AUTENTICACIÓN BIOMÉTRICA BASADA EN RECONOCIMIENTO FACIAL Y DE VOZ: UN PROTOTIPO DE MÓDULO SOFTWARE PARA LA AUTENTICACIÓN DE USUARIOS/ESTUDIANTES DE CURSOS/AULAS VIRTUALES

JOSÉ JULIÁN GARCÍA FUENTES
DAVID FERNANDO JURADO BLANCO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICO-MECANICAS
ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMATICA
BUCARAMANGA
2018

AUTENTICACIÓN BIOMÉTRICA BASADA EN RECONOCIMIENTO FACIAL Y DE VOZ: UN PROTOTIPO DE MÓDULO SOFTWARE PARA LA AUTENTICACIÓN DE USUARIOS/ESTUDIANTES DE CURSOS/AULAS VIRTUALES

JOSÉ JULIÁN GARCÍA FUENTES
DAVID FERNANDO JURADO BLANCO

Trabajo de grado para optar al título de
Ingeniero de Sistemas

Director
SERGIO FERNANDO CASTILLO CASTELBLANCO
Ingeniero de Sistemas PhD

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICO-MECANICAS
ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMATICA
BUCARAMANGA
2018

DEDICATORIA

El autor José Julián García Fuentes dedica este logro a:

A Dios por guiarme correctamente durante toda mi carrera, por darme la salud y vitalidad para afrontar cada uno de los días en mi proceso de formación y por permitirme alcanzar este logro.

A mis padres José Ángel García Galvis y Nubia Estella Fuentes por estar siempre ahí cuando los necesite, por su gran apoyo, consejos y motivación. Son ustedes mi gran ejemplo a seguir, muchas gracias por todo lo que me han brindado, todo lo que soy se lo debo su esfuerzo y amor.

A mi hermana que siempre ha estado apoyándome y haciendo cada uno de mis días en todo el proceso sea más divertido, por su forma de ver la vida, su carisma y alegría.

Igualmente, a mi novia Diana Carolina Velandia Celis que me acompañó durante gran parte de mi carrera y con la cual pude vivir experiencias inolvidables durante mi tiempo en la universidad, gracias por hacerme sentir siempre el mejor estudiante.

Finalmente quiero este logro a todos los profesores que conocí durante mi tiempo en la universidad, por sus enseñanzas y porque gracias a ellos he podido aprender lo necesario para desarrollarme como profesional y en especial a mi director de proyecto Sergio Castillo por todo lo que nos ha enseñado, por su paciencia y apoyo en diferentes ocasiones. Por darnos la confianza necesaria y guiarnos correctamente durante la etapa final de nuestra carrera.

DEDICATORIA

El autor David Fernando Jurado Blanco dedica este logro a:

Primeramente, debo dedicar este logro a Dios por haberme guiado durante todo el trayecto hasta este punto.

A mis padres, Oswaldo Jurado y Blanca Blanco, quienes, con su apoyo incondicional y confianza en mí, hicieron posible este logro.

Agradezco inmensamente a mis abuelos paternos, María Bello y José Jurado, por su enorme paciencia y todo el esfuerzo que hicieron por sacarme adelante desde el momento que llegué a este mundo.

A todos los demás miembros que de mi familia que me brindaron su ayuda y valiosos consejos a lo largo de mi vida.

A mi novia Jeily García por haberme respaldado y motivado en los momentos más difíciles, por sus consejos y la alegría que me ha brindado.

Y finalmente a nuestro director de proyecto Sergio Castillo,
gracias por su apoyo y confianza, toda mi admiración para usted.

AGRADECIMIENTOS

A Dios por darnos sabiduría y permitirnos culminar este proyecto.

A la escuela de Ingeniería de Sistemas e Informática y cada uno de sus profesores que con su compromiso y dedicación han aportado conocimiento en este proceso de formación.

A nuestro director de proyecto, Sergio Fernando Castillo, por el compromiso, paciencia, colaboración y confianza, que permitieron realizar este proyecto de grado.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

Pág.

