ANÁLISIS DE BUENAS PRÁCTICAS PARA LA SELECCIÓN DE SOLUCIONES DE BIOMETRÍA DACTILAR

JORGE LIBARDO MORA SARMIENTO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

ANÁLISIS DE BUENAS PRÁCTICAS PARA LA SELECCIÓN DE SOLUCIONES DE BIOMETRÍA DACTILAR

JORGE LIBARDO MORA SARMIENTO

MONOGRAFÍA
Presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

DANNY FERNANDO LEON JARAMILLO
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

“Para lograr grandes cosas, no sólo debemos actuar, sino también soñar; no solo planear, sino también creer” ~ Anatole France

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Dedico este trabajo a mi hijo Dante Matías Mora Beltrán y a mi esposa Carolina Beltrán, quienes siempre estuvieron a mi lado, brindándome su apoyo incondicional para sacar adelante este proyecto de vida, también a mis padres, quienes me infundieron sus valores y ganas de salir adelante para cumplir mis metas, y a dios por concederme tantas oportunidades como esta, en mi vida personal y profesional.

AGRADECIMIENTOS

Quiero agradecer a la Universidad Nacional Abierta y a Distancia, por brindar estas oportunidades de desarrollo profesional en nosotros como estudiantes, con el fin de que salgamos adelante, por todo el apoyo brindado por los tutores durante este tiempo de estudio, en los que obtuvimos un gran aprendizaje en las diferentes áreas, a mi esposa, mi hijo, familia y amigos, quienes estuvieron apoyándome de manera incondicional, para sacar adelante este proyecto.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

GLOSARIO

ACCESIBILIDAD: Es definida para la tecnología en general porque amplia, equitativa y amistosamente la entrada, recolección o recepción de datos diversos para interactuar o investigar, para trabajar etc. [1]

ALFANUMERICO: Tipo de teclado del PC que integra el teclado alfabético normal y el numérico además de las teclas de función y las especialidades.

ALGORITMO: Rutina secuencial o procedimiento acumulativo de pasos lineales para la resolución de una operación o problema.

ALMACENAMIENTO: Dispositivos y Software dedicados al archivo y guardado de datos e información.

ARCHIVO: Documento de texto, sonido o imagen en forma digital.

BACKUP: Del inglés, copia de seguridad que se realiza de las aplicaciones o archivos de un soporte magnético para prevenir la posible pérdida de información.

BASES DE DATOS: Programa o aplicación que permite la gestión de datos y el manejo de información. La mayoría permite hacer listados, consultas y acceso rápido.

BINARIO: Sistema de numeración de bases de datos donde se utilizan solamente dos símbolos para escribir cualquier número 0 y 1.

BIOMETRÍA: Es el estudio para el reconocimiento inequívoco de personas basado en uno o más rasgos conductuales o físicos intrínsecos.

CIBERSEGURIDAD: Es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, a través de las redes de computadoras.

CODIFICACION: Asignación de un código a un mensaje.

CONECTIVIDAD: Se Manifiesta en la tecnología de redes y establece la posibilidad de comunicación infinita en internet o intranets en organizaciones.

[1] ELIBRO. Diccionario practico de Tecnología Educativa [Sitio WEB]. Buenos Aires. Argentina. La entidad. [Consultado 16, Noviembre, 2022]. Pg. 15,24,25,45,57,58,61,85,104 Disponible en: https:// https://elibro-net.bibliotecavirtual.unad.edu.co/

DATOS: Elemento básico de la información, pueden ser procesados o generados por una computadora a fin de convertirse en información.[2]

DIGITALIZAR: Procesos de transformación de un texto, una imagen fija o de un video, un sonido, etc., de formato analógico a un conjunto digital o de bits, a fin de permitir el procesamiento de sus datos en un entorno informático.

DIGITALIZACIÓN: Caracteriza al proceso que compromete al conjunto del sistema tecnológico de las comunicaciones electrónicas telemáticas actuales donde es necesario transformar las señales analógicas para un tratamiento digital.

ENCRIPTACIÓN: Se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

FIREWALL: Método para dar a los usuarios acceso a internet mientras se mantiene la seguridad interna en la red, impidiendo la entrada a sitios no seguros y/o virus.

GESTORES DE BASES DE DATOS: Programas que organizan y gestionan grandes volúmenes de información de acuerdo con una determinada estructura prefija.

HACKER: En informática es el pirata informático, persona que penetra en las redes e intenta tener acceso a zonas vedadas, información secreta o contenidos reservados.

HARDWARE: En informática se trata del equipo informático, ya sean ordenadores, servidores, plataformas tecnológicas, periféricos complementarios al software o programas.

INFORMACIÓN: Se trata de datos procesados pero que aún no constituyen conocimiento.

INFORMATICA: Es el procesamiento automático y veloz de la información hoy ejecutado a través del lenguaje digital de 0 y 1, y antes, históricamente a través de diversos soportes, como el ábaco chino y otros dispositivos matemáticos y lógicos.

INTELIGENCIA ARTIFICIAL: Se entienden en general, los intentos de construcción de sistemas no naturales que presentan realizaciones efectivas, tales que, si se observaran en los seres humanos, se calificarían de inteligentes.

---

[2] ELIBRO. Diccionario practico de Tecnología Educativa [Sitio WEB]. Buenos Aires. Argentina. La entidad. [Consultado 16, Noviembre, 2022]. Pg. 134,145,208,219,224,238,239,248 Disponible en: https:// https://elibro-net.bibliotecavirtual.unad.edu.co/

INTERNET: Red telemática mundial, conjunto de ordenadores o servidores conectados en una red de redes mundial.[3]

NORMAS DE CALIDAD: Se apoyan en definiciones y parámetros para el logro de procesos y productos de calidad, reuniendo la máxima demostración de los criterios de eficacia eficiencia y pertinencia, relevancia y efectividad acordados contextuada mente desglosables según situaciones y que varían a lo largo del tiempo.

PROTOCOLO: En informática apunta a la interacción entre dos elementos de un programa de aplicación y materiales que garantizan una comunicación confiable y sin error.

REDES: Espacios sociales de asociación, circulación de recursos, información y conocimiento social.

SOFTWARE: Conjunto de programas informáticos y telemáticos instalados en servidores y computadoras que les permiten operar, ya que son el conjunto de instrucciones programadas o componentes no físicos del equipamiento informático.

SQL: Se trata de un lenguaje estructurado estándar de acceso y consulta a bases de datos en una red cliente servidor.

TECNOLOGÍA: Posee varias acepciones desde el conjunto de conocimientos, herramientas, maquinarias, información habilidades, procedimientos técnicos, y materiales empleados para transformar procesos y completar tareas en una organización.

TRANSFERENCIA: Consiste en replicar los conocimientos y el tipo de análisis de los resultados de la evaluación en otros contextos para ver que tienen en común y los aspectos específicos.

VIRTUAL: Entorno o espacio telemático generado por nodos sintéticos conectados a tiempo real y escala global.

VIRUS: Tipo de programa informático destructivo y que intenta interferir en la normal operación de una PC, como también reescribir y borrar información del disco físico o de los discos accesorios y en algunos casos causa daño físico al PC.

[3] ELIBRO. Diccionario practico de Tecnología Educativa [Sitio WEB]. Buenos Aires. Argentina. La entidad. [Consultado 16, Noviembre, 2022]. Pg. 258, 320,360,371,408,409,415,443,459,460 Disponible en: https:// https://elibro-net.bibliotecavirtual.unad.edu.co/

RESUMEN

El avance de la tecnología hoy en día sorprende a cada momento, con el desarrollo de múltiples herramientas y aplicaciones que se implementan, que se van perfeccionando para hacer mucho más sencilla la vida cotidiana, actualmente existe gran variedad de alternativas para la validación de la información de una persona, como con su número de cedula, con su firma, mediante usuarios y contraseñas, entre otras.

Debido a esta tendencia, una persona puede tener la funcionalidad de manejar desde su celular, hasta sus cuentas bancarias, también se ha convertido de un objetivo por parte de los ciberdelincuentes, y este es un punto crítico por el cual se debe focalizar, para brindar un óptimo desempeño de las tecnologías y que cada día sean mucho más seguras.

Una de las opciones más utilizadas hoy en día para la verificación de identidad es el reconocimiento biométrico o reconocimiento de huellas dactilares, el cual es muy utilizado en sistemas de control de acceso peatonal, entidades bancarias, entidades gubernamentales, fuerzas militares entre otras.

Esta alternativa es una muy buena opción para todo tipo de empresas, ya que permite el acceso a toda la información de una persona solo con colocar su huella sobre un lector, y con esto poder realizar múltiples tramites en el día a día.

Si bien es una alternativa muy utilizada existen muchos tipos de dispositivos y múltiples proveedores de hardware y software, y dependiendo de las características de cada uno, lo va a hacer mucho más seguro o al contrario más inseguro, y precisamente en este proyecto se realizará una validación de requerimientos y especificaciones que se estudiaran, ayudando a establecer una buena seguridad de la información, mediante el uso de esta tecnología biométrica.

ABSTRACT

The advancement of technology nowadays surprises at every moment, with the development of multiple tools and applications that are implemented and that are being perfected to make daily life much easier, currently there is a wide variety of alternatives for the validation of information. of a person such as with their identity card number, with their signature, through usernames and passwords, among others.

But due to this trend that each person can have the functionality of managing from their cell phone to their bank accounts, it has also become a objective by cybercriminals, and this is a critical point on which to focus to provide optimal performance of technologies and that every day they are much more secure.

One of the most widely used options today for identity verification is biometric recognition or fingerprint recognition, which is widely used in pedestrian access control systems, banks, government entities, military forces, among others.

This alternative is a very good option for all types of companies, since it allows access to all the information of a person just by placing their fingerprint on a reader, and with this, they can carry out multiple procedures on a day-to-day basis.

Although it is a widely used alternative, there are many types of devices and there are multiple providers of this hardware and software, and depending on the characteristics of each one, it will make it much more secure or, on the contrary, much more insecure, and precisely in this project will carry out a validation of requirements and specifications that we will study, helping to establish good information security through the use of this biometric technology.

INTRODUCCIÓN

Cada ser humano en la actualidad cuenta con mucha información personal e intransferible, por lo que hoy en día es de vital importancia el contar con las herramientas adecuadas en la protección de la información, en este caso, la información que se maneja con equipos de reconocimiento biométrico, que prácticamente la mayoría de individuos, hoy en día tiene una interacción y mucho más aun, a la información que se maneja de cada persona, como su capital personal (dinero) el cual es muy importante se pueda proteger.

Es así por lo que un sistema de reconocimiento biométrico (lector de huella digital) debe contar con la tecnología y seguridad que pueda brindar esta protección a sus usuarios para cuidar sus intereses. Por lo que uno de los sistemas más utilizados en la actualidad es la utilización de equipos de reconocimiento biométrico o reconocimiento de huella (ya que existen algunos como reconocimiento de iris, venas entre otros), los cuales brindan un medio para el reconocimiento de los usuarios que tienen en sus sistemas, los cuales hacen un uso a diario para realizar movimientos de su información.

En este caso la información que se maneja es muy delicada, por lo que se requiere contar con equipos que garanticen la identificación de las personas y con lo que se pueda evitar ser suplantados por los delincuentes, teniendo en cuenta esto, se podrá dar a conocer que recomendaciones y tecnología será la más adecuada para la validación de los usuarios y que garantice su tranquilidad a la hora de tener sus datos en un sistema y que este a su vez cumpla con la normatividad vigente.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La inseguridad es un problema que ha venido creciendo a través de los años, y hoy en día es algo que lastimosamente forma parte del entorno, con el paso del tiempo se han desarrollado varias alternativas para la protección de la información, por lo que se vienen implementando nuevas tecnologías para mitigar este tipo de debilidades en sus sistemas, precisamente para evitar que sean vulnerables a cualquier forma de fraude.

El 2022 fue otro año de cambio sísmico en la verificación de identidad digital. Los ataques cibernéticos continuaron evolucionando dramáticamente. La demanda de los consumidores de una mayor protección en línea contra la usurpación de datos personales y otros delitos cibernéticos aumentó exponencialmente, y las organizaciones del sector público y privado de todo el mundo aceleraron significativamente los programas de verificación de datos de individuos, destinados a aumentar la confianza en tiempo real y permitir que los consumidores demuestren que son quienes dicen ser de forma segura, pero con facilidad[4].

Por lo que se buscó con la implementación de tecnologías de reconocimiento biométrico (lectura de huellas digitales), tener una protección de la información mejorada y que sea más segura tanto para los usuarios como para las empresas que implementan estos sistemas, pero sin embargo estos problemas de vulnerabilidades se siguen presentando en algunos proyectos donde se implementa esta tecnología.

[4] TECHNOCIO. iProov presenta sus 10 predicciones para la identidad digital y la biometría. [Sitio WEB]. Bogota. Colombia. Portal de Noticias. [Consultado 13, Marzo, 2023]. Disponible en: https://technocio.com/iproov-presenta-sus-10-predicciones-para-la-identidad-digital-y-la-biometria/

1.2 FORMULACIÓN DEL PROBLEMA

¿Como analizar los tipos de vulnerabilidades de los equipos de reconocimiento de huellas digitales en un sistema de acceso?

Uno de los principales problemas de esta clase de sistemas, consiste básicamente en el tipo de tecnología y cifrado de los datos, que utiliza para realizar la verificación de la información, en este caso la validación de las huellas de los usuarios, este es un factor muy importante a la hora de evitar tener ciberataques a estos sistemas por no contar con los equipos que se encuentren correctamente certificados y validados para el proceso.

Las principales falencias de este sistema consisten en que la tecnología no solo tenga que detectar que la huella coincida o no a cierta persona, sino que a su vez realice una validación, que la huella que se está presentando realmente corresponda a un usuario y no se trate de una manipulación con fines criminales.

Existen muchos casos en los cuales se utilizan diferentes estrategias criminales con el fin de “engañar” a el equipo, con la utilización de duplicaciones de huellas de silicona o calcadas, con los que un sistema que no cuente con las especificaciones adecuadas para detectar que se trata de una usurpación de la identidad podría otorgar el acceso de manera errónea y entregar información confidencial a quien no corresponde.[5]

[5] BUGUROO. Biometría el comportamiento para garantizar confianza y seguridad. Luisa Esguerra. [Sitio WEB]. Madrid. España. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.buguroo.com/es/blog/biometria-del-comportamiento-para-garantizar-confianza-y-seguridad

2 JUSTIFICACIÓN

Mediante este proyecto se busca analizar buenas prácticas, que se podrán utilizar para la selección de soluciones de sistemas de Biometría (lectura de huellas) o validación de huellas digitales para su sistema, buscando minimizar los riesgos de fraudes que se realizan por estos medios tecnológicos y que tanto han afectado a muchas empresas en los últimos años.

Con el desarrollo de este trabajo, se compartirá la información sobre los tipos de equipos sobre reconocimiento de huellas digitales, que en muchos casos se puede contar con él, pero que no cumple con las especificaciones de ciberseguridad recomendadas, y que no cumple con la normatividad que debería tener, para evitar ataques informáticos o suplantaciones, ya que el contar con el hardware y software necesario, y conocer los datos adecuados, se puedan tomar decisiones objetivas.

