' **FIRMA**
ING. RAUL HUMBERTO CUZCO NARANJO MSC. **DIRECTOR**	RAUL HUMBERTO CUZCO NARANJO Firmado digitalmente por RAUL HUMBERTO CUZCO NARANJO Fecha: 2021.05.26 10:49:21 -05'00' **FIRMA**
ING. SAUL YASACA PUCUNA MSC. **MIEMBRO**	Firmado electrónicamente por: SAUL YASACA PUCUNA **FIRMA**
ING. BRAULIO ADRIÁN CAISAGUANO VILLA MSC. **MIEMBRO**	**FIRMA**

Febrero, 2021

DERECHOS INTELECTUALES

Yo, Rene Humberto Alvarado Alvarado, con cédula de identidad, 0301677779 declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación,** y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

Rene Humberto Alvarado Alvarado
N° de Cédula: 0301677779

DECLARACIÓN DE AUTENTICIDAD

Yo, Rene Humberto Alvarado Alvarado, declaro que el presente Proyecto de Investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados. Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.

_____

Rene Humberto Alvarado Alvarado
N° de Cédula: 0301677779

DEDICATORIA

La presente investigación está dedicada a Dios por ser mi luz y a las personas que más influyeron en mi vida, dándome los mejores consejos, guiándome y haciendo de mí una persona de bien mi familia.

Rene Humberto Alvarado Alvarado

AGRADECIMIENTO

A todos quienes participaron para la realización y ejecución de este proyecto, a mi familia por su apoyo incondicional y un especial reconocimiento y agradecimiento a mi director del trabajo de titulación Ing. Raúl Cuzco quien fue mi guía para que el proyecto se llevara a cabo.

Rene Humberto Alvarado Alvarado

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

RESUMEN

La presente investigación realizó un análisis comparativo de las principales técnicas biométricas para disminuir las vulnerabilidades a la confidencialidad en dispositivos móviles, se aplicó un proceso sistemático y continuo para comparar o evaluar productos, servicios y procesos para encontrar las diferencias y de esta manera escoger la mejor opción. Se utilizó un formulario de usabilidad manejando los criterios de evaluación de sistemas biométricos: efectividad, seguridad y eficacia. Los resultados fueron que el 72% de los usuarios de dispositivos móviles prefieren utilizar técnicas de seguridad biométrica y un 28% utilizan los sistemas convencionales para proteger su información, la cual se puede ver vulnerada por diferentes amenazas pudiendo poner en peligro su integridad. Con los resultados obtenidos en base a los parámetros presentados y con la huella dactilar como técnica biométrica más aceptada para el acceso a los dispositivos móviles, se presentó tres escenarios comparativos, el nivel de exposición es alto en los datos de información de usuario y datos sensibles cuando se utiliza los sistemas de seguridad tradicionales, porque estos sistemas son de fácil detección. Cuando existen amenazas y fallos de seguridad los datos del dispositivo móvil quedan totalmente expuestos. De acuerdo con los resultados obtenidos en el escenario seguro con la aplicación de las técnicas de seguridad biométricas, es notoria la disminución de la información expuesta con respecto al escenario vulnerable sin la aplicación de estas tecnologías. Se concluye que de todas las técnicas biométricas la más segura es la de los iris de los ojos, pero la técnica más aceptada por los usuarios es la de la huella digital.

Palabras Clave: ANÁLISIS COMPARATIVO. TÉCNICAS BIOMÉTRICAS, VULNERABILIDADES, CONFIDENCIALIDAD, DISPOSITIVOS MÓVILES

ABSTRACT

This research carried out a comparative analysis of the main biometric techniques to reduce vulnerabilities to confidentiality in mobile devices, a systematic and continuous process was applied to compare or evaluate products, services and processes to find the differences and in this way choose the best one option. A usability form was used, handling the evaluation criteria of biometric systems: effectiveness, safety and efficacy. The results were that 72% of mobile device users prefer to use biometric security techniques and 28% use conventional systems to protect their information, which can be compromised by different threats and could jeopardize its integrity. With the results obtained based on the parameters presented and with the fingerprint as the most accepted biometric technique for accessing mobile devices, three comparative scenarios were presented, the level of exposure is high in user information data and sensitive data when using traditional security systems, because these systems are easy to detect. When there are threats and security flaws, the data on the mobile device is totally exposed. According to the results obtained in the safe scenario with the application of biometric security techniques, the decrease in the information exposed with respect to the vulnerable scenario without the application of these technologies is noticeable. It is concluded that of all the biometric techniques the safest is that of the iris of the eyes, but the technique most accepted by users is that of the fingerprint.

Keywords: COMPARATIVE ANALYSIS. BIOMETRIC TECHNIQUES, VULNERABILITIES, CONFIDENTIALITY, MOBILE DEVICES

CAPÍTULO I

1 INTRODUCCIÓN

Hoy en día, las personas hacemos uso con mucha frecuencia equipos electrónicos para comunicarnos entre nosotros, almacenar información y realizar diferentes acciones de nuestro día a día. Por ejemplo, es frecuente que una persona se comunique llamando por el teléfono móvil, acceda a su correo electrónico y agenda desde su ordenador portátil o realice operaciones bancarias en un cajero automático.

Muchas de estas comunicaciones, accesos a información personal u operaciones re- quieren, en primer lugar, determinar o confirmar la identidad del individuo que trata de llevarlas a cabo, para así evitar fraudes por acciones realizadas por personas no autorizadas y, de esta manera, ofrecer una protección de seguridad a la persona legítima. Por ello, ha existido y existe, la necesidad de desarrollar nuevos sistemas de identificación personal y mejorar y adaptar los sistemas de autenticación existentes a las nuevas tecnologías y posibilidades de fraude.

Según (Cortés, 2010) La biometría consiste en medir una de las características del cuerpo humano con el fin de identificar un individuo. Para esto se debe elegir una característica dotada de una fuerte variabilidad de un individuo a otro. Dentro de los principales métodos utilizados en la biometría se encuentran: la cara, la huella, la geometría de la mano, el iris, la voz, las venas, las orejas, el pulso cardiaco, la radiografía dental, el ADN, la forma de escribir a mano y la forma de digitar en el computador.

El sistema más común en la práctica es el reconocimiento de huellas digitales, y como en cualquier otro método siempre existirá un margen de error, siendo considerado menor en este. El método de las huellas digitales se encuentra entre las diez tecnologías emergentes que cambiarán el mundo según un informe realizado por el Massachussets Institute of Technology (Cortés, 2010)

Actualmente el uso de dispositivos móviles ha cobrado gran auge debido, en mayor medida, al peso y tamaño reducido de estos aparatos, lo cual ofrece la posibilidad de llevarlos prácticamente a cualquier lugar; a su capacidad de conectarse a internet y a otros dispositivos; además sus costos son accesibles. Debido al avance tecnológico los dispositivos móviles manejan diferentes tipos de información como son: personal, salud, bancaria, laboral, entre otros; esto implica que su nivel de seguridad debe ser el suficiente para mantener la privacidad del contenido del dispositivo.

En consecuencia, las amenazas que atentan contra la seguridad de los dispositivos móviles: malware, robo, fuga de información, vulnerabilidades de software y phishing entre otras ponen

en riesgo la seguridad personal de los usuarios y de los activos de información de las organizaciones en las que estos trabajan.

Este trabajo investigativo tiene como finalidad contribuir en el campo de interés para que quienes estudian problemáticas relacionadas a la seguridad de la información en dispositivos móviles, puedan expandir sus análisis a ambientes organizacionales. Se presentan las líneas de trabajo abordadas, herramientas probadas, guías y buenas prácticas generadas para usar de manera segura dispositivos móviles.

1.1. Planteamiento del problema

1.1.1 Situación problemática

En la era de la tecnología móvil uno de los aspectos más importantes a tener en cuenta es la seguridad de la información en los dispositivos móviles, ya que en ellos almacenamos datos sensibles como claves personales, bancarias de la empresa además que los llevamos con nosotros todo el día y pueden ser objeto de miradas indiscretas mientras los estamos usando, perdida, robo, por ello, es importante minimizar los riesgos de seguridad para proteger la información confidencial en nuestros dispositivos, tanto si nos conectamos para uso personal o hacemos uso de nuestros dispositivos para el trabajo diario.

Existen diferentes tipos de amenazas como el malware que es una aplicación de software que tiene un objetivo malicioso en el dispositivo móvil donde se instala y se ejecuta sin el consentimiento del usuario. Puede tener objetivos muy variados, siendo los más comunes obtener datos personales y beneficio económico, por ejemplo, mediante la suscripción a un servicio SMS Premium, robo de credenciales, envió de información mal intencionado. Su modo de funcionamiento suele ser automático en modo background y controlado de forma remota desde un servidor, de forma transparente para el usuario.

Un equipo de investigadores de la Universidad de Darmstadt (Alemania) y el Instituto Fraunhofer para la Seguridad en las Tecnologías de la Información ha analizado 750.000 aplicaciones para Android y iOS y ha descubierto que sus desarrolladores no se toman la seguridad de este importante paso del proceso (el ‘login’ o autenticación) tan en serio como deberían.

Estos expertos aseguran que entre las apps analizadas se cuentan algunas muy populares, aunque no han dado nombres concretos y que las vulnerabilidades se han detectado en todo tipo de aplicaciones, desde juegos hasta mensajería instantánea, pasando por redes sociales, servicios financieros o incluso software vinculado con la salud.

Según los hallazgos de este grupo de académicos, muchos programadores están gestionando de forma inadecuada o negligente la información necesaria para este login, dejando nombres de usuario, direcciones de correo o contraseñas al alcance de terceros con dudosas intenciones. Durante sus análisis, han encontrado hasta 56 millones de conjuntos de datos desprotegidos.

"Los desarrolladores de apps utilizan bases de datos en la Nube para almacenar la información de los usuarios, pero aparentemente ignoran los consejos de seguridad que ofrecen los proveedores de almacenamiento", afirma el profesor Eric Bodden, autor principal del estudio, en referencia a los servicios cloud que ofrecen gigantes como Facebook (Parse) o Amazon (AWS) (Security, 2018).

1.2. Formulación del problema

¿La comparativa de las principales técnicas biométricas ayudará a identificar la adecuada, logrando así disminuir los ataques a la confidencialidad en los dispositivos móviles?

1.3. Justificación de la Investigación

El proyecto de investigación se justifica ya que se plantea ofrecer nuevas técnicas de seguridad para el acceso a los dispositivos móviles como son las biométricas que conllevan grandes ventajas sobre las seguridades convencionales que se han venido utilizando. La biometría puede ayudar a reducir de forma significativa el robo de identidad de una persona, ya que para ingresar a revisar información personal y muy sensible en el dispositivo móvil solicitara cualquiera de los rasgos o característica propia del individuo dueño del móvil para poder ingresar a las aplicaciones, y en caso de que el dispositivo sea robado el delincuente necesariamente necesitara tener conocimientos avanzados de biometría para que pueda vulnerar la seguridad si existiera y eso es casi imposible para un delincuente ordinario.

Debido a la importancia de los datos y a los beneficios que pueden generarle a los cibercriminales que buscan adueñarse de ellos, continuamente observamos brechas de seguridad relacionadas con

la fuga de información, en los cuales se utilizan distintos vectores de ataque para lograr los fines maliciosos.

Por ejemplo, en 2018 se conocieron casos de fuga de información relacionados con malware Point of Sale, en compañías como Target, Home Depot o UPS, donde los atacantes lograron obtener más de 40 millones de números de tarjetas de crédito y débito de usuarios. Empresas como eBay o Yahoo! también se vieron en la necesidad de notificar a miles de usuarios que sus cuentas y contraseñas habían sido filtradas a través de un ataque.

En 2015 otras industrias también se han visto afectadas, tal es el caso de Comunity Health System (CHS) en los Estados Unidos, que fue víctima de la fuga de 4.5 millones de registros médicos. De acuerdo con el comunicado de la entidad, sus sistemas fueron víctimas de una APT. Otro de los casos más conocidos este año, fue el robo de datos confidenciales a Ashley Madison, sitio de citas online especializado en relaciones extramaritales, que puso en potencial peligro a sus 37 millones de usuarios.

Sin importar las actividades de las empresas, la industria a la que pertenezcan, su tamaño o ubicación geográfica, e independientemente del ataque utilizado para afectarlas, la consecuencia más común suele ser la fuga de información, con los conocidos daños a la imagen de las organizaciones. En esta lista se cuentan empresas, gobiernos y otras entidades, impactado de manera negativa a sus miles, e incluso millones de usuarios.

Por estas razones, en distintos países se han emitido leyes orientadas a la protección de los datos personales, que deben cumplir entidades del sector público o privado que traten información de carácter personal. La protección de los datos es un derecho ciudadano, que brinda la facultad para controlar a voluntad la información personal de cada individuo, que es almacenada, procesada o transmitida por terceros.

1.3. Objetivos

1.3.1. Objetivos General de la Investigación

- Realizar un análisis comparativo de las principales técnicas biométricas para disminuir las vulnerabilidades a la confidencialidad en dispositivos móviles.

1.3.2. Objetivos específicos de la investigación

- Analizar las principales técnicas Biométricas en dispositivos móviles.
- Identificar las principales vulnerabilidades a la confidencialidad en dispositivos móviles.
- Determinar la técnica biométrica más segura que ayude a reducir las amenazas a la confidencialidad en dispositivos móviles.

1.4. Hipótesis

La aplicación de una técnica biométrica como es la huella digital si incrementara el nivel de seguridad a la confidencialidad en dispositivos móviles.

1.4.1. Identificación de Variables

Variable independiente: Técnica biométrica como es la huella digital.
Variable dependiente: Incrementar el nivel de confidencialidad en dispositivos móviles.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Antecedentes del Problema

El número de ciberataques a nivel mundial va en aumento día a día y los dispositivos móviles no están exceptos de esta problemática, para tener una idea más real de cómo evolucionan los ataques a nivel mundial se puede realizar un monitoreo a través de la herramienta informática Digital Attack Map (Digitalattack, 2020). Ya específicamente en dispositivos móviles España junto a Singapur, son los países del mundo en el que con más fuerza han penetrado los teléfonos móviles en la sociedad. El 92 % de la población nacional dispone de al menos uno de estos dispositivos, que nos permiten tener en el bolsillo o en la mano un sistema con el que realizar y recibir llamadas, sino que se ha convertido en una herramienta indispensable para trabajo, ocio y relaciones sociales. En total, España dispone de 56 millones de estos teléfonos, el equivalente a más de uno por persona. En las figuras 1:2 (ataques ocurridos el 1 de enero del 2016) y 2:2 (ataques ocurridos el 26 julio del 2020) se presenta un monitoreo diario de las vulnerabilidades que ocurren a nivel mundial. Dentro de estos equipos se almacena información personal muy importante, desde fotografías o contactos hasta aplicaciones que conducen a información bancaria y confidencial, de tal manera que es fundamental que estos teléfonos estén bien protegidos ante amenazas externas. A su vez, el habitual alto precio de estas nuevas tecnologías añade un factor negativo a perder el móvil.

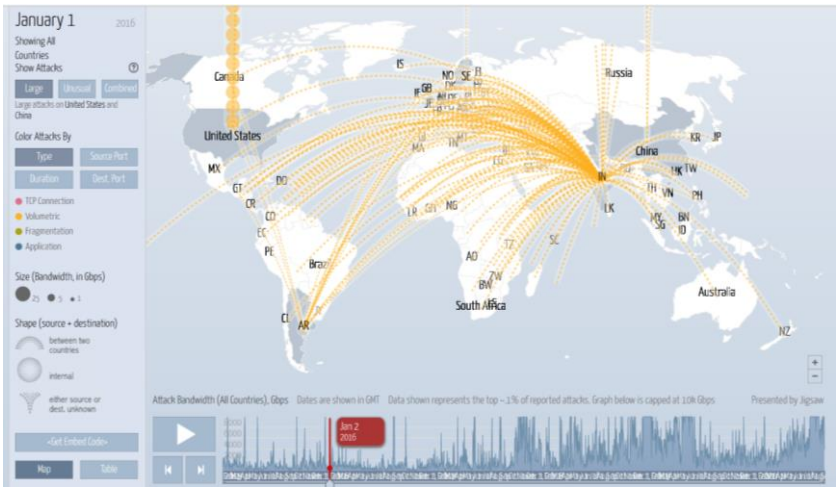

Figura 1-2 Vulnerabilidades 1 de enero 2016

Fuente: (Digitalattack, 2020)

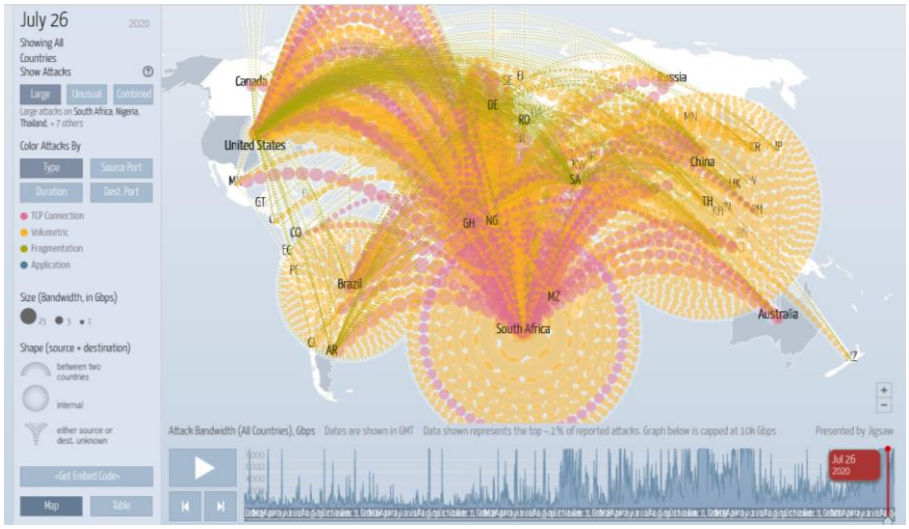

Figura 2-2 Vulnerabilidades 26 de julio 2020

Fuente: (Digitalattack, 2020)

Más allá de códigos de desbloqueo o contraseñas, el presente y el futuro está encaminado al uso de la biometría. Esta clase de soluciones convierte en una cuestión del pasado usar patrones numéricos o dibujos para acceder al móvil, que pueden ser detectados con facilidad, o contraseñas numéricas que no son difíciles de percibir.

Las técnicas biométricas tienen como forma de autentificar al usuario al propio cuerpo humano y sus rasgos individuales. El uso de la huella dactilar es ya una realidad en varios modelos teléfonos móviles, que han apostado por esta tecnología para brindar un valor añadido en la seguridad de sus millones de clientes.

Que las marcas se inclinen por estos modernos recursos de seguridad tiene mucho que ver con lo cotizado que están los teléfonos móviles entre los ladrones. Según la Secretaría de Estado, en España se roba uno de ellos cada dos minutos, pues en su último informe hubo un total de 279.319 denuncias por dispositivos sustraídos.

Dado que la huella dactilar es inimitable, ni se puede copiar o robar, la utilización de la biometría en la seguridad del teléfono móvil dificulta notablemente que un móvil robado pueda utilizarse con normalidad. Puesto que las soluciones biométricas ya están presentes en muchos ámbitos de la seguridad colectiva y privada, son varias las marcas que han apostado claramente por estas modernas técnicas de protección. No obstante, es importante señalar que no es lo mismo un sensor que un lector biométrico, pues este último es el sistema

Prestigiosos fabricantes de telefonía móvil como Apple, Microsoft o Samsung llevan ya varios años incluyendo lectores de acceso por huella para que solo el propietario del dispositivo pueda entrar en el mismo a partir de un lector ubicado en la parte de atrás del aparato. Otras firmas, como Alcatel, ZTE o Xiaomi, ya incluyen técnicas de acceso por huella biométrica para prestar un extra de seguridad y protección a los usuarios.

Este mercado está dejando atrás las tradicionales contraseñas o códigos de desbloqueo en favor de soluciones sustentadas en la biometría. El factor diferencial que esta aporta no es otro que la imposibilidad de imitar, robar o copiar el cuerpo humano, que tiene gracias a los dispositivos biométricos la llave de acceso al actual almacén de buena parte de la información indispensable de millones de personas: el teléfono móvil.

El iPhone 5S de Apple fue el primer teléfono inteligente con un sensor que reconoce las huellas dactilares. Y el sistema o servicio Apple Pay abrió las puertas a la autenticación de huellas digitales para realizar los pagos mediante dispositivos móviles.
Otros dispositivos "ya incorporan el desbloqueo mediante escaneo de iris, señala Anna Martí, editora del sitio especializado Xataka Móvil (XATAKA-móvil, 2020).

En el caso de los teléfonos tope de gama de Microsoft -los Lumia 950 y 950 XL-, el sistema funciona con el software Windows Hello y trabaja mediante reconocimiento del iris mediante dos cámaras específicas: una para tomar una foto de los ojos del usuario y otra con iluminación infrarroja.

La información obtenida se compara con la almacenada en menos de dos segundos". Otros modelos y compañías ya habían incorporado el desbloqueo por iris antes que Microsoft: Fujitsu -con el equipo NX F-04G, disponible en Japón-, el Vivo X5Pro, el ZTE Grand S3, el Alcatel Idol 3 y el UMI Iron. Por otro se espera que el modelo Samsung Galaxy Note 6, que se lanzará en septiembre de este año, incluya sensores de reconocimiento de iris.

La biometría en la banca. En el segmento bancario, si bien los reconocimientos de rostro y de huellas dactilares ya comenzaron a utilizarse, "la biometría de voz sigue siendo el método más dominante cuando se trata de agregar seguridad a la banca móvil, ya que funciona independientemente del tipo de dispositivo y es un método rentable en comparación con otros biométricos –asegura Hilal Bakanay, referente de marketing de la firma Sestek-. Al usar los micrófonos existentes en los móviles, no requiere ninguna inversión en hardware y elimina los costos relacionados".

Desde esta perspectiva, los continuos desarrollos -incluida una mayor capacidad de captura de voz por mejoras en los micrófonos, y el uso de algoritmos más sofisticados como resultado de una mayor capacidad de procesamiento computacional- "permiten que la biometría de voz proporcione una autenticación más fiable y precisa, convirtiéndose en una medida eficaz, rápida y cómoda contra el fraude –asegura Bakanay-. Además, elimina la necesidad de llevar las credenciales de seguridad personales, o de mantenerlas en un dispositivo móvil".

Un caso de aplicación concreta es el de la entidad financiera Atom, del Reino Unido, que lanzó recientemente la modalidad de reconocimiento de rostro y de voz para que los clientes se autentiquen en su app de banca móvil. Este banco registra las credenciales de identidad creando un identificador único de rostro, voz y clave de acceso, con lo cual el cliente puede elegir la forma en que desea iniciar sesión.

Soluciones biométricas en dispositivos móviles

Los smartphones ofrecen cada vez más funcionalidades y nos sirven para acceder a un creciente número de servicios. Esto los convierte en una potencial fuente de amenaza (INCIBE, 2016). Los dispositivos biométricos ofrecen un excelente nivel de seguridad en el proceso de autenticación, muy superior a la ofrecida por los códigos PIN (Personal Identification Number) que se han venido utilizando tradicionalmente. Gran número de smartphones ya incluyen dispositivos de autenticación biométricos (INCIBE, 2016).

Gestión de riesgos en biometría

La implantación y el empleo de tecnologías biométricas están expuestos a una serie de riesgos, algunos específicos y otros compartidos con las demás tecnologías y técnicas de identificación (INCIBE, 2016).