RESUMEN

TITULO: AUTENTICACIÓN BIOMÉTRICA BASADA EN RECONOCIMIENTO FACIAL Y DE VOZ: UN PROTOTIPO DE MÓDULO SOFTWARE PARA LA AUTENTICACIÓN DE USUARIOS/ESTUDIANTES DE CURSOS/AULAS VIRTUALES*

AUTORES:

David Fernando Jurado Blanco**

José Julián García Fuentes**

PALABRAS CLAVE: Autenticación, biometría, módulo web, reconocimiento facial, reconocimiento vocal.

DESCRIPCIÓN:

Para otorgar el acceso a la información, bienes o servicios es necesario realizar una validación de quien está intentando acceder, esto es un proceso conocido como autenticación, el cual tiene como propósito asegurar que una persona es auténtica o es quien dice ser, todo esto para proteger información y/o bienes valiosos, o bien restringir el acceso a lugares y/o servicios a personas que no autorizadas; Entre estos lugares que en los que se hace necesaria la autenticación de usuarios se encuentran los portales y paginas enfocadas a la educación, tales como aulas o cursos virtuales, en los que se han evidenciado casos de suplantación de identidad lo que conlleva no solo graves consecuencias para el estudiante y su aprendizaje sino también para la institución y su modelo de enseñanza.

En este proyecto se presenta el desarrollo de un prototipo de módulo software para la autenticación de usuarios en cursos virtuales, basándose en la autenticación biométrica facial y de voz, este módulo brinda mayor seguridad durante la autenticación de los usuarios que ingresan a los portales educativos, haciendo uso un micrófono y una cámara, hardware presente en la mayoría de los computadores y smartphones.

Con el desarrollo de este proyecto se busca ofrecer una alternativa a los métodos tradicionales de autenticación en portales educativos, garantizar una mayor seguridad durante el ingreso de usuarios y así evitar posibles suplantaciones.

*Trabajo de grado.

** Facultad Ingeniería Físico-Mecánicas. Escuela Ingeniería de Sistemas. Director Ing. Sergio Fernando Castillo Castelblanco.

SUMMARY/ABSTRACT

TITLE: BIOMETRIC AUTHENTICATION BASED ON FACIAL AND VOICE RECOGNITION: A SOFTWARE MODULE PROTOTYPE FOR THE AUTHENTICATION OF USERS / STUDENTS OF VIRTUAL COURSES / CLASSROOMS *

AUTHORS:

David Fernando Jurado Blanco **

José Julián García Fuentes **

KEY WORDS: Authentication, biometrics, web module, facial recognition, voice recognition.

DESCRIPTION:

To grant access to information, goods or services it is necessary to validate the person who is trying to access, this is a process known as authentication, which aims to ensure that a person is authentic or is who is supposed to be, all this to protect information and / or valuable assets, or restrict access to places and / or services to people who are not authorized; Among these places are those that are needed to access education, such as classrooms or virtual courses, which have evidenced the cases of identity theft, grievance for the student and their learning, also for the institution and its model of teaching.

This project presents the development of a prototype software module for user authentication in virtual courses (also known as online classrooms), based on facial and voice biometric authentication, this module provides greater security during the authentication of users who enter the educational portals, using a microphone and a camera, hardware present in most computers and smartphones.

The development of this project seeks to offer an alternative to traditional methods of authentication in educational portals such as the passwords, to ensure greater security for the entry of users and to avoid possible spoofing or impersonation.

* Bachelor Thesis.

** Facultad Ingeniería Físico-Mecánicas. Escuela Ingeniería de Sistemas. Director Ing. Sergio Fernando Castillo Castelblanco.

INTRODUCCIÓN

La digitalización de la información ha hecho de las tecnologías actuales unas herramientas presentes en la vida cotidiana, el uso de estas se ha masificado haciendo que de ellas dependa gran parte de lo que somos y hacemos, pues hoy en día gracias a los distintos avances tecnológicos como la velocidad del internet, los dispositivos móviles, las redes sociales, entre otros, es posible almacenar contenido de gran valor de manera fácil y rápida, este contenido se ve representado en cuentas bancarias, correos electrónicos, base de datos, información académica, fotos personales, etc. Todo este tipo de información puede llegar a poseer un valor intangible enorme, incluso de carácter económico o sentimental.