Actualmente existen diferentes tecnologías que se utilizan para la validación de la información, como algoritmos de reconocimiento de huellas y cifrado de datos de la información, sobre los datos según los ID asociados por usuario, complementarios a este sistema de reconocimiento de huellas digitales, y la idea es contar con la información adecuada de uso para prevenir cualquier tipo de suplantación u perdida de información.

Según Marcelo Felman, director de Ciberseguridad para Latinoamérica en Microsoft, explicó que implementar un modelo de Confianza Cero ayudará a proteger a las compañías contra el 98% de los ataques, así como también el utilizar la autenticación multifactorial (MFA) en todo lugar con una guía de contraseñas fuertes, y continuar el camino hacia un ambiente sin claves digitales. El uso adicional de la biometría asegura una identificación rigurosa para las identidades de usuario.[6]

[6] PORTAFOLIO. Biometría, entre las claves para evitar los ciberataques. [Sitio WEB]. Bogota. Colombia. Portal de Noticias. [Consultado 13, Marzo, 2023]. Disponible en: https://www.portafolio.co/innovacion/biometria-una-de-las-claves-para-evitar-ciberataques-573389

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar diferentes tipos de soluciones en biometría dactilar, especificando sus técnicas y el cumplimiento de los estándares internacionales ISO/IEC y/o FBI Mobile ID FAP20-30 acogido por Colombia, con el fin de generar recomendaciones para los usuarios que vayan a implementar esta tecnología.

3.2 OBJETIVOS ESPECÍFICOS

- Recomendar algunos fabricantes de equipos especializados en la biometría (reconocimiento de huellas digitales), que cuenten con un alto nivel en precisión de reconocimiento Biométrico y con una baja probabilidad de error, además de cumplir con los estándares internacionales ISO/IEC y/o FBI Mobile ID FAP20-30, que puedan brindar mayor seguridad de la información a las compañías que estén interesadas en adquirir un sistema biométrico.

- Analizar vulnerabilidades en los controles físicos y digitales de sistemas biométricos, determinando las fallas principales o que se podrían presentar, para proponer técnicas que permitan mejorar la seguridad de la información de estos a este tipo de sistemas de biometría.

- Evaluar las técnicas que permitan explorar vulnerabilidades a estos sistemas biométricos, brindando recomendaciones y buenas prácticas, para concientizar a las personas sobre los equipos recomendados que cumplen la normatividad y brindan un servicio adecuado en este tipo de soluciones.

4 MARCO REFERENCIAL

4.1 MARCO CONCEPTUAL

La biometría ha crecido bastante en los últimos años, ya que abrió el camino a muchas aplicaciones además de las que se creó inicialmente en los años 80 por Alphonse Bertillon, el concepto de biometría parte de una aplicación con la que bastaba realizar búsquedas forenses, pero con el pasar del tiempo, ha tenido múltiples usos, las cuales hoy en día son de mucha ayuda para realizar una identificación de información o resguardarla.

Por ejemplo en sistemas de seguridad electronica, como el control de acceso y principalmente en el control de registro y validación de datos como se utiliza en muchas compañías, lo que permite poseer una manera alternativa de seguridad de los datos, en la que solo la persona con los privilegios puede acceder a ella, esta modalidad actualmente es muy utilizada en entidades financieras donde la información es de carácter confidencial (ya que se maneja dinero) por lo que las características que deben tener estos sistemas son muy avanzadas en cuanto a los niveles de seguridad y algoritmos de reconocimiento dactilar que utilizan los equipos con los que trabajan. [7]

El sector empresarial en la actualidad viene implementando exitosamente la identificación biométrica en sus oficinas para procesos de captación, validación y tramites de sus productos. A la fecha, según datos de la Registraduría Nacional del Estado Civil RNEC, algunas compañías como las entidades bancarias han realizado más de 25 millones de consultas contra la base de datos biométrica de la RNEC, desde el año 2016, y hoy en día la mayoría de las entidades financieras manejan sistemas de validación de la información mediante los sistemas de reconocimiento biométrico.[8]

La Biometría es catalogada como una ciencia y su campo de estudio no es nuevo en el mundo. Los términos de Biometría vienen del latín bios, Vida y metria, medidas. Por tanto, los datos biométricos son construidos con base en medidas y características físicas y morfológicas manuales o automatizadas.

Durante los años 80, los temas relacionados con la evolución del ser humano tenían gran trascendencia, por lo que la investigación sobre la identificación de personas,

[7] BUGUROO. Biometría el comportamiento en ciberseguridad. Juan David Castañeda. [Sitio WEB]. Madrid. España. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.buguroo.com/es/blog/biometria-del-comportamiento-en-ciberseguridad-acceso-y-sesion-protegidos-en-tiempo-real

[8] EL BOLETIN. Reconocimiento del iris y la seguridad biométrica: ¿El sistema perfecto? [Sitio WEB]. Madrid. España. Portal Tecnológico. [Consultado 06, Mayo, 2021]. Disponible en: https://www.elboletin.com/reconocimiento-del-iris-y-la-seguridad-biometrica-el-sistema-perfecto/

enfocada en la biometría forense, avanzó notoriamente en la intención de identificar seres humanos a partir de la medición del cráneo y demás partes del cuerpo.
Una definición concisa de biometría es “el reconocimiento automático de una persona usando rasgos distintivos”[9]. Una definición más amplia de biometría es “cualquier característica física o rasgo personal automáticamente medible, robusto y distintivo que pueda usarse para identificar a un individuo o verificar la identidad reclamada de un individuo”[10].

Esta definición requiere elaboración. Mensurable significa que la característica o rasgo se puede presentar fácilmente a un sensor, localizarlo y convertirlo en un formato digital cuantificable. Esta capacidad de medición permite que se produzca la coincidencia en cuestión de segundos y lo convierte en un proceso automatizado.

La solidez de una biometría se refiere a la medida en que la característica o rasgo está sujeto a cambios significativos a lo largo de los años. Estos cambios pueden ocurrir como resultado de la edad, lesión, enfermedad, uso ocupacional o exposición química. Una biometría altamente robusta no cambia significativamente con el tiempo, mientras que una biométrica menos fuerte cambiará. Ejemplo, el iris, que cambia muy poco en la vida de una persona, es más robusto que la voz.

El carácter distintivo es una medida de las variaciones o diferencias en el dato dactilar entre la población corriente. Cuanto mayor sea el grado de distinción, más individual es el identificador. Un bajo grado de distinción indica un patrón biométrico que se encuentra con frecuencia en la población general. El iris y la retina tienen grados más altos de distinción que la geometría de la mano o el dedo. [11]

4.2 MARCO HISTÓRICO

La biometría, su nombre se deriva del griego bios-Vida y Metron-Medida, la cual se traduce como la toma de medidas con determinado estándar para un ser vivo o para un proceso biológico. También se le llama Biometría al estudio inequívoco de personas basado en uno o más rasgos físicos de un ser humano. La biometría no se puso en práctica sino hasta finales de siglo XIX en occidente, aunque en China era utilizada desde el siglo XIV, según escritos de Joao Barros[12], los comerciantes

[8] [9]UNIVERSIDAD AUTONOMA DE MADRID. Reconocimiento Facial Basado en Puntos Característicos de la Cara en entornos no controlados [Proyecto Fin de Carrera]. Madrid. España. [Consultado 17, Noviembre, 2022 p.1]. Disponible en: http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20130206LuisBlazquezPerez.pdf

[11] EBOOK. Biometrics: A Look at Facial Recognition [Sitio WEB]. Santa Monica. California. La entidad. [Consultado 17, Noviembre, 2022]. Disponible en: https://acortar.link/uVjZIE

[12] Universidad Nacional de la Patagonia San Juan Bosco. Técnicas biométricas: análisis de las técnicas actuales y nuevas tendencias [Ensayo]. Buenos Aires. Argentina. [Consultado 17, Noviembre, 2022 p.1]. Disponible en: https://acortar.link/4ICglU

chinos estampaban las impresiones y las huellas de la palma de los niños en papel con tinta y realizaban este acto para distinguirse entre los niños jóvenes.

La biometría surge en los años 80 y su precursor fue Alphonse Bertillon, quien era jefe del departamento fotográfico de la policía de París, y desarrollo un sistema Antropométrico conocido como Bertillonage, este sistema científico era utilizado para identificar criminales y a causa de esto convirtió a la Biometría en un campo de estudio, esta técnica funcionaba midiendo en forma precisa determinadas longitudes y anchuras de la cabeza y el cuerpo, posteriormente las fuerzas de policía occidental empezaron a utilizar la huella dactilar con el mismo sistema que se había visto en China hacia cientos de años.

Durante los últimos años la biometría ha crecido significativamente, no solo con el uso de las huellas dactilares sino con la utilización de distintos métodos de identificación de medidas físicas y de comportamiento, por lo que se tenían ideas del uso del iris para reconocimiento dactilar el cual fue propuesta por Frank Burch, oftalmólogo en el año 1936, esta idea también había sido vista en películas de James Bond de la década de 1980 pero esto permanecía en ese entonces como ciencia ficción.

En el año 1985 Leonard Flom y Aran Safir retoman esta idea del reconocimiento de iris, quienes en 1989 recurrieron a John Dougman para crear el algoritmo de reconocimiento de iris, estos algoritmos fueron patentados por Dougman y son propiedad de Iridian Technologies, los cuales son la base para todos los productos que tienen reconocimiento de iris. [13]

En el año de 1993 la Agencia Nuclear de Defensa empezó a trabajar con IrisCan (Compañía especializada en OCR o reconocimiento óptico de caracteres) para desarrollar un prototipo, 18 meses después se lanzó comercialmente el primer prototipo. Una medida biométrica mide su rendimiento en términos de falso positivo (False Acceptance Rate-FAR), Falso negativo (False NonMatch Rate-FNMR) y tasa de fallo de aislamiento (Failure-to-enroll Rate-FER). En sistemas biométricos reales FAR y FRR, puede transformarse en los demás con el cambio de un solo parámetro en el cual es la taza (valor N) que acepta o rechaza los errores (Equal Error Rate-EER), si más bajo es el EER se considera que el sistema es más exacto.[14]

Durante la Asamblea General de 2002, el delegado H. Morgan Griffith patrocinó una legislación que establecería parámetros legales para el uso de la tecnología de reconocimiento facial en el sector público de Virginia. La legislación, conocida como

[13] EBSCOHOST. Biometría dactilar: una nueva alternativa de controlar efectivamente la asistencia a clases [Sitio WEB]. Buenos Aires. Argentina. La compañía. [Consultado 17, Noviembre, 2022]. Disponible en: https://doaj.org/article/95890ca6c223405aaa367616dfec4444

[14] ELIBRO. Diccionario practico de Tecnología Educativa [Sitio WEB]. Buenos Aires. Argentina. La entidad. [Consultado 16, Noviembre, 2022]. Pg. 134,145,208,219,224,238,239,248 Disponible en: https:// https://elibro-net.bibliotecavirtual.unad.edu.co/

Proyecto de Ley de la Cámara de Representantes No. 454 (incluido como Apéndice), fue aprobada por la Cámara de delegados con una votación de 74 a 25 a principios del año 2002, y se trasladó al Comité de Tribunales de Justicia del Senado mientras la Comisión de Delitos del Estado de Virginia lo examinaba. La Comisión del Crimen del Estado de Virginia, una comisión legislativa permanente de la Asamblea General de Virginia tiene el mandato estatutario de hacer recomendaciones en todas las áreas de seguridad pública en la Mancomunidad de Virginia.[15]

4.3 ANTECEDENTES O ESTADO ACTUAL

La Registraduría Nacional del Estado Civil (RNEC) Cuenta con el sistema Henry Canadiense, que permite la clasificación de fichas Deca-dactilares a través de una formula alfanumérica. En 1952 la RNEC expide la primera generación de cedulas de personas donde se integraban estos datos dactilares, comprendido en el periodo de 1953 a 1993, por lo que con el continuo avance tecnológico se implementa el Automatic Fingerprint Identificación System o Sistema Automático de Identificación Dactilar (AFIS), este permite procesar las fichas dactilares y los rastros para interpretarlos en fórmulas matemáticas (no usa imágenes).

El AFIS permite realizar el enrolamiento, comparación y validación de todo tipo de búsqueda del modo ficha-ficha, ficha-rostro, rastro-ficha, además la RNEC cuenta con distintas bases de datos con las cuales realiza la validación como SIRC (Registro Civil) o ANI (Archivo Nacional de Identificación).

La RNEC a través de la Resolución 5633 de 2016 (Por la cual se reglamentan las condiciones y el procedimiento para el acceso a las bases de datos de la información que produce y administra la Registraduría Nacional del Estado Civil) y sus anexos técnicos, controla el acceso a la base de datos biométricos y biográficos más completa, confiable y actualizada del país, la cual cuenta con más de 500 millones de huellas dactilares, de aproximadamente 50 millones de colombianos, y se encuentra blindada por altos estándares de seguridad que brindan garantías de integridad, confidencialidad y disponibilidad de la información, así como por requisitos que aseguran el cumplimiento de las normas de protección de datos personales y hábeas data. [16]

Actualmente también se utiliza en sistemas de video que se envían a través de una red a una instalación de control central (por ejemplo, "Sala de control"). En esa instalación central, las computadoras encuentran rostros en el video y luego intentan

[15] OAS.ORG. CIDH Capítulo IV.A. Desarrollo de los Derechos Humanos en la Región. [Sitio WEB]. Virginia. USA. La compañía. [Consultado 17, Noviembre, 2022]. p574 Disponible en: https://www.oas.org/es/cidh/docs/anual/2020/capitulos/IA2020cap.4A-es.pdf

[16] CERTICAMARA. El futuro de la biometría en el sector colombiano. [Sitio WEB]. Bogota D.C. La Entidad. [Consultado 06, Mayo, 2021]. Disponible en: https://web.certicamara.com/files/futurodelabiometriasectorfinanciero.html

encontrar una coincidencia en una base de datos de individuos objetivo. Si encuentra una coincidencia probable, el sistema alerta a un oficial; le presenta la imagen de la coincidencia sospechosa, así como la imagen del individuo en la base de datos.

Este paso de verificación utiliza oficiales capacitados para garantizar que las falsas alarmas generadas por el sistema sean detectadas y registradas. Si el oficial decide que la coincidencia no es una falsa alarma, envía la alerta a los oficiales de patrulla, que se encuentran en las cercanías de donde la cámara original filmó al sospechoso.

4.4 MARCO CIENTÍFICO O TECNOLÓGICO

El incremento del uso de la biometría responde a los procesos de transformación digital del sector que, a su vez, suponen retos tecnológicos y jurídicos desde el punto de vista de la privacidad y la seguridad digital.

Uno de los principales beneficios en avance tecnológico con la biometría es que no es necesario el uso de una tarjeta o llave para lograr tener acceso ya sea a un lugar o a consultar una información ya que con un dedo usted podrá tener un acceso de manera segura, como se realiza con las grandes entidades del estado como el sector salud, militar, servicios sociales, entre otros, los cuales actualmente se están beneficiando con el uso de este tipo de verificaciones.

Relacionada con otros tipos de restricción para accesos, la Biometría es una de las mejores alternativas por sus altos niveles de autenticación y menos franqueables de la actualidad, además de los inconvenientes de utilizar otros métodos como un password o una contraseña que a veces son difíciles de recordar, los cuales son cada día superados por este tipo de tecnología Biométrica. [17]

La biometría se utiliza para el reconocimiento humano que consiste en identificación y verificación, los términos difieren significativamente con la identificación, el sistema biométrico pregunta e intenta responder la pregunta: "¿Quién es X?" En una aplicación de identificación, el dispositivo biométrico lee una muestra y compara esa muestra con cada registro o plantilla en la base de datos.