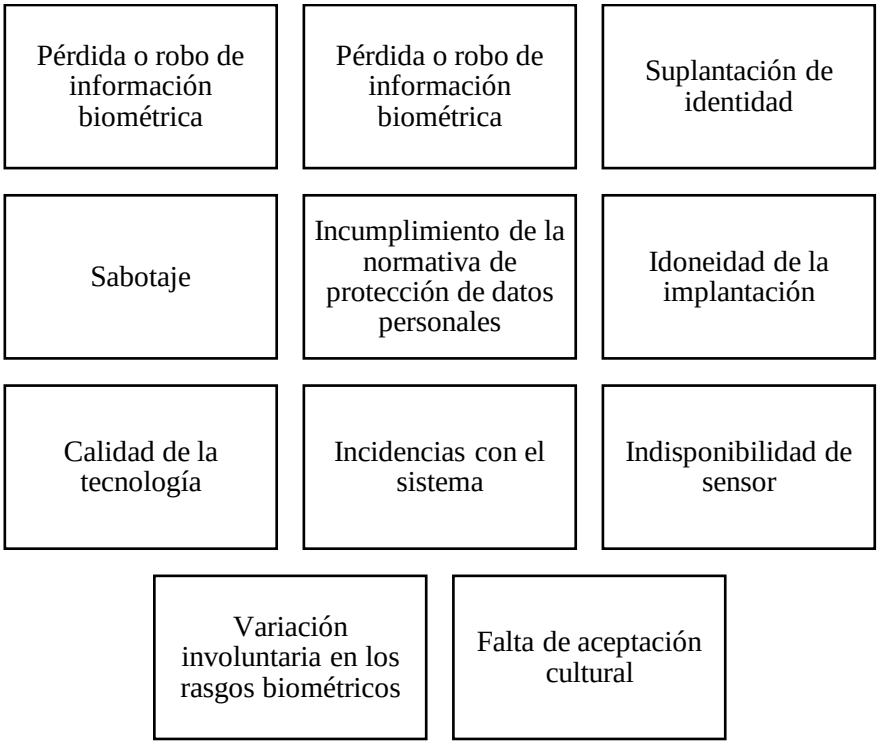

Figura 3-2 Consideraciones en biometría

Fuente: (INCIBE, 2016)

Elaborado por: Alvarado, René 2020

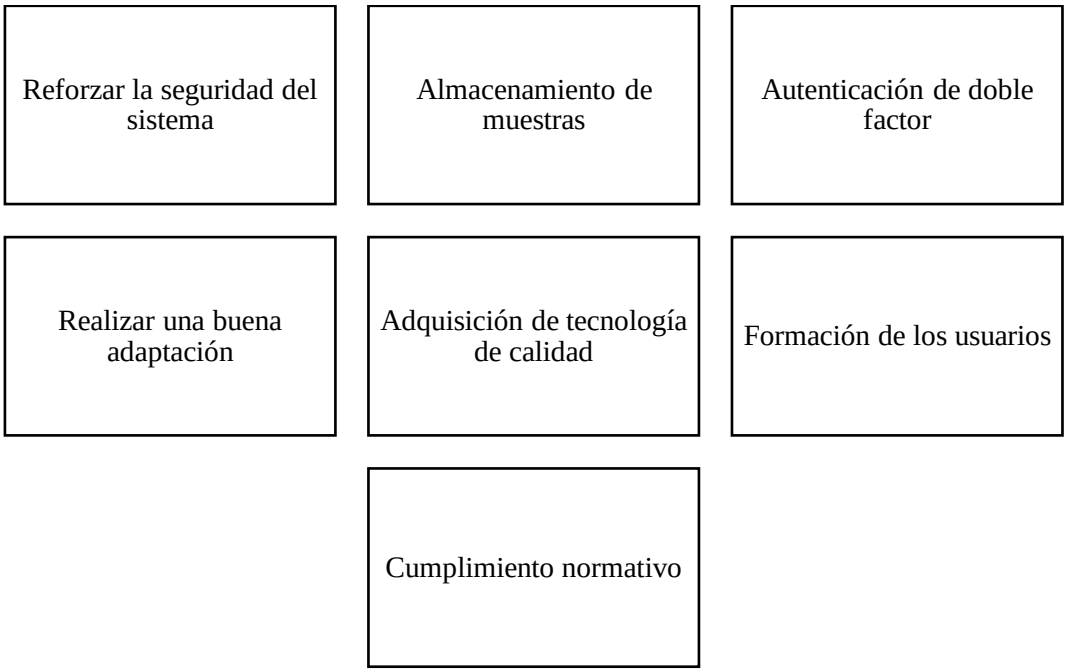

Figura 4-2 Buenas prácticas en el empleo de técnicas biométricas

Fuente: (INCIBE, 2016)

Elaborado por: Alvarado, René 2020

2.2. Dispositivos móviles

Un dispositivo móvil se define como un aparato o dispositivo pequeño que cuenta con capacidades de procesamiento, conexión permanente o intermitente a una red, memoria limitada, diseños específicos para una función principal y versatilidad para el desarrollo de otras funciones. Tanto su posesión como su operación se asocian al uso individual de una persona, quien puede configurarlo a su necesidad y a su gusto (Escobar & Quinto, 2015).

2.3 Principales Vulnerabilidades a la confidencialidad en dispositivos móviles

2.3.1 Vulnerabilidades

Los dispositivos móviles se han convertido en una herramienta básica en la vida cotidiana, debido a su popularidad "enfrentan una serie de amenazas que aprovechan las numerosas vulnerabilidades que comúnmente se encuentran en tales dispositivos.

Estas vulnerabilidades pueden ser el resultado de controles técnicos inadecuados, pero también consecuencia de las malas prácticas de seguridad de los consumidores (Escobar & Quinto, 2015).

2.3.1.1 Vulnerabilidades conocidas y que son las más comunes en las plataformas móviles.

- ✓ **Los dispositivos móviles no tienen contraseñas habilitadas.**

Muchos de los usuarios, al adquirir estos dispositivos móviles, no registran el acceso con contraseñas para poder salvaguardar los datos almacenados. Muchos dispositivos tienen la capacidad técnica para soportar contraseñas, números de identificación personal (PIN) o patrones de clave en la pantalla para la autenticación (Escobar & Quinto, 2015).

- ✓ **Las transmisiones inalámbricas no siempre están encriptadas.**

Las redes públicas o gratis de Wi-Fi, no sólo están abiertas a los usuarios, sino también a ataques de piratas informáticos que intentan robar datos confidenciales.

La información generada por un dispositivo móvil no suele estar cifrada durante su transmisión. Muchas aplicaciones no encriptan los datos que transmiten y reciben a través de la red, lo que

facilita que puedan ser interceptados. Por ejemplo, si una aplicación está transmitiendo datos a través de una red WiFi sin encriptar y utilizando HTTP (en lugar de HTTP seguro), los datos pueden ser fácilmente interceptados. Cuando una transmisión inalámbrica no está cifrada, los datos pueden ser interceptados fácilmente (Escobar & Quinto, 2015).

- ✓ **Los dispositivos móviles pueden contener malware**

Los usuarios pueden descargar aplicaciones que contienen malware. Los consumidores descargan estos programas sin saberlo, ya que pueden estar disfrazados como un juego, parche de seguridad, utilidad o aplicación. Es difícil que los usuarios noten la diferencia entre una aplicación legítima y una que contenga un software malicioso. Cuando una transmisión inalámbrica no está cifrada, los datos pueden ser fácilmente interceptados por intrusos que pueden obtener acceso no autorizado a información sensible (Escobar & Quinto, 2015).

- ✓ **Los dispositivos móviles a menudo no utilizan software de seguridad.**

Al adquirir un dispositivo móvil, las empresas distribuidoras no instalan un software para protegerse de aplicaciones como virus, troyanos, spyware y spam; además los usuarios, por desconocimiento del funcionamiento del móvil, no saben instalar dicho software, por ende, no conocen la importancia de tener un aplicativo de seguridad (Escobar & Quinto, 2015).

- ✓ **Los canales de comunicación pueden estar mal asegurados.**

Uno de los problemas más comunes de seguridad es dejar abiertos los canales de comunicación. El Bluetooth, o en el modo 'descubrimiento' (que permite que el dispositivo sea visto por otros dispositivos compatibles con Bluetooth para que se puedan hacer conexiones), podría permitir que un atacante instale malware a través de esa conexión, o active subrepticiamente un micrófono o una cámara para espiar al usuario (Escobar & Quinto, 2015).

- ✓ **Descargar nuevas aplicaciones solamente a través de los canales oficiales de los fabricantes.**

El software malicioso no es un problema exclusivo de los ordenadores, también afecta a los Smartphone y Tablets, por tanto, necesitan la misma protección que se utiliza en cualquier PC.

Al instalar aplicaciones de cualquier otra fuente, como páginas web u otras tiendas de aplicaciones, estamos corriendo el riesgo de instalar aplicaciones maliciosas (Escobar & Quinto, 2015).

- ✓ **El dispositivo móvil y las aplicaciones actualizadas.**

Uno de los problemas principales de seguridad en los dispositivos móviles es tener desactualizadas sus apps. Un inconveniente de los parches de seguridad para las aplicaciones de terceros es que no siempre se desarrollan y se publican en el momento oportuno. Además, las aplicaciones móviles de terceros, incluyendo los navegadores web, no siempre notifican a los consumidores cuando hay actualizaciones disponibles.

- ✓ **Protección ante el robo o la pérdida de un terminal móvil.**

Los dispositivos móviles como los Smartphone y las Tablets correen un riesgo diario de robo o extravío; la solución ante estos escenarios no es dejar de usarlos, sino salvar la información contenida para que la pérdida del equipo no sea traumática.

- ✓ **Los dispositivos móviles a menudo no utilizan firewall de seguridad.**

Los dispositivos móviles como los Smartphone y las Tablets corren un riesgo al momento de conectarse a una red WI-FI desconocida, donde automáticamente empieza a descargar o actualizar las apps instalados, dando la posibilidad de que se instale un software malicioso o malintencionado y pueda dañar o robar la información.

- ✓ **Software de seguridad.**

Para prevenir problemas de seguridad, en el mercado existen varias opciones de antivirus y según cada necesidad, las licencias pueden obtenerse en forma gratuita o pagando una suscripción. Algunos de los antivirus más conocidos son kaspersky, mcafee, avg, norton antivirus, eset nod32, ¡Avast!, panda, avira antivirus, entre otros.

2.3.1.2 Vulnerabilidades poco conocidas y que son las más comunes en las plataformas móviles.

- ✓ **Masquerading.**

  Acción en la que el atacante suplanta la identidad de alguna entidad del sistema (estación base o dispositivo móvil) para obtener acceso a recursos de este sistema. Este ataque incide directamente en la propiedad de autenticación. Para prevenirlo, es necesario un buen proceso de autenticación, tanto por parte del dispositivo móvil como de los puntos de acceso a la red. Ejemplo de masquerading: un atacante puede suplantar una estación base de la red (emitiendo una señal de más potencia que la de la estación base legítima) y así capturar mensajes de autenticación de los usuarios. Una vez obtenida la información de estos mensajes, se puede hacer pasar por uno de los usuarios legítimos de la red para obtener acceso a los recursos.

- ✓ **Denegación de servicio.**

  Acción en la que el atacante consigue que el servicio no esté disponible para los usuarios legítimos o que el servicio se retrase o se interrumpa. Este hecho se debe a que estos ataques se suelen llevar a cabo incluso con anterioridad al proceso de autenticación, justamente con el envío masivo de solicitudes de este tipo. Ejemplo de ataque de denegación de servicio: un ataque de denegación de servicio en una red inalámbrica se puede llevar a cabo mediante la generación de una señal de radio de la misma frecuencia que la de la red inalámbrica, pero con una potencia superior. De esta manera se atenúa la señal de la red, con lo cual no se permite a los usuarios utilizarla. Este tipo de ataques también se conoce como jamming. En inglés, deny of service (DoS).

- ✓ **Eavesdropping.**

  Acción en la que el atacante obtiene información de una comunicación de la que no es ni emisor ni receptor. En este caso, el atacante vulnera la confidencialidad de la información que ha interceptado. Este tipo de ataque se clasifica como ataque pasivo, ya que el atacante obtiene información de los datos en tráfico, pero no puede realizar ninguna acción sobre la red ni sobre la información que circula. Es importante tener en cuenta, sin embargo, que la información obtenida en un ataque de eavesdropping puede dar lugar a un posterior ataque de masquerading. La palabra eavesdropping no tiene equivalente en castellano y se traduce como escuchar secretamente.

- ✓ Confidencialidad de posicionamiento. Acción en la que el atacante obtiene, mediante diferentes técnicas, la posición física de un dispositivo móvil y, por lo tanto, la de su propietario. Este tipo de ataque puede afectar seriamente a la privacidad de las personas, en tanto que pueden ser localizadas en cualquier momento por el mero hecho de tener un dispositivo móvil en funcionamiento. Ejemplo de ataque de confidencialidad de posicionamiento: La posición del dispositivo móvil se puede utilizar de manera positiva en aplicaciones para controlar flotas de transportes, pero también se puede utilizar de manera maligna, por ejemplo, para el envío de propaganda no deseada (spamming) relacionada con establecimientos próximos a la localización de los dispositivos móviles (Domingo, 2017).

Tabla 1-2 Amenazas y vulnerabilidades de técnicas biométricos en dispositivos móviles

Amenaza	**Descripción**
Pérdida o robo de la información biométrica	Las técnicas biométricas manejan información exclusiva y propia del individuo por lo tanto esta amenaza es considerada un incidente de seguridad grave.
Suplantación de identidad	Es cuando el acceso a espacios o aplicaciones restringidas se da con el uso de información biométrica falsa o robada.
Sabotaje	Evitar el correo funcionamiento de las técnicas biométricas realizando ataques consientes a los sensores.
Incumplimiento de la normalidad de protección de datos personales	No cumplir con la ley de protección de datos (Ley 1581 de 2012) o dar un trato inadecuado a los datos biométricos.
Idoneidad de la implantación	Es la necesidad de realizar un análisis entre costo y beneficio de la implementación de un sistema biométrico
Calidad de la tecnología	El uso de tecnología de punta y adecuada, garantiza mayor seguridad en el uso de técnicas biométricas, se requiere incluir en este punto todos los elementos de un sistema biométrico, para garantizar la calidad de los sensores, el desempleo eficiente del algoritmo de comparación, los controles criptográficos de la base de datos y la integración con otras técnicas.
Incidencias con el sistema	Tener en cuenta un plan de contingencia que supla fallos eléctricos y de comunicación.

Elaborado por: Alvarado, René 2020

Fuente: (INCIBE, 2016)

Se entiende por vulnerabilidad o fallo de seguridad todo aquello que provoca que los sistemas informáticos funcionen de manera diferente a lo programado, afectando la seguridad y pudiendo llegar a provocar la pérdida y/o robo de información sensible (Escobar & Quinto, 2015)

La seguridad móvil juega un rol cada vez más importante en la protección de los activos de información, tanto para usuarios hogareños como corporativos. De hecho, con el advenimiento de la Internet de las Cosas y de los miles de dispositivos no tradicionales que son controlados mediante aplicaciones móviles, la seguridad de nuestros teléfonos se vuelve cada vez más relevante para proteger los equipos que a ellos se conectan (Giusto , 2019).

2.2.1. Vulnerabilidades en Android

En lo que a vulnerabilidades en Android respecta, hasta junio del corriente año se publicaron 86 fallos de seguridad, lo cual representa el 14% del total de vulnerabilidades reportadas para esta plataforma en 2018, año en que la cantidad de CVE alcanzó los 611 fallos publicados.

El 68% de los fallos publicados en 2019 fueron de criticidad alta y el 29% de ellos permitía la ejecución de código malicioso. Esto resulta una desmejora considerable respecto a años anteriores, donde el porcentaje de fallos graves era más bajo (Giusto , 2019).

Figura 5-2 Vulnerabilidades de criticidad alta en Android a lo largo de los años

Fuente: (Giusto Bilic, 2019)

1.6.1.1 *Detecciones de malware*

Ha decrecido un 8% con respecto al primer semestre de 2018 y un 10% respecto al segundo semestre del pasado año, quizás como resultado a los esfuerzos que Google e investigadores de seguridad realizan para detectar amenazas e impedir su propagación (Giusto , 2019).

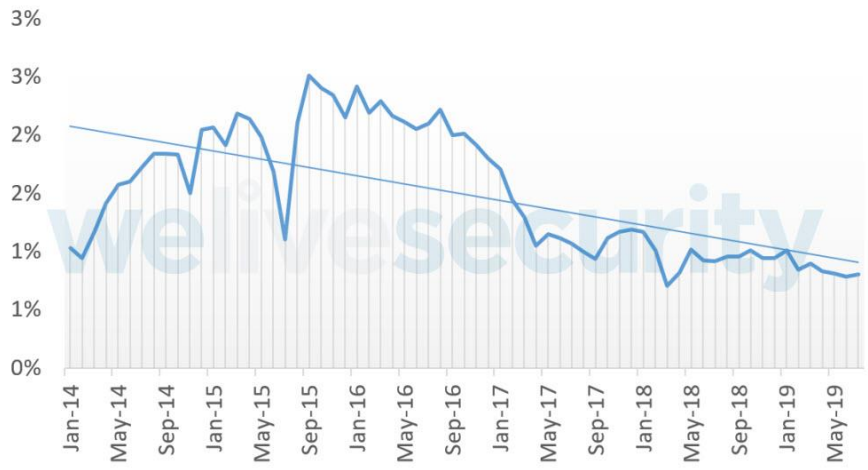

Figura 6-2 Detecciones de malware para Android en 2019

Fuente: (Giusto Bilic, 2019)

A pesar de este decrecimiento, las criptomonedas siguen bajo la mira de los atacantes. Otra de las modalidades que usan para obtenerlas es mediante el robo de credenciales de acceso a billeteras en línea a través de troyanos inmiscuidos en Google Play Store, como ocurrió con estas falsas apps de billeteras electrónicas recientemente descubiertas (Giusto , 2019).

Mientras, el malware bancario para Android también ha dado que hablar. Desde sus comienzos, la cantidad de nuevas variantes de spyware móvil y, particularmente, de troyanos dedicados al robo de datos financieros no para de aumentar. Variantes de Cerberus, un malware que superpone pantallas para robar credenciales bancarias se ha encontrado siendo vendidas mediante redes sociales en el último tiempo (Giusto , 2019).

2.2.2. *Detecciones de malware para Android por país*

En el primer semestre de 2019, las detecciones de malware para Android se concentraron en los siguientes países.

Tabla 2-2 Detecciones de malware para Android por país.

A NIVEL MUNDIAL	
PAÍS	**PORCENTAJE**
Rusia	16%
Irán	15%
Ucrania	8%
A NIVEL DE LATINOAMÉRICA	
México**,**	26%
Perú	16%
Brasil	12%

Se concentraron mundialmente en Rusia (16%), Irán (15%) y Ucrania (8%). Si tomamos en cuenta los países latinoamericanos, los países con mayores detecciones fueron México (26%), Perú (16%) y Brasil (12%) (Giusto , 2019).

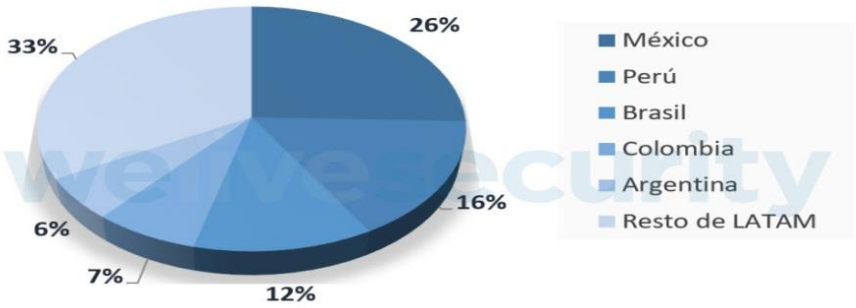

Figura 7-2 Países de Latinoamérica con mayor cantidad de detecciones de malware para Android en 2019

Fuente: (Giusto , 2019)

2.2.3. *Seguridad en iOS.*

Para iOS se publicaron 156 vulnerabilidades en lo que va de 2019, cifra que representan un aumento de 25% en la cantidad de fallos encontrados para este sistema operativo con respecto a 2018 y casi el doble de las encontradas en Android durante el corriente año. Es un claro indicador de que la cantidad de vulnerabilidades superará a fin de año la cifra obtenida en 2018. Sin embargo, el porcentaje de fallas de criticidad alta es inferior a Android, rondando el 20% (Giusto , 2019)

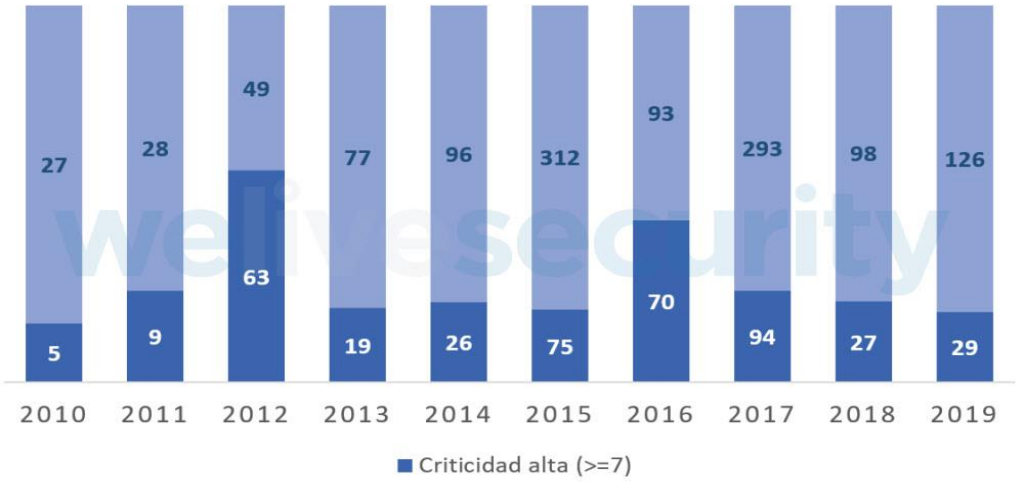

Figura 8-2 Vulnerabilidades de criticidad alta en iOS a lo largo de los años

Fuente: (Giusto , 2019)

2.3.3 Detecciones de malware

Por otro lado, las detecciones de malware para iOS aumentaron un 43% con respecto al primer semestre del pasado año. La cantidad de nuevas variantes de malware continúa siendo muy baja, lo cual nos indica que el interés de los cibercriminales continúa posándose sobre Android, donde se encuentra la mayor cantidad de usuarios (Giusto , 2019).

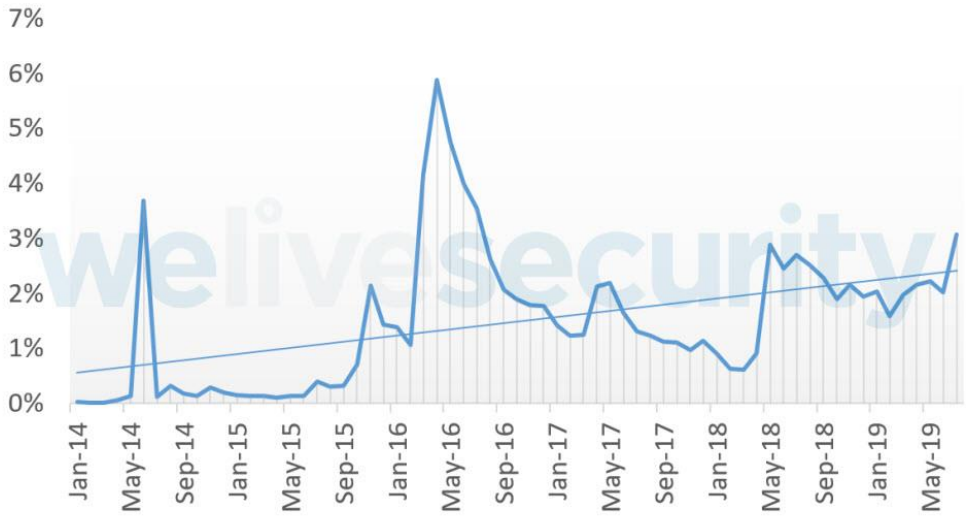

Figura 9-2 Detecciones de malware para iOS en 2019

Fuente: (Giusto , 2019).