Debido a ese gran valor nace esa necesidad de proteger la información, es por esto que actualmente se pueden encontrar diversos tipos de métodos para restringir el ingreso y/o la modificación de los dichos datos por parte de personas no deseadas, esto métodos son contraseñas, patrones, pines numéricos, bloqueos de imagen y muchos más; Sin embargo debido al gran valor de la información siempre existirá alguien que intente violar dicha seguridad y acceder sin ninguna autorización, lo cual hace que el porcentaje de confiabilidad y seguridad sea de gran importancia. Aun así, ningún método actual tiene un porcentaje de seguridad del cien por ciento y muchas veces los pines o contraseñas se hacen tediosos o difíciles de recordar, lo que incentiva a que use de manera repetitiva una misma contraseña para distintos accesos a la información personal, debilitando gravemente la seguridad del método.

Los humanos poseemos características únicas por medio de las cuales podemos ser reconocidos o reconocer a otra persona, algunas de estas están son la voz, el rostro, la escritura, los ojos o unos conjuntos de estas. La biometría es un método que permite reconocer a una persona por medio de alguno de estos rasgos únicos lo cual se puede usar para autenticar a individuos y así evitar posibles intentos de suplantación o el robo de identidad. Los rasgos utilizados

para la identificación biometría son específicos y se puede acoplar dicho tipo de reconocimiento en el desarrollo de software, para así velar por la protección y seguridad de la información. La biometría no garantiza un cien por ciento de seguridad, pero si puede llegar a tener un porcentaje mayor al de muchos de los sistemas o métodos tradicionales, además elimina una gran cantidad de pasos y la necesidad de memorizar contraseñas o patrones.

En los últimos años se ha presenciado un gran cambio en los procesos formativos que son ofrecidos por parte de las instituciones educativas, ya que, gracias a las nuevas tecnologías se han logrado romper barreras geográficas, permitiendo brindar a los estudiantes todos los materiales de aprendizaje de manera remota a través de cursos virtuales, sin embargo, este modelo de enseñanza ha evidenciado casos de fraude por parte de los estudiantes, por lo que se hace necesario la implementación de procesos de autenticación más seguros.[1]

El presente proyecto de grado busca desarrollar un prototipo de módulo software que permita la verificación de estudiantes pertenecientes a cursos virtuales, para esto se hará uso de técnicas de reconocimiento facial y de voz, métodos de autenticación biométrica que utilizan características que permiten reconocer a un individuo sin el uso de algún sensor especial, ya pueden ser utilizadas en la mayoría de los teléfonos móviles o computadoras actuales, esto con el fin de hacer más fácil su uso e implementación y así poder ampliar el campo de aplicación de la herramienta.

[1] ONLINE SCHOOLS CENTER. How students cheat online [En línea]. Online schools center, 2018 (Recuperado en 02 de febrero 2018). Disponible en https://www.onlineschoolscenter.com/cheating-online/

ESTRUCTURA DEL PROYECTO

A continuación, se muestra cómo se implementó y distribuyo el desarrollo del proyecto, el cual se realizó mediante una distribución de capítulos con el fin de ordenar el proceso de diseño, implementación y ejecución de este.

CAPITULO 1. Descripción del proyecto: en este capítulo se encuentra el planteamiento y justificación del problema, objetivo general y específicos y alcance.

CAPITULO 2. Marco teórico y herramientas: en este capítulo se presenta el marco de referencia, el marco teórico, Herramientas, Herramientas de reconocimiento vocal y facial, Evaluación de herramientas biométricas, tabla de comparación/elección y metodología.

CAPITULO 3. Especificación de requisitos: en este capítulo se encuentra la metodología mediante la cual se desarrolló el proyecto, el documento de especificación de requisitos y los casos de uso.

CAPITULO 4. Diseño: en este capítulo se encuentran los prototipos de interfaz de usuarios y el diseño.

CAPITULO 5. Descripción del sistema: en este capítulo se presenta una descripción del sistema desarrollado y de cada una de las pantallas.

CAPITULO 6. Pruebas: en este capítulo se presentan las pruebas aplicadas al prototipo las cuales son las pruebas funcionales y sus resultados, pruebas de seguridad y las tablas de cumplimiento de objetivos.