Este tipo de comparación se denomina búsqueda uno a muchos (1:N). Dependiendo de cómo esté diseñado el sistema, puede hacer una coincidencia mejorada, o puede anotar posibles coincidencias, clasificándolas en orden de probabilidad. Las aplicaciones de identificación son comunes cuando el objetivo es identificar a

[17] TALES. Los datos biométricos y el Reglamento general de protección de datos. [Sitio WEB]. América Latina. La compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.thalesgroup.com/es/countries/americas/latin-america/dis/gobierno/biometria/datos-biometricos.

criminales, terroristas u otros posibles delincuentes, particularmente a través de la vigilancia. La verificación ocurre cuando el sistema biométrico pregunta e intenta responder la pregunta: "¿Es esto X?" después de que el usuario afirme ser X. En una aplicación de verificación, el sistema biométrico requiere información del usuario, momento en el cual el usuario afirma su identidad a través de una contraseña, token o nombre de usuario (o cualquier combinación de los tres). Esta entrada de usuario dirige el sistema a una plantilla en la base de datos.[18]

El sistema también requiere una muestra biométrica del usuario. Luego compara la muestra con o contra la plantilla definida por el usuario. Esto se denomina búsqueda “uno a uno” (1:1). El sistema encontrará o no encontrará una coincidencia entre los dos. La verificación se usa comúnmente para el acceso físico o informático.

La arquitectura general para los sistemas de biometría está compuesta por varios componentes, dentro de los cuales encontramos los equipos, los cuales son los encargados de tomar el registro de las huellas de los usuarios y transmitir esta información, pueden funcionar como esclavos de un controlador inteligente, o pueden funcionar de manera independiente sin la necesidad de un controlador maestro.

De esta manera la distribución de los datos se realiza por medio de una red de datos, donde vamos a poder tener la comunicación de los múltiples equipos de biometría del sistema, para realizar la administración desde un software de gestión que permitirá tener control total del sistema y realizar operaciones como para el enrolamiento de nuevos usuarios, dar de baja usuarios, descargar informes, entre otros.

Esta administración de software en la mayoría de sistemas, se hace por medio de una base de datos, que integra el software de gestión como SQL u ORACLE alojada en un servidor de respaldo del sistema (Figura 14).

4.5 MARCO LEGAL

Según la ley 1581 de 2012 para la recolección de datos biométricos es necesario contar con la autorización escrita de la persona y no puede restringirse una actividad al suministro de tales datos y del decreto 1377 de 2013, para la recolección de datos biométricos es necesario contar con la autorización escrita de la persona y no puede restringirse una actividad al suministro de tales datos (artículo 6 del decreto 1377 de 2013). (SIC, 2018)

[18] EBOOK. Biometrics: A Look at Facial Recognition [Sitio WEB]. Santa Monica. California. La entidad. [Consultado 17, Noviembre, 2022]. Disponible en: https://eds-s-ebscohost-com.bibliotecavirtual.unad.edu.co/eds/detail/detail?vid=11&sid=67baac92-ba6e-4d9f-99d6-

El Reglamento Internacional 2012/0011 fue adoptado oficialmente el 27 de abril de 2016, y las disposiciones del Reglamento que rigen desde el 25 de mayo de 2018, La ley de privacidad de datos de la UE define los datos biométricos como "categorías especiales de datos personales" y prohíbe su "procesamiento", lo que protege a las personas de que su información se comparta con terceros sin su consentimiento.

Los datos biométricos son "datos personales que resultan de un procesamiento técnico específico relacionado con las características físicas, fisiológicas o de comportamiento de una persona física, que permite o confirma la identificación única de esa persona física, como imágenes faciales o datos dactiloscópicos".[19]

Que el artículo 18 del Decreto-ley 0019 de 2012 determinó que en los trámites y actuaciones que se cumplan ante las entidades públicas y los particulares que ejerzan funciones administrativas en los que se exija la obtención de la huella dactilar como medio de identificación inmediato de la persona, esta se hará por medios electrónicos y que las referidas entidades y particulares contarán con los medios tecnológicos de interoperabilidad necesarios para cotejar la identidad del titular de la huella con la base de datos de la Registraduría Nacional del Estado Civil; Que conforme a lo anterior, la imposición de la huella dactilar será remplazada por su captura mediante la utilización de medios electrónicos;

Aunque Actualmente no existe una figura dentro de la legislación colombiana sobre un reglamento general de protección de datos como el RGPD de Naciones Unidas, el cual hoy en día es acogido por muchos países en el mundo y se esperaría que a futuro la legislación Colombiana también se acoja a él, no obstante, a esto, la organización que maneje este sistema de información debe establecer un responsable para dar una respuesta a los reclamos y consultas presentadas por los titulares, la guía de responsabilidad de la SIC establece la figura del oficial de protección de datos así como las obligaciones que tienen en el marco del principio de Accountability (Guía para la implementación del Principio de Responsabilidad Demostrada).

Actualmente fabricantes como Suprema INC manejan dentro de su plataforma de BioStar 2 las certificaciones ISO 27001 e ISO 27701, normas de seguridad y de privacidad de la información reconocidas internacionalmente. ISO 27001 garantiza que se implementen las medidas adecuadas para la protección de datos y la gestión de la información. ISO 27701, instituida en agosto del año pasado, se otorga a los sistemas que cumplen con el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) y con otras legislaciones similares, como la Ley de Privacidad del Consumidor de California (CCPA, por sus siglas en inglés). Ambas

[19] PRESIDENCIA DE COLOMBIA. Cundinamarca, Bogota D.C. CONGRESO DE LA REPUBLICA. FUNCION PUBLICA. Decreto 1100 (15, Mayo, 2015). Decreto reglamentario 0188 de 2013. [Consultado 06, Mayo, 2021]. 1p - 3p Disponible en: https://acortar.link/WgGFK6

certificaciones son publicadas y gestionadas por la Organización Internacional de Normalización (ISO).[20]

Por otra parte, el fabricante HID Corporación, firma fabricante de control de accesos, HID Global informó que su sensor multiespectral Lumidgm V421-NC-01 recibió la certificación de la Registraduría Nacional del Estado Civil de Colombia por cumplir los requisitos técnicos de seguridad de la nueva versión del anexo técnico de la reglamentación de este país. Con esto, V421-NC 01 se convierte en el único producto en su tipo en cumplir con los nuevos estándares colombianos para procesos de validación de huellas dactilares, según la compañía.

La versión 2 del anexo técnico 2 de la Registraduría Nacional del Estado Civil busca garantizar la protección de la identidad de los ciudadanos colombianos cuando estos realicen operaciones con entidades, públicas o privadas, donde se requiera validar huellas contra la base de datos del registro gubernamental.[21]

[20] SUPREMA. Blog de Noticias y Artículos. [Sitio WEB]. Corea. La compañía. [Consultado 05, Diciembre, 2022]. Disponible en: https://www.supremainc.com/es/about/news-detail.asp?iBOARD_CONT_NO=3551

[21] REVISTA MAS SEGURIDAD. Sensor HID con Normativa de seguridad en Colombia. [Sitio WEB]. México. La compañía. [Consultado 05, Diciembre, 2022]. Disponible en: https://www.revistamasseguridad.com.mx/sensor-biometrico-hid-primero-cumplir-nueva-normativa-seguridad-colombiana/

5 DESARROLLO DE LOS OBJETIVOS

5.1 DESARROLLO DE OBJETIVO 1

Recomendar algunos fabricantes de equipos especializados en la biometría (reconocimiento de huellas digitales), que cuenten con un alto nivel en precisión de reconocimiento Biométrico y con una baja probabilidad de error, además de cumplir con los estándares internacionales ISO/IEC y/o FBI Mobile ID FAP20-30, que puedan brindar mayor seguridad de la información a las compañías que estén interesadas en adquirir un sistema biométrico.
Fabricantes Recomendados:

Suprema, fabricante de sistemas de control de acceso, biometría y soluciones para gestión de tiempo y asistencia, fue elegida como una de las “50 principales empresas de seguridad global de 2022” por la revista A&S, una publicación de medios de seguridad global; Suprema ha establecido un récord al ganar el premio durante 12 años consecutivos, sumado a que fue catalogado como uno de los cinco principales proveedores de sistemas de control de acceso del mundo este año (2022) [22].

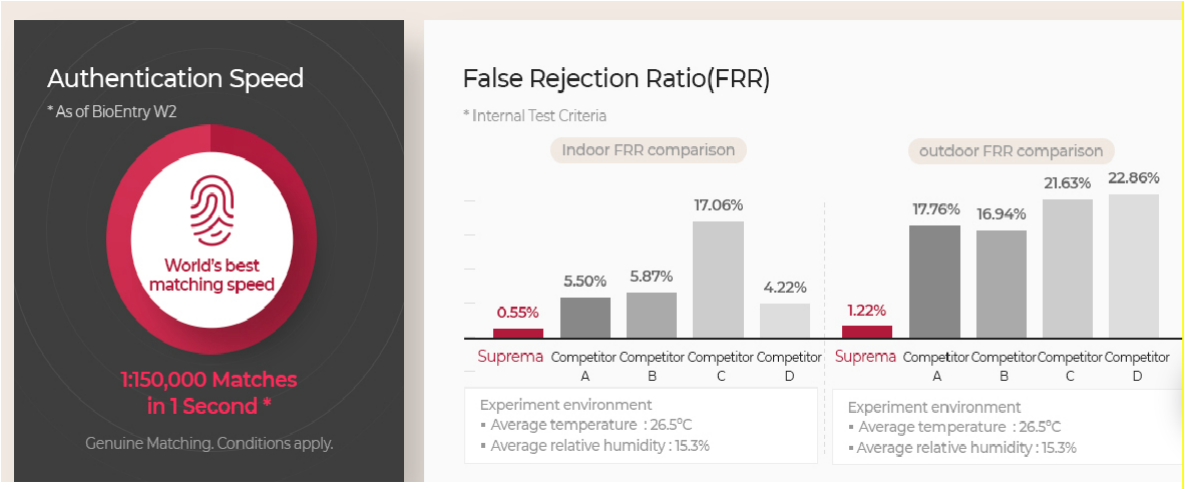
5.1.1 SUPREMA

En la Actualidad la marca SUPREMA es una de las más reconocidas por sus soluciones de controles de acceso y biometría, ya que utiliza algoritmos de biometría muy reconocidos a nivel mundial, los cuales cuentan con una ingeniería especializada y en continua innovación en la industria de seguridad por muchos años.

Suprema cuenta con una amplia gama de equipos y soluciones para controlar el acceso con biometría, sistemas de tiempo y asistencia, huellas digitales en vivo, verificación de identidad móvil y funciones de huellas digitales integradas, actualmente Suprema fue nombrado como uno de los 50 principales fabricantes de sistemas de seguridad en el mundo, siendo una de las mejores soluciones en más de 140 países, el número 1 en biometría.

[22] TECNOSEGURO. Tras 12 años consecutivos Suprema continúa clasificando en el ‘Top 50 de las principales empresas de Seguridad Global. [Sitio WEB]. Bogota. Colombia. La compañía. [Consultado 13, Marzo, 2023]. Disponible en: https://www.tecnoseguro.com/noticias/empresas/tras-12-anos-consecutivos-suprema-continua-clasificando-top-50-principales-empresas-seguridad-global

(Figura 1 – Medición de efectividad en reconocimiento dactilar)



(Fuente Suprema) [23]

La referencia BioMini Slim 2S (Figura 2) se ha convertido en el equipo más utilizado para soluciones como las que se manejan en la actualidad, en temas de reconocimiento y validación de identidad mediante biometría, ya que su escáner óptico FAP20 cuenta con certificación PIV y es uno de los más delgados del mundo.

El equipo cuenta con una placa de 0,71 "x 1,0" (18 mm x 25,4 mm) ancho, el cual sobrepasa el estándar FAP20 de 0.6 "x 0.8", este equipo está diseñado con altos estándares de seguridad ya que cuenta con un sistema de cifrado de datos con minucias en la huellas dactilares y también soportan protocolos como HTTPS, Wi-Fi (Wireless Fidelity o Fidelidad inalámbrica) y WAP2 (Acceso Wi-Fi protegido 2), por lo que cuenta con una tecnología avanzada que permite la identificación de huellas vivas ya que cuenta con un método de análisis y clasificación de patrones de estas imágenes con sus características ópticas. [24]

El equipo cuenta con certificación ISO/IEC 19794-4 (hoja técnica anexa), el cual utiliza un formato para intercambiar de registro de datos para que almacene, registre o transmita información entre varias áreas con imágenes de dedos o palmas de una estructura de datos ISO / IEC 19785-1, además de contar con certificaciones FBI PIV, la cual, valida el acceso seguro a sus equipos, software, redes solo usando una huella digital.

(Hoja técnica BioMini slim2S, anexa).

[23] SUPREMA. Hardware – Productos Biométricos. [Sitio WEB]. Corea. La compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.supremainc.com/es/hardware/biometric-products.asp
[24] SUPREMA. LECTORES DE AUTENTIFICACIÓN. [Sitio WEB]. Corea. La compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.suprema-id.com/es/contents/detail.php?code=010108

(Figura 2 – BioMini Slim 2S)

(Fuente Suprema) [25]

5.1.1.1 EQUIPOS ADICIONALES Y TECNOLOGIAS SUPREMA

Actualmente la fabricante suprema también cuenta con soluciones adicionales a la anterior referencia mencionada, que complementan su portafolio según los diferentes requerimientos de sus clientes, dentro de las cuales, tiene soluciones para sus sistemas de controles de acceso que utilizan tecnologías de:[26]

- Validación con PIN o código de acceso.
- Lectura de proximidad (tecnologías de proximidad EM, HID Prox, Mifare, Iclass, Iclass Seos).
- Medición de temperatura.
- Lectura de códigos QR.
- Reconocimiento Facial.

Según la recomendación del fabricante es posible manejar combinaciones de diferentes tecnologías para la validación de los usuarios con el fin de aumentar los niveles de seguridad en el sistema, como, por ejemplo, el siguiente equipo tiene la capacidad de manejar varias tecnologías de validación:

[25] SUPREMA. Hardware – Productos Biométricos. [Sitio WEB]. Corea. La compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.supremainc.com/es/hardware/biometric-products.asp
[26] SUPREMA. Hardware – Productos Biométricos. [Sitio WEB]. Corea. La compañía. [Consultado 19, Noviembre, 2022]. Disponible en: https://www.supremainc.com/es/hardware/biometric-products.asp

(Figura 3 – FaceStation Suprema referencia FSF2-ODB)

(Fuente Suprema) [27]

Suprema también cuenta con diferentes soluciones alternativas al control de acceso con las que también realiza su constante desarrollo tecnológico con el fin de brindar las mejores soluciones a sus clientes como:

5.1.1.2 CONTROL DE TIEMPO Y ASISTENCIA:

La solución de administración de horario y asistencia de Suprema permite simplificar el monitoreo de la planilla de tiempos del empleado, el cálculo de las horas de trabajo y la recopilación de los datos de horario y asistencia. No es posible delegar la autenticación, porque es un sistema de administración de horario y asistencia basado en biometría, por lo que puede configurar varios tipos de horario o turnos de trabajo. Permite la administración por parte de recursos humanos y el manejo de horarios y asistencia en un sistema, ya que puede conectarse fácilmente con sistemas de RR. HH. o ERP, además de ver fácilmente informes personalizados de horario y asistencia, y una vista de calendario con rapidez.