En cuanto a la distribución geográfica de estas detecciones, vemos que mundialmente estas se concentran principalmente en China (75%), India (7%) y Taiwán (4%). En este sentido, es interesante notar la aparición de India entre los primeros puestos, desplazando a Hong Kong de su posición.

Ahora bien, dentro de América Latina, en 2019 los países con mayores detecciones fueron Ecuador (20%), Colombia (18%) y México (17%) (Giusto , 2019).

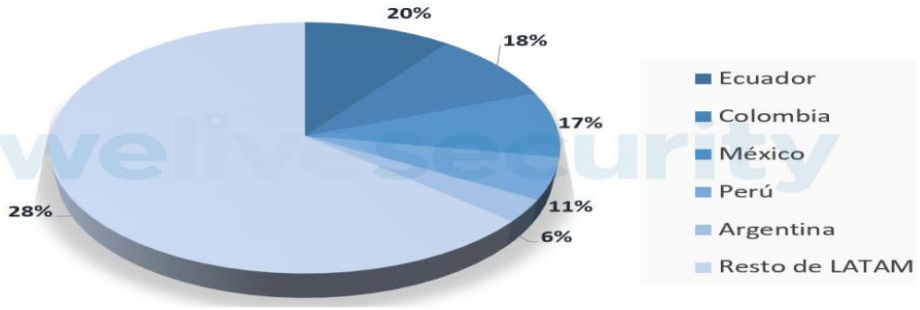

Figura 10-2 Países de Latinoamérica con mayor cantidad de detecciones de malware para iOS en 2019

Fuente: (Giusto , 2019)

2.3. Técnicas Biométricas en dispositivos móviles.

2.4. Biometría

Todos los seres humanos tenemos características físicas y conductuales únicas que nos diferencian. La geometría de las partes de nuestro cuerpo tales como la de las manos, cara, nuestros ojos y tal vez la más conocida, la huella digital, componen algunos rasgos que nos diferencian del resto de los seres humanos figura 11-2

Además, proporciona un nivel más alto de seguridad, al constituir una unívoca "firma" de una característica humana que no puede ser fácilmente adivinada o falsificada. La identificación y autentificación biométrica explota el hecho de que ciertas características biológicas son singulares e inalterables y, además, imposibles de perder, transferir u olvidar [Hong, 1998]. Esto las hace más confiables, amigables y seguras que las ampliamente usadas palabras clave (passwords) (Villalobos Castaldi, 2011).

Figura 11-2 Rasgos físicos que diferencian a los seres humanos

Fuente: (Villalobos Castaldi, 2011)

2.5. Concepto de Biometría.

La biometría es la ciencia de la identificación de los seres humanos sobre la base de características físicas únicas. A la biometría se le define también como la ciencia dedicada al estudio estadístico de las características cuantitativas de los seres vivos como son: peso, longitud, entre otros. Este término es utilizado para referir a los métodos automáticos que analizan determinadas características humanas con el fin de identificar y autenticar a las personas (Perez, 2011).

El término se deriva de las palabras griegas "bios", vida y "metrón", medida. Todos los seres humanos poseemos características morfológicas únicas que nos diferencian, las que bien pueden ser estáticas (huellas dactilares, retina, iris, patrones faciales, venas de la mano, la geometría de la palma de la mano, etc.) o dinámicas (firma, paso o caminata, tecleo, etc.) (Villalobos Castaldi, 2011)

2.6. Características de un indicador biométrico.

Un indicador biométrico es alguna característica con la cual se puede realizar biometría.

Cualquiera sea el indicador, debe cumplir los siguientes requerimientos:

- ***Universalidad:*** cualquier persona posee esa característica.
- ***Unicidad:*** la existencia de dos personas con una característica idéntica tiene una probabilidad muy pequeña
- ***Permanencia:*** la característica no cambia en el tiempo
- ***Cuantificación:*** la característica puede ser medida en forma cuantitativa.

Los requerimientos anteriores sirven como criterio para descartar o aprobar a alguna característica como indicador biométrico. Luego de seleccionar algún indicador que satisfaga los requerimientos antes señalados, es necesario imponer restricciones prácticas sobre el sistema que tendrá como misión recibir y procesar a estos indicadores (Alvarado, Landeta , & Sánchez , 2010)

2.7. Arquitecturas de las técnicas biométricas

Las técnicas biométricas se utilizan para reconocer a personas según ciertos rasgos distintivos. Estas técnicas pueden funcionar únicamente de acuerdo con dos arquitecturas:

2.7.1. *Autenticación o verificación*

Se corresponde con la pregunta "¿Es quién dice ser?". Así pues, se trata de averiguar si la persona que se identifica en el sistema es realmente quien dice ser. Para ello, en primer lugar, la persona ha de comunicar su identidad y a continuación se realiza una única comprobación para verificar si los rasgos biométricos del usuario que trata de acceder son los del usuario que dice ser (que deben estar previamente almacenados en el sistema). Por tanto, es una comparación 1:1. (Guerra Casanova, 2014)

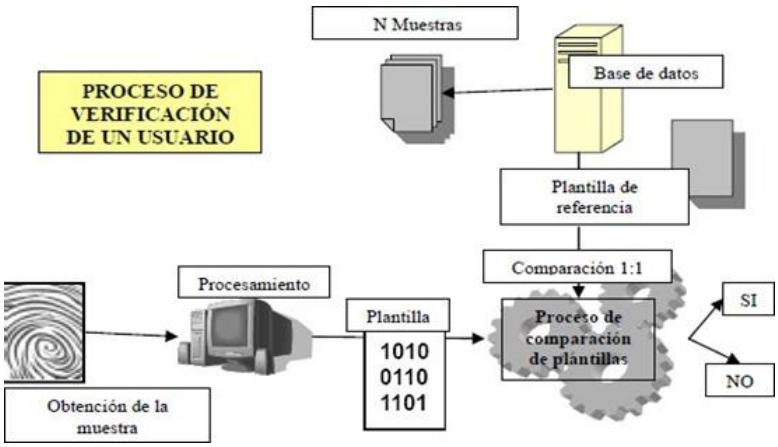

Figura 12-2 Esquema del proceso de verificación

Fuente: (Villalobos Castaldi, 2011)

2.7.2. *Identificación o reconocimiento*

Se pretende responder a la pregunta: "¿Quién es?". En este caso, se trata de identificar a un individuo entre una población de N personas conocidas por el sistema, con el objetivo de averiguar quién es. Para ello se requiere una comparación 1: N, donde el sistema indica la persona más parecida a todas las que se conoce (o bien, si no existe una persona suficientemente parecida registrada) (Guerra Casanova, 2014).

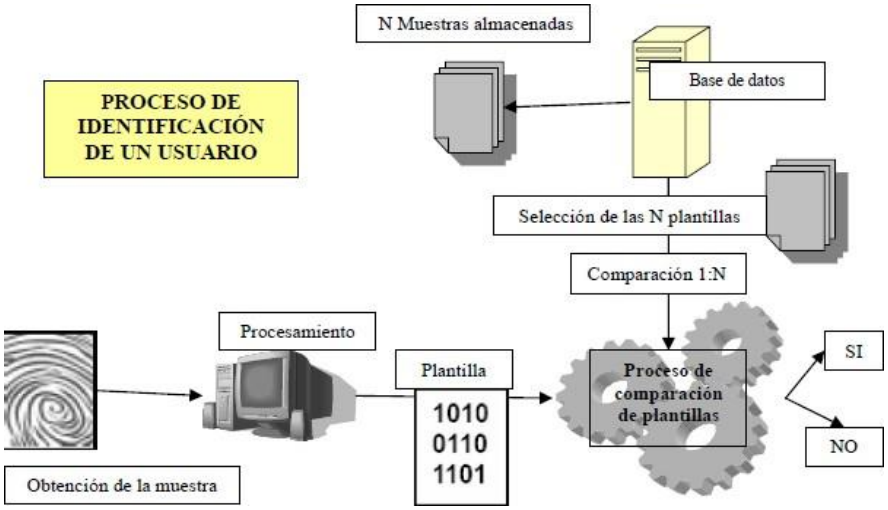

Figura 13-2 Esquema del proceso de identificación

Fuente: (Villalobos Castaldi, 2011)

En general, las técnicas biométricas para identificación son más complejos, requieren más tiempo (tienen que hacer más comparaciones) y obtienen peor rendimiento que los sistemas de verificación (Guerra Casanova, 2014).

Aunque existen técnicas biométricas que se pueden utilizar para identificación y verificación, su funcionamiento en identificación está muy limitado por el tiempo de procesamiento y el número de usuarios de la base de datos entre los que se trata de identificar. De hecho, un sistema de verificación puede entenderse como un sistema de identificación sencillo de una única persona (Guerra Casanova, 2014).

Para cualquiera de estas arquitecturas, el funcionamiento del sistema biométrico se divide en dos fases, la fase de enrolamiento y la fase de acceso.

- **En la fase de enrolamiento:** El sistema ha de aprender quién es el usuario. Para ello, toma distintas muestras del rasgo biométrico que utilice el sistema y, a partir de ellas, calcula y almacena un patrón ligado a la identidad del usuario. Una vez que el usuario ya esté enrolado en el sistema, puede ser verificado o identificado cuando se requiera (Guerra Casanova, 2014).
- **En la fase de acceso:** El sistema extrae una muestra de la característica bio- métrica del usuario, y la compara respecto al patrón que tiene almacenado suyo (en caso de verificación) o respecto a todos los patrones de su base de datos (en caso de identificación). A partir de la comparación (o comparaciones), el sistema indica de manera automática si el usuario es quien dice ser (verificación) o si se ha encontrado un

usuario en la base de datos que se ajuste al usuario que trata de acceder (identificación) (Guerra Casanova, 2014).

Cada una de las fases tiene distintas etapas, donde se realizan acciones concretas necesarias para el correcto funcionamiento del sistema biométrico. Estas etapas pueden observarse en la Figura 2:14. Puede comprobarse que existen etapas comunes para el modo de enrolamiento y el modo de acceso.

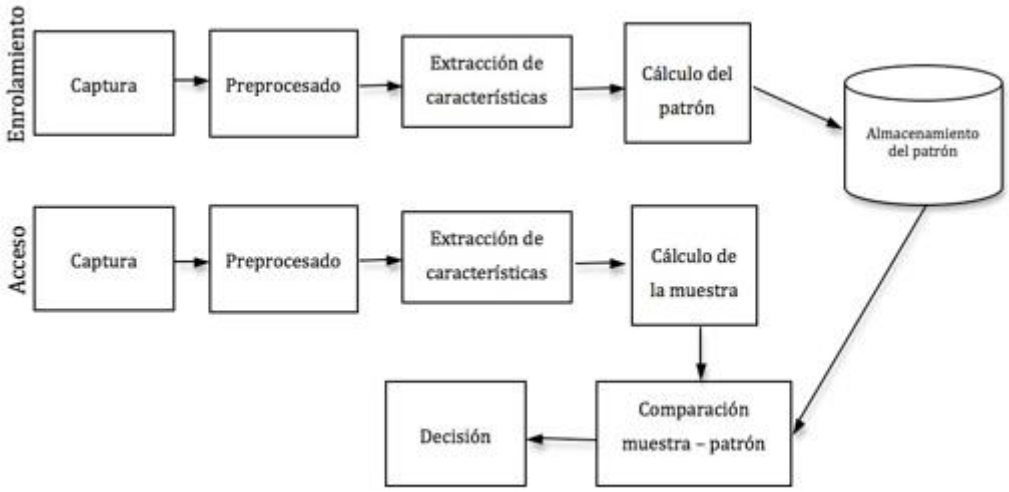

Figura 14-2 Etapas de un sistema biométrico completo.

Fuente: (Guerra Casanova, 2014)

2.8. Etapas de las técnicas biométricas

2.8.1. *Captura o adquisición*

El sistema toma una muestra del rasgo biométrico deseado. Para ello, es necesario un dispositivo con un sensor que recoja los datos biométricos. Por ejemplo, una huella dactilar puede capturarse a partir de cámaras de vídeo, cámaras de fotos, ultrasonidos, láser, tinta, etc. (Guerra Casanova, 2014).

2.8.2. *Preprocesado y control de calidad*

Las técnicas de preprocesado permiten mejorar la calidad con la que se han obtenido las muestras o seleccionar las zonas donde reside el patrón biométrico, de cara a que la siguiente etapa de

extracción de características pueda recoger los datos de la manera más precisa y distintiva del usuario posible (Guerra Casanova, 2014).

Por ejemplo, pueden utilizarse filtros, canceladores de ruido, técnicas de segmentación, etc. Además, en esta fase, es necesario asegurar la calidad de la toma de muestras, solicitando una nueva muestra al usuario si no se ha capturado de manera correcta (por ejemplo, en una captura de iris el usuario tenía el ojo cerrado) (Guerra Casanova, 2014).

2.8.3. *Extracción de características*

Esta etapa traduce una muestra en un vector de características, con los valores numéricos de las características que el sistema biométrico considera unívocas. Por ejemplo, traduce una foto de una cara en un vector con las distancias entre puntos de referencia de zonas de la cara (distancia entre ojos, anchura de la cara, etc.) (Guerra Casanova, 2014).

Etapas que se llevan a cabo únicamente en el momento del enrolamiento:

2.8.4. *Cálculo del patrón*

A partir del vector de características de una o varias mues- tras se forma un patrón biométrico, que se asocia con una identidad de una persona concreta. Es muy común calcular el patrón biométrico a partir de varias muestras de enrolamiento del usuario (Guerra Casanova, 2014)

2.8.5. *Almacenamiento del patrón*

El patrón biométrico ha de ser almacenado de manera segura, puesto que, en los siguientes accesos del usuario, es necesario realizar una comparación respecto a él para comprobar la veracidad de la identidad del usuario o identificarle en una base de datos (Guerra Casanova, 2014).

Etapas que se realizan tan sólo cuando el usuario quiere acceder al sistema:

2.8.6. *Cálculo de la muestra*

El vector de características se traduce en una muestra a partir de la cual se compara con el patrón biométrico asociado a su identidad. En numerosas ocasiones la muestra es directamente el vector de características (Guerra Casanova, 2014).

2.8.7. *Etapa de comparación*

En esta etapa se contrasta la muestra obtenida del intento de acceso del usuario con el patrón biométrico almacenado en la fase de enrolamiento de este, o bien con todos los patrones de la base de datos si se trabaja en identificación. El resultado de dicha comparación (o comparaciones) es un valor directa o inversamente proporcional a la similitud entre la muestra y el patrón (Guerra Casanova, 2014)

2.8.8. *Etapa de decisión*

En esta etapa se decide si el usuario es quien dice ser (en verificación) o la identidad del usuario entre una población (en identificación) (Guerra Casanova, 2014).

2.9. Tipos de técnicas Biométricos.

Como se ha comentado ya en varias ocasiones, la biometría es el estudio de métodos automáticos para el reconocimiento de individuos. Dicho reconocimiento se basa en el examen de las características biométricas. Así, se pueden distinguir tres tipos de técnicas biométricos principalmente (Hernández , 2015)

- Biometría estática: es el tipo de biometría que se basa en el reconocimiento de rasgos físicos propios del ente a reconocer. Para ello se buscan rasgos propios de todas las personas, tales como la huella dactilar, la geometría de la cara, el análisis de la retina, etc.
- Biometría dinámica: es el tipo de biometría que se basa en comportamientos particulares de cada usuario. Para este análisis se buscan comportamientos como el patrón de voz, la firma manuscrita, la dinámica del tecleo, etc.
- Biometría multimodal: es el tipo de biometría que combina tanto los rasgos físicos como los de comportamiento.

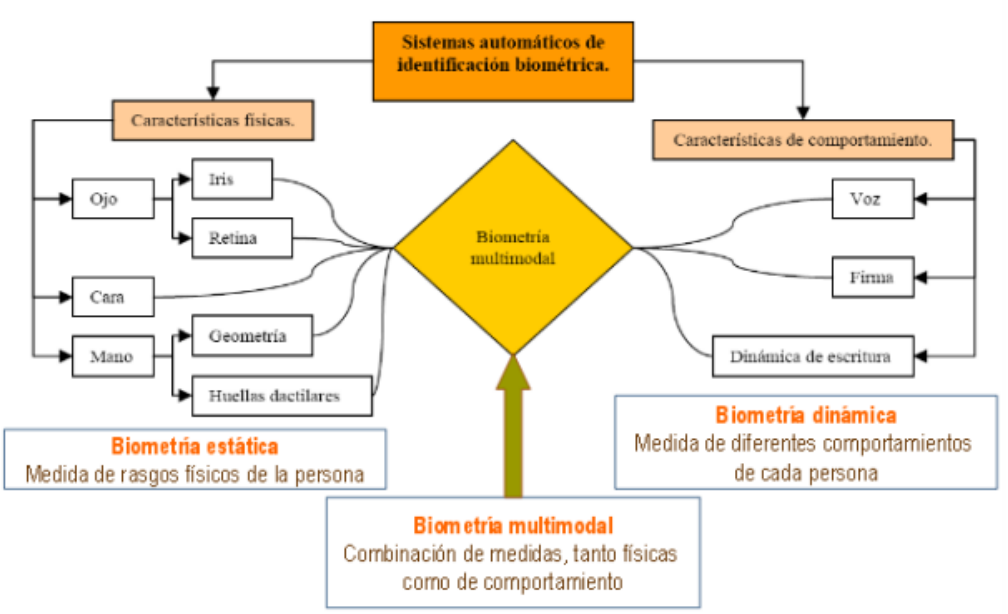

Figura 15-2 Técnicas de identificación biométrica según se analicen características físicas o de comportamiento

Fuente: (Villalobos Castaldi, 2011)

2.9.1. *ADN*

La tecnología del ADN es usada para comparar la muestra de un sospechoso contra la muestra encontrada en la escena de un crimen (Figura 2:16**)** También es usada en pruebas de paternidad y en procesos de identificación de personas extraviadas (Guerra Casanova, 2014).

La toma de la muestra de ADN eventualmente puede ser invasiva, pues puede requerirse tejido, sangre u otra muestra corporal, aunque también puede obtenerse de la saliva, el cabello, etc. El análisis de ADN no se realiza en tiempo real y actualmente toma en promedio 10 minutos (Villalobos Castaldi, 2011).

Figura 16-2 Identificación biométrica basada en el ADN

Fuente: (Villalobos Castaldi, 2011)

2.9.2. *Reconocimiento de firmas.*

Es la tecnología biométrica menos problemática, en la actualidad resulta la más difundida en el mundo ya que, entre otras ventajas, es muy económica si se requiere implementar. Un sistema de este tipo solo necesita una tableta de escritura conectada al computador (Cortés, 2010).

El escaneo de la firma se analiza desde dos puntos de vista, siendo estos la firma en sí y el modo en que se efectúa. Los datos almacenados incluyen la velocidad, la presión, la dirección, el largo del trazado y las áreas donde el lápiz se levanta. El gran inconveniente de este método es que una persona nunca firma de manera idéntica dos veces (Cortés, 2010).

Figura 17-2 Identificación biométrica basada en el reconocimiento dinámico de la firma

Fuente: (Villalobos Castaldi, 2011)

2.9.3. *Rasgos faciales.*

Según National Science and Technology Counci describe: "El reconocimiento facial está basado en rasgos (geométrico) y lo visual (fotométrico), en el desarrollo de los avances del reconocimiento facial los investigadores desarrollaron algoritmos para obtener precisión según los más estudiados son: Análisis de componentes principales (Principal Components Analysis, PCA), Análisis lineal discriminante (Linear Discriminant Analysis, LDA), y Correspondencia entre agrupaciones de grafos elásticos Elastic Bunch Graph Matching, EBGM)" (Giraldo & Gomez , 2017).

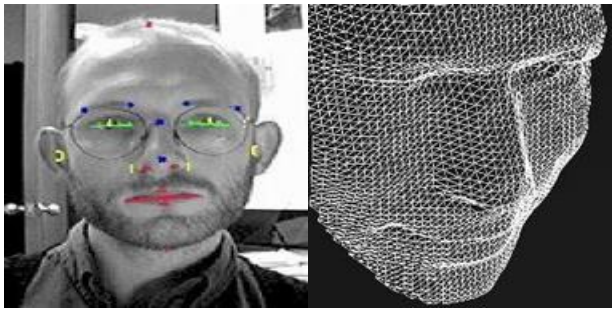

Figura 18-2 Los vectores de los rasgos

Fuente: Biometrics Overview Biometrics. Disponible en: https://www.nist.gov/programsprojects/biometrics

2.9.4. *Rasgos de la mano*

La forma, longitud y estructura de la mano junto con la forma y longitud de los dedos, se puede usar también como una forma de reconocimiento biométrico (Figura 19-2). Este tipo de identificación es popular y ha sido instalado en numerosos lugares del mundo, debido a que es barato y fácil de usar. El reconocimiento de la geometría de la mano no se ve afectado por factores climáticos o condiciones específicas (Villalobos Castaldi, 2011).

Sin embargo, es un método muy poco discriminante, además de que la estructura de la mano es muy variable en algunas épocas de la vida, sobre todo en la infancia y la joyería o las limitaciones en el movimiento de la mano (como artritis) pueden afectar el proceso de escaneo. Este instrumento cuenta con precisión aceptable, económica, aceptación decente e intrusión aceptable (Villalobos Castaldi, 2011).

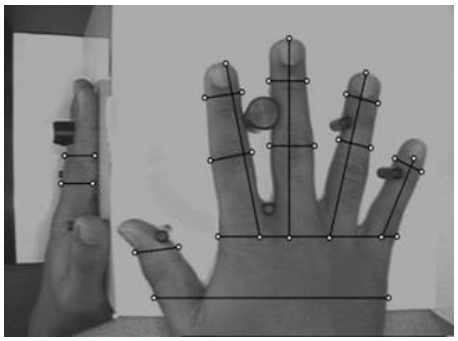

Figura 19-2 Identificación biométrica basada en la geometría de la mano

Fuente: (Villalobos Castaldi, 2011)

2.9.5. *Palma de la mano*

Al igual que el reconocimiento de huellas dactilares, el reconocimiento de la palma de la mano está basado en la información presentada por la fricción de las crestas con una superficie Esta información incluye el sentido de las crestas, la presencia o ausencia de minucias en la huella palmar, etc. (Figura 2:20.) (Villalobos Castaldi, 2011)

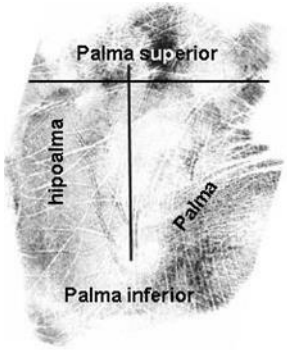

Figura 20-2 Identificación biométrica basada en la palma de la mano

Fuente: (Villalobos Castaldi, 2011)

2.9.6. *Patrón del iris.*

Es una de las técnicas biométricas más confiables debido a que el iris posee alrededor de 266 puntos únicos mientras que la mayoría de técnicas biométricas poseen alrededor de 13 a 60 características distintas. Cada ojo es único y permanece estable con el paso del tiempo y en diferentes ambientes de clima. (Cortés, 2010).