1. DESCRIPCIÓN DEL PROYECTO

1.1 PLANTEAMIENTO Y JUSTIFICACIÓN DEL PROBLEMA

En las tecnologías de la información se ha venido trabajando en sistemas de autenticación de usuarios cada vez más seguros y ágiles debido a necesidades como proteger información valiosa, tener un control de acceso a sitios físicos o virtuales, realizar operaciones bancarias, entre muchas otras. Dentro de las posibles técnicas para lograr satisfacer estas y más necesidades, ha sido la biometría el campo donde se puede conseguir una mayor versatilidad y rendimiento a la hora de certificar la identidad de una persona.

La verificación de la identidad de individuos ha sido una tarea que se ha logrado realizar gracias a procesos biométricos tradicionales como la huella dactilar o la firma física, pero generalmente es necesario tener un lector de huellas dactilares o de firma, en el peor de los casos hay que darse a la tarea de comparar físicamente los patrones biométricos, así mismo un porcentaje de la población está inhabilitada para la ejecución de registros de este tipo.

Actualmente existen métodos de identificación por biometría más especializados, tales como identificación de iris, retina, geometría de la mano, e incluso venas, para realizar la toma y verificación de estas características físicas es necesario contar con equipos especializados de gran costo; Por otro lado existe la identificación facial y de voz, las cuales se pueden realizar incluso desde dispositivos móviles, estos métodos de identificación se han venido perfeccionando a lo largo de los años y actualmente no se necesita realizar todas las operaciones y procesos de cómputo desde nuestro equipo de trabajo, ya que se han desarrollado en la web servicios de reconocimiento facial y de voz (facial recognition as a service & voice recognition as a service).

Se encuentran varias prácticas en el área educacional para determinar cuánto han aprendido los estudiantes y que tan eficaz ha sido el proceso de enseñanza,

algunas de estas prácticas se han conseguido realizar a distancia, haciendo el tiempo más productivo y más activo el proceso formativo. Sin embargo, una de las desventajas de la educación a distancia es la falta de procesos de verificación más seguros, haciendo relativamente fácil la suplantación de identidad de los estudiantes durante varias etapas claves del proceso educativo tales como exámenes y talleres.

Como marco de prueba de los procesos de biometría voz y facial, se considera realizar un trabajo en esta área que permita revisar el estado del arte, comparar las diferentes herramientas de reconocimiento facial y de voz que están disponibles actualmente y hacer pruebas de estas, esto surge de la necesidad de verificar la identidad de estudiantes en aulas virtuales. Los resultados de este proceso se aplicarán para el desarrollo de un prototipo de módulo de identificación de usuarios/estudiantes.

1.2 OBJETIVOS

1.2.1 Objetivo general. Diseño y desarrollo de prototipo de módulo web en el que los usuarios puedan ser identificados por reconocimiento biométrico (facial y de voz) y ejecución mediante un escenario de prueba (emulador de aula virtual).

1.2.2 Objetivos específicos

1) Elaboración del Documento de especificación de requisitos del módulo de autenticación biométrica y del escenario de prueba.

2) Elaboración de una tabla comparativa y selección de las herramientas de biometría facial y de voz a usar en el módulo de autenticación.

3) Diseño del módulo de autenticación biométrica que permita:

- Crear y gestionar el banco de huellas faciales y el banco de huellas vocales para el reconocimiento biométrico.

- Verificar la identidad de un usuario a partir de sus características biométricas faciales y de voz.

- Proporcionar la información requerida para la adecuada toma de los datos biométricos.

4) Diseño del escenario de prueba del módulo de autenticación biométrica, esto es un emulador de aula virtual que permita:

- Registro del usuario-estudiante con sus datos personales e información biométrica (huella facial y vocal) usando la cámara y el micrófono.
- Brindar al usuario una alternativa de autenticación en caso de fallo en la autenticación biométrica (por causas de hardware, fallas en el servidor o plataforma).

5) Implementación del módulo de autenticación biométrica y del escenario de prueba.

6) Ejecución de pruebas para evaluar la usabilidad y rendimiento del módulo software.