[27] SUPREMA. Hardware – Productos Biométricos. [Sitio WEB]. Corea. La compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.supremainc.com/es/hardware/biometric-products.asp

5.1.1.3 CREDENCIALES MOVILES DE ACCESO:

Suprema Mobile Access le permite usar su propio teléfono (Smartphone) como llave para acceder a puertas, instalaciones y más. Al usar su teléfono como credencial, administrar y usar una tarjeta de acceso se hace más fácil, rápido y seguro.

Con las soluciones de seguridad exclusivas de Suprema, todo el proceso está protegido por la arquitectura de sistema certificada ISO 27001. Es menos probable que los usuarios den su teléfono a otros, por lo que evita que personas no autorizadas entren en su propiedad.[28]

5.1.1.4 SOFTWARE CON LAS ULTIMAS ACTUALIZACIONES EN SEGURIDAD:

BioStar 2 es una plataforma de seguridad basada en la Web, abierta e integrada que proporciona una funcionalidad completa para el control de acceso. Debido a su estructura modular y flexible, la plataforma proporciona un sistema personalizado según la escala, la cantidad de usuarios y la estructura del sistema que se utilizó. Proporciona un sistema personalizado con BioStar 2, que es compatible con dos tipos de estructura de sistema de control de acceso en una plataforma.

La fuga de huellas dactilares reales o de imágenes faciales registradas para la autenticación, puede suponer una grave amenaza para la seguridad. Las imágenes reales se reorganizan como plantillas binarias a través de un algoritmo de análisis avanzado, el cual nunca se puede revertir en una imagen real en vivo.

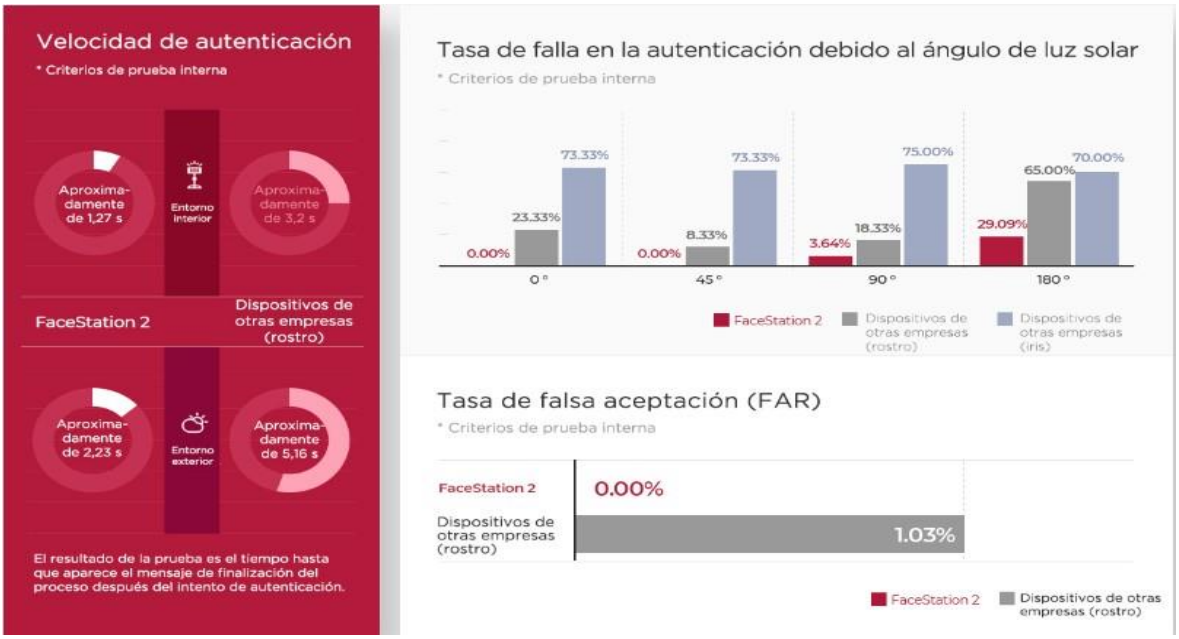
Cifra los datos personales utilizados para la autenticación, como contraseñas, plantillas de huellas y de rostros, como también todos los datos disponibles que pueden estar vinculados a una persona. Para obtener más detalles, consulte Ciberseguridad. Con certificación ISO 27001 e ISO 27701, BioStar 2 está equipado con seguridad de información y un sistema de gestión de la información de privacidad. Todos estos datos se almacenan de forma segura en el servidor, el dispositivo, o incluso tarjeta con cifrado de datos usando AES 256, AES 128, DES/3DES basado en ubicación.

Actualmente Suprema es uno de los lideres en los sistemas de reconocimiento facial ya que sus equipos están diseñados con los más altos estándares de calidad y seguridad, frente a otras marcas en el mercado ya que su Tasa de falla en la autenticación es equivalente (Figura 3) a 0.00% lo que la hace muy eficiente y segura, ya que si se observa, existen otros fabricantes que manejan unas tasas de falla de hasta un 3.64% (Figura 4).

[28] SUPREMA. PRODUCTOS-PLATAFORMA-BIOSTAR2. [Sitio WEB]. Corea. La compañía. [Consultado 19, Noviembre, 2022]. Disponible en: https://www.supremainc.com/es/platform/hybrid-security-platform-biostar-2.asp

Este equipo también maneja una tasa de falsa aceptación que es equivalente al 0.00% que es muy segura, frente a otros fabricantes que manejan tasas de aceptación hasta del 1.03% lo que es inseguro (Figura 4).

(Figura 4 – Tasa de falla y falsa aceptación FaceStation2)



(Fuente Suprema) [29]

HID Global, reconocida a nivel mundial, por entregar soluciones confiables de identificación, anunció que la serie TouchChip TC de sensores capacitivos de huellas dactilares, recibió la certificación de Nivel 1 por parte del laboratorio de pruebas independiente iBeta Quality Assurance.

Estas pruebas de conformidad, realizadas de acuerdo con la norma ISO/IEC 30107-3, concluyeron que el dispositivo biométrico de HID Global, funciona según los más altos estándares logrando un 0 % de penetración[30].

[29] SUPREMA. SOLUCIONES-APLICACIONES-CIBERSEGURIDAD. [Sitio WEB]. Corea. La compañía. [Consultado 19, Noviembre, 2022]. Disponible en: https://www.supremainc.com/es/solutions/cybersecurity.asp

[30] TECNOSEGURO. HID Global recibió certificación de Nivel 1 de detección de ataques de suplantación. [Sitio WEB]. Bogota. Colombia. La compañía. [Consultado 13, Marzo, 2023]. Disponible en: https://www.tecnoseguro.com/noticias/empresas/hid-global-certificacion-nivel-1-deteccion-ataques-suplantacion

5.1.2 HID GLOBAL

La compañía HID Global es un fabricante de sistemas de control de acceso que trabaja actualmente en muchos países en el mundo, brindando niveles de identificación muy confiables para las personas, gracias a los desarrollos tecnológicos que han tenido durante los últimos años, con el fin de que las personas trabajen de manera eficaz, con libertad y confianza.

En la actualidad cuenta con presencia en más de 100 países, donde millones de personas utilizan estos productos y servicios tanto físicos como digitales, donde cuentan con niveles de seguridad avanzados para millones de objetos que se puedan identificar, rastrear o verificar, y todo esto se realiza con la tecnología de HID Global.

HID trabaja con diferentes sectores de desarrollo en cada país, como gobierno, educación, salud, banca o sectores privados, que se encuentran en continua innovación tecnología de sus sistemas, o que los ayuda a crecer en su entorno físico y de sus colaboradores, o clientes brindándoles seguridad y explotando sus capacidades.

(Figura 5 – DigitalPersona 5300)

(Fuente HID Global) [31]

HID en este caso cuenta con un equipo que se le denomina Digital Persona 5300 (Figura 5), el cual es un equipo bastante fuerte, que cuenta con un lector óptico para una huella, y este lector cuenta con la normatividad FIPS 201/PIV y FBI Mobile ID FAP 30 (hoja técnica anexa). Su diseño es muy versátil y le permite cumplir a cabalidad con requerimientos de alto flujo, con aplicaciones de bastante demanda para registro y autentificación de identificación de usuarios a un sistema, por lo que,

[28] [31] HID GLOBAL. Una persona, una verdadera identidad, El ciudadano Biométrico [Sitio WEB]. USA. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://acortar.link/9gCv95

debido a esto, también cuenta con un vidrio con protección IP64, que es bastante resistente a cualquier posible daño químico y/o físico al equipo, en algunas ocasiones, lo utilizan en ambientes externos.[32]

5.1.2.1 Principales características

- Certificación FIPS 201/PIV
- Certificación Mobile ID FAP 30
- Imágenes con resolución de 500 dpi
- Tamaño compacto
- Rechazo de huella dactilar falsa
- Compatible con SDK Digital Persona

El equipo digital Persona 5300 (Figura 5), puede capturar y producir imágenes de huellas dactilares, las cuales cuentan con una resolución de 500 DPI, formato estándar ANSI e ISO/IEC. Sus componentes electrónicos pueden controlar automáticamente su calibración y transfiere los datos por medio de su interfaz USB, lo cual hace que sea muy fácil de integrar con cualquier equipo.

Otra de sus funcionalidades más representativas es que puede utilizar tanto cotejador, como extractor de huellas de diferentes desarrollos, los cuales deben cumplir con la normatividad, y cuenta con un motor biométrico Digital Persona Finger Jet. La combinación del Motor Finger Jet y el Digital Persona brindan una capacidad muy exacta y ágil, incluso si se manejan huellas dactilares que no sean muy fáciles de leer.[33]

Actualmente HID también cuenta con tecnologías adicionales, con las que busca brindar un mayor nivel de seguridad para sus sistemas, dentro de los cuales se encuentra, por ejemplo, el iCLASS SE® RKLB40 y cuenta con las siguientes características:

(Figura 6 – Lector HID iCLASS SE® RKLB40)

- Validación con PIN o código de acceso.
- Lectura de proximidad (tecnologías de proximidad, Mifare, Iclass, Iclass Seos).
- Reconocimiento Biométrico.

(Fuente HID Global)[34]

---

[29] [33] HID GLOBAL. Una persona, una verdadera identidad, El ciudadano Biométrico [Sitio WEB]. USA. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://acortar.link/9gCv95

Actualmente el Fabricante HID trabaja continuamente en el desarrollo de nuevas tecnologías, que aportan significativamente en la ciberseguridad de sus sistemas y equipos, es por esto que, para entornos de misión crítica, que no pueden correr el riesgo de un paso en falso de identidad, los lectores biométricos de huellas dactilares, con tecnología de imágenes multiespectrales (MSI), patentada por HID, ofrecen el más alto nivel de seguridad y precisión de coincidencia.

La capacidad de capturar huellas dactilares difíciles en entornos desafiantes, detectar vida con gran precisión y proporcionar seguridad de punto final, es lo que distingue a los lectores de huellas dactilares de MSI al ofrecer coincidencias confiables y seguras una y otra vez, especialmente para aplicaciones críticas, en implementaciones comerciales y gubernamentales.

La biometría es un método comprobado de autenticación de identidad, para garantizar que otra persona no esté usando su identidad, de manera fraudulenta. Las capacidades de la tecnología de huellas dactilares, ha seguido mejorando con el tiempo. En situaciones de alto riesgo, es vital trabajar con un lector de huellas dactilares avanzado, que pueda manejar situaciones del mundo real, que incluye:

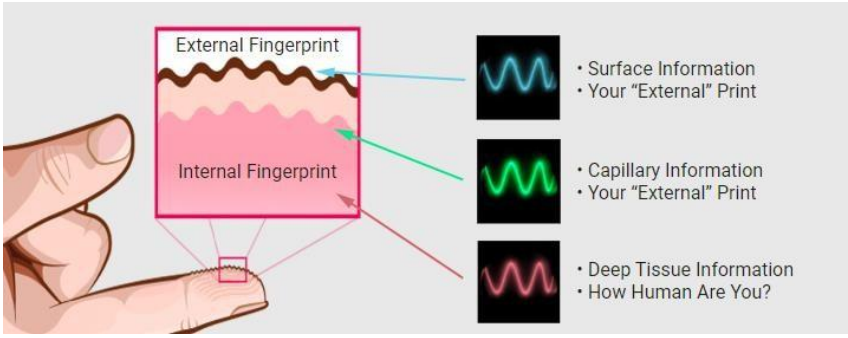
- Capacidad para capturar huellas dactilares difíciles (secas, húmedas, sucias, aceitosas, arrugadas, dañadas)
- Capacidad para desempeñarse en entornos desafiantes (luz solar directa, oscuridad, calor, frío, lluvia, nieve)
- Capacidad para detectar huellas dactilares falsas (detección de vida)
- Capacidad para hacer coincidir con alta precisión (aceptar usuarios legítimos)

La ingeniería avanzada, utilizada para desarrollar lectores de huellas dactilares de imágenes multiespectrales (MSI), dio como resultado, dispositivos probados en el campo para aplicaciones de misión crítica. Las organizaciones que requieren el mejor rendimiento de su clase, para niveles incomparables de seguridad y facilidad de uso, invierten en dispositivos de huellas dactilares basados en MSI.

Mientras que otros tipos de tecnología de huellas dactilares, capturan solo las capas más externas de la piel, la tecnología MSI, penetra dentro del dedo y recopila información interna de huellas dactilares para mejorar el rendimiento y la facilidad de uso, la singularidad de esta técnica está en la luz.[35]

[35] HID GLOBAL. Guía de la tecnología MSI [Sitio WEB]. USA. La Compañía. [Consultado 19, Noviembre, 2022]. Disponible en: https://blog.hidglobal.com/2022/10/guide-msi-technology-how-it-works

(Figura 7 – Tecnología MSI de HID)



(Fuente HID Global)[36]

Todo esto sucede, utilizando técnicas avanzadas y patentadas de proyección y captura de luz HID. La tecnología MSI (Figura 7), envía múltiples colores de luz al dedo, en diferentes ángulos para penetrar la piel y alcanzar el tejido profundo del dedo. La luz azul recopila los datos de la superficie. Las luces rojas y verdes recopilan los datos del subsuelo a diferentes profundidades.

Usando luces multicolor, en diferentes ángulos, los lectores MSI recopilan hasta 12 imágenes diferentes, que se combinan en una única imagen óptima. La ventaja de combinar varias imágenes es capturar datos de huellas dactilares de forma fiable, que funcionan en una amplia variedad de situaciones del mundo real. El sistema no está mirando solo una imagen, de una fuente de luz en un solo ángulo, sino que está mirando una combinación de información que mejora la confiabilidad, especialmente en condiciones difíciles, como impresiones secas, envejecidas o dañadas (Figura 7).