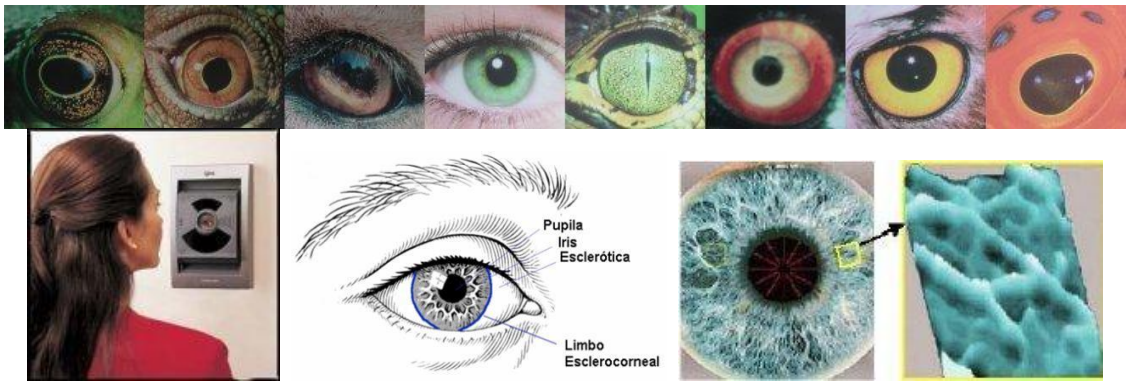

Figura 21-2 Identificación biométrica basada en el mapeo del iris

Fuente: Técnicas Biométricos. Disponible en: http://148.204.63.111/SABERv3/Repositorios/webVerArchivo/26203

Procedimiento del reconocimiento del iris, se realiza según las siguientes etapas:

- Captura de Imagen del Ojo.
- Segmentación: se realiza la detección de la imagen capturando los círculos de la pupila y del iris, la segmentación de parpados y filtros consiste en aislar las pestañas y por medio de una matriz la cual obtiene el radio y las coordenadas del circulo que segmenta la pupila y el iris. Como resultado se obtienen: las coordenadas (x, y) de ambos círculos y sus correspondientes radios, se genera además una matriz que identifica el ruido detectado.
- Los esquemas blancos indican la localización del iris y los límites de los párpados.
- Normalización: se calcula el desplazamiento de la pupila del centro del iris, localizando la ubicación cartesiana el rededor del iris y los valores de interpolación (Giraldo & Gomez , 2017).

2.9.7. *Retina*

El patrón que forman las venas que están debajo de la superficie de la retina es un patrón estable y único. Por lo tanto, es un método biométrico confiable. Usando procedimientos ópticos similares a los de un retinoscopio, se pueden obtener imágenes digitales del patrón de la retina de un individuo mediante la proyección de un tenue haz de luz (puede ser infrarroja) hacia el ojo (Figura 22-2**)** Para captar la imagen necesaria para el reconocimiento, se requiere que el sujeto a identificar mire fijamente y muy de cerca un dispositivo y mantenga su vista fija en un punto determinado [Hill, 1978], [Hill, 1992], [Marshall y Usher, 2006], [Retinal Tech, 2010]. A pesar de su confiabilidad, en muchas ocasiones no se puede hacer que los sujetos a identificación cumplan con el procedimiento, además de que requiere de un equipo bastante costoso. Algunas prisiones de alta seguridad usan el reconocimiento basado en los patrones de la retina (Villalobos Castaldi, 2011)

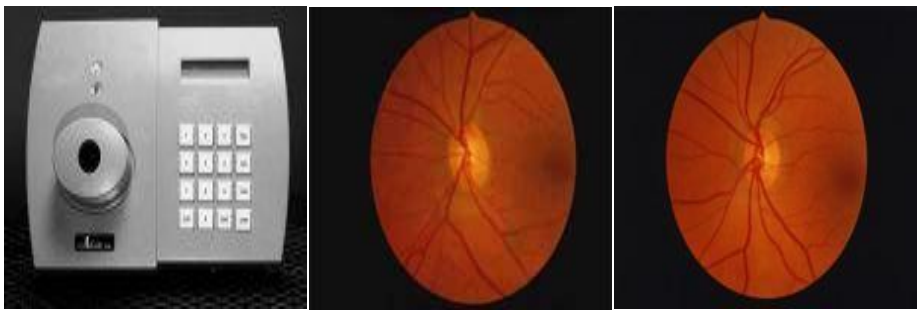

Figura 22-2 Identificación biométrica basada en el patrón vascular de la retina

Fuente: Técnicas *Biométricos. Disponible en: http://148.204.63.111/SABERv3/Repositorios/webVerArchivo/26203*

2.8.8. Termografía facial

Es un área de interés relativamente nueva que mide los patrones infrarrojos de la emisión de calor de la cara, causado por el flujo de sangre bajo la piel. Los sensores termográficos miden la temperatura de un objeto. Es una tecnología no invasiva, que no requiere de contacto físico, es continua y accesible a la mayoría de los usuarios. La verificación o identificación puede ser lograda a 1m de distancia y sin que el usuario tenga que esperar largos periodos de tiempo o no hacer nada más que mirar a la cámara (Figura 23-2). Por otro lado, el sistema vascular presente en el rostro genera una "firma facial" única cuando el calor es emitido por la cara. Se dice que el termograma facial es único para cada persona y no puede ser falsificado. Incluso la cirugía plástica no puede falsificar un termograma facial debido a que dicha cirugía no redirecciona el flujo de la sangre. Una ventaja de los termogramas faciales es que es un método biométrico no invasivo, por lo que puede usarse para verificar una identidad sin necesidad de hacer contacto con ella. [TRS, 1998]. Además, presenta bastantes ventajas frente al simple reconocimiento facial basado en imágenes, ya que la cámara infrarroja puede obtener el termograma facial en un ambiente con poca luz e incluso en ausencia de ella. Aunque el termograma facial es único para cada persona, aún no se ha probado que este método es lo suficientemente discriminante. El termograma facial puede depender de una serie de factores como el estado emocional y la temperatura corporal (Villalobos Castaldi, 2011).

Figura 23-2 Identificación biométrica basada en el termograma facial

Fuente: Técnicas Biométricas. Disponible en: http://148.204.63.111/SABERv3/Repositorios/webVerArchivo/26203

2.9.8. *Espectroscopia de la piel*

La calidad óptica de la piel humana está determinada por sus propiedades químicas y estructurales, que varían de una persona a otra (Figura 24-2). Estas propiedades pueden ser

medidas mediante espectroscopia óptica de reflexión difusa. Esta tecnología biométrica usa un sensor biométrico basado en un diodo emisor de luz (LED) y fotodetectores de silicio que fueron desarrollados para mejorar las medidas biométricas basadas en las propiedades ópticas de la piel en los dedos, manos u otros sitos de la piel (Villalobos Castaldi, 2011).

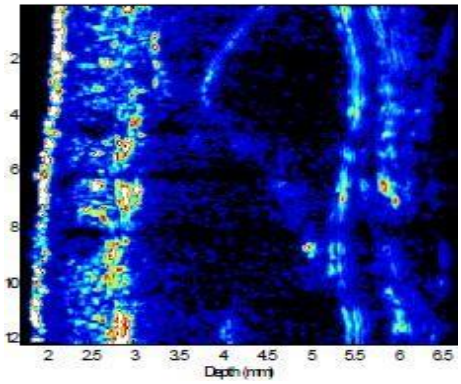

Figura 24-2 Identificación biométrica basada en la espectroscopia de la piel

Fuente: Técnicas Biométricos. Disponible en: http://148.204.63.111/SABERv3/Repositorios/webVerArchivo/26203

2.9.9. *Reconocimiento de la voz.*

El análisis de la voz inicia a mediados de la década de los años 60. El habla se considera como una de las técnicas biométricas más eficaces, debido a su naturalidad. Se ha podido comprobar que los patrones con que una persona dice una palabra son únicos. El reconocimiento de voz funciona mediante la digitalización de diferentes palabras de una persona. Cada palabra se descompone en segmentos, de los cuales se obtienen 3 o 4 tonos dominantes que son capturados en forma digital y almacenados en una tabla o espectro, que se conoce con el nombre de plantilla de la voz (voice print) (Cortés, 2010).

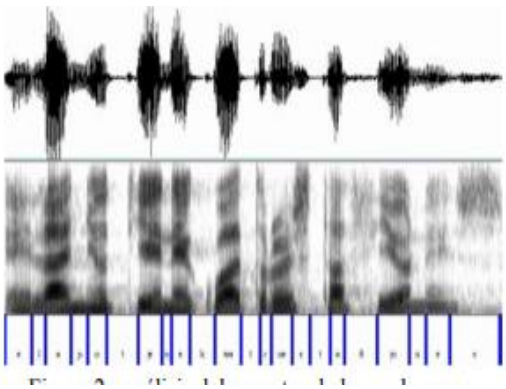

Figura 25-2 Análisis del espectro de la voz humana.

Fuente: https://dialnet.unirioja.es/servlet/articulo?codigo=4528099

Este sistema biométrico tiene tres formas de reconocimiento:

- Dependencia: Siempre se repite el mismo texto
- Texto Aleatorio: El sistema de forma automática escoge un texto a repetir
- Independencia de texto: El usuario tiene la libertad de escoger lo que quiere decir (Giraldo & Gomez , 2017).

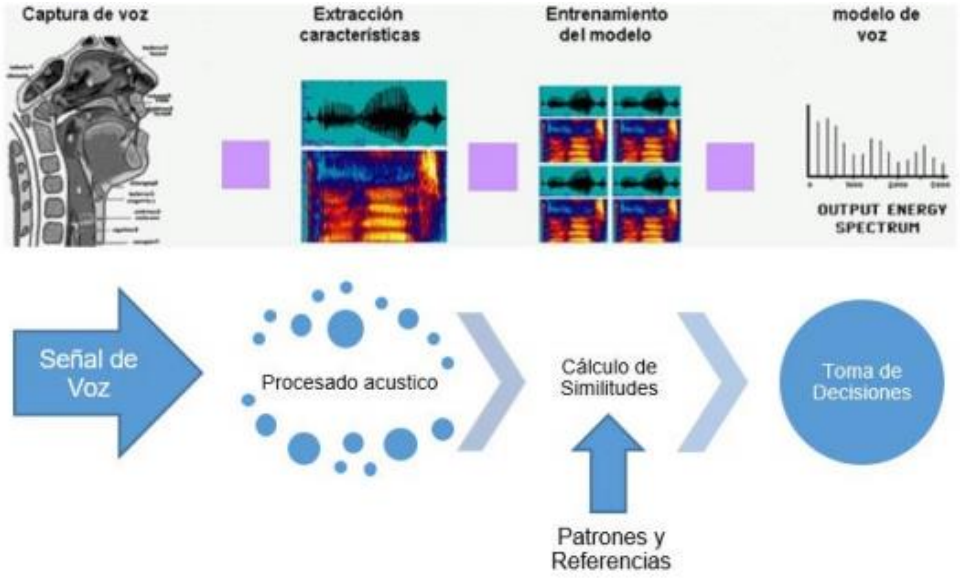

Figura 26-2 Proceso de reconocimiento de voz

Fuente: Adaptada Propuesta de estándar para el uso seguro de Tecnologías Biométricas Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/biometria/index.html

2.9.10. *Red vascular*

Esta tecnología biométrica es de reciente desarrollo; también se le conoce como reconocimiento del patrón de venas de la mano. Al igual que el reconocimiento por medio de la retina, esta tecnología usa luz infrarroja a corta distancia para detectar los patrones de la red vascular; actualmente también se están extrayendo patrones vasculares de otras partes del cuerpo como los patrones vasculares de la palma de la mano, del reverso de la mano y dedos (Villalobos Castaldi, 2011)

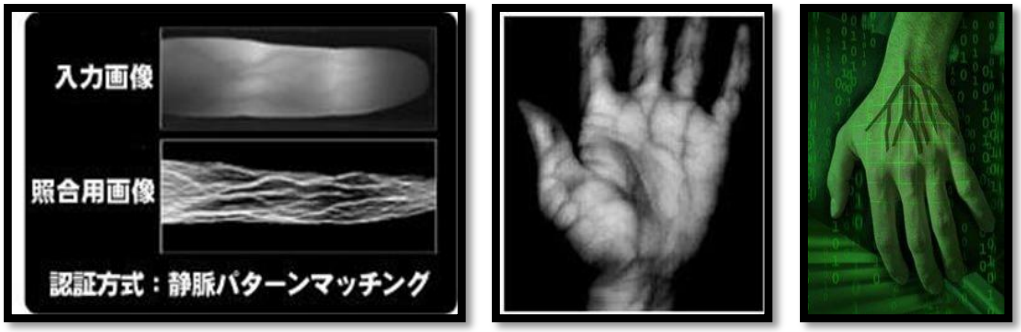

Figura 27-2 Identificación biométrica basada en el patrón vascular de la palma de la mano y del dedo

Fuente: https://dialnet.unirioja.es/servlet/articulo?codigo=4528099

2.9.11. *Huellas dactilares.*

Biometría menciona que en la huella dactilar usualmente aparecen una serie de líneas oscuras que representan los relieves, tienen una superficie irregular de crestas (líneas oscuras) y valles (líneas claras) que forman un patrón único para cada individuo, entre estas crestas aparecen como espacio en blanco y están en bajo relieve, la porción subyacente de las crestas de fricción ver (Figura 28-2). La identificación por medio del patrón de huella dactilar se obtiene a través de las minucias, la ubicación y dirección de la final cresta y una bifurcación (separaciones) de las crestas a lo largo su trayectoria (Giraldo & Gomez , 2017).

Figura 28-2 Reconocimiento de la huella digital.

Fuente: GAO adaptación de datos del FBI.

2.9.12. *Caminata*

La forma de andar y correr es distintiva de cada persona (Figura 29-2). Este rasgo biométrico tiene una tasa de acierto menor que otros rasgos, pero es aplicable cuando se tiene la grabación de un criminal en donde ingresa andando y escapa corriendo, o cuando se carece de algún otro rasgo biométrico, debido a que no hay huellas dactilares, la cara está tapada, etc (Villalobos Castaldi, 2011)

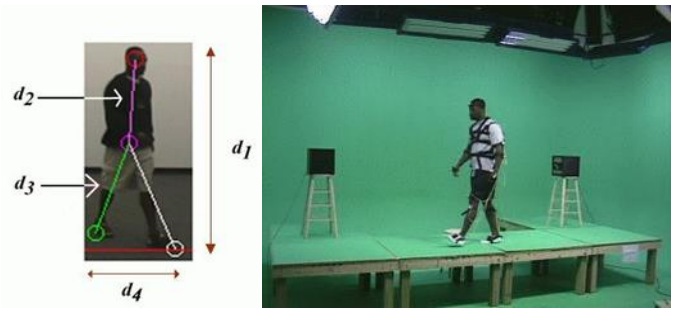

Figura 29-2 Identificación biométrica basada en el reconocimiento de la marcha por análisis de silueta

Fuente: http://148.204.63.111/SABERv3/Repositorios/webVerArchivo/26203

2.9.13. *Tecleo*

Es un tipo de biométrico conductual usado para verificar la identidad de un individuo mediante el examen de sus patrones de tecleo en un teclado (Figura 30-2). Esta tecnología se sostiene sobre la premisa de que cada individuo exhibe un patrón distintivo y una cadencia de tecleo. La mayoría de los estudios usan la duración entre tecleos sucesivos (latencias) como característica de verificación de usuario, aunque hay otros que utilizan el tiempo que permanece la tecla presionada. Esta tecnología no requiere de hardware adicional o dispositivo de captura, sino se soporta sobre un software de captura de la dinámica de tecleo del teclado. Esta tecnología usa clasificadores bayesianos, redes neuronales y sistemas difusos (Villalobos Castaldi, 2011).

Figura 30-2 Identificación biométrica basada en la verificación de patrones de tecleo

Fuente: Técnicas Biométricos. Disponible en: http://148.204.63.111/SABERv3/Repositorios/webVerArchivo/26203

2.9.14. *Firma Auditiva*

En esta técnica biométrica la identificación se realiza escuchando el sonido que se produce al firmar (Figura 31-2**)** (Villalobos Castaldi, 2011)

Figura 31-2 Identificación biométrica basada en la firma auditiva

Fuente: Técnicas Biométricos. Disponible en: http://148.204.63.111/SABERv3/Repositorios/webVerArchivo/26203

2.9.15. *Código gráfico*

En esta técnica se tiene que dibujar sobre una imagen conocida un dibujo; la forma en que se dibuja en combinación con la posición del dibujo genera la clave (Figura 32-2**)** (Villalobos Castaldi, 2011)

Figura 32-2 Identificación biométrica basada en el código gráfico

Fuente: Técnicas Biométricos. Disponible en: http://148.204.63.111/SABERv3/Repositorios/webVerArchivo/26203

2.9.16. *Pabellón auricular*

Esta tecnología biométrica se ha desarrollado especialmente para la medicina legal y forense. Es una reproducción bidimensional del pabellón auricular y se maneja de manera similar a la huella digital o la huella palmar (Figura 33-2) (Villalobos Castaldi, 2011)

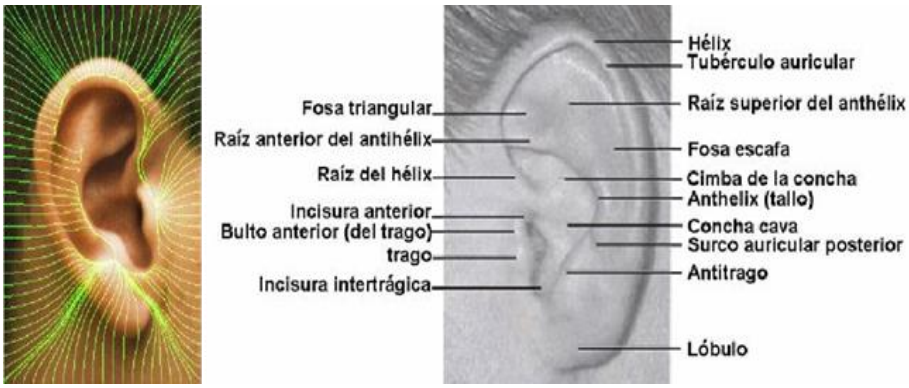

Figura 33-2 Identificación biométrica basada en las partes del pabellón auricular

Fuente: Técnicas Biométricos. Disponible en: http://148.204.63.111/SABERv3/Repositorios/webVerArchivo/26203

2.9.17. *Nariz*

A diferencia de otros rasgos faciales usados para aplicaciones biométricas, tales como los ojos o la oreja, la nariz es difícil de ocultar y es difícil que se modifique por las expresiones faciales (Figura 34-2). Los Drs. Adrián Evans y Adrián Moorhouse, investigaron la posibilidad de utilizar las imágenes de la nariz de las personas para identificar a los individuos (Villalobos Castaldi, 2011).

Figura 34-2 Identificación biométrica basada en la nariz.

Fuente: Técnicas Biométricos. Disponible en: http://148.204.63.111/SABERv3/Repositorios/webVerArchivo/26203

2.9.18. *Dinámica del mouse*

En este caso es necesario dibujar algo, siempre lo mismo (su nombre, etc.), con la ayuda del mouse (Figura 35-2). Se extraen algunas características relevantes (posición, velocidad, ángulo, etc.) y son utilizadas para el reconocimiento posterior (Villalobos Castaldi, 2011).

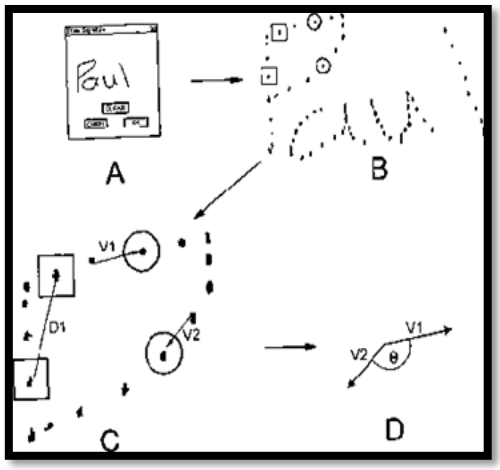

Figura 35-2 Identificación biométrica basada en la dinámica del mouse

Fuente: Técnicas Biométricos. Disponible en: http://148.204.63.111/SABERv3/Repositorios/webVerArchivo/26203

2.9.19. *Olor*

Es una tecnología biométrica basada en las características físicas de la composición química del olor del cuerpo. La principal tarea del reconocimiento de olor es crear un modelo tan similar como sea posible al modelo humano. Las narices electrónicas/artificiales (E-Noses) han sido desarrolladas como un sistema para la detección automática y clasificación de los olores, vapores y gases (Figura 36-2). Este proceso utiliza la estadística y redes neuronales artificiales entre otras (Villalobos Castaldi, 2011).

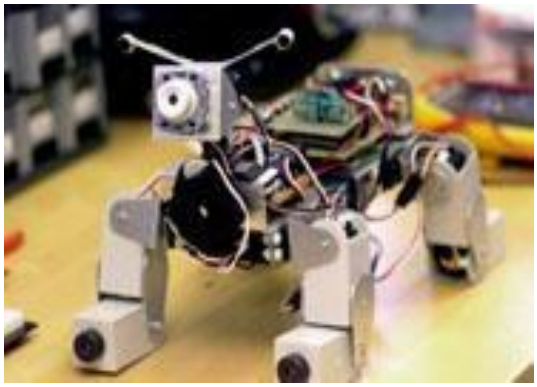

Figura 36-2 Identificación biométrica basada en el olor corporal

Fuente: Técnicas Biométricos. Disponible en: http://148.204.63.111/SABERv3/Repositorios/webVerArchivo/26203

2.9.20. *Labios*

Esta tecnología biométrica se divide en tres subcategorías que son: huella de los labios, movimiento de los labios y forma de los labios. La huella de los labios es conocida en la ciencia forense por ser diferente para cada individuo, así como las huellas dactilares. El movimiento de los labios ayuda a la identificación asociada con el reconocimiento de la voz. La forma de los labios puede ser usada como una característica o rasgo individual para lograr la autentificación (Villalobos Castaldi, 2011).

Figura 37-2 Identificación biométrica basada en los labios

Fuente: Técnicas Biométricos. Disponible en: http://148.204.63.111/SABERv3/Repositorios/webVerArchivo/26203

2.9.21. *Uña*

Tecnología emergente que no ha sido aún muy estudiada. Escanea la estructura dérmica debajo de la uña. Esta estructura está constituida por canales de piel casi paralelos (Figura 38-2). La distancia entre cada canal es medida para obtener el código biométrico (Villalobos Castaldi, 2011).

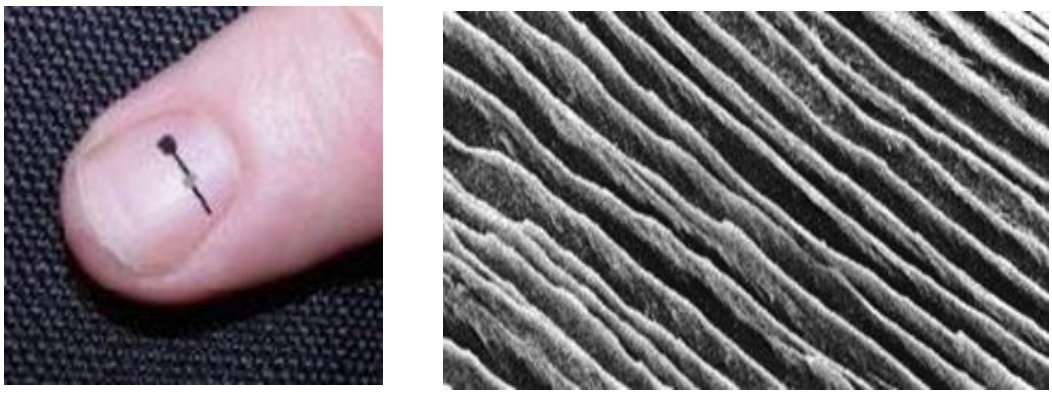

Figura 38-2 Identificación biométrica basada en la uña

Fuente: Técnicas Biométricos. Disponible en: http://148.204.63.111/SABERv3/Repositorios/webVerArchivo/26203

2.10. Técnicas biométricas aplicadas en dispositivos móviles

Los teléfonos móviles inteligentes se han introducido en el mercado con gran éxito. Desde estos dispositivos se puede acceder a distintos servicios en Internet que requieren una autenticación, como por ejemplo mirar el saldo de una cuenta corriente, comprar un producto en una tienda "online" o realizar ciertas operaciones en sitios Web seguros. Además, en estos dispositivos se

almacena una gran cantidad de información personal, como la agenda, mensajes de texto o correos electrónicos. Por ello, es necesario dotar a los teléfonos móviles de mecanismos de seguridad potentes para la verificación de la identidad del usuario que trata de utilizar el teléfono móvil para ciertas operaciones, asegurándose que es el dueño del mismo (o una persona con permiso).