1.3 ALCANCE

Se desarrollará un prototipo de módulo web que permita la autenticación de los usuarios usando los rasgos biométricos voz y cara, permitiendo el registro del usuario/estudiante con sus datos personales e información biométrica; En caso de que la autenticación por métodos biométricos sea fallida al momento de ingresar al sistema, se permitirá al usuario la opción de autenticación por contraseña; Al ser un prototipo no se implementará la opción de restablecer

contraseña por correo electrónico en caso de olvido por parte del usuario, para solucionar esto el usuario se debe comunicar con el administrador del módulo.
El objetivo principal del proyecto es el estudio de las técnicas biométricas para voz y cara, se usa el aula virtual como un escenario de prueba por tanto se trata de un prototipo o emulador de un aula virtual la cual contará con la opción de registro de usuarios, creación de las huellas facial y de voz y la opción de login en la cual se utilizará la autenticación biométrica para el acceso. Dicha plataforma solo dará el aspecto de un aula virtual pero no poseerá cursos o exámenes puesto que el fin de esta es probar y ejecutar el módulo de autenticación biométrica.

No es posible definir por cuánto tiempo esté prototipo estará disponible en la web ya que algunas de las herramientas de análisis de patrones biométricos ofrecen un tiempo limitado para su uso gratuito, no obstante, toda la documentación de cómo crear un acceso para el uso de estas herramientas y el código fuente del módulo estarán disponibles en GitHub para que toda persona interesada pueda implementarlo o modificarlo.

2. MARCO TEÓRICO Y HERRAMIENTAS

2.1 MARCO DE REFERENCIA

Actualmente la biometría permite identificar a una persona por rasgos como la huella, firma, iris, voz, rostro y hasta en base a las venas y distribución de estas, muchos de estos tipos de identificación ya tienen aplicación hoy en día y están al alcance de cualquier usuario mientras que otros, debido a que requieren distintos lectores, sensores o dispositivos de hardware hacen que su implementación no sea sencilla y que los costos de esta sean más elevados.

La biometría facial y de voz actualmente permiten una implementación sencilla, pues en cuanto a hardware se refiere tan solo se necesita una cámara y un micrófono respectivamente, encontramos estos componentes físicos en dispositivos móviles o computadores lo que no solo reduce costos, sino que también aumenta su sencillez y usabilidad.

2.2 MARCO TEÓRICO

La palabra biometría proviene de las palabras griegas *Bios*, que significa vida y *metron* que significa medida, en las tecnologías de la información la biometría es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para su autenticación, es decir, verificar su identidad.[2]

Existen dos tipos de características principales con las que se puede realizar el proceso de autenticación biométrica, estas son las características físicas y las características de comportamiento; Las primeras corresponden aquellos rasgos estáticos tales como la huella dactilar, la retina, el iris, los patrones faciales, de

[2] COLABORADORES DE WIKIPEDIA. Biometría [En línea]. Wikipedia, La enciclopedia libre, 2018 (Recuperado en 02 de septiembre 2017). Disponible en https://es.wikipedia.org/w/index.php?title=Biometr%C3%ADa&oldid=105463937

venas e incluso geometría de la palma de la mano, por otra parte se encuentran las características de comportamiento que corresponden a patrones dinámicos tales como la firma, el paso y el tecleo; Existen algunos rasgos como la voz que comparten aspectos tantos físicos como de comportamiento.

En un sistema de Biometría típico, la persona se registra en el sistema cuando una o más de sus características físicas y de conducta es obtenida, procesada por un algoritmo, e introducida en una base de datos. Idealmente, cuando entra, casi todas sus características concuerdan; entonces cuando alguna otra persona intenta identificarse, no empareja completamente, por lo que el sistema no le permite el acceso.

Muchos de los diferentes aspectos de la fisiología humana, la química o el comportamiento se puede utilizar para la autenticación biométrica. La selección de un aspecto biométrico particular para su uso en una aplicación específica implica una ponderación de varios factores. Jain et al. (1999) identificó siete de estos factores que se utilizarán al evaluar la idoneidad de cualquier rasgo para su uso en la autenticación biométrica.

- Universalidad: significa que cada persona que usa un sistema debe poseer el rasgo.
- Unicidad: significa que el rasgo debe ser suficientemente diferente para los individuos en la población pertinente de tal manera que se pueden distinguir entre sí.
- Permanencia: se refiere a la manera en que un rasgo varía con el tiempo. Más específicamente, un rasgo con “buena” permanencia será razonablemente invariante en el tiempo con respecto al algoritmo de coincidencia específico.
- Colectividad: se relaciona con la facilidad de adquisición o medición del rasgo. Además, los datos adquiridos deben estar en una forma que permita el posterior procesamiento y extracción de los conjuntos de características relevantes.