La seguridad de los endpoints o servidores, es una consideración importante al seleccionar un lector de huellas dactilares de alto rendimiento. La tecnología sofisticada que cifra los datos hacia y desde el dispositivo, utilizando algoritmos de cifrados certificados por el FBI, se incorpora a los mejores dispositivos de huellas dactilares de MSI. Si un pirata informático obtiene acceso al dispositivo de huellas dactilares, la tecnología de seguridad de los endpoints, utiliza funciones de detección de manipulaciones para borrar las claves de cifrado del dispositivo. Esto evita que los delincuentes capturen y decodifiquen datos protegidos y reduce el riesgo de ciberataques en toda la empresa.[37]

---

[31] [37] HID GLOBAL. Guía de la tecnología MSI [Sitio WEB]. USA. La Compañía. [Consultado 19, Noviembre, 2022]. Disponible en: https://blog.hidglobal.com/2022/10/guide-msi-technology-how-it-works

La compañía Futronic y otros participantes de la industria conocidos, se enumeran en la investigación, junto con otras empresas clave, con el fin de aumentar su alcance geográfico y sus operaciones comerciales en soluciones de autenticación sólidas, ahora son más importantes que nunca para los sectores comercial y residencial debido a la rápida digitalización y la necesidad constante de adoptar protocolos de identificación más sólidos para detener el fraude y el robo de identidad. Se prevé que el mercado biométrico de reconocimiento de venas crezca como resultado de este avance técnico[38].

5.1.3 FUTRONIC

Futronic es otro fabricante muy reconocido a nivel mundial por sus productos de hardware y software avanzados, en sistemas de control de acceso y biometría con los que logra tener una óptima gestión de identidad de sus usuarios, uno de los equipos que más se utilizan es el FS10 (Figura 8), el cual tiene un escáner para reconocimiento de huellas dactilares de 1” x 1”, el cual se encuentra en el mercado de huellas dactilares de un solo dedo, cuenta con la certificación del FBI con calidad de imagen PIV-071006 (hoja técnica anexa), y cumple con el estándar de procesamiento federal 201 (FIPS 201) de EE.UU. (PVI) verificación de trabajadores y contratistas federales.

Este equipo FS10 (Figura 8), cuenta con sensor CMOS avanzado y un sistema óptico de precisión para dar cumplimiento con los estándares de calidad de imagen que exige PIV-071006, la capa sobre la que se realiza el escaneo es un vidrio de corona el cual está diseñado para resistir rayones, golpes u otras malas manipulaciones con el fin de garantizar un uso continuo y duradero, a pesar de que tiene lectura de un solo dedo es ideal y muy rentable para aplicaciones como licencias de conducir, control de fronteras, documentos de identidad, elecciones u aplicaciones civiles AFIS (Sistema automatizado de identificación de huellas dactilares).

Cada equipo FS10 (Figura 8), cuenta con un número de serie único e irrepetible, el cual viene programado de fabrica en el descriptor del dispositivo USB, por lo que se puede rastrear y esto es un factor muy importante para trabajar en proyectos del sector de gobierno.

[38] GLOBENEWSWIRE. Se espera que el mercado biométrico de reconocimiento de venas progrese a una CAGR del 19,2 % para alcanzar los 5.977,0 millones de dólares estadounidenses a finales de 2032, afirma Fact.MR [Sitio WEB]. Paris. Francia. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: https://www.globenewswire.com/en/news-release/2022/11/25/2562681/0/en/Vein-Recognition-Biometrics-Market-Is-Expected-To-Progress-At-A-CAGR-Of-19-2-To-Reach-US-5-977-0-Million-By-The-End-Of-2032-States-Fact-MR.html

(Figura 8 – Futronic FS10)

(Fuente Futronic) [39]

5.1.3.1 Cumple con los siguientes estándares

- Especificación de calidad de imagen FIPS 201 / PIV 071006
- Identificación móvil FAP30
- Microsoft WHQL
- FCC y CE
- RoHS

El equipo Futronic FS10 (Figura 8), cuenta con un módulo de integración con sistemas propios de clientes, para ello el módulo que se utiliza es el FS11, este módulo les permitirá la integración de este equipo con sus sistemas propios como maquinas POS, portátiles, estaciones de registro rotativas, el módulo FS11 es similar al FS10 (Figura 8), pero sin la carcasa de plástico y el cable USB lo que permite la fácil integración con sistemas de terceros. [40]

Adicional esta compañía ofrece soluciones muy innovadoras, las cuales son soluciones alternas a las que normalmente son comunes encontrar en el mercado, ya que también maneja niveles de seguridad muy apropiados, dentro de las cuales maneja soluciones como el FS64 EBTS/F (Figura 9) con:

---

[39] FUTRONIC. Escáner de huellas dactilares FS10. [Sitio WEB]. Hong Kong. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.futronic-tech.com/pro-detail.php?pro_id=1533

[36] [40] FUTRONIC. Escáner de huellas dactilares FS10. [Sitio WEB]. Hong Kong. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.futronic-tech.com/pro-detail.php?pro_id=1533

- Escáner plano de huellas dactilares.
- Escáner de dos dedos.
- Escáner de venas del dedo.
- Lectura de proximidad.

(Figura 9 – FS64 EBTS/F y Mobile ID FAP60 Escáner plano de huellas dactilares)

(Fuente Futronic)[41]

Futronic desarrolló la tecnología Live Finger Detection (LFD) para detener el acceso a datos y ubicaciones protegidos utilizando dedos falsos hechos de silicona, goma, plastilina, etc.

5.1.3.2 Futronic tiene 3 opciones de detección de dedos en vivo (LFD)

I. **Detección tradicional de dedos en vivo (TLFD):** Esta es una tecnología (Figura 10), de detección activa para detectar dedos humanos vivos. Para que TLFD funcione correctamente, es necesario que los usuarios hagan que los dedos toquen una ubicación especial en el escáner de huellas dactilares. Las siguientes imágenes son una simple ilustración. TLFD es compatible con FS80H, FS82HC, FS88H, FS88HS, FS26, FS26E y FS26EU.

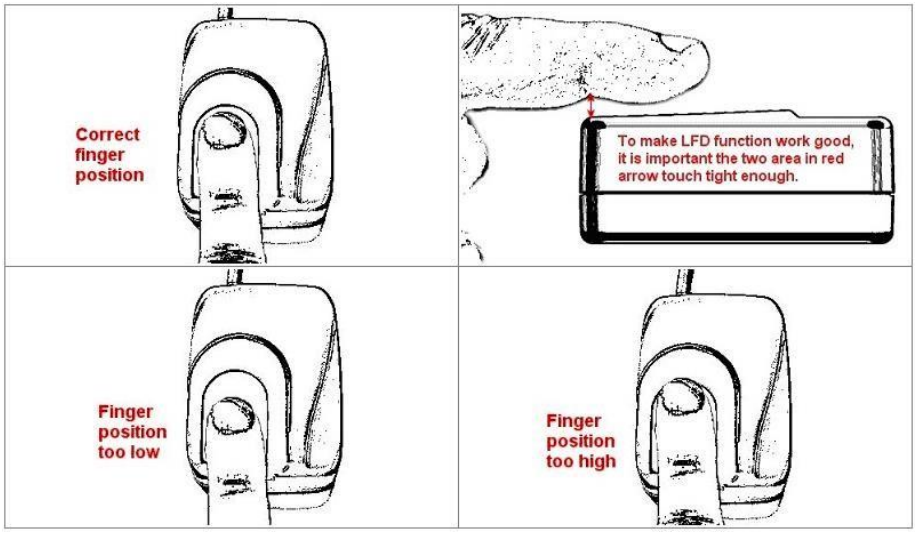
II. **Detección mejorada de dedos vivos (ELFD):** La mejora del rendimiento se logra mediante la adición de iluminación adicional en el escáner de huellas dactilares para recopilar más información. ELFD es compatible con FS88HE

[41] FUTRONIC. Escáner de huellas dactilares FS10. [Sitio WEB]. Hong Kong. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.futronic-tech.com/pro-detail.php?pro_id=1533

y FS26E. También hay 3 niveles secundarios de detección de suplantación de identidad para ELFD, Fácil, Estándar y Seguro (consulte la siguiente imagen, figura 10). Los usuarios pueden seleccionar el adecuado para usar en función de sus requisitos de comodidad y seguridad.

III. **Detección avanzada de dedos vivos (ALFD):** Esta es la última tecnología y su rendimiento es mejor que los otros dos. ALFD es compatible con FS88H, FS89H, FS88HE, FS88HS, FS26E, FS26EU, FS10, FS11, FS50, FS51, FS52, FS53 y FS64.

(Figura 10 – Tecnología LFD FUTRONIC)



(Fuente Futronic) [42]

[42] FUTRONIC. Escáner de huellas dactilares FS10. [Sitio WEB]. Hong Kong. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.futronic-tech.com/pro-detail.php?pro_id=1533

5.2 DESARROLLO DE OBJETIVO 2

Analizar vulnerabilidades en los controles físicos y digitales de estos sistemas, y proponer técnicas que permitan mejorar la seguridad de la información de estos a este tipo de sistemas de biometría.

Actualmente compañías en todo el mundo, invierten cientos de millones en tecnología Biométrica, puesto que con esta innovación permite a sus usuarios accedan de forma ágil y segura a su información, mediante características físicas aparentemente inimitables, como en este caso, lo son las huellas dactilares, evitando procesos de autentificación engorrosos como por celulares o equipos electrónicos que son más fácilmente vulnerables.

En este momento (año 2022), el porcentaje de inversión y de crecimiento de los consumidores a nivel mundial en Biometría, tiene una buena proyección durante los siguientes 4 años que continúan, de acuerdo con la implementación de esta tecnología[43], por lo que las compañías han adoptado la biometría, como principal prioridad estratégica para los próximos años, aunque con la constante de crecimiento, cada día hay nuevas tecnologías que se derivan de la biometría, como las de reconocimiento de palma, reconocimiento facial, reconocimiento de IRIS, lector de venas entre otros (Figura 11), los cuales han ido creciendo con toda la transformación tecnológica, a la que las personas son sometidas cada día, pero que indiscutiblemente, cuentan con falencias, por las cuales continuamente los desarrolladores trabajan para mitigarlas el mínimo posible. [44]

(Figura 11– Métodos de identificación similares a la Biometría)

(Fuente Suprema) [45]

[43] MOBBEEL. Rafael Campillo. Estadísticas sobre la industria de la biometría. [Sitio WEB]. Cáceres, España. Portal de Noticias. [Consultado 12, Marzo, 2023]. Disponible en: https://www.mobbeel.com/blog/estadisticas-sobre-biometria-para-2021-mercado-y-sectores/

[44] EL UNIVERSAL. Europa busca prohibir la vigilancia biométrica por violación a derechos humanos. [Sitio WEB]. México. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: https://www.eluniversal.com.mx/techbit/europa-busca-prohibir-la-vigilancia-biometrica-por-violacion-derechos-humanos

[45] BLURADIO. Biometría y algoritmos genéticos: la tecnología que implementa UNAD en los exámenes universitarios. [Sitio WEB]. Bogota D.C. Portal de Noticias. [Consultado 06, Mayo, 2021].

Sin embargo, aunque la Biometría parece una buena estrategia, tanto para compañías como para sus clientes, a quienes les prestan sus servicios, como en la mayoría de tecnología también implica un riesgo, ya que los ciberdelincuentes han empezado a explotar posibles vectores de ataques, diseñados para sacar provecho de esta tecnología [46].

La base de datos Aadhaar, una de las bases gubernamentales de datos biométricos más grandes del mundo, ha sido comprometida por un parche de software, que permite evitar algunas de las funciones de seguridad más importantes, para inscribir a nuevos miembros. Aadhaar sirve como un número identificador para los ciudadanos de la India y se vuelve un número vital para hacer trámites o recibir apoyos del gobierno. La base de datos cuenta actualmente con datos biométricos de 1.2 mil millones de habitantes [47].

El tipo de vulnerabilidades que se pueden evidenciar principalmente en estos sistemas de reconocimiento de huellas digitales se deriva en:

5.2.1 SENSOR

En el mercado hay muchos equipos, que son utilizados para este tipo de verificaciones de identidad, así como su origen, ya que actualmente estos dispositivos suelen tener procedencia oriental y existen distintos niveles de eficacia, de los materiales que se utilizan para su elaboración, que en algunas ocasiones, con la finalidad de su reducción en costos, pueden realizar la adquisición de componentes que no cuentan tanto con la calidad como los estándares y normatividad que deben cumplir para su funcionamiento de manera segura.

Aunque existe una gran variedad de dispositivos, estos no cumplen con las especificaciones para evitar la usurpación de identidad, ya que normalmente también los delincuentes utilizan otros métodos, para violar la seguridad de estos equipos, como lo son, huellas dactilares falsas hechas de diversos materiales como arcilla, caucho, silicona, pegamento, papel, película y más (Figura 12).

Disponible en: https://www.bluradio.com/tecnologia/biometria-y-algoritmos-geneticos-la-tecnologia-que-implementa-unad-en-los-examenes-universitarios

[46] OPTICAL. ¿Qué son los vectores de ataque en ciberseguridad? [Sitio WEB]. Lima. Perú. Portal de Noticias. [Consultado 12, Marzo, 2023]. Disponible en: https://www.optical.pe/blog/vectores-de-ataque-ciberseguridad/

[47] R3D. AADHAAR, LA BASE DE DATOS BIOMÉTRICOS DE LA INDIA, ES VULNERABLE A UN PARCHE DE SOFTWARE DE 35 DÓLARES.?. [Sitio WEB]. D.F. México. Portal de Noticias. [Consultado 12, Marzo, 2023]. Disponible en: https://acortar.link/VhJDKf

(Figura 12 – Métodos de los delincuentes para la usurpación de identidad en dispositivos Biométricos)

(Fuente Suprema) [48]

Existe otro factor que se debe tener en cuenta y que representa una constante significativa para su funcionamiento y es su hardware interno para el procesamiento de la información que reciba desde el sensor, actualmente existen varias tecnologías, que pueden disminuir las posibilidades de riesgo, el sensor es el que permite la digitalización de la imagen, depende del hardware que tenga, se tardaría más o menos según la tecnología que utilice, así como también su grado de exposición según las condiciones en la que se trabaje, ya que algunos equipos normalmente cuentan con vulnerabilidades al realizar su validación y estar expuestos a un lugar muy iluminado, lo que hace que su porcentaje de error se incremente (Figura 13).

(Figura 13 – Exposición dispositivo Biométrico a la luz)

(Fuente HID Global)[49]

[48] FAD. Enrolamiento a motor Biométrico. Enrolamiento Biométrico. [Sitio WEB]. México. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://acortar.link/RMwy0K
[49] HID GLOBAL. Una persona, una verdadera identidad, El ciudadano Biométrico [Sitio WEB]. USA. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://acortar.link/9gCv95

A veces no solo basta con tener la mejor tecnología, pues también se debe tener en cuenta que es una tecnología que se puede dañar según el uso, algunos equipos no están diseñados para trabajo en lugares donde se encuentren considerablemente expuestos.