En este contexto móvil, la seguridad suele dejarse en manos de contraseñas o códigos PIN que se supone que sólo el usuario sabe. Pero ese hecho esconde un gran riesgo ya que las contraseñas pueden ser robadas o adivinadas comprometiendo la seguridad del teléfono móvil y todas las operaciones que puedan realizarse a través de él.

La utilización de técnicas biométricas es una opción para solucionar estos problemas. De esta manera, el usuario no puede olvidarse de su clave, puesto que él mismo es la clave. Por otro lado, si la técnica biométrica es suficientemente distintiva, ningún usuario va a poder realizar operaciones o acceder a los teléfonos móviles de otros usuarios.

En la actualidad existen muchas investigaciones que tratan de adaptar las técnicas clásicas de biometría en escenarios móviles. Algunas de estas líneas de trabajo son las siguientes:

- Reconocimiento de iris utilizando las cámaras frontales o traseras de los teléfonos móviles [Cho06, Kurkovsky10, Jeong06].
- Reconocimiento facial a través de las cámaras de los teléfonos móviles [Tao06, Han07].
- Reconocimiento por voz al hablar por teléfono [Shabeer07, Lapere97].
- Reconocimiento de la persona por la forma de andar llevando un teléfono móvil que integre un acelerómetro en el bolsillo [Ailisto05].
- Reconocimiento del usuario legítimo del dispositivo móvil mediante dinámica de tecleo y presión de las teclas [Saevanee08].
- Reconocimiento de la firma de un usuario realizada con el dedo en la pantalla táctil [Mendaza11].

2.11. Comparación de métodos

En la siguiente tabla 2:2 se recogen las diferentes características de las técnicas biométricas son su debida comparación.

Tabla 3-2 Comparativa de las principales técnicas biométricas en dispositivos móviles.

	Fiabilidad	Facilidad De Uso	Prevención de ataques	Aceptación	Estabilidad	Accesibilidad segura
Huella dactilar	**Muy Alta**	Alta	Alta	Alta	Alta	**Muy Alta**
Ojo (Iris)	**Muy Alta**	Media	**Muy Alta**	Media	Alta	**Muy Alta**
Ojo (retina)	**Muy Alta**	**Baja**	**Muy Alta**	**Baja**	Alta	Alta
Vascular dedo	**Muy Alta**	**Muy Alta**	**Muy Alta**	Alta	Alta	Baja
Geometría de la mano	Alta	Alta	Alta	Alta	Media	Media
Escritura y firma	Media	Alta	Media	**Muy Alta**	**Baja**	**Baja**
Voz	Alta	Alta	Media	Alta	Media	Alta
Cara 3D	Alta	Alta	Alta	**Muy Alta**	Alta	Media
Cara 2D	Media	Alta	Media	**Muy Alta**	Media	Media

Fuente: (INCIBE, 2016)

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

El presente capitulo puntualizara el proceso metodológico empleado en este trabajo investigativo. Las pruebas y mediciones empleadas para comprobar la hipótesis planteada, desarrollando un análisis investigativo apropiado (Monje, 2011).

3.1. Diseño de la investigación

La investigación para efectuar será de tipo cuali - cuantitativo porque se identificará a través de un minucioso estudio científico la problemática, estudiando las variables que conllevan a ella y planteando una observación directa y la contribución en el problema (Monje, 2011).

Se identificará además las posibles causas que relacionan entre si problema de esta investigación. Dicho estudio realizado se orientará hacia la comprobación de la hipótesis centrando el estudio sobre el fenómeno en su totalidad (Monje, 2011).

3.2. Tipo de investigación

El tipo de investigación a utilizar en este proyecto es de tipo correlacional indicando el nivel de relación existente entre las variables estudiadas, es decir la relación o dependencia entre ellas. Acepando o rechazando las hipótesis en relación con el nivel de confiabilidad en dispositivos móviles con la aplicación del modelo de seguridad con tecnología biométrica (INTER, 2019).

Este estudio se basa en investigación documental argumentativa exploratoria, el proceso investigativo inicia con la búsqueda de antecedentes y las referencias del tema seleccionado en documentos como trabajos de investigación, ensayos, artículos, documentados publicado en revistas indexadas, tesis de grado a nivel de pregrado, maestrías y doctorado. Este tipo de investigación permite una vez recopilada la información sea posible realizar un análisis para dar cumplimiento a cada uno de los objetivos definidos (INTER, 2019).

3.3. Métodos, técnicas e instrumentos

La metodología que se utilizara en esta investigación consiste en un proceso sistemático y continuo para comparar o evaluar productos, servicios y procesos para encontrar las diferencias y de esta manera escoger la mejor opción. Que se describe a continuación.

3.3.1. Método Científico

La presente investigación se fundamenta en el uso de métodos, técnicas e instrumentos que ayuden a la interpretación final de la misma. Se considera que el método científico es el más adecuado, ya que, hace referencia a una serie de etapas ordenadas y relacionadas para obtener un conocimiento verdadero desde el punto de vista científico (Gonzales, 2003).

Las fases del método científico son:

- Planteamiento del problema.
- Formulación de la hipótesis.
- Levantamiento de la información.
- Análisis e interpretación de resultados.
- Comprobación de la hipótesis.
- Difusión de resultados.

3.3.2. Método Sintético

Dentro de este método la síntesis permite incorporar diferentes alternativas de solución para mitigar las vulnerabilidades previamente identificadas en lo concerniente a la confidencialidad de los dispositivos móviles (Pérez, 2009).

3.3.3. Método Comparativo

Se establece un escenario sin la implementación del modelo de seguridad propuesto que pruebe una mayor confidencialidad a la información vulnerable de los usuarios en dispositivos móviles, frente al mismo escenario con la implementación del modelo de seguridad biométrico (Pérez, 2009).

3.3.4. Técnicas

Los métodos seleccionados para el presente trabajo de investigación se complementan con la aplicación de las siguientes técnicas:

Tabla 1-3 Variables

<table>
<tr><th>Variable</th><th>Indicador</th><th>Técnica</th></tr>
<tr><td>V. INDEPENDIENTE
Técnica biométrica huella digital</td><td>Comparación de escenarios</td><td>Comparación de escenarios: vulnerable y seguro</td></tr>
<tr><td></td><td>Evaluación de la usabilidad y seguridad</td><td>Formulario de usabilidad
1. Género:
2. Edad:
3. Nivel de estudios:
4. A que se dedica:
5. ¿Utiliza técnicas de seguridad en su dispositivo móvil para proteger su información?
6. ¿Cuál es el sistema de seguridad que usted utiliza en su dispositivo móvil para proteger su información?
7. Califique la efectividad, satisfacción y eficiencia del sistema de seguridad que usted utiliza para proteger su información en su dispositivo móvil:
<table>
<tr><th rowspan="2">SISTEMA DE SEGURIDAD</th><th colspan="4">EFECTIVIDAD</th></tr>
<tr><th>Muy Alta</th><th>Alta</th><th>Media</th><th>Baja</th></tr>
<tr><td>Huella_Dactilar</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Ojos_Iris</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Ojo_Retina</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Vascular_Dedo</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Geometria_De_La_Mano</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Escritura_Y_Firma</td><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
</table>

Voz					
Cara_3d					
Cara_2d					
Patron_Numerico					
Patron_Dibujo					

SISTEMA DE SEGURIDAD	**SATISFACION**			
	Muy Alta	**Alta**	**Media**	**Baja**
Huella_Dactilar				
Ojos_Iris				
Ojo_Retina				
Vascular_Dedo				
Geometria_De_La_Mano				
Escritura_Y_Firma				
Voz				
Cara_3d				
Cara_2d				
Patron_Numerico				
Patron_Dibujo				

SISTEMA DE SEGURIDAD	**EFICIENCIA**			
	Muy Alta	**Alta**	**Media**	**Baja**
Huella_Dactilar				
Ojos_Iris				
Ojo_Retina				
Vascular_Dedo				
Geometria_De_La_Mano				

		<table><tr><td>Escritura_Y_Firma</td><td></td><td></td><td></td><td></td></tr><tr><td>Voz</td><td></td><td></td><td></td><td></td></tr><tr><td>Cara_3d</td><td></td><td></td><td></td><td></td></tr><tr><td>Cara_2d</td><td></td><td></td><td></td><td></td></tr><tr><td>Patron_Numerico</td><td></td><td></td><td></td><td></td></tr><tr><td>Patron_Dibujo</td><td></td><td></td><td></td><td></td></tr></table> <table><tr><th>SISTEMA DE SEGURIDAD</th><th colspan="4">Accesibilidad segura</th></tr><tr><th></th><th>Muy Alta</th><th>Alta</th><th>Media</th><th>Baja</th></tr><tr><td>Huella_Dactilar</td><td></td><td></td><td></td><td></td></tr><tr><td>Ojos_Iris</td><td></td><td></td><td></td><td></td></tr><tr><td>Ojo_Retina</td><td></td><td></td><td></td><td></td></tr><tr><td>Vascular_Dedo</td><td></td><td></td><td></td><td></td></tr><tr><td>Geometria_De_La_Mano</td><td></td><td></td><td></td><td></td></tr><tr><td>Escritura_Y_Firma</td><td></td><td></td><td></td><td></td></tr><tr><td>Voz</td><td></td><td></td><td></td><td></td></tr><tr><td>Cara_3d</td><td></td><td></td><td></td><td></td></tr><tr><td>Cara_2d</td><td></td><td></td><td></td><td></td></tr><tr><td>Patron_Numerico</td><td></td><td></td><td></td><td></td></tr><tr><td>Patron_Dibujo</td><td></td><td></td><td></td><td></td></tr></table> Tabulación de datos, análisis y prueba chi-cuadrado
Variable dependiente: Incrementar el nivel de confidencialidad en	Vulnerabilidades detectadas	

dispositivos móviles		

Elaborado por: Alvarado, Rene 2020.

3.3.5. Instrumentos

Los instrumentos son las herramientas utilizadas para realizar las pruebas dentro del escenario y a su vez facilitarán el análisis y el desarrollo de la prueba chi-cuadrado para validar el modelo de seguridad biométrica para disminuir las vulnerabilidades a la confidencialidad en dispositivos móviles.

3.3.5.1. Instrumentos Bibliográficos

Se emplearán como instrumentos las técnicas de seguridad biométricos descritos en esta tesis y artículos científicos a fin de determinar los componentes que formarán parte del modelo biométrico para disminuir las vulnerabilidades a la confidencialidad en dispositivos móviles.

3.3.5.2. Validación de los Instrumentos

La aplicación de los instrumentos permitirá realizar el análisis de datos, mediciones y comparaciones de técnicas biométricas que forman parte del objeto de estudio, a fin de llegar a la evaluación de la hipótesis planteada.

3.4. Población y Muestra

Al realizar una investigación se considera a la población como elemento principal, es decir, son quienes nos proporcionarán los datos sobre los cuales se enfoca este estudio, y la parte representativa de dicha población, es decir la muestra que facilite su análisis e interpretación.

3.4.1. Población

Es el conjunto total de individuos, objetos o medidas que poseen algunas características comunes, observables en un lugar y en un momento determinado; ésta constituye el objeto de la investigación de donde se extrae la información requerida para el estudio. En la presente

investigación, la población está constituida por todas las vulnerabilidades a la confidencialidad de la información almacenada en los dispositivos móviles tanto en técnicas de seguridades biométricas y convencionales que se detallan a continuación:

Tabla 2-3 Comparativa de sistemas de autentificación

ASPECTO	**BIOMETRÍA**	**CONTRASEÑAS Y TARJETAS**
Necesidad de secreto		
Posibilidad de robo (baja)		
Posibilidad de pérdida (baja)		
Registro inicial y posibilidad de regeneración		
Proceso de comparación (fácil) Comodidad del usuario		
Vulnerabilidad ante el espionaje (baja)		
Vulnerabilidad a un ataque por fuerza bruta (baja)		
Medidas de prevención		
Autentificación de usuarios “reales”		
Coste de implantación (bajo)		
Coste de mantenimiento (bajo)		

Fuente: (INCIBE, 2016)

3.4.2. Muestra

Para obtener un mejor resultado para un proceso estadístico sería estudiar a toda la población. Pero esto generalmente resulta improbable, ya sea, porque supone un coste económico alto o porque requiere demasiado tiempo.

La muestra es una parte representativa de la población en la que se reproduce de la mejor manera sus rasgos esenciales, datos que son importantes para la investigación. La función básica del muestreo es determinar que parte de una población debe examinarse, con la finalidad de hacer inferencias sobre dicha población.

3.4.3. Selección de la muestra

Para determinar la muestra se considera algunos de los ataques más comunes en los inicios de sesión como: Aplicaciones Maliciosas, Conexiones Inseguras, pueden contener Malware, Los canales de comunicación pueden estar mal asegurados, no utilizan software de seguridad, Descarga software de canales oficiales, Crear copias de seguridad de datos. Archivos encriptados; los cuales se encuentran dentro de las vulnerabilidades, tomadas de forma no probabilística, que serán evaluadas para la creación de un modelo seguro y aplicación en los dispositivos móviles.

3.5. Procedimiento

Para la realización del presente estudio de investigación se establecen lineamientos y pasos que otorgarán una secuencia lógica de cada proceso.

Los pasos establecidos se describen a continuación:

1) Escenario vulnerable
   - Observación y análisis de vulnerabilidades.
2) Escenario seguro
   - Observación y análisis de vulnerabilidades.
3) Evaluación de usabilidad
4) Observación y análisis de resultados mediante la tabulación y generación de datos estadísticos.

3.6. Planteamiento de la hipótesis

La aplicación de una técnica biométrica como es la huella digital si incrementara el nivel de seguridad a la confidencialidad en dispositivos móviles.

Variable independiente: Técnica biométrica como es la huella digital.
Variable dependiente: Incrementar el nivel de confidencialidad en dispositivos móviles.

3.7. Operacionalización Conceptual

Tabla 3-3 Operacionalización conceptual de variables

VARIABLE	TIPO	CONCEPTO
Técnica biométrica huella digital	Independiente	Una técnica de Seguridad de la Información es el conjunto de procesos, procedimientos, metodologías, principios, políticas, estándares y controles que se ha adoptado para promover la implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información, basado en mejores prácticas tendientes a preservar la confidencialidad, integridad y disponibilidad de la información, y que nos permiten contar con lineamientos claros para mantener un entorno razonablemente seguro, apoyando los objetivos estratégicos del negocio.
Confidencialidad	Dependiente	Requisito básico de seguridad que garantiza que solo las personas, entidades o procesos autorizados pueden acceder a la información.

Elaborado por: Alvarado, Rene 2020.

3.8. Operacionalización Metodológica

Tabla 4-3 Operacionalización metodológica de la variable independiente

Variable	Categoría	Indicadores	Técnicas e Instrumentos
Técnica biométrica huella digital	Dispositivos Móviles	-Políticas de seguridad que los usuarios de dispositivos móviles deben conocer y aplicar. - Periodicidad en la verificación de la efectividad de las medidas de seguridad biométricas. -Frecuencia de cumplimiento en las políticas de seguridad	Formulario de usabilidad Observación Científica Software especializado en ataques a la confidencialidad de la seguridad de la información. Informe estadístico de los ataques ocurridos por el no cumplimiento de políticas no utilizadas a la seguridad de la información

Elaborado por: Alvarado, Rene 2020.

Tabla 5-3 Operacionalización metodológica de la variable dependiente

Variable	Categoría	Indicadores	Técnicas e Instrumentos
Confidencialidad de la información	Nivel de seguridad de acceso a la información.	Mecanismos de seguridad. Número de ataques exitosos al inicio de sesión en dispositivos móviles Políticas de privacidad y confidencialidad Evaluación de riesgos, monitoreo, gestión de incidencias.	Comparación de escenarios Prueba chi-cuadrado Prueba chi-cuadrado Cuestionario estructurado para aplicarse a profesionales de seguridad de la información. Ejecución de programas de seguridad.

Elaborado por: Alvarado, Rene 2020.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

En este capítulo de resultados y discusión se realiza un análisis en base a cuatro aspectos que sin duda son los más importantes en lo que se refiere a la utilización de cualquier técnica de seguridad de la información como son la: Usabilidad, Eficiencia, Satisfacción y la Efectividad, para que con estos resultados obtenidos se disponga de una base sólida y realizar un análisis comparativo entre las técnicas de seguridad convencionales utilizadas en dispositivos móviles para el acceso a los mismos frente a una técnica biométrica.

4.1. Evaluación de la usabilidad

Tabulación de datos y generación de gráficos en el programa Excel.

4.1.1. Usabilidad

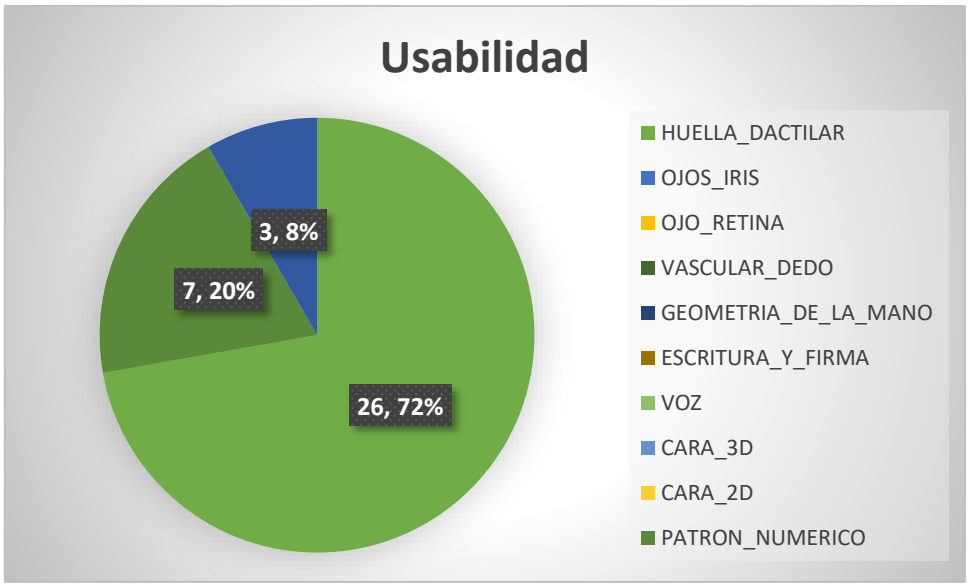

Gráfico 1-4 Usabilidad

Elaborado por: Alvarado, Rene 2020.

En el grafico se puede observar que el 72% de los usuarios de dispositivos móviles prefieren utilizar técnicas de seguridad biométrica y un 28% utilizan los sistemas convencionales para proteger su información, la cual se puede ver vulnerada por diferentes amenazas pudiendo poner en peligro su integridad.

4.1.2. Efectividad

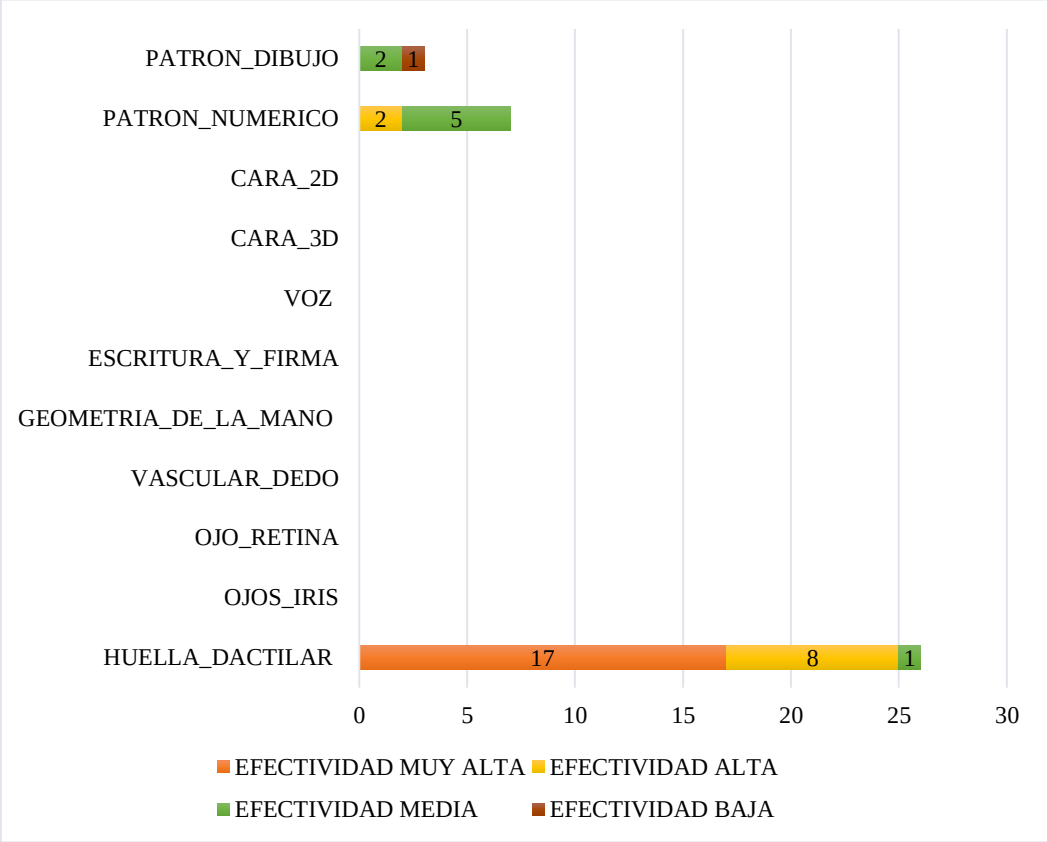

Gráfico 2-4 Efectividad

Elaborado por: Alvarado, Rene 2020.

4.1.3. Eficiencia

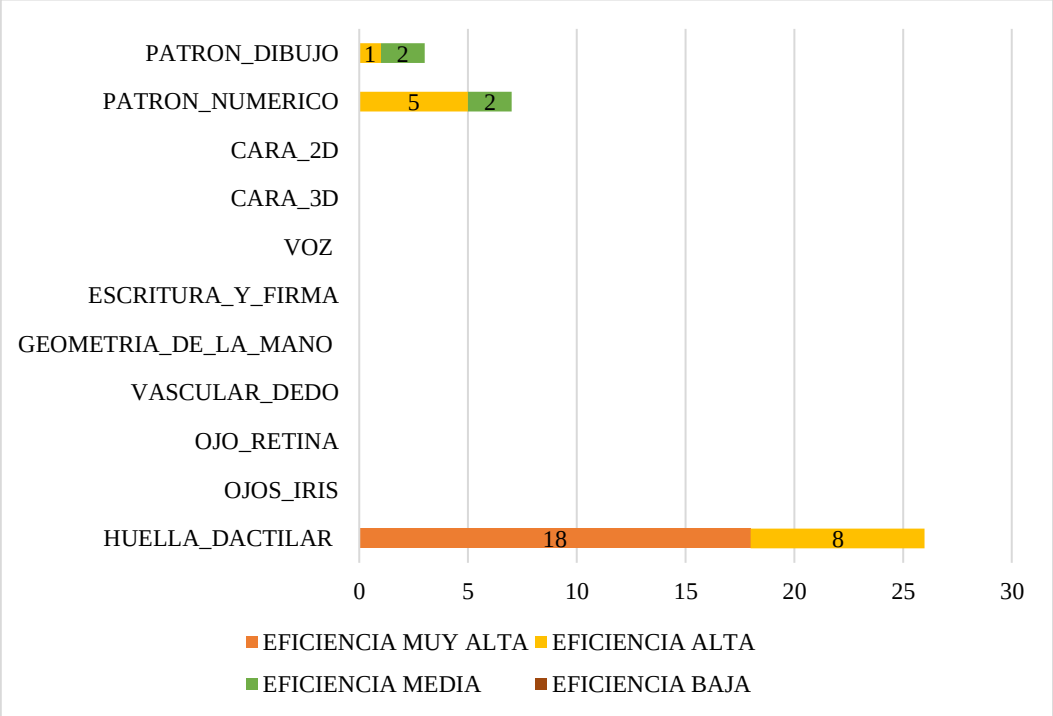

Gráfico 3-4 Eficiencia

Elaborado por: Alvarado, Rene 2020.