- Rendimiento: se refiere a la precisión, velocidad y robustez de la tecnología utilizada.
- Aceptabilidad: se refiere a la forma en que los individuos de la población pertinente aceptan la tecnología de tal manera que están dispuestos a que su rasgo biométrico sea capturado y evaluado.
- Evasión: se refiere a la facilidad con que un rasgo puede ser imitado usando un artefacto o un sustituto.

El uso biométrico adecuado es muy dependiente de la aplicación. Cierta técnica biométrica será mejor que otras basadas en los niveles requeridos de conveniencia y seguridad. Ningún método biométrico único cumplirá todos los requisitos de todas las aplicaciones posibles.

Los sistemas biométricos multimodales utilizan múltiples sensores o técnicas de biometría para superar las limitaciones de los sistemas biométricos unimodales y aumentar la seguridad a la hora de autenticar a un individuo. Por ejemplo, los sistemas de reconocimiento del iris pueden verse comprometidos por el envejecimiento del iris y los sistemas de huella por desgaste o cortaduras. Si bien los sistemas biométricos unimodales están limitados por la integridad de su identificador, es improbable que varios sistemas unimodales sufran de limitaciones idénticas, por lo tanto, se espera que un sistema biométrico multimodal proporcione mejores resultados de reconocimiento. Los sistemas biométricos multimodales pueden obtener conjuntos de información del mismo marcador (es decir, múltiples imágenes de un iris o exploraciones del mismo dedo) o información de diferentes rasgos biométricos.

2.2.1 Biometría facial. La biometría facial permite determinar la identidad de una persona analizando su rostro. A diferencia de otras técnicas biométricas tipo iris o huella dactilar esta tecnología no es intrusiva y no necesita de colaboración por parte del usuario, sólo es necesario que su rostro sea adquirido por una cámara.[3]

[3] COLABORADORES DE WIKIPEDIA. Sistema de reconocimiento facial [En línea]. Wikipedia, La enciclopedia libre, 2018 (Recuperado en 04 de septiembre 2017). Disponible en https://es.wikipedia.org/w/index.php?title=Sistema_de_reconocimiento_facial&oldid=104630687

El objetivo de un sistema de reconocimiento facial es, generalmente, el siguiente: dada una imagen de una cara "desconocida", o imagen de test, encontrar una imagen de la misma cara en un conjunto de imágenes "conocidas", o imágenes de entrenamiento. Puede operar en dos modos:

Verificación o autenticación: compara una imagen de la cara con otra imagen con la cara de la que queremos saber la identidad. El sistema confirmará o rechazará la identidad de la cara.

Identificación o reconocimiento: compara la imagen de una cara desconocida con todas las imágenes de caras conocidas que se encuentran en la base de datos para determinar su identidad.

Por su naturaleza amigable, este tipo de sistemas siguen siendo atractivos a pesar de la existencia de otros métodos muy fiables de identificación personal biométricos, como el análisis de huellas dactilares y el reconocimiento del iris.

El funcionamiento del reconocimiento facial consta de cuatro módulos principales:

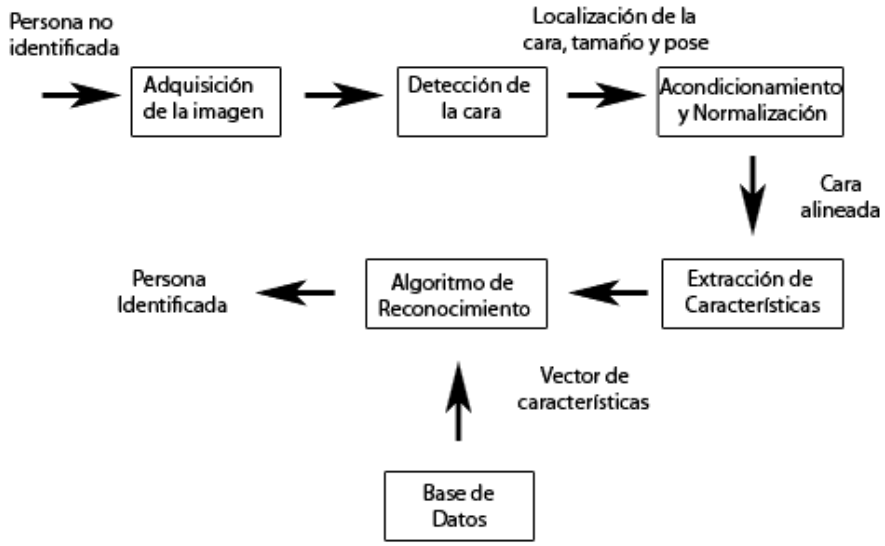
- Detección de la cara: detecta que hay una cara en la imagen, si se trata de un video, también es posible hacer un seguimiento de la cara.