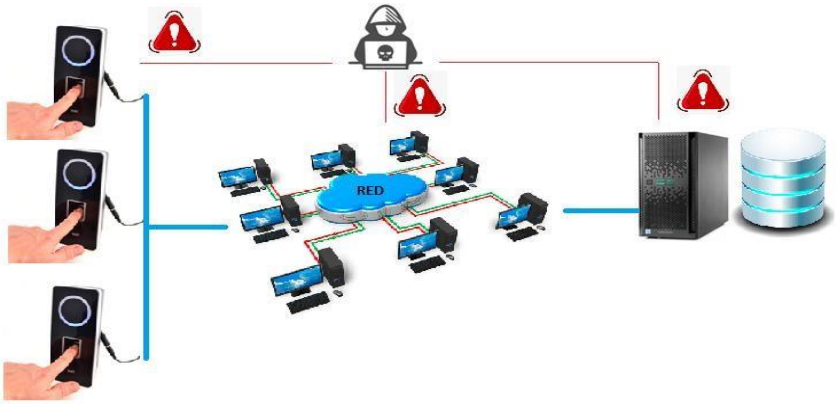
Por esto se debe contar con grados de protección IP66 (grado de protección para ambientes con polvo y agua) o IK10 (grado de protección donde se requiera que sea anti-vandalismo), por lo que esto acarrea gastos de reparaciones y mantenimiento constante de los equipos para asegurar su funcionamiento y estado de estos, lo que ayudara a identificar que riesgos serian provenientes para estos casos.

5.2.2 TRANSMISIÓN DE DATOS DEL SENSOR

Debido al uso constante de estos equipos, principalmente si se trata de aplicaciones remotas, este tipo de ataques consiste en el introducir continuamente datos biométricos suministrados anteriormente en el host remoto, que lleva a cabo el reconocimiento, hasta lograr su cometido.

Los protocolos de seguridad con que se recomienda tengan estos dispositivos, para la transmisión de la información, debe realizarse, de manera en la que no pueda ser fácilmente interceptada, ya que dependiendo el tipo de conexión que manejen los equipos, estos deben contar con cifrado de datos de la información, desde su medio físico hasta su sistema de gestión, el no tener estos protocolos de cifrado de datos resultara muy inseguro a la hora de realizar diferentes tipos de validaciones (Figura 14). [50]

(Figura 14 - Transmisión de datos del sensor)



(Fuente Propia)

[50] FAD. Enrolamiento a motor Biométrico. Enrolamiento Biométrico. [Sitio WEB]. México. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://acortar.link/RMwy0K

5.2.3 BASE DE DATOS

Un complemento para todo este tipo de sistemas es que su funcionamiento no es autónomo, (aunque en algunos casos los equipos pueden trabajar de manera autónoma en determinado momento), siempre necesitan complementarse con un sistema o software de administración para realizar todas las tareas necesarias como enrolamiento, creación y eliminación de usuarios, asignación de permisos entre otros.

Por lo que es indispensable la utilización de bases de datos, en este caso con los equipos biométricos la autentificación depende de la comparación con las plantillas previamente cargadas en la base de datos.

Por lo que si se logra acceder, a alterar alguna de estas plantillas de la base de datos, el sistema estará craqueado de forma permanente, de esta forma será posible ingresar en las plantillas información de un usuario no autorizado y que este tenga el acceso que desea (Figura 15).

(Figura 15 – Acceso no autorizado a Base de datos)

(Fuente) [51]

Por lo que ya no se trata solamente del dispositivo que se utiliza, para realizar la validación de cada persona o usuario, sino que para la implementación de este sistema también se requiere de un software administrador del mismo, con el que se ejecuten las diferentes tareas que se requieran y la generación de informes, se podrá determinar que al tener alojada esta información dentro de un equipo servidor y su base de datos, se está expuesto a diferentes amenazas de ataques a esta base de datos como cualquier compañía, por lo que teniendo en cuenta estas

[51] Gemma Juanes. Los sistemas biométricos se utilizaron en seguridad electrónica en 1981. [Sitio WEB]. Madrid. España. Cuadernos de Seguridad. [Consultado 06, Mayo, 2021]. Disponible en: https://cuadernosdeseguridad.com/2021/04/sistemas-biometricos-aes-seguridad-electronica/

observaciones, se dará a conocer algunas de las principales vulnerabilidades que se presentan en las Bases de Datos, las cuales son la las siguientes: [52]

5.2.3.1 Contraseñas de Acceso No seguras

Esta vulnerabilidad es muy común por sus deficiencias de seguridad en el uso de contraseñas, las cuales no cuentan con niveles de seguridad altos, como la utilización de letras en mayúscula y minúsculas combinadas con la utilización de números y caracteres especiales.

5.2.3.2 Privilegios de grupo otorgados

Esta es una vulnerabilidad en la que normalmente los administradores del sistema, le brindan permisos innecesarios a determinado usuario, y esto conlleva a que posiblemente este usuario pueda utilizar esta información para malos fines.

5.2.3.3 Complementos innecesarios de base de datos

Las bases de datos normalmente utilizan algunos complementos para su funcionamiento, pero hay algunos que no son necesarios, y lo que hacen es volver vulnerable el ingreso al sistema, debido a que se convierten en una puerta de entrada auxiliar, por la que se podría originar algún ataque a la base de datos.

5.2.3.4 Desbordamiento de Buffer

Este es uno de los principales ataques que realizan los ciberdelincuentes, el cual consta del envío masivo de paquetes de información, en el que se sobrepasa del que puede recibir la aplicación, y logran vulnerar sus niveles de seguridad.

5.2.3.5 Inyección de SQL

Este ataque consiste en introducir un código en la base de datos, con el que pueda otorgar permisos de acceso, hasta apoderarse de ella, esto suele suceder debido a una mala limpieza de los datos que se procesan.[53]

---

[52] EL PERIODICO / ESPAÑA. La ciberdelincuencia pone en jaque la inversión de la Banca en Controles Biométricos. [Sitio WEB]. Madrid. España. Portal Tecnológico. [Consultado 06, Mayo, 2021]. Disponible en: https://www.elperiodico.com/es/economia/20160929/biometrica-seguridad-banca-5426348

[53] LEVELUP. Hackeo a Capcom no vulneró datos bancarios de los jugadores. [Sitio WEB]. Filipinas. La compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.levelup.com/noticias/618006/Hackeo-a-Capcom-no-vulnero-datos-bancarios-de-los-jugadores

(Figura 16 – Vulnerabilidades de Base de datos)

(Fuente) [54][55]

5.2.3.6 TÉCNICAS PARA MEJORAR LA SEGURIDAD

- ✓ Seleccionar equipos con tecnología de reconocimiento de dedo vivo.
- ✓ Mejorar la gestión de las contraseñas.
- ✓ Habilitar factores de doble autentificación.
- ✓ Realizar Actualizaciones del software instalado.
- ✓ Realizar copias de seguridad de la base de datos de usuarios.
- ✓ Verificar regularmente los accesos y alertas del sistema.
- ✓ Implementar seguridad en la red mediante Firewall y antivirus.
- ✓ Capacitación técnica y de seguridad del sistema al personal.

[54] BUGUROO. ¿Qué lleva a los Fraudsters a cometer fraude bancario? [Sitio WEB]. Madrid. España. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.buguroo.com/es/blog/que-lleva-los-fraudsters-a-cometer-fraude-bancario

[55] CONLETRAGRANDE. Como proteger tus bolsillos y los de tu familia de las estafas. [Sitio WEB]. Chile. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: https://www.conletragrande.cl/guia-las-estafas-bancarias-online-mas-comunes-y-como-protegerte-de-ellas

5.3 DESARROLLO DE OBJETIVO 3

Evaluar las técnicas que permitan explorar vulnerabilidades a estos sistemas biométricos, brindando recomendaciones y buenas prácticas, para concientizar a las personas sobre los equipos recomendados que cumplen la normatividad y brindan un servicio adecuado en este tipo de soluciones.

Según la información y tecnologías de los fabricantes recomendados (en el apartado 5 de este trabajo), para la implementación de este tipo de sistemas de reconocimiento Biométrico, se debe tener en cuenta varios factores, con los que se deberá diseñar la solución, según las especificaciones técnicas recomendadas y que se vayan a utilizar en diferentes ambientes, como por ejemplo para lugares exteriores y de bastante tráfico, deben contar con equipos que tengan un grado de protección IP65 resistente a la suciedad y el agua, además de la protección de anti vandalismo IK10, en caso de que el equipo sea golpeado y que no se dañe con facilidad.

Por otra parte, también se utiliza la tecnología de Rango Multi-Dinámico en algunos equipos, que es bastante interesante, ya que permite tener una imagen de la huella digital de calidad, incluso en condiciones de luz directa extrema de hasta 100.000 Lux de exposición, así como su velocidad que procesa cada huella en tan solo 6 ms, gracias a que estos equipos cuentan con una CPU de 1Ghz o superior.

Cada uno de los equipos que se toman como referencia, y validando que su utilización es para fines muy similares, muestra que el funcionamiento y los estándares de cumplimiento son un factor diferencial que los hace ser unos de los mejores equipos del mercado, los cuales se pueden fácilmente incluir en soluciones bastante robustas como, por ejemplo, la Registraduría Nacional del estado civil actualmente cuenta con la homologación de estos equipos para el uso en sus sistemas de información.[56]

Suprema, HID Global y Futronics, actualmente unas marcas muy reconocidas como fabricantes de este tipo de sistemas en el mercado, ya que manejan equipos con tecnología avanzada y de calidad para su validación tanto en la parte de hardware como de software.

Utilizan algoritmos de identificación en sus soluciones biométricas, que los hace manejar márgenes de error muy bajos, además de cumplir con las recomendaciones de normatividad vigente, lo que ayuda bastante a contar con mayor confiabilidad de nuestro sistema de reconocimiento biométrico, aunque también se debe tener en

[56] SUPREMA. Hardware – Productos Biométricos. [Sitio WEB]. Corea. La compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.supremainc.com/es/hardware/biometric-products.asp

cuenta otros factores adicionales como la seguridad en la red, que permiten tener un complemento de la seguridad en el proyecto.

Según informe de Kaspersky en 2019, en conjunto se bloquearon un número significativo de muestras de malware convencional, incluyendo troyanos de acceso remoto (5,4%), malware utilizado en ataques de phishing (5,1%), ransomware (1,9%) y troyanos bancarios (1,5%). Esta es una de las conclusiones del informe «Amenazas a los sistemas de procesamiento y almacenamiento de datos biométricos» elaborado por Kaspersky ICS CERT [57].

En primer lugar, la precisión del reconocimiento de datos biométricos por parte de los sistemas de autenticación, aunque relativamente alta, puede ser insuficiente para muchas aplicaciones. Los sistemas biométricos generalmente tienen una probabilidad mayor que cero de resultados falsos negativos y falsos positivos.

En segundo lugar, la investigación demuestra que muchas características biométricas humanas pueden ser falsificadas por actores maliciosos, y copiar datos biométricos digitalizados puede ser incluso más fácil que copiar biometría física.

En tercer lugar, los datos biométricos, una vez comprometidos, se ven comprometidos para siempre: los usuarios no pueden cambiar sus huellas dactilares robadas de la misma manera que las contraseñas robadas. Además, los datos biométricos pueden verse comprometidos para todas las aplicaciones al mismo tiempo. Por lo tanto, un individuo se verá potencialmente afectado por el resto de su vida, internet y los ataques de phishing son la mayor amenaza para la biometría.[58]

Cuando se requiere proteger datos personales, correos electrónicos u otro tipo de información como firmas digitales, huellas dactilares normalmente se utilizan diversas técnicas para conseguir aumentar los niveles de seguridad.

Existen métodos para incrementar la confidencialidad de la información como:

5.3.1 CIFRADO DE DATOS

Actualmente esta técnica es una de las más utilizadas para la protección de datos personales y empresariales, y funciona a través de algoritmos matemáticos, que convierten la información en otro tipo de dato ilegible, y estos datos cifrados cuentan con dos claves para descifrarlos, algunas ventajas de utilizar estos métodos son:

[57] CUADERNOS DE SEGURIDAD. Uno de cada tres equipos de biometría ha sufrido algún intento de infección de malware. [Sitio WEB]. España. La compañía. [Consultado 06, Diciembre, 2022]. Disponible en: https://acortar.link/w1Aeqq

[58] CUADERNOS DE SEGURIDAD. Uno de cada tres equipos de biometría ha sufrido algún intento de infección de malware. [Sitio WEB]. España. La compañía. [Consultado 06, Diciembre, 2022]. Disponible en: https://acortar.link/w1Aeqq

5.3.1.1 DATOS INSERVIBLES

En caso de que se pierda un dispositivo de almacenamiento o que sean robados, este cifrado de los datos hacen que sea inservible para las personas que no dispongan de las claves de cifrado de la información.

5.3.1.2 MEJORA LA REPUTACIÓN

Todas las empresas que trabajan con el cifrado de datos ofrecen a sus clientes una forma muy segura de protección de la información y confidencialidad de sus comunicaciones y datos, mostrando su profesionalidad y seguridad.

5.3.1.3 MENOR EXPOSICIÓN A SANCIONES

Debido a que este tipo de entidades son obligadas por la ley a tener un nivel de protección por el cifrado de datos que manejan.[59][60]

5.3.2 AUTENTICACIÓN

La autenticación es uno de los métodos más sencillos, pero a la vez muy eficientes a la hora de proteger la información, si se agreda una doble validación como la de contraseña y reconocimiento biométrico aumenta mucho la capa de seguridad de esta. [61]

Adicional se puede implementar una tercera validación, que sería la de la clave móvil, ya que además de las anteriores se debe contar con el equipo celular de la persona correspondiente, a pesar de que se trata de un sistema muy eficiente algunos usuarios no disponen de él. [62]

---

[59] SUPREMA. Hardware – Productos Biométricos. [Sitio WEB]. Corea. La compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.supremainc.com/es/hardware/biometric-products.asp

[60] BUGUROO. Biometría el comportamiento para garantizar confianza y seguridad. Luisa Esguerra. [Sitio WEB]. Madrid. España. La Compañía. [Consultado 06, Mayo, 2021]. https://www.buguroo.com/es/blog/biometria-del-comportamiento-para-garantizar-confianza-y-seguridad

[61] BUGUROO. Biometría el comportamiento para garantizar confianza y seguridad. Luisa Esguerra. [Sitio WEB]. Madrid. España. La Compañía. [Consultado 06, Mayo, 2021]. https://www.buguroo.com/es/blog/biometria-del-comportamiento-para-garantizar-confianza-y-seguridad

[62] BOSCHSECURITY. Lectores Multiclass. [Sitio WEB]. Bogota D.C. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://commerce.boschsecurity.com/xl/es/Fingerprint-Reader-Multiclass/p/F.01U.359.912/

Los sistemas de procesamiento de datos biométricos digitales, fueron utilizados principalmente por agencias gubernamentales y servicios especiales (policía, aduanas, etc.). Sin embargo, la rápida evolución de la tecnología de la información ha hecho que los equipos biométricos sean accesibles para su uso cotidiano. Estos dispositivos están aumentando y reemplazando los métodos de autenticación tradicionales, como los basados en inicios de sesión y contraseñas.