4.1.4. Satisfacción.

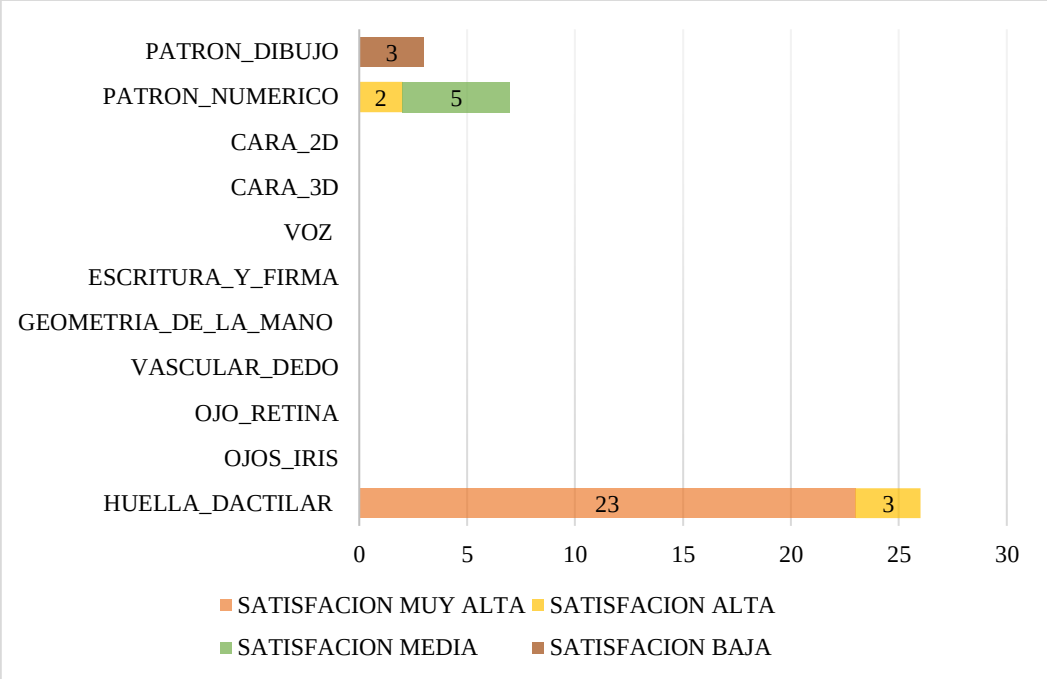

Gráfico 4-1 Satisfacción

Elaborado por: Alvarado, Rene 2020.

4.2. Prueba Chi-cuadrado

En este trabajo, se ha realizado un formulario de usabilidad utilizando los criterios de evaluación de sistemas biométricos como son: efectividad, seguridad y eficacia. Los cuales se van a analizar a continuación utilizando la prueba chi-cuadrado en el programa ESTADISTICO IBM SPSS

- Pasamos los datos obtenidos del formulario de usabilidad al programa estadístico IBM SPSS

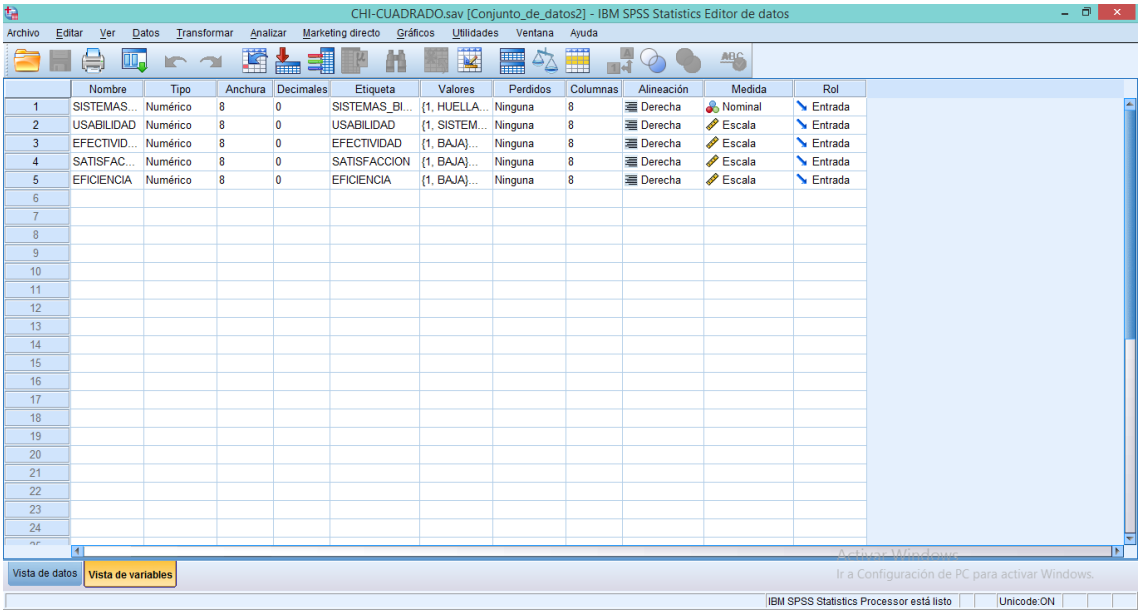

Figura 1-4 Vista de variables

Elaborado por: Alvarado, Rene 2020.

- Insertamos los datos obtenidos en el formulario

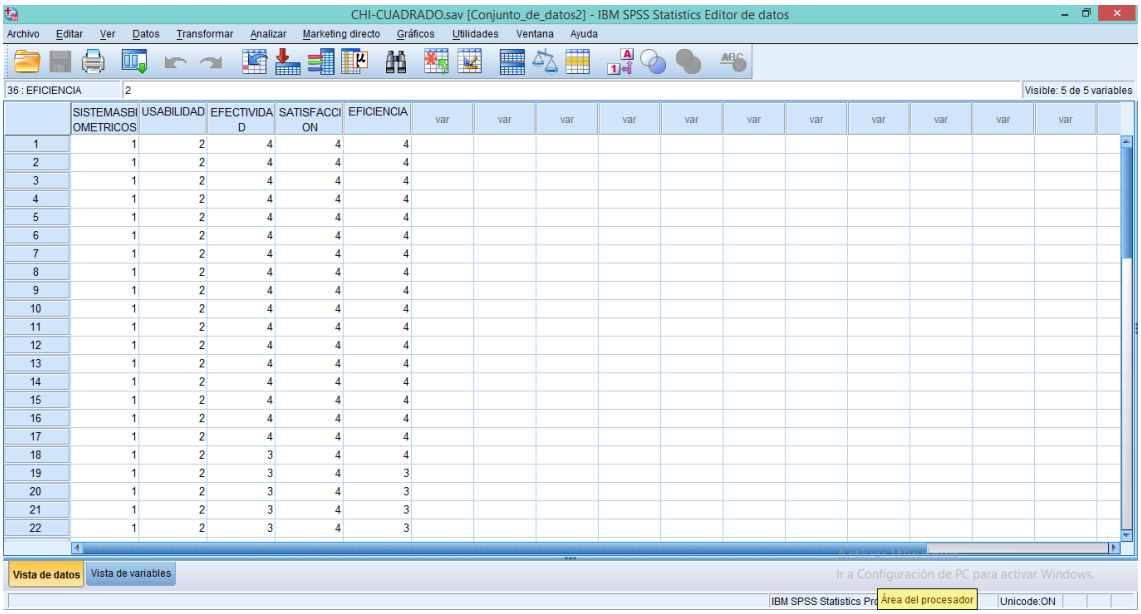

Figura 2-4 Vista de variables

Elaborado por: Alvarado, Rene 2020.

- Procedemos a realizar la prueba chi-cuadrado:
- Presionamos Analizar

- Estadísticos descriptivos
- Elegimos tablas cruzadas

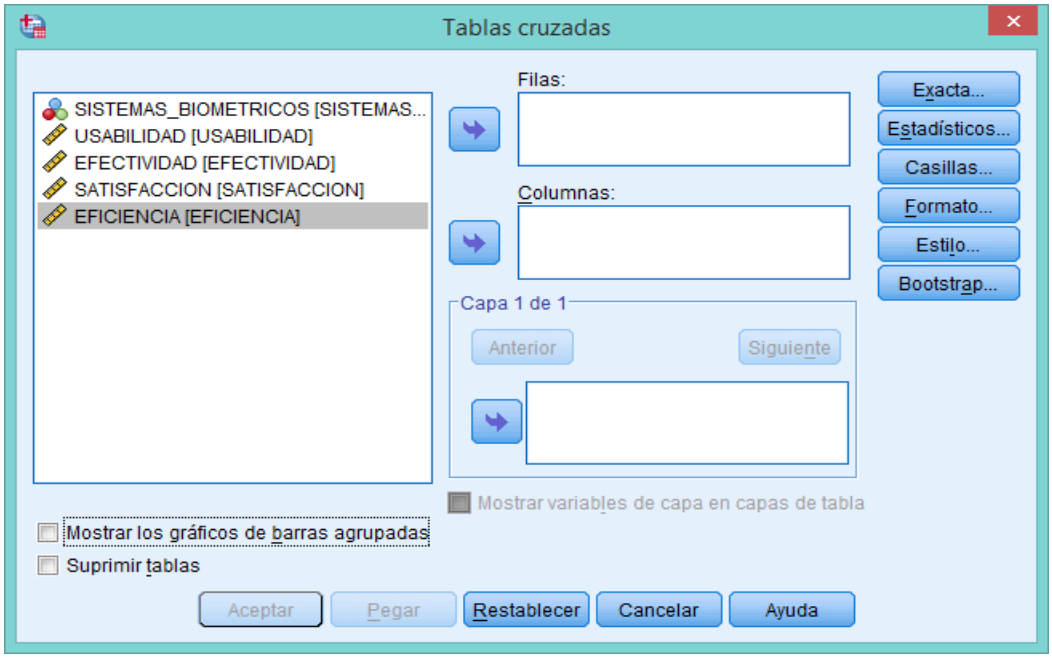

Figura 3-4 Tablas cruzadas

Elaborado por: Alvarado, Rene 2020.

- En columnas: insertamos los grupos
- En filas: insertamos la variable cuya frecuencia queremos analizar
- Presionamos estadísticos
- Señalamos el casillero Chi-cuadrado

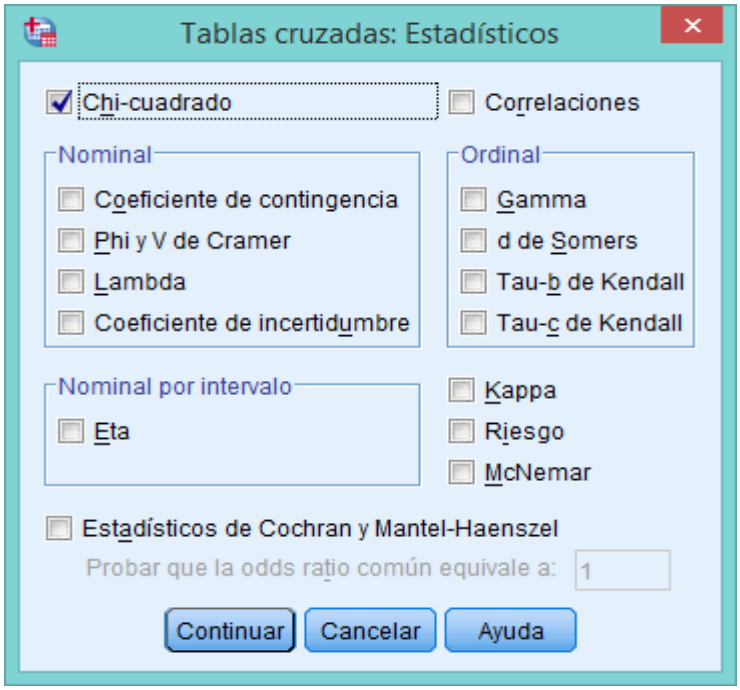

Figura 4-4 Tablas cruzadas estadísticas

Elaborado por: Alvarado, Rene 2020.

- Presionamos continuar
- Elegimos casillas

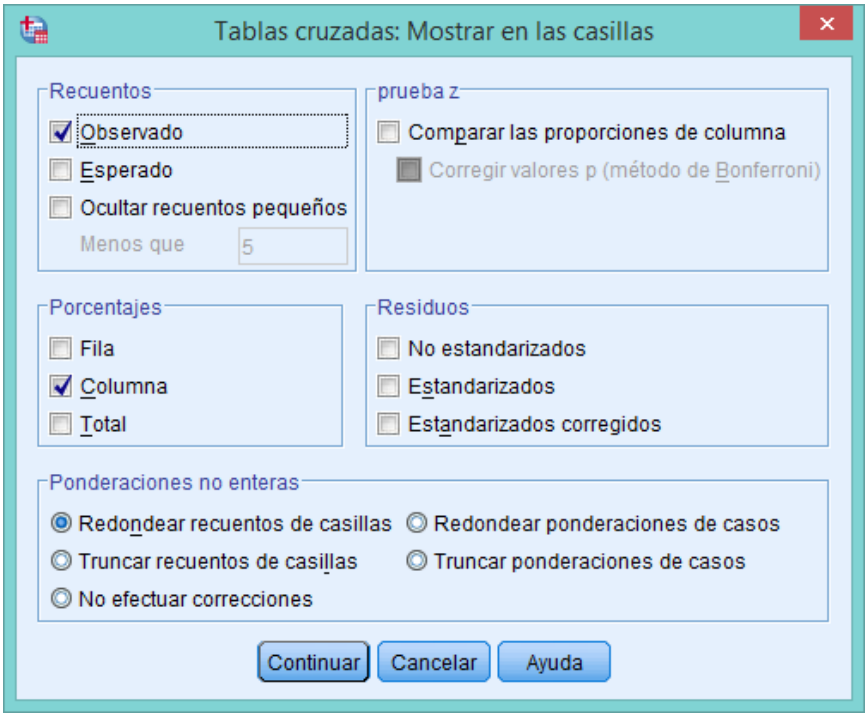

Figura 5-4 Tablas cruzadas en las casillas

Elaborado por: Alvarado, Rene 2020.

- Señalamos columnas
- Presionamos continuar
- Finalmente marcamos la casilla mostrar grafico de barras observadas

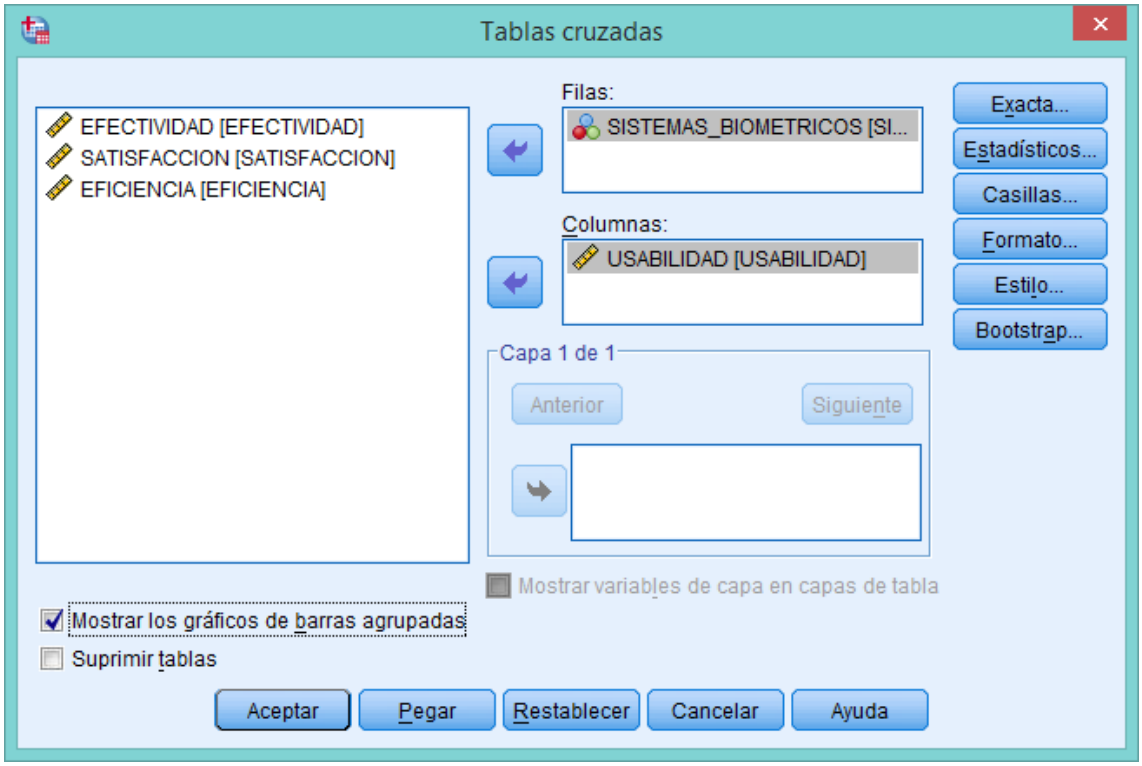

Figura 6-4 Tablas cruzadas

Elaborado por: Alvarado, Rene 2020.

- Damos clic en aceptar

✓ Prueba 1 usabilidad de sistemas de protección en el dispositivo móvil de los usuarios

Tabla 1-4 TÉCNICAS_BIOMETRICAS*USABILIDAD tabulación cruzada

			USABILIDAD		
			SISTEMA CONVENCIONAL	TECNOLOGIA BIOMETRICA	Total
TECNICAS_BIOMETRICAS	HUELLA_DACTILAR	Recuento	0	26	26
		% dentro de USABILIDAD	0,0%	100,0%	72,2%
	PATRON_NUMERICO	Recuento	7	0	7
		% dentro de USABILIDAD	70,0%	0,0%	19,4%
	PATRON_DIBUJO	Recuento	3	0	3
		% dentro de USABILIDAD	30,0%	0,0%	8,3%
Total		Recuento	10	26	36
		% dentro de USABILIDAD	100,0%	100,0%	100,0%

Elaborado por: Alvarado, Rene 2020.

- Observamos la significancia asintótica la cual debe ser es menor al 0.05%

Tabla 2-4 Pruebas de chi-cuadrado usabilidad

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	36,000[a]	2	,000
Razón de verosimilitud	42,541	2	,000
Asociación lineal por lineal	29,862	1	,000
N de casos válidos	36		

Elaborado por: Alvarado, Rene 2020.

Al realizar el análisis estadístico de acuerdo con la usabilidad de dispositivos móviles, el valor chi-cuadrado calculado es de 36.00, que a su vez es superior al valor de la tabla (anexo B) de distribución de 5,99.

El valor calculado de chi-cuadrado está en la región de rechazo de la hipótesis nula (Ho) por lo tanto se acepta la hipótesis de investigación (Hi). Obteniendo un valor de significancia de 0.000 en relación con nuestro α=5% = 0.05 consiguiendo un nivel de confianza del 100%. Demostrando la viabilidad de la investigación **"Implementación de un modelo de seguridad biométrica incrementará el nivel de confidencialidad en dispositivos móviles.**

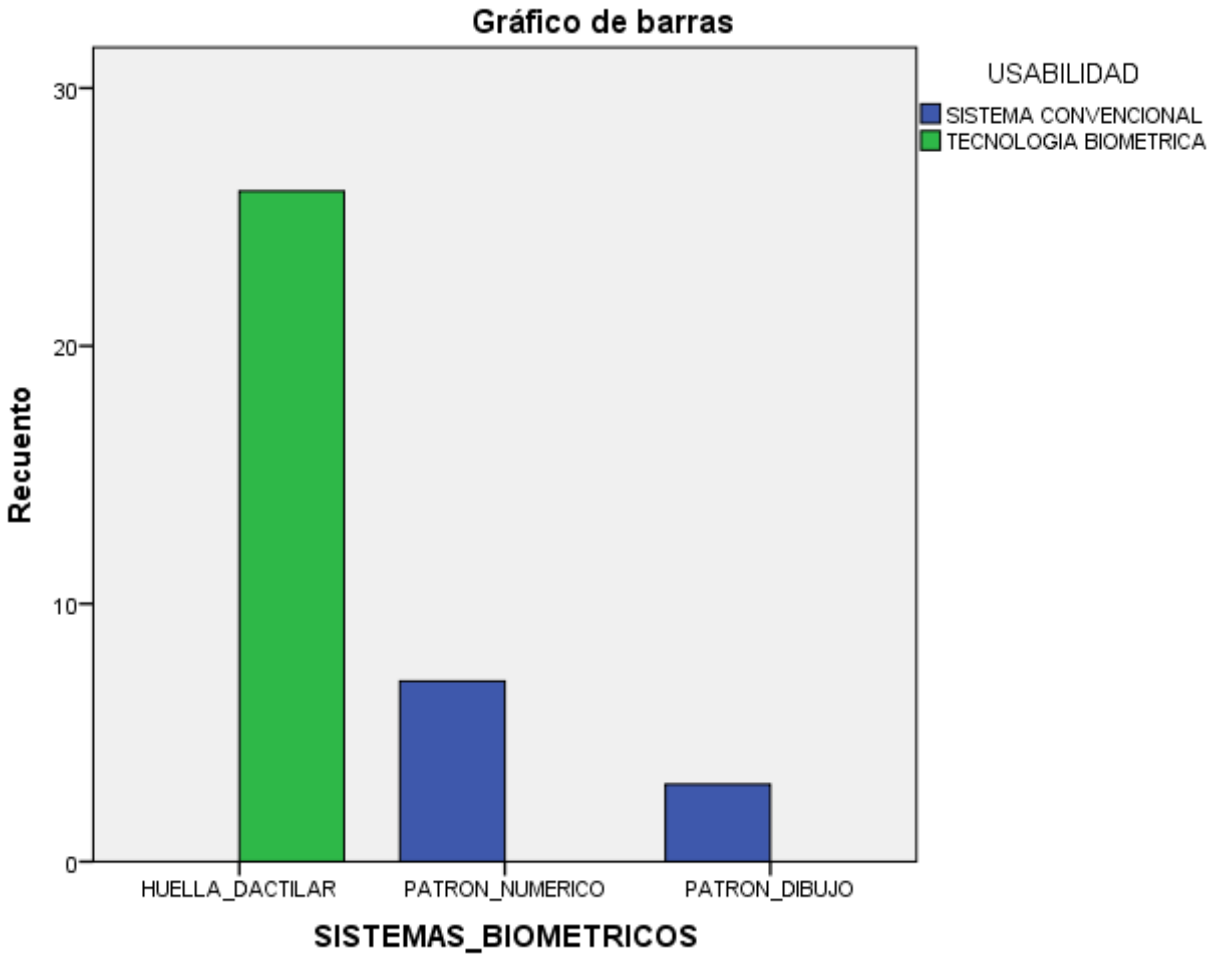

Gráfico 5-4 Usabilidad

Elaborado por: Alvarado, Rene 2020.

Tabla 3-4 TÉCNICAS_BIOMETRICAS*EFECTIVIDAD tabulación cruzada

			EFECTIVIDAD				
			BAJA	MEDIA	ALTA	MUY ALTA	Total
TÉCNICAS_BIOMETRICAS	HUELLA_DACTILAR	Recuento	0	1	8	17	26
		% dentro de EFECTIVIDAD	0,0%	12,5%	80,0%	100,0%	72,2%
	PATRON_NUMERICO	Recuento	0	5	2	0	7
		% dentro de EFECTIVIDAD	0,0%	62,5%	20,0%	0,0%	19,4%
	PATRON_DIBUJO	Recuento	1	2	0	0	3
		% dentro de EFECTIVIDAD	100,0%	25,0%	0,0%	0,0%	8,3%
Total		Recuento	1	8	10	17	36
		% dentro de EFECTIVIDAD	100,0%	100,0%	100,0%	100,0%	100,0%

Elaborado por: Alvarado, Rene 2020.