- Alineación de la cara: localiza los componentes de la cara y mediante transformaciones geométricas, la normaliza respecto a propiedades geométricas, como el tamaño y la pose, y fotométricas, como la iluminación.

- Extracción de características: proporciona información para distinguir entre las caras de diferentes personas según variaciones geométricas o fotométricas.

- Reconocimiento: el vector de características extraído se compara con los vectores de características extraídos de las caras de la base de datos. Si encuentra uno con un porcentaje elevado de similitud, devuelve la identidad de la cara; si no, indica que es una cara desconocida.

Figura 1. Funcionamiento de un sistema de reconocimiento facial



Fuente: Proceso de un sistema de reconocimiento facial, Cris Palmero, 12 de diciembre 2010.

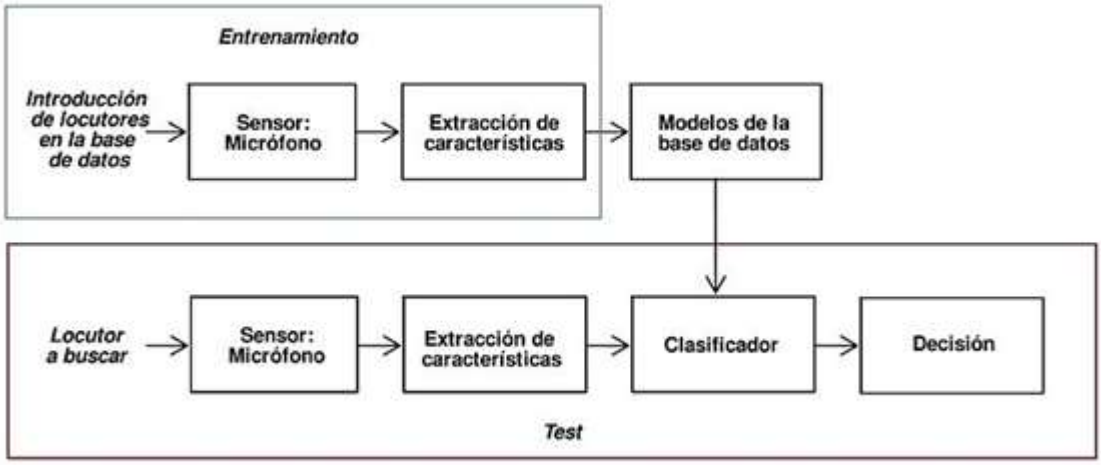
2.2.2 Biometría de voz. El reconocimiento voz consiste en la identificación automática de una persona a través de su voz. El hecho de poder distinguir una persona de otra está relacionado mayoritariamente con las características fisiológicas y los hábitos lingüísticos de cada uno de ellos. El reconocimiento consta de un procesado de audio que permite extraer un conjunto características del locutor y posteriormente la búsqueda de coincidencias mediante un proceso de reconocimiento de patrones.[4]

[4] COLABORADORES DE WIKIPEDIA. Reconocimiento del habla [En línea]. Wikipedia, La enciclopedia libre, 2018 (Recuperado en 04 de septiembre 2017). Disponible en https://es.wikipedia.org/w/index.php?title=Reconocimiento_del_habla&oldid=105422942

Cada sistema de reconocimiento de habla tiene dos fases: el entrenamiento y la verificación. Durante el entrenamiento, la voz del hablante se registra y típicamente el número de características se extraen para formar la huella vocal, plantilla o modelo.