Estos sistemas que utilizan más de una validación son una muy buena alternativa para tener niveles de seguridad superior y cada uno de estos fabricantes que recomendamos, manejan variedad de equipos para los sistemas de control de accesos corporativos, por lo que se presentara en la parte final de este objetivo, unos de equipos más recomendados, con sus especificaciones por uno de los fabricantes como lo es SUPREMA (Figura 17): [63]

(Figura 17 – Tecnologías de acceso)

(Fuente Suprema) [64]

[63] SUPREMA. LECTORES DE AUTENTIFICACIÓN. [Sitio WEB]. Corea. La compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.suprema-id.com/es/contents/detail.php?code=010108
[64] SUPREMA. Hardware – Productos Biométricos. [Sitio WEB]. Corea. La compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.supremainc.com/es/hardware/biometric-products.asp

(Tabla 1 – Características de Tecnologías de acceso)

REFERENCIA	BEP2-OD	XS2-DPB	BLN2-ODB	BS2-OMPW	FSF2-DB
FABRICANTE	SUPREMA	SUPREMA	SUPREMA	SUPREMA	SUPREMA
NOMBRE	BIOENTRY P2	X-STATION 2	BIOLITE N2	BIOSTATION 2	FACESTATION F2
TIPO DE LECTURA	Biométrico y tarjeta	Biométrico y código QR	Biométrico y código numérico	Biométrico, Tarjeta, Código Numérico	Lector facial y tarjeta
GRADO DE PROTECCION	IP65	IP65	IP67	IP65	IP65
TIPO DE SENSOR	Optical Sensor (OP6)	Optical Sensor (OP5)	Optical Sensor (OP6)	Optical Sensor (OP5)	N/A
MEMORIA	8GB Flash + 64 MB RAM	16 GB Flash + 1 GB RAM	4GB Flash + 64MB RAM	8GB Flash + 256MB RAM	16GB Flash + 2GB RAM
CPU	1.0 GHz	1.5 GHz Quad Core	1.2 GHz	1.0 GHz Single Core	1.8 GHz Dual Core + 1.4 GHz Quad Core
CERTIFICACION	CE, FCC, KC, RoHS, REACH, WEEE	KC, CE, UKCA, FCC, RCM (Compliance: RoHS, REACH, WEEE)	CE, FCC, KC, RoHS, REACH, WEEE, FBI PIV(BLN2-PAB Sensor only)	CE, FCC, KC, RoHS, REACH, WEEE	CE, FCC, KC, RoHS, REACH, WEEE

(Fuente Propia) [65]

En la actualidad todos los sistemas de información deben estar debidamente establecidos y dando cumplimiento a la normatividad establecida ISO/IEC y/o FBI Mobile ID FAP20-30, que se rige según la ley 1581 de 2012 y del decreto 1377 de 2013, el Reglamento Internacional 2012/0011, adoptado oficialmente el 27 de abril de 2016, y las disposiciones del Reglamento que rigen desde el 25 de mayo de 2018.

La ley de privacidad de datos de la UE, para la recolección de datos biométricos y que es necesario contar con la autorización escrita de la persona y no puede restringirse una actividad al suministro de tales datos (artículo 6 del decreto 1377 de 2013).[66]

[65] SUPREMA. Hardware – Productos Biométricos. [Sitio WEB]. Corea. La compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.supremainc.com/es/hardware/biometric-products.asp
[66] COLOMBIA. Cundinamarca, Bogota D.C. Super Intendencia de Industria y comercio. Ley 1581 de 2012 (24, junio, 2018). Datos personales Eliminados. [Consultado 06, Mayo, 2021]. 1p - 8p

5.4 DESARROLLO DE OBJETIVO GENERAL

Analizar diferentes tipos de soluciones en biometría dactilar, especificando sus técnicas y el cumplimiento de los estándares internacionales ISO/IEC y/o FBI Mobile ID FAP20-30 acogido por Colombia, con el fin de generar recomendaciones para los usuarios que vayan a implementar esta tecnología.

Según la información relacionada en este documento, sobre cada uno de los fabricantes seleccionados para dar a conocer, como SUPREMA, HID Y FUTRONICS, son compañías que ya cuentan con una trascendencia en este mercado de más de 10 años y ellos se encuentran comprometidos con la seguridad de sus equipos y seguridad de sus clientes. Según lo que plantean, dentro de estas compañías, se cuenta con un área de desarrollo e innovación con la cual están en la búsqueda de nuevas tecnologías y estrategias para hacer que sus equipos sean mucho más seguros, innovadores y confiables para sus clientes.

El fabricante Suprema con su tecnología en sus equipos tanto de reconocimiento facial como de reconocimiento dactilar donde los fallos por error de reconocimiento del usuario eran inferiores al 0.00%, la cual se menciona con más a profundidad en el apartado 5.1.1.4 (Software con las ultimas actualizaciones en seguridad), lo que es un porcentaje muy bajo comparado con otros fabricantes (como se muestra en la Figura 1), y esto supone una confianza muy objetiva frente a este tipo de soluciones en reconocimiento facial y biométrico en el mercado.

Este Fabricante Suprema cuenta con técnicas de procesamiento de la información en sus equipos, que son bastante eficientes ya que la mayoría de estos biométricos son muy completos, en cuanto al almacenamiento interno y procesamiento de información, con las diferentes operaciones que realizan (Tabla 1), con funcionalidades como el trabajo de manera autónoma, sin estar sincronizado con el servidor en tiempo real (como lo hacen otros de sus competidores), lo que lo hace mucho más versátil frente a posibles pérdidas de energía o intermitencia de la red de datos del sistema.

Algunos equipos cuentan con certificación ISO/IEC 19794-4, el cual utiliza un formato para intercambiar de registro de datos para que almacene, registre o transmita información entre varias áreas con imágenes de dedos o palmas de una estructura de datos ISO / IEC 19785-1, además de contar con certificaciones FBI PIV, la cual, valida el acceso seguro a sus equipos, software, redes solo usando una huella digital.[67]

Disponible en: https://www.sic.gov.co/sites/default/files/normatividad/082018/Rad180171259TratamientoDatosSensibles.pdf

[67] SUPREMA. PRODUCTOS-PLATAFORMA-BIOSTAR2. [Sitio WEB]. Corea. La compañía. [Consultado 19, Noviembre, 2022]. Disponible en: https://www.supremainc.com/es/platform/hybrid-security-platform-biostar-2.asp

Como recomendación final en este apartado se puede decir que este fabricante Suprema, cuenta con un portafolio bastante amplio de equipos y con diferentes tecnologías de validación, ya que si se requiere que el sistema sea más seguro, lo ideal sería incluir tecnologías adicionales, y no solo la identificación de biometría dactilar, como por ejemplo el reconocimiento facial, validación de credenciales móviles o códigos QR, y con esto se garantiza que los niveles de seguridad del sistema sean mucho más altos.

La otra opción que se plantea en la solución del objetivo 1, es con el fabricante HID Global, donde planteó la tecnología MSI de HID, la cual es un desarrollo patentado de ellos, donde muestra una solución que utiliza luces multicolor en diferentes ángulos, para que los lectores con MSI recopilen hasta 12 imágenes diferentes, que se combinan en una única imagen óptima y esto permite generar una gran ventaja, ya que si se combinan varias imágenes, se puede capturar datos de huellas dactilares de forma fiable que funcionan en una amplia variedad de situaciones del mundo real, esto se expuso más a profundidad en el apartado 5.1.2.1 Principales características.

Según el portal Tecnoseguro (Portal de noticias de sistemas de seguridad), HID Global, HID es reconocida a nivel mundial por entregar soluciones confiables de identificación, y anunció que la nueva serie TouchChip TC de sensores capacitivos de huellas dactilares recibió la certificación de Nivel 1 por parte del laboratorio de pruebas independiente iBeta Quality Assurance, ya que los algoritmos de seguridad de la compañía frustraron el 100 % de los intentos de ataques simulados de suplantación de identidad realizados por el laboratorio iBeta, quienes entregaron el reconocimiento a HID Global. [68]

Otro factor fundamental es que la mayoría de sus equipos cuenta con la normatividad FIPS 201/PIV y FBI Mobile ID FAP 30 y cuentan con pruebas de conformidad, realizadas de acuerdo con la norma ISO/IEC 30107-3, que concluyen que el dispositivo biométrico de HID Global funciona según los más altos estándares logrando un 0 % de penetración lo que lo hace altamente recomendado para su implementación.[69]

FUTRONICS por otra parte plantea, el desarrollo que han estado trabajando para la identificación de los usuarios del sistema, por lo que indica como se ha desarrollado en su tecnología de identificación de dedos vivos, sus sistemas y manejan 3 tipos

[68] TECNOSEGURO. HID Global recibió certificación de Nivel 1 de detección de ataques de suplantación. [Sitio WEB]. Bogota. Colombia. La compañía. [Consultado 13, Marzo, 2023]. Disponible en: https://www.tecnoseguro.com/noticias/empresas/hid-global-certificacion-nivel-1-deteccion-ataques-suplantacion

[69] HID GLOBAL. Una persona, una verdadera identidad, El ciudadano Biométrico [Sitio WEB]. USA. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://acortar.link/9gCv95

diferentes de niveles de autentificaciones, clasificados según la solución a la cual se desee implementar esta solución.

La tecnología principal es la LFD y con estas sus tres niveles de seguridad para cada una de ellas como, TLFD que es un nivel básico de lectura de huellas en dedo vivo, con una mejora en sus capacidades, con la tecnología ELFD, en cuanto al rendimiento y su escáner para la detección de dedos vivos y por último la más avanzada que es la ALFD, cuya tecnología es mucho mejor que los anteriores versiones y se utiliza con en soluciones donde los niveles de seguridad son muy críticos, según se planteó en el apartado 5.1.3.2 (Futronic tiene 3 opciones de detección de dedos en vivo LFD).

Algunos equipos cuentan con la certificación del FBI con calidad de imagen PIV-071006, y cumple con el estándar de procesamiento federal 201 (FIPS 201) de EE.UU. (PVI), verificación de trabajadores y contratistas federales.[70]

De acuerdo con las especificaciones de los equipos que se incluyeron en la presente Monografía, dan cumplimiento a los estándares internacionales ISO/IEC y/o FBI Mobile ID FAP20-30 acogido por Colombia, ya que cuentan con las certificaciones solicitadas y de seguridad para tal fin, por lo que se recomiendan en las diferentes soluciones como de control de acceso y control de validación de usuario.[71]

Los niveles de seguridad se pueden mejorar utilizando otras tecnologías complementarias, que también manejan estos equipos como los lectores de proximidad y biometría, o la lectura de palma, que son innovaciones que realizo este fabricante y con lo cual también brindan muy buenos niveles de seguridad y confianza para sus clientes.

[70] FUTRONIC. Escáner de huellas dactilares FS10. [Sitio WEB]. Hong Kong. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.futronic-tech.com/pro-detail.php?pro_id=1533

[71] COLOMBIA. Cundinamarca, Bogota D.C. Super Intendencia de Industria y comercio. Ley 1581 de 2012 (24, junio, 2018). Datos personales Eliminados. [Consultado 06, Mayo, 2021]. 1p - 8p Disponible en: https://www.sic.gov.co/sites/default/files/normatividad/082018/Rad180171259TratamientoDatosSensibles.pdf

6 CONCLUSIONES

Mediante la estructuración y desarrollo de cada uno de los objetivos planteados para este trabajo, para la selección de soluciones de biometría dactilar, se concluye lo siguiente:

Como primera medida se concluye que se está planteando, tres compañías que ya llevan bastantes años con el desarrollo de tecnología en sistemas de control de acceso y biométrica, que son muy reconocidos en el mercado a nivel mundial, los cuales brindan excelentes equipos con innovaciones tecnológicas, bastante avanzadas en el reconocimiento biométrico, utilizando diferentes técnicas como lectura de huellas, reconocimiento de rostros, Iris entre otras, y de seguridad, con los que se lograra contar con total confianza y que cuentan con certificaciones y estándares internacionales que respaldan su calidad.

Por otra parte se plantean algunas vulnerabilidades que se pueden manejar, ya que cuentan con varios parámetros de protección, sus especificaciones técnicas como algoritmo de cifrado de datos, Base de Datos, tipo de sensor, conectividad, transferencia de información, memoria interna, CPU entre otros, que determinan los niveles de seguridad y/o procesamiento de los datos, lo que se convierte en un sistema bastante seguro, por lo menos dentro de los equipos que se plantean en este trabajo (aunque de la mano con las recomendaciones de control para que sean mucho más efectivos).

Con la evaluación de algunas formas de plagio, a las que continuamente están expuestos sistemas, se logra determinar algunas acciones para combatirlas, existen varios métodos utilizados para el cifrado de datos de la información, esto es algo fundamental en este tipo de compañías, ya que constantemente son el foco de los ciberdelincuentes, además de lograr mejorar su imagen ante sus clientes, con la utilización de un sistema que cumpla con estándares de seguridad, lo que lo hace mucho más seguro y confiable.

El estudio permitió concluir, que el desarrollo tecnológico, en cuanto a temas de biometría es muy amplio, y cada día avanza con la implementación de nuevas tecnologías y mejoras con sus desarrollos en el tema de ciberseguridad, ya que es otro factor muy crucial de este tipo de sistemas, donde también avanza la ciberdelincuencia para hacer más vulnerable esta tecnología, por lo que es muy importante el contar con los equipos Hardware y Software, con sus actualizaciones, para que sean muy seguros y confiables, y que podamos realizar cualquier trámite de manera ágil y segura.

7 RECOMENDACIONES

Antes de dar por terminado el desarrollo de la presente Monografía, se sugiere algunas recomendaciones, las cuales son de vital importancia para contar con buenos niveles de seguridad en este tipo de sistemas.

Analizar que fabricantes y equipos se pudieren implementar, a la hora de realizar un proyecto de biométrica de este tipo, y que nuevos niveles de seguridad se están implementando, que cumplan con la normatividad vigente en Colombia, con el fin de mitigar los posibles riesgos encontrados.

Desarrollar programas que permitan extender estos estudios realizados, sobre las vulnerabilidades de seguridad en este tipo de sistemas de biometría, ya que es un tema bastante interesante que ayudaría mucho, en el desarrollo tecnológico de estos sistemas.

Plantear propuestas de trabajos sobre otras tecnologías de reconocimiento complementarias que estén en desarrollo, ya que son temas bastantes interesantes para trabajar, estudios de este tipo en sistemas de Biometría.

Promover y fortalecer los trabajos sobre los sistemas de biometría en las universidades, con el fin de lograr desarrollos importantes sobre los productos, que estén en la vanguardia tecnológica, a fin de que se puedan implementar en las soluciones del día a día.

Con esta Monografía se evidencia el desarrollo tecnológico de los sistemas biométricos, y estas recomendaciones se ajustan a lo planteado en este trabajo (aunque complementando los niveles de seguridad en software y red, en casos donde los equipos se implementan para el funcionamiento) ya que aunque se han logrado desarrollos importantes en este ámbito, los ataques cibernéticos siempre están a la par de las innovaciones tecnológicas, por lo que se requiere manejar un constante desarrollo investigativo en este tipo de soluciones, para evitar vulnerabilidades de seguridad estos sistemas.