Tabla 4-4 Pruebas de chi-cuadrado efectividad

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	32,702[a]	6	,000
Razón de verosimilitud	30,346	6	,000
Asociación lineal por lineal	21,343	1	,000
N de casos válidos	36		

Elaborado por: Alvarado, Rene 2020.

Al realizar el análisis estadístico de acuerdo con la efectividad, el valor chi-cuadrado calculado es de 32.7, que a su vez es superior al valor de la tabla (anexo) de distribución de12.59.

El valor calculado de chi-cuadrado está en la región de rechazo de la hipótesis nula (Ho) por lo tanto se acepta la hipótesis de investigación (Hi). Obteniendo un valor de significancia de 0.000 en relación con nuestro α=5% = 0.05 consiguiendo un nivel de confianza del 100%. Demostrando la viabilidad de la investigación **"Implementación de un modelo de seguridad biométrica incrementará el nivel de confidencialidad en dispositivos móviles.**

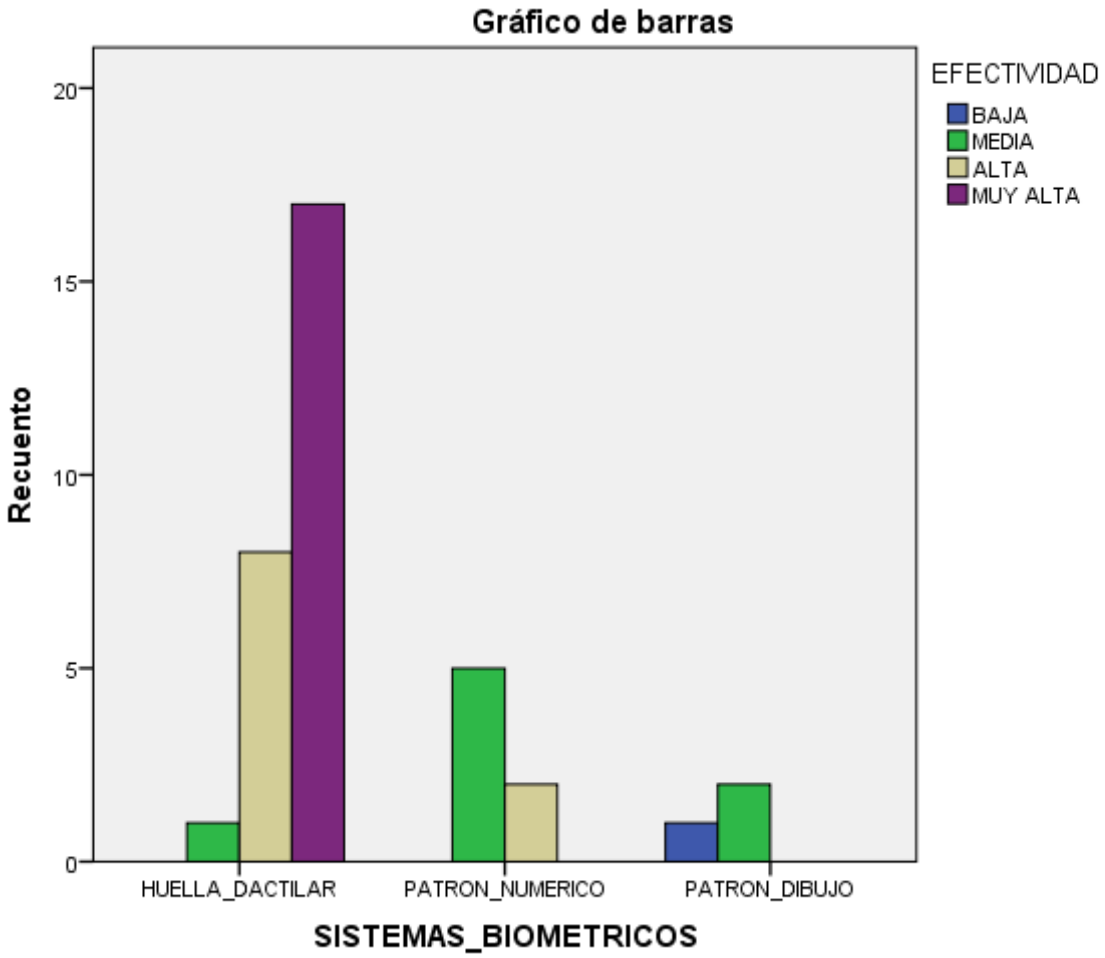

Gráfico 6-4 Efectividad

Elaborado por: Alvarado, Rene 2020.

Tabla 5-4 TÉCNICAS_BIOMETRICAS*SATISFACCION tabulación cruzada

			SATISFACCION				
			BAJA	MEDIA	ALTA	MUY ALTA	Total
TECNICAS_BIOMETRICOS	HUELLA_DACTILAR	Recuento	0	0	3	23	26
		% dentro de SATISFACCION	0,0%	0,0%	100,0%	92,0%	72,2%
	PATRON_NUMERICO	Recuento	0	5	0	2	7
		% dentro de SATISFACCION	0,0%	100,0%	0,0%	8,0%	19,4%
	PATRON_DIBUJO	Recuento	3	0	0	0	3
		% dentro de SATISFACCION	100,0%	0,0%	0,0%	0,0%	8,3%
Total		Recuento	3	5	3	25	36
		% dentro de SATISFACCION	100,0%	100,0%	100,0%	100,0%	100,0%

Elaborado por: Alvarado, Rene 2020.

Tabla 6-4 Pruebas de chi-cuadrado satisfacción

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	59,989[a]	6	,000
Razón de verosimilitud	40,819	6	,000
Asociación lineal por lineal	26,920	1	,000
N de casos válidos	36		

Elaborado por: Alvarado, Rene 2020.

Al realizar el análisis estadístico de acuerdo con la satisfacción, el valor chi-cuadrado calculado es de 59.98, que a su vez es superior al valor de la tabla (anexo) de distribución de12.59.

El valor calculado de chi-cuadrado está en la región de rechazo de la hipótesis nula (Ho) por lo tanto se acepta la hipótesis de investigación (Hi). Obteniendo un valor de significancia de 0.000 en relación con nuestro α=5% = 0.05 consiguiendo un nivel de confianza del 100%. Demostrando la viabilidad de la investigación **"Implementación de un modelo de seguridad biométrica incrementará el nivel de confidencialidad en dispositivos móviles.**

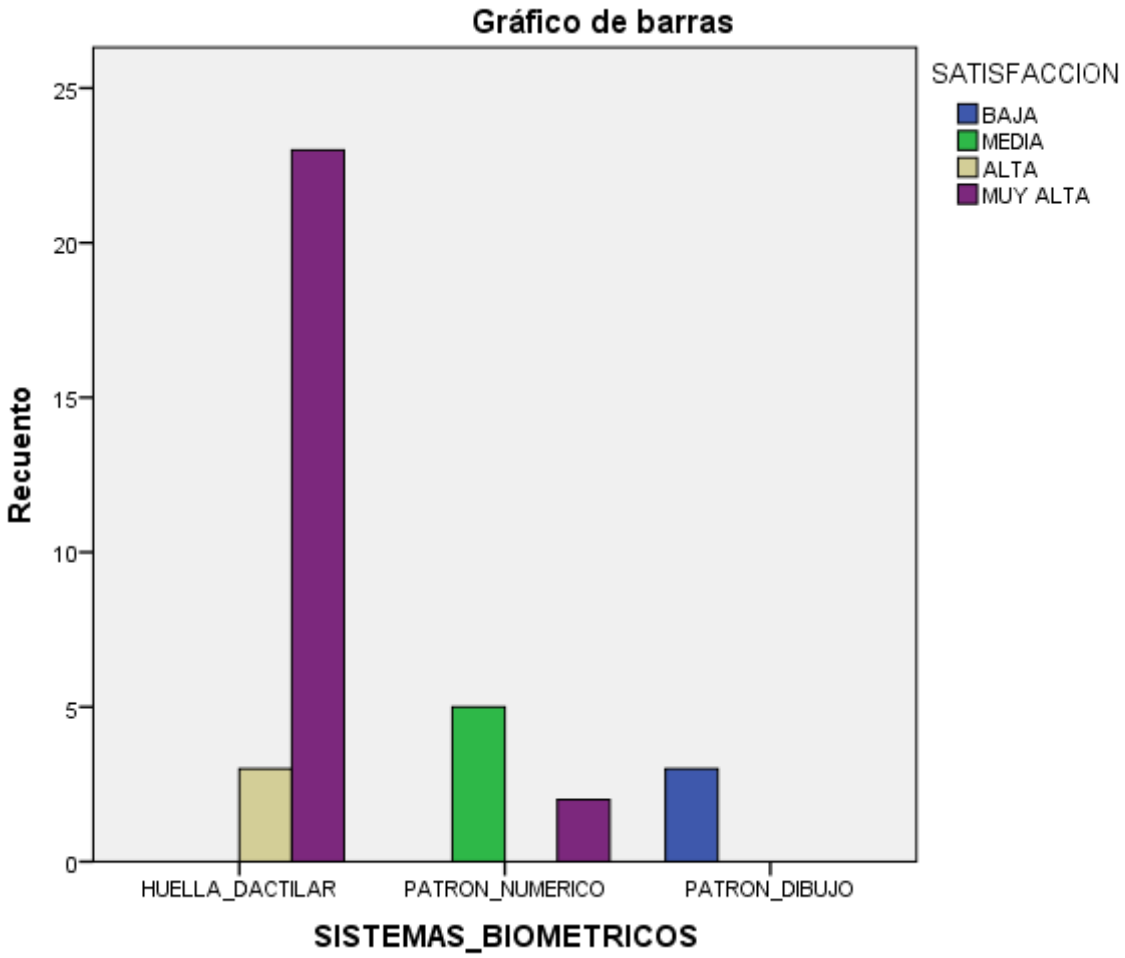

Gráfico 7-4 Satisfacción

Elaborado por: Alvarado, Rene 2020.

Tabla 7-4 TÉCNICAS_BIOMETRICAS*EFICIENCIA tabulación cruzada

			EFICIENCIA			
			MEDIA	ALTA	MUY ALTA	Total
TECNICAS_BIOMETRICOS	HUELLA_DACTILAR	Recuento	0	8	18	26
		% dentro de EFICIENCIA	0,0%	57,1%	100,0%	72,2%
	PATRON_NUMERICO	Recuento	1	6	0	7
		% dentro de EFICIENCIA	25,0%	42,9%	0,0%	19,4%
	PATRON_DIBUJO	Recuento	3	0	0	3
		% dentro de EFICIENCIA	75,0%	0,0%	0,0%	8,3%
Total		Recuento	4	14	18	36
		% dentro de EFICIENCIA	100,0%	100,0%	100,0%	100,0%

Elaborado por: Alvarado, Rene 2020.

Tabla 8-4 Pruebas de chi-cuadrado eficiencia

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	36,763[a]	4	,000
Razón de verosimilitud	31,138	4	,000
Asociación lineal por lineal	21,478	1	,000
N de casos válidos	36		

Elaborado por: Alvarado, Rene 2020.

Al realizar el análisis estadístico de acuerdo con la eficiencia, el valor chi-cuadrado calculado es de 36.7, que a su vez es superior al valor de la tabla (anexo) de distribución de 9.48.

El valor calculado de chi-cuadrado está en la región de rechazo de la hipótesis nula (Ho) por lo tanto se acepta la hipótesis de investigación (Hi). Obteniendo un valor de significancia de 0.000 en relación con nuestro α=5% = 0.05 consiguiendo un nivel de confianza del 100%. Demostrando la viabilidad de la investigación **"Implementación de un modelo de seguridad biométrica incrementará el nivel de confidencialidad en dispositivos móviles.**

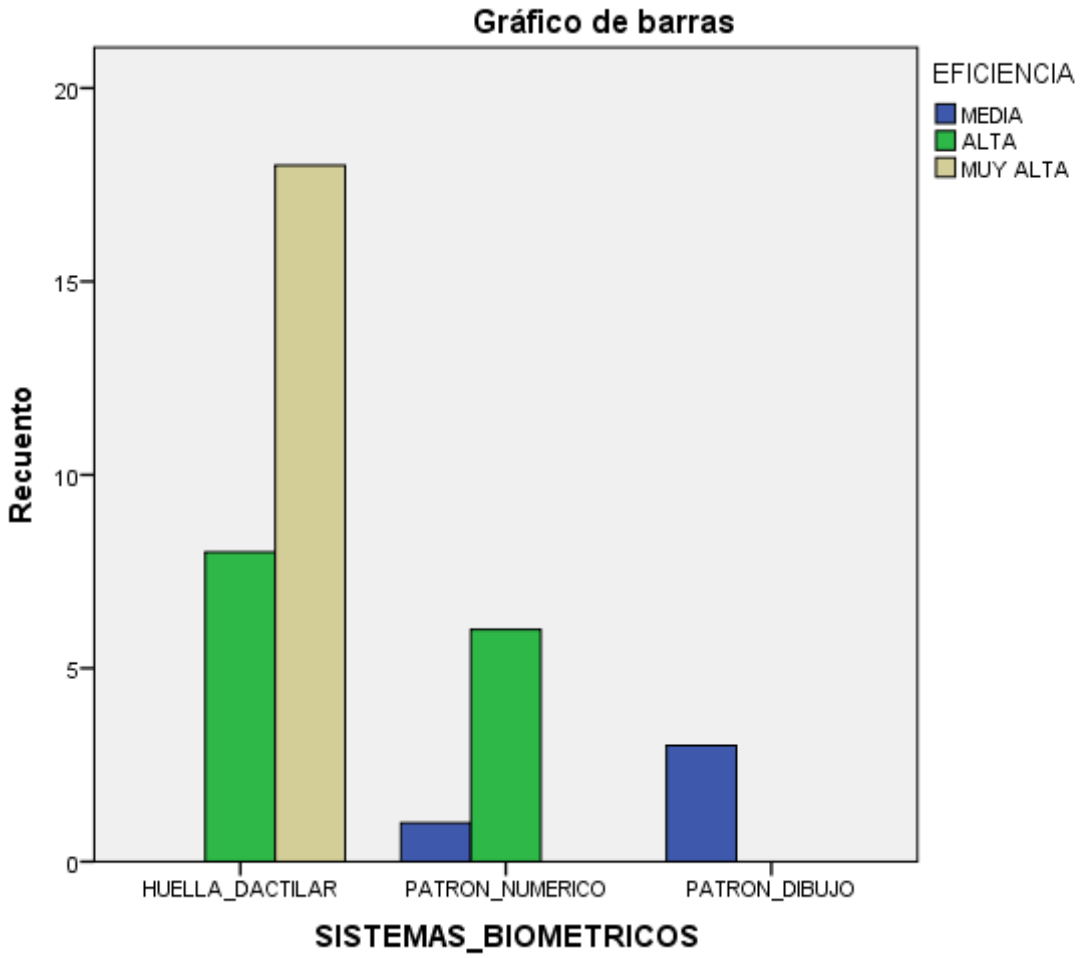

Gráfico 8-4 Eficiencia

Elaborado por: Alvarado, Rene 2020.

4.3. Escenarios Comparativos

Con los resultados obtenidos en base a los cuatro parámetros presentados y con la huella dactilar como técnica biométrica más aceptada para el acceso a los dispositivos móviles presentamos tres escenarios comparativos que a la vez nos servirán para la comprobación de la hipótesis general y final:

- ***Primer escenario:*** denominado *Escenario comparativo 1,* se realizará la comparativa entre patrón de desbloqueo y huella dactilar frente a los tipos de ataques que están expuestos los dispositivos móviles.
- ***Segundo escenario:*** denominado *Escenario comparativo 2,* se realizará la comparativa entre pin de seguridad y huella dactilar frente a los tipos de ataques que están expuestos los dispositivos móviles.

- ***Tercer escenario:*** denominado *Escenario comparativo 3,* se realizará la comparativa entre contraseña alfanumérica y huella dactilar frente a los tipos de ataques que están expuestos los dispositivos móviles.

Las fases para analizar las vulnerabilidades presentes en los dispositivos móviles son:

1) Generación de ataques.
2) Análisis de la vulnerabilidad de información
3) Aplicación del sistema biométrico.
4) Análisis comparativo de los resultados de los escenarios de prueba (Castro, 2017).

4.3.1. Escenario comparativo 1:

A continuación, se describen los instrumentos utilizados y el esquema del escenario 1.

Tabla 9-4 Escenario comparativo 1

ESCENARIO	INSTRUMENTOS	TIPO DE ATAQUE
Escenario comparativo 1	Patrón de desbloqueo vs Huella dactilar	Grabación de un video
		Software (miracle box crack)
		Patrones largos

Elaborado por: Alvarado, Rene 2020.

4.3.2. Escenario comparativo 2

A continuación, se describen los instrumentos utilizados y el esquema del escenario 2.

Tabla 10-4 Escenario **comparativo** 2

ESCENARIO	INSTRUMENTOS	TIPO DE ATAQUE
Escenario comparativo 2	Pin de seguridad vs Huella dactilar	Acceso a los datos de sensor de pantalla
		Software (miracle box crack)
		Ataque diccionario

Elaborado por: Alvarado, Rene 2020.

4.3.3. Escenario comparativo 3

A continuación, se describen los instrumentos utilizados y el esquema del escenario 3.

Tabla 11-4 Escenario **comparativo** 3

ESCENARIO	INSTRUMENTOS	TIPO DE ATAQUE
Escenario comparativo 3	Contraseña alfanumérica vs Huella dactilar	contraseñas débiles, poco creativas y muy fáciles de adivinar
		Ataque diccionario
		Malware y Keylogger

Elaborado por: Alvarado, Rene 2020.

La seguridad en los dispositivos móviles es de suma importancia para salvaguardar nuestra información confidencial, sin embargo, esta tecnología es vulnerable a ataques que afectan la integridad de la información sensible que se encuentra almacenada en estos equipos.

La afirmación anterior se deriva de la investigación realizada y de la implementación de los escenarios de prueba, cuyos resultados serán tratados en este capítulo.

4.4. Dispositivos móviles almacenamiento

Los dispositivos móviles permiten el acceso a nuestra información personal de manera fácil a redes sociales, correo electrónico, fotos, compras online, etc., si bien es cierto el patrón de desbloqueo y el código de acceso protegen nuestra privacidad, pero ¿son suficientes? , Existe la posibilidad de que se realice un mal uso de nuestros datos por parte de personas malintencionadas, si éstas tienen acceso a la información que almacenamos en nuestros dispositivos móviles. Publicación de datos y contenidos sin nuestro permiso, coacción debido a la información obtenida, secuestro de identidades y cuentas de servicios que en muchos casos incluyen daño económico y moral.

La información que almacenamos en los dispositivos móviles es más importante de lo que nos podemos imaginar y si cae en malas manos, puede afectar a nuestra vida social, laboral y familiar. Por eso, es muy importante protegerlos correctamente, en caso de que lo perdamos, nos lo roben o lo tomen "prestado" temporalmente sin nuestro consentimiento, impidamos que puedan acceder a dicha información evitando así problemas de privacidad y seguridad.

Almacenamiento de información en el dispositivo móvil:

Correos electrónicos, documentos, fotos, notas, datos bancarios, videos, chats, notas de audio y redes sociales.

Figura 7-4 Datos almacenados en un dispositivo móvil

Figura 8-4 Aplicaciones en dispositivos móviles

Las aplicaciones permiten al usuario efectuar un conjunto de tareas de cualquier tipo, profesional, de ocio, educativas, de acceso a servicios, etc., facilitando las gestiones o actividades a desarrollar.

Por lo general, se encuentran disponibles a través de plataformas de distribución, operadas o las compañías propietarias de los sistemas operativos móviles como Android, iOS, BlackBerry OS, Windows Phone, entre otros. Existen aplicaciones móviles gratuitas u otras de pago, donde en promedio el 20 a 30 % del coste de la aplicación se destina al distribuidor y el resto es para el desarrollador.

4.5. Proceso de la Información

Para el proceso y manejo de la información en las tablas, se utilizó la siguiente abreviatura:

- **Indicador:** Indicadores planteados en la Operacionalización de las Variables.
- **Escenario:** Escenario sin/con modelo de seguridad aplicado.
- **Información expuesta:** Tipo de vulnerabilidad.
- **Número:** Número de vulnerabilidades encontradas.

La tabla 20-4 permitirá la recolección de datos de los resultados obtenidos en los escenarios de prueba, la cual posee la siguiente estructura:

Tabla 12-4 Información de dispositivos móviles

INFORMACIÓN	TIPO DE INFORMACIÓN	CANTIDAD
datos de información de usuario	Correos Electrónicos, Documentos, Fotos, Notas, Datos Bancarios, Videos, Chats, Notas De Audio Y Redes Sociales.	9
amenazas de datos de información de usuario	Secuestro De Cuenta, Publicación De Imágenes O Videos Privados Sin Consentimiento, Chantaje Y Extorción, Obtención De Datos Bancarios, Pérdida De Identidad.	5
datos sensibles del usuario	Contraseña, Pin, Firma, Huella Dactilar. Reconocimiento Facial, Retina, Patrón De Voz	7
amenazas o fallo de seguridad del dispositivo móvil	Aplicaciones Maliciosas, Localización, Conexiones Inseguras, Configuraciones	3

Elaborado por: Alvarado, Rene 2020.

Para establecer el nivel de exposición de la información en los escenarios de prueba, se ha elaborado la **tabla 21-4** para ponderar cada uno de los niveles.

Tabla 13-4 Nivel de integridad de los datos

Nivel	Valor	Descripción
1	Nulo	Datos completamente vulnerables
2	Bajo	Datos sensibles expuestos
3	Medio	Datos no relevantes expuestos
4	Alto	Datos sin riesgo

Elaborado por: Alvarado, Rene 2020.

Dónde:

- **Nivel 1:** Los datos son expuestos en su totalidad y son vulnerables.
- **Nivel 2:** Los datos sensibles son expuestos tras el ataque.
- **Nivel 3:** Únicamente datos no relevantes son expuestos tras el ataque.
- **Nivel 4:** Integridad garantizada.

4.5.1. Escenario vulnerable

Tabla 14-4 Datos escenario 1 vulnerable

Escenario	Información expuesta	Escenario Vulnerable	
		Número	Nivel
Escenario 1 Vulnerable	Datos de información de usuario	9	2
	Amenazas de datos de información de usuario	5	2
	Datos sensibles del usuario	7	2
	Amenazas o fallo de seguridad del dispositivo móvil	3	1

Elaborado por: Alvarado, Rene 2020.

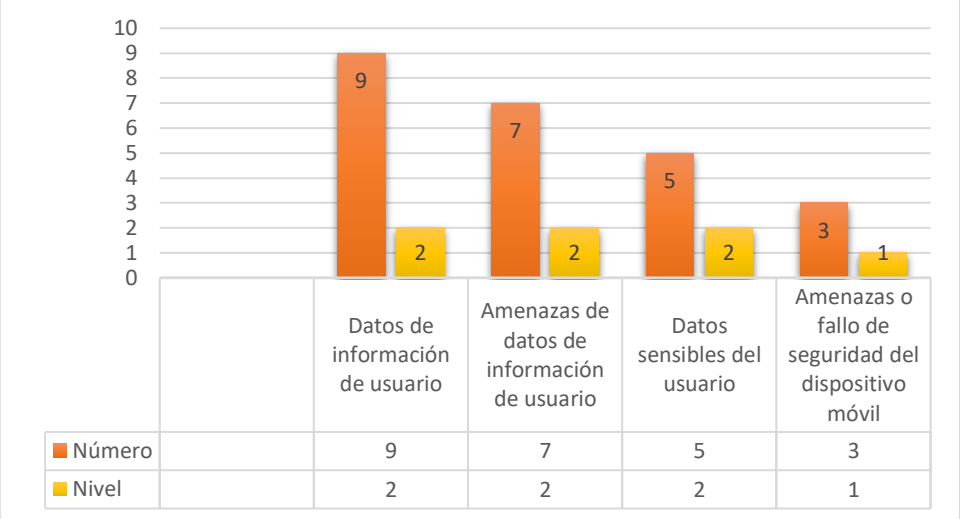

Gráfico 9-4 Datos escenario vulnerable

Elaborado por: Alvarado, Rene 2020.