8 BIBLIOGRAFÍA

AMERICA RETAIL. ¿Cómo realizar compras online sin ingresar datos bancarios? [Sitio WEB]. Lima, Perú. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: https://www.america-retail.com/peru/como-realizar-compras-online-sin-ingresar-datos-bancarios/

ASOBANCARIA. Autenticación Biométrica para el sector financiero. Biometría [Sitio WEB]. Bogota D.C. La entidad. [Consultado 06, Mayo, 2021]. Disponible en: https://www.asobancaria.com/biometria/

BBVA. Los Bancos tienen muchísimo que ganar con la biometría. [Sitio WEB]. Bogota D.C. La entidad. [Consultado 06, Mayo, 2021]. Disponible en: https://www.bbva.com/es/bancos-tienen-muchisimo-ganar-biometria/

BLURADIO. Biometría y algoritmos genéticos: la tecnología que implementa UNAD en los exámenes universitarios. [Sitio WEB]. Bogota D.C. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: https://www.bluradio.com/tecnologia/biometria-y-algoritmos-geneticos-la-tecnologia-que-implementa-unad-en-los-examenes-universitarios

BOSCHSECURITY. Lectores Multiclass. [Sitio WEB]. Bogota D.C. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://commerce.boschsecurity.com/xl/es/Fingerprint-Reader-Multiclass/p/F.01U.359.912/

BUGUROO. ¿Qué lleva a los Fraudsters a cometer fraude bancario? [Sitio WEB]. Madrid. España. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.buguroo.com/es/blog/que-lleva-los-fraudsters-a-cometer-fraude-bancario

BUGUROO. Biometría el comportamiento para garantizar confianza y seguridad. Luisa Esguerra. [Sitio WEB]. Madrid. España. La Compañía. [Consultado 06, Mayo, 2021]. https://www.buguroo.com/es/blog/biometria-del-comportamiento-para-garantizar-confianza-y-seguridad

BUGUROO. Biometría el comportamiento en ciberseguridad. Juan David Castañeda. [Sitio WEB]. Madrid. España. La Compañía. [Consultado 06, Mayo, 2021]. https://www.buguroo.com/es/blog/biometria-del-comportamiento-en-ciberseguridad-acceso-y-sesion-protegidos-en-tiempo-real

CERTICAMARA. El futuro de la biometría en el sector colombiano. [Sitio WEB]. Bogota D.C. La Entidad. [Consultado 06, Mayo, 2021]. Disponible en: https://web.certicamara.com/files/futurodelabiometriasectorfinanciero.html

CINCO DÍAS. El doble reto de la biometría: conquistar al cliente y al regulador. [Sitio WEB]. Madrid. España. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: https://cincodias.elpais.com/cincodias/2021/03/21/companias/1616319560_020260.html

COLOMBIA. Cundinamarca, Bogota D.C. CONGRESO DE LA REPUBLICA. FUNCION PUBLICA. Decreto 1377 (27, junio, 2018). Gestor normativo. [Consultado 06, Mayo, 2021]. 1p - 5p Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php

COLOMBIA. Cundinamarca, Bogota D.C. Super Intendencia de Industria y comercio. Ley 1581 de 2012 (24, junio, 2018). Datos personales Eliminados. [Consultado 06, Mayo, 2021]. 1p - 8p Disponible en: https://www.sic.gov.co/sites/default/files/normatividad/082018/Rad180171259TratamientoDatosSensibles.pdf

CONLETRAGRANDE. Como proteger tus bolsillos y los de tu familia de las estafas. [Sitio WEB]. Chile. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: https://www.conletragrande.cl/guia-las-estafas-bancarias-online-mas-comunes-y-como-protegerte-de-ellas

CUADERNOS DE SEGURIDAD. Uno de cada tres equipos de biometría ha sufrido algún intento de infección de malware. [Sitio WEB]. España. La compañía. [Consultado 06, Diciembre, 2022]. Disponible en: https://acortar.link/w1Aeqq

DERECHOS DIGITALES. El cuerpo como dato. [Sitio WEB]. América Latina. Portal Tecnológico. [Consultado 06, Mayo, 2021]. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf

EBOOK. Biometrics: A Look at Facial Recognition [Sitio WEB]. Santa Monica. California. La entidad. [Consultado 17, Noviembre, 2022]. Disponible en: https://acortar.link/uVjZIE

EBSCOHOST. Biometría dactilar: una nueva alternativa de controlar efectivamente la asistencia a clases [Sitio WEB]. Buenos Aires. Argentina. La compañía. [Consultado 17, Noviembre, 2022]. Disponible en: https://doaj.org/article/95890ca6c223405aaa367616dfec4444

ELIBRO. Diccionario practico de Tecnología Educativa [Sitio WEB]. Buenos Aires. Argentina. La entidad. [Consultado 16, Noviembre, 2022]. Pg. 258, 320,360,371,408,409,415,443,459,460 Disponible en: https:// https://elibro-net.bibliotecavirtual.unad.edu.co/

EL BOLETIN. Reconocimiento del iris y la seguridad biométrica: ¿El sistema perfecto? [Sitio WEB]. Madrid. España. Portal Tecnológico. [Consultado 06, Mayo, 2021]. Disponible en: https://www.elboletin.com/reconocimiento-del-iris-y-la-seguridad-biometrica-el-sistema-perfecto/

EL FINANCIERO. ¿Quiénes tienen nuestros datos biométricos? [Sitio WEB]. México. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: https://www.elfinanciero.com.mx/opinion/jeanette-leyva/2021/04/15/quienes-tienen-nuestros-datos-biometricos/

EL PERIODICO / ESPAÑA. La ciberdelincuencia pone en jaque la inversión de la Banca en Controles Biométricos. [Sitio WEB]. Madrid. España. Portal Tecnológico. [Consultado 06, Mayo, 2021]. Disponible en: https://www.elperiodico.com/es/economia/20160929/biometrica-seguridad-banca-5426348

EL TIEMPO. ¿Cómo denunciar fraudes bancarios por internet? [Sitio WEB]. Bogota D.C. Periódico. [Consultado 06, Mayo, 2021]. Disponible en: https://www.eltiempo.com/economia/finanzas-personales/como-denunciar-fraudes-bancarios-por-internet-580611

EL UNIVERSAL. Europa busca prohibir la vigilancia biométrica por violación a derechos humanos. [Sitio WEB]. México. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: https://www.eluniversal.com.mx/techbit/europa-busca-prohibir-la-vigilancia-biometrica-por-violacion-derechos-humanos

ELLASTECUENTAN. El Gobierno De La Biometría Mercado Tendencias recientes, análisis en profundidad, pronóstico del informe de investigación del tamaño del mercado hasta 2031: Daon, Gemalto N. V., Safran de la Electronica y de Defensa SAS. [Sitio WEB]. USA. Portal tecnológico. [Consultado 06, Mayo, 2021]. Disponible en: https://ellastecuentan.com/el-gobierno-de-la-biometria-retos-y-pronostico-2022-2031/

EUROSOFT. Beneficios de la biometría en el sector bancario. Control acceso. [Sitio WEB]. México. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://solucioneseurosoft.com/control-acceso/biometria-en-el-sector-bancario/

FAD. Enrolamiento a motor Biométrico. Enrolamiento Biométrico. [Sitio WEB]. México. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://acortar.link/RMwy0K

FUTRONIC. Escáner de huellas dactilares FS10. [Sitio WEB]. Hong Kong. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.futronic-tech.com/pro-detail.php?pro_id=1533

Gemma Juanes. Los sistemas biométricos se utilizaron en seguridad electrónica en 1981. [Sitio WEB]. Madrid. España. Cuadernos de Seguridad. [Consultado 06, Mayo, 2021]. Disponible en: https://cuadernosdeseguridad.com/2021/04/sistemas-biometricos-aes-seguridad-electronica/

GLOBENEWSWIRE. Se espera que el mercado biométrico de reconocimiento de venas progrese a una CAGR del 19,2 % para alcanzar los 5.977,0 millones de dólares estadounidenses a finales de 2032, afirma Fact.MR [Sitio WEB]. Paris. Francia. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: https://www.globenewswire.com/en/news-release/2022/11/25/2562681/0/en/Vein-Recognition-Biometrics-Market-Is-Expected-To-Progress-At-A-CAGR-Of-19-2-To-Reach-US-5-977-0-Million-By-The-End-Of-2032-States-Fact-MR.html

HID GLOBAL. Una persona, una verdadera identidad, El ciudadano Biométrico [Sitio WEB]. USA. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://acortar.link/9gCv95

IDEMIA. Servicios Bancarios [Sitio WEB]. Francia. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.idemia.com/es/servicios-bancarios-donde-quieras-y-cuando-quieras

INFOTEC. Manual para uso de los datos Biométricos en los servicios financieros [Sitio WEB]. México. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/329/1/INFOTEC_MDTIC_LASC_10102019.pdf

ISO. Tecnología de la información - Formatos de intercambio de datos biométricos - Parte 4: Datos de imágenes digitales (2011). Recuperado de: https://www.iso.org/standard/50866.html

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Compendio de normas para trabajos escritos. NTC-1486-6166. Bogotá D.C.: El instituto, 2018. 153 p.

IT Group. Pagos móviles seguros: ¿qué técnica biométrica acabará imponiéndose? [Sitio WEB]. Madrid. España. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: https://www.ituser.es/seguridad/2021/04/pagos-moviles-seguros-que-tecnica-biometrica-acabara-imponiendose

LA SILLA ROTA. Después de geolocalización, bancos van por tus datos biométricos. [Sitio WEB]. México. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: https://lasillarota.com/dinero/despues-de-geolocalizacion-bancos-van-por-tus-datos-biometricos/498937

LEVELUP. Hackeo a Capcom no vulneró datos bancarios de los jugadores. [Sitio WEB]. Filipinas. La compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.levelup.com/noticias/618006/Hackeo-a-Capcom-no-vulnero-datos-bancarios-de-los-jugadores

MOBBEEL. Rafael Campillo. Estadísticas sobre la industria de la biometría. [Sitio WEB]. Cáceres, España. Portal de Noticias. [Consultado 12, Marzo, 2023]. Disponible en: https://www.mobbeel.com/blog/estadisticas-sobre-biometria-para-2021-mercado-y-sectores/

MOTORESFERA. Cuota de mercado de la biometría de voz 2021 principales fabricantes, tendencias, tamaño del mercado, oportunidades de crecimiento y pronóstico para 2366. [Sitio WEB]. España. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: https://acortar.link/a8VuZn

OAS.ORG. CIDH Capítulo IV.A. Desarrollo de los Derechos Humanos en la Región. [Sitio WEB]. Virginia. USA. La compañía. [Consultado 17, Noviembre, 2022]. p574 Disponible en: https://www.oas.org/es/cidh/docs/anual/2020/capitulos/IA2020cap.4A-es.pdf

OPTICAL. ¿Qué son los vectores de ataque en ciberseguridad? [Sitio WEB]. Lima. Perú. Portal de Noticias. [Consultado 12, Marzo, 2023]. Disponible en: https://www.optical.pe/blog/vectores-de-ataque-ciberseguridad/

PRESIDENCIA DE COLOMBIA. Cundinamarca, Bogota D.C. CONGRESO DE LA REPUBLICA. FUNCION PUBLICA. Decreto 1100 (15, Mayo, 2015). Decreto reglamentario 0188 de 2013. [Consultado 06, Mayo, 2021]. 1p - 3p Disponible en: https://acortar.link/WgGFK6

PRIMICIAS. Grupos delictivos roban datos bancarios a través de engaños por Internet. [Sitio WEB]. Quito. Ecuador. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: https://www.primicias.ec/noticias/sociedad/grupos-delictivos-datos-bancarios-internet/

R3D. AADHAAR, LA BASE DE DATOS BIOMÉTRICOS DE LA INDIA, ES VULNERABLE A UN PARCHE DE SOFTWARE DE 35 DÓLARES.?. [Sitio WEB]. D.F. México. Portal de Noticias. [Consultado 12, Marzo, 2023]. Disponible en: https://acortar.link/VhJDKf

RBH. Productos / Lectores y Teclados. [Sitio WEB]. Ontario. Canadá. La Compañía. [Consultado 06, Mayo, 2021]. Disponible en: http://www.rbh-access.com/products/readers-keypads

Revista Byte. El coronavirus impulsará la biometría. [Sitio WEB]. Madrid. España. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: https://revistabyte.es/opinion-byte-ti/cibercotizante/el-coronavirus-impulsara-la-biometria/

Revista Crossover. Análisis Cualitativo del Mercado La biometría militar (2021-2030) Evaluación Estratégica, Tendencias Emergentes y Estadísticas de Crecimiento | Marketresearch.biz [Sitio WEB]. Nueva york. USA. Portal de Noticias. [Consultado 06, Mayo, 2021]. Disponible en: http://revistacrossover.com/la-biometria-militar-healthy-growth-rate/

REVISTA MAS SEGURIDAD. Sensor HID con Normativa de seguridad en Colombia. [Sitio WEB]. México. La compañía. [Consultado 05, Diciembre, 2022]. Disponible en: https://www.revistamasseguridad.com.mx/sensor-biometrico-hid-primero-cumplir-nueva-normativa-seguridad-colombiana/

Ruiza, M., Fernández, T. y Tamaro, E. (2004). Biografía de Alphonse Bertillon. En Biografías y Vidas. La enciclopedia biográfica en línea. Barcelona (España). Recuperado de https://www.biografiasyvidas.com/biografia/b/bertillon.htm el 19 de octubre de 2020.

SUPREMA. Hardware – Productos Biométricos. [Sitio WEB]. Corea. La compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.supremainc.com/es/hardware/biometric-products.asp

SUPREMA. LECTORES DE AUTENTIFICACIÓN. [Sitio WEB]. Corea. La compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.suprema-id.com/es/contents/detail.php?code=010108

SUPREMA. Blog de Noticias y Artículos. [Sitio WEB]. Corea. La compañía. [Consultado 05, Diciembre, 2022]. Disponible en: https://www.supremainc.com/es/about/news-detail.asp?iBOARD_CONT_NO=3551

TALES. Los datos biométricos y el Reglamento general de protección de datos. [Sitio WEB]. América Latina. La compañía. [Consultado 06, Mayo, 2021]. Disponible en: https://www.thalesgroup.com/es/countries/americas/latin-america/dis/gobierno/biometria/datos-biometricos

TECHNOCIO. iProov presenta sus 10 predicciones para la identidad digital y la biometría. [Sitio WEB]. Bogota. Colombia. Portal de Noticias. [Consultado 13, Marzo, 2023]. Disponible en: https://technocio.com/iproov-presenta-sus-10-predicciones-para-la-identidad-digital-y-la-biometria/

TECNOSEGURO. HID Global recibió certificación de Nivel 1 de detección de ataques de suplantación. [Sitio WEB]. Bogota. Colombia. La compañía. [Consultado 13, Marzo, 2023]. Disponible en: https://www.tecnoseguro.com/noticias/empresas/hid-global-certificacion-nivel-1-deteccion-ataques-suplantacion

TECNOSEGURO. Tras 12 años consecutivos Suprema continúa clasificando en el 'Top 50 de las principales empresas de Seguridad Global. [Sitio WEB]. Bogota. Colombia. La compañía. [Consultado 13, Marzo, 2023]. Disponible en: https://www.tecnoseguro.com/noticias/empresas/tras-12-anos-consecutivos-suprema-continua-clasificando-top-50-principales-empresas-seguridad-global

UNIVERSIDAD AUTONOMA DE MADRID. Reconocimiento Facial Basado en Puntos Característicos de la Cara en entornos no controlados [Proyecto Fin de Carrera]. Madrid. España. [Consultado 17, Noviembre, 2022 p.1]. Disponible en: http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20130206LuisBlazquezPerez.pdf

Universidad Nacional de la Patagonia San Juan Bosco. Técnicas biométricas: análisis de las técnicas actuales y nuevas tendencias [Ensayo]. Buenos Aires. Argentina. [Consultado 17, Noviembre, 2022 p.1]. Disponible en: https://acortar.link/4ICglU

ANEXOS

Hoja técnica - BioMini Slim 2S

Hoja técnica - DigitalPersona 5300

Hoja técnica - FS10-1

Enlace del video de presentación

https://youtu.be/0aiEKqVUsmk