En el gráfico anterior podemos observar que el nivel exposición es alto en los datos de información de usuario y datos sensibles cuando se utiliza los sistemas de seguridad tradicionales, ya que su nivel de protección a esta información es bajo, esto se debe a que estos sistemas son de fácil detección. Cuando existen amenazas y fallos de seguridad los datos del dispositivo móvil quedan totalmente expuestos.

4.5.2. Escenario seguro

Tabla 15-4 Datos escenario 1 seguro

Escenario	Información expuesta	Escenario Vulnerable	
		Número	Nivel
Escenario 1 Seguro	Datos de información de usuario	9	3
	Amenazas de datos de información de usuario	5	4
	Datos sensibles del usuario	7	4
	Amenazas o fallo de seguridad del dispositivo móvil	3	4

Elaborado por: Alvarado, Rene 2020.

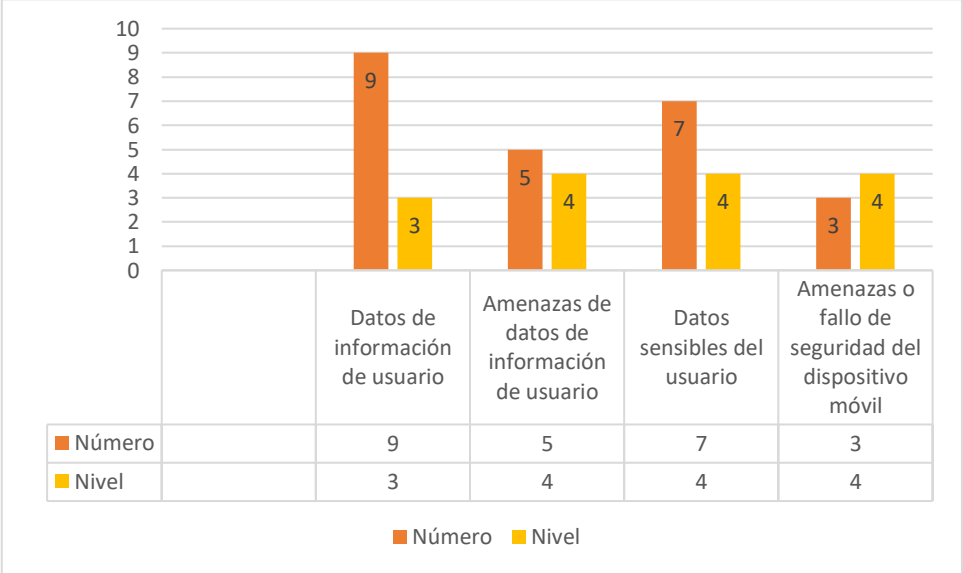

Gráfico 10-4 Datos escenario seguro

Elaborado por: Alvarado, Rene 2020.

En la tabla podemos observar que, de acuerdo con los resultados obtenidos en el Escenario seguro con la aplicación de las técnicas de seguridad biométricas, es notoria la disminución de la información expuesta con respecto al escenario vulnerable sin la aplicación de estas tecnologías.

Tabla 16-4 Contingencia de los escenarios propuestos

Información expuesta	Escenario comparativo 1 patrón de desbloqueo vs huella dactilar				Escenario comparativo 2 Pin de seguridad vs huella dactilar				Escenario comparativo 3 contraseña alfanumérica vs huella dactilar			
	Patrón de desbloqueo		Huella dactilar		Pin de seguridad		Huella dactilar		Contraseña alfanumérica		Huella dactilar	
	Escenario Vulnerable		Escenario seguro		Escenario Vulnerable		Escenario seguro		Escenario Vulnerable		Escenario seguro	
	Número	Nivel	Número	Nivel	Número	Nivel	Número	Nivel	Número	Nivel	Número	Nivel
Datos de información de usuario	9	2	9	3	9	1	9	3	9	1	9	3
Amenazas de datos de información de usuario	5	2	5	4	5	1	5	4	5	2	5	4
Datos sensibles del usuario	7	2	7	4	7	2	7	4	7	2	7	4
Amenazas o fallo de seguridad del dispositivo móvil	3	1	3	4	3	1	3	4	3	1	3	4
TOTAL	24	7	24	15	24	5	24	15	24	6	24	15

Elaborado por: Alvarado, Rene 2020.

4.6. Verificación de la hipótesis

Utilizaremos el estadístico Chi cuadrado, para comprobar si los datos observados se encuentran dentro de los parámetros aceptables y poder aprobar o rechazar la hipótesis planteada, para lo cual necesitamos encontrar el Chi cuadrado tabla (Xt) y Chi cuadrado calculado (Xc), determinando que si el Xc es mayor o igual que el Xt se acepta la hipótesis de trabajo y se rechaza la hipótesis nula. (Rene Alvarado 2020).

Cálculo de Chi cuadrado calculado (Xc):

$$\mathbf{X} = \mathbf{\Sigma}\ \frac{(fo - Fe)^2}{Fe}$$

X^2 = Chi-cuadrado
Σ= Sumatoria
Fo = Frecuencia observada
Fe = Frecuencia esperada o teórica

Tabla 17-4 Verificación de hipótesis

	Fo	Fe	Fo-Fe	$(Fo-Fe)^2$	$\frac{(Fo-Fe)^2}{Fe}$
Datos de información de usuario	2	3	-1	1	0,5
Amenazas de datos de información de usuario	2	4	-2	4	1
Datos sensibles del usuario	2	4	-2	4	1
Amenazas o fallo de seguridad del dispositivo móvil	1	4	-3	9	2,25
Datos de información de usuario	1	3	-2	4	1,3
Amenazas de datos de información de usuario	1	4	-3	9	2,25
Datos sensibles del usuario	2	4	-2	4	1
Amenazas o fallo de seguridad del dispositivo móvil	1	4	-3	9	2,25
Datos de información de usuario	1	3	-2	4	1,3
Amenazas de datos de información de usuario	2	4	-2	4	1
Datos sensibles del usuario	2	4	-2	4	1
Amenazas o fallo de seguridad del dispositivo móvil	1	4	-3	9	2,25
				TOTAL	17,1

Elaborado por: Alvarado, Rene 2020.

Entonces Chi Cuadrado calculado es 17,1

4.7. Cálculo de Chi cuadrado tabla

Primero calcularemos los grados de libertad que se obtendrá a través de la formula.

$$\boldsymbol{G1} = (f - 1)(c - 1)$$

Dónde:

G1= Grado de libertad

F=Filas

C= Columnas.

Es decir:

$$\boldsymbol{G1 = (4 - 1)(2 - 1)}$$

$$\boldsymbol{G1 = 3}$$

Para obtener el Chi cuadrado tabla se buscó con grados de libertad 3 y el nivel de confianza 0,05 en la tabla Anexo B, obteniendo Chi-cuadrado tabla (X^2t) = 7,8147

$$\boldsymbol{X^2c=17,1 > X^2t=7,8147}$$

De acuerdo con estos resultados pudo comprobarse que el chi-cuadrado calculado es mayor que el chi-cuadrado tabla, por lo cual se acepta la Hipótesis de trabajo y se rechaza la Hipótesis nula, Es decir **"La aplicación de una técnica biométrica como es la huella digital si incrementara el nivel de seguridad a la confidencialidad en dispositivos móviles".**

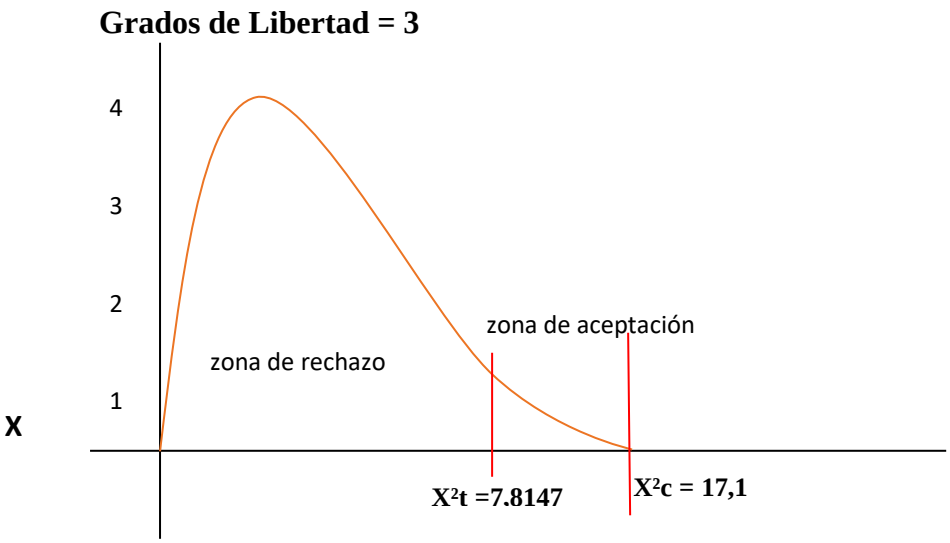

Gráfico 11-4 Comprobación de la Hipótesis

Elaborado por: Alvarado, Rene 2020.

CONCLUSIONES

- Realizada la investigación se puede concluir que de todas las técnicas biométricas que se pueden aplicar a los dispositivos móviles la más segura es la de los iris de los ojos, pero la técnica más aceptada por los usuarios es la de la huella digital.

- Las principales vulnerabilidades que afectan a los dispositivos móviles tienen que ver con la suplantación de identidad en las estaciones base y la intercepción de los datos en el tráfico de las comunicaciones.

- El iris del ojo es la técnica más segura que puede ser implementada en los dispositivos móviles ya que posee alrededor de 266 puntos únicos mientras que la mayoría de las técnicas biométricas poseen alrededor de 13 a 60 características distintas, además se encuentra protegida por la córnea que no permite que se deteriore o sufra cambios.

RECOMENDACIONES

- Se recomienda la utilización de una técnica biométrica en lo posible la mejor para la autenticación a los dispositivos móviles ya que son mucho más segura que contraseñas, patrón de desbloqueo, pin, mismas que están predispuestas a hackeo, en cambio la biométrica es característica única del ser humano.

- Para una mejor seguridad de la información que se almacena en los dispositivos móviles es aconsejable utilizar las técnicas biométricas que en algunos equipos inalámbricos ya vienen instalados.

- Esta investigación es solo una parte de un proyecto que tiene como finalidad el diseño de un modelo biométrico para dispositivos móviles, por lo cual se recomienda continuar en una siguiente etapa, que sería el desarrollo, diseño e implementación de un modelo biométrico para acceder a la información de los dispositivos móviles.

BIBLIOGRAFÍA

Alvarado, B., Landeta , C., & Sánchez , J. (2010). *"ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE INMÓTICA.* Obtenido de http://repositorio.ucsg.edu.ec/bitstream/3317/8551/1/T-UCSG-PRE-TEC-ITEL-218.pdf

Carri, J., Pasini, A., Pesado, P., & De Giusti, A. (s.f.). *Reconocimiento biométrico en aplicaciones de E-Government. Análisis de confiabilidad / tiempo de respuesta.* . Obtenido de https://digital.cic.gba.gob.ar/bitstream/handle/11746/3693/11746_3693.pdf-PDFA.pdf?sequence=1&isAllowed=y

Castro, C. (Diceimbre de 2017). MODELO DE SEGURIDAD PARA GARANTIZAR . Ecuador. Recuperado el Septiembre de 2019, de http://dspace.espoch.edu.ec/bitstream/123456789/7842/1/20T00952.pdf

Cortés, J. A. (Diciembre de 2010). *SISTEMAS DE SEGURIDAD BASADOS EN BIOMETRÍA. SECURITY SYSTEMS BASED ON BIOMETRICS.* Obtenido de Scientia et Technica Año XVII: https://dialnet.unirioja.es/servlet/articulo?codigo=4528099

Coskun, V., Ozdenizci, B., & Ok, K. (2012). A survey on near field communication (NFC) technology. *Wireless Personal Communications*

Digitalattack. (Agosto de 2020). Mapa de ataque digital. Obtenido de https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18489

Domingo, M. (2017). Seguridad en dispositivos móviles. *6*. Obtenido de https://www.exabyteinformatica.com/uoc/Informatica/Tecnologia_y_desarrollo_en_dispositivos_moviles/Tecnologia_y_desarrollo_en_dispositivos_moviles_(Modulo_6).pdf

El-Abed, M., & Christophe, C. (Mayo de 2014). Evaluation of Biometric Systems. Recuperado el Septiembre de 2019, de https://hal.archives-ouvertes.fr/hal-00990617/file/InTech-Evaluation_of_biometric_systems.pdf

Escobar, J., & Quinto, L. (2015). Vuknerabilidad de los equipos moviles. *(7)*. Antioquia. Recuperado el 2019, de file:///C:/Users/Usuario/Downloads/248-Texto%20del%20art%C3%ADculo-474-1-10-20160721.pdf

Escobar, J., & Quinto, L. (24 de Abril de 2015). *Vulnerabilidad en dispositivos móviles con sistema operativo Android.* Obtenido de http://webcache.googleusercontent.com/search?q=cache:1FTEpXY0rBYJ:ojs.tdea.edu.co/index.php/cuadernoactiva/article/download/248/240/+&cd=3&hl=es-419&ct=clnk&gl=ec

Giraldo , A., & Gomez , D. (Diciembre de 2017). *ESTADO DEL ARTE DE LA SEGURIDAD EN SISTEMAS BIOMETRICOS.* Obtenido de https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/14348/1/52752700.pdf

Giusto Bilic, D. (Septiembre de 2019). Análisis de la seguridad en dispositivos móviles durante el primer semestre de 2019. *Análisis de la seguridad en dispositivos móviles durante el primer semestre de 2019*. Recuperado el Septiembre de 2019, de https://www.welivesecurity.com/la-es/2019/09/03/analisis-seguridad-dispositivos-moviles-primer-semestre-2019/

Gonzales, R. (2003). Metodología de la Investigación. Recuperado el 2019, de http://www.sld.cu/galerias/pdf/sitios/bmn/metodologia_de_la_investigacion.diseno_teorico_y_formulacion_proyecto_investigacion.pdf

Guerra Casanova, J. (2014). *Propuesta, implementación y evaluación de la Biometría de firma en el aire como sistema de verificación en teléfonos móviles*. Obtenido de http://oa.upm.es/30437/1/JAVIER_GUERRA_CASANOVA.pdf

Hernández , C. (27 de Septiembre de 2015). *ESTUDIO DEL RENDIMIENTO BIOMÉTRICO DE DISPOSITIVOS DE HUELLA DACTILAR*. Obtenido de https://core.ac.uk/download/pdf/79176660.pdf

INCIBE. (2016). ESPAÑA. Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

INTER. (2019). Investigacion correlacional. Recuperado el Septiembre de 2019, de http://metodologiainter.weebly.com/uploads/1/9/2/6/19268119/investigacin_correlacional.pdf

Mateu, C. (2010). *Desarrollo de Aplicaciones Web.* Barcelona: Eureca Media.

Miller, C. (2012). *Exploring the NFC attack surface*. (SecTor) Obtenido de http://2012.video.sector.ca/video/51115364

Monje, C. (2011). Metodologia de la investigacion. Colombia. Obtenido de https://www.uv.mx/rmipe/files/2017/02/Guia-didactica-metodologia-de-la-investigacion.pdf

Pérez, A. (2009). El método comparativo y el análisis de configuraciones causales. Obtenido de http://www.uca.edu.sv/mcp/media/archivo/8da94d_lemetodocomparativoyelanalisisdeconfiguracionescausales.pdf

Perez, S. (2011). *Guía sobre las tecnologías biometricas aplicadas a la seguridad.* Obtenido de http://www.inteco.es

Security. (2018). Dispositivos moviles. Recuperado el 2019, de https://www.pandasecurity.com/spain/mediacenter/dispositivos-moviles/seguridad-login-android-ios/

SGSI, N. D. (2013). *Sistema de Gestión de la Seguridad de la Información*. Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

Tolosa , C., & Giz , Á. (s.f.). *Sistemas Biométricos.* Obtenido de https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

Villalobos Castaldi, F. (Junio de 2011). *USO DE LA RED VASCULAR DE LA RETINA COMO MEDIO BIOMÉTRICO DE IDENTIFICACIÓN.* Obtenido de http://148.204.63.111/SABERv3/Repositorios/webVerArchivo/26203

XATAKA-móvil. (2020). La estafa del SMS ahora se hace pasar por DHL: nueva oleada de malware con el mensaje de 'El envío se ha devuelto dos veces'. Obtenido de https://www.xatakamovil.com/

Yoorah, J. (2019). Seguridad y Biometría en el Móvil. España. Recuperado el Septiembre de 2019, de http://www.ceditec.etsit.upm.es/index.php?option=com_content&view=article&id=21670&Itemid=1371&lang=es

ANEXOS

ANEXOS A

FORMULARIO DE USABILIDAD

Formulario de usabilidad

Investigación de seguridad y usabilidad

La finalidad de este formulario es obtener datos estadísticos que nos ayuden a comprender las preferencias de los usuarios para diseñar el modelo biométrico que disminuya la vulnerabilidad a la confidencialidad en dispositivos móviles. Toda la información que recopilada será anónima. Llénelo con calma. Muchas gracias por su colaboración.

1. **Género:**

Masculino	
Femenino	

2. **Edad:**

18-30	
31-50	
51-70	
71-80	

3. **Nivel de estudios:**

Ciclo básico	
Bachillerato	
Universidad	

4. **A que se dedica:**

Estudios	

Trabajo de campo	
Trabajo de oficina	

5. **¿Utiliza sistemas de seguridad en su dispositivo móvil para proteger su información?**

Si	
No	

6. **¿Cuál es el sistema de seguridad que usted utiliza en su dispositivo móvil para proteger su información?**

Huella_Dactilar	
Ojos_Iris	
Ojo_Retina	
Vascular_Dedo	
Geometria_De_La_Mano	
Escritura_Y_Firma	
Voz	
Cara_3d	
Cara_2d	
Patron_Numerico	
Patron_Dibujo	

7. **Califique la efectividad, satisfacción y eficiencia del sistema de seguridad que usted utiliza para proteger su información en su dispositivo móvil:**

SISTEMA DE SEGURIDAD	EFECTIVIDAD			
	Muy Alta	Alta	Media	Baja
Huella_Dactilar	26			
Ojos_Iris				
Ojo_Retina				
Vascular_Dedo				
Geometria_De_La_Mano				
Escritura_Y_Firma				
Voz				
Cara_3d				
Cara_2d				
Patron_Numerico				
Patron_Dibujo				

SISTEMA DE SEGURIDAD	SATISFACION			
	Muy Alta	Alta	Media	Baja
Huella_Dactilar				
Ojos_Iris				
Ojo_Retina				
Vascular_Dedo				
Geometria_De_La_Mano				
Escritura_Y_Firma				
Voz				

Cara_3d				
Cara_2d				
Patron_Numerico				
Patron_Dibujo				

SISTEMA DE SEGURIDAD	**EFICIENCIA**			
	Muy Alta	Alta	Media	Baja
Huella_Dactilar				
Ojos_Iris				
Ojo_Retina				
Vascular_Dedo				
Geometria_De_La_Mano				
Escritura_Y_Firma				
Voz				
Cara_3d				
Cara_2d				
Patron_Numerico				
Patron_Dibujo				

ANEXO B

TABLA DE DISTRIBUCIÓN CHI-CUADRADO

v/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45	0,5
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,5970	1,3863
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649	3,2831	2,9462	2,6430	2,3660
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784	4,4377	4,0446	3,6871	3,3567
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644	5,5731	5,1319	4,7278	4,3515
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311	6,6948	6,2108	5,7652	5,3481
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834	7,8061	7,2832	6,8000	6,3458
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245	8,9094	8,3505	7,8325	7,3441
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564	10,0060	9,4136	8,8632	8,3428
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807	11,0971	10,4732	9,8922	9,3418
11	31,2635	28,7291	26,7569	24,7250	21,9200	19,6752	17,2750	15,7671	14,6314	13,7007	12,8987	12,1836	11,5298	10,9199	10,3410
12	32,9092	30,3182	28,2997	26,2170	23,3367	21,0261	18,5493	16,9893	15,8120	14,8454	14,0111	13,2661	12,5838	11,9463	11,3403
13	34,5274	31,8830	29,8193	27,6882	24,7356	22,3620	19,8119	18,2020	16,9848	15,9839	15,1187	14,3451	13,6356	12,9717	12,3398
14	36,1239	33,4262	31,3194	29,1412	26,1189	23,6848	21,0641	19,4062	18,1508	17,1169	16,2221	15,4209	14,6853	13,9961	13,3393
15	37,6978	34,9494	32,8015	30,5780	27,4884	24,9958	22,3071	20,6030	19,3107	18,2451	17,3217	16,4940	15,7332	15,0197	14,3389
16	39,2518	36,4555	34,2671	31,9999	28,8453	26,2962	23,5418	21,7931	20,4651	19,3689	18,4179	17,5646	16,7795	16,0425	15,3385
17	40,7911	37,9462	35,7184	33,4087	30,1910	27,5871	24,7690	22,9770	21,6146	20,4887	19,5110	18,6330	17,8244	17,0646	16,3382
18	42,3119	39,4220	37,1564	34,8052	31,5264	28,8693	25,9894	24,1555	22,7595	21,6049	20,6014	19,6993	18,8679	18,0860	17,3379
19	43,8194	40,8847	38,5821	36,1908	32,8523	30,1435	27,2036	25,3289	23,9004	22,7178	21,6891	20,7638	19,9102	19,1069	18,3376
20	45,3142	42,3358	39,9969	37,5663	34,1696	31,4104	28,4120	26,4976	25,0375	23,8277	22,7745	21,8265	20,9514	20,1272	19,3374
21	46,7963	43,7749	41,4009	38,9322	35,4789	32,6706	29,6151	27,6620	26,1711	24,9348	23,8578	22,8876	21,9915	21,1470	20,3372
22	48,2676	45,2041	42,7957	40,2894	36,7807	33,9245	30,8133	28,8224	27,3015	26,0393	24,9390	23,9473	23,0307	22,1663	21,3370
23	49,7276	46,6231	44,1814	41,6383	38,0756	35,1725	32,0069	29,9792	28,4288	27,1413	26,0184	25,0055	24,0689	23,1852	22,3369
24	51,1790	48,0336	45,5584	42,9798	39,3641	36,4150	33,1962	31,1325	29,5533	28,2412	27,0960	26,0625	25,1064	24,2037	23,3367
25	52,6187	49,4351	46,9280	44,3140	40,6465	37,6525	34,3816	32,2825	30,6752	29,3388	28,1719	27,1183	26,1430	25,2218	24,3366
26	54,0511	50,8291	48,2898	45,6416	41,9231	38,8851	35,5632	33,4295	31,7946	30,4346	29,2463	28,1730	27,1789	26,2395	25,3365
27	55,4751	52,2152	49,6450	46,9628	43,1945	40,1133	36,7412	34,5736	32,9117	31,5284	30,3193	29,2266	28,2141	27,2569	26,3363
28	56,8918	53,5939	50,9936	48,2782	44,4608	41,3372	37,9159	35,7150	34,0266	32,6205	31,3909	30,2791	29,2486	28,2740	27,3362
29	58,3006	54,9662	52,3355	49,5878	45,7223	42,5569	39,0875	36,8538	35,1394	33,7109	32,4612	31,3308	30,2825	29,2908	28,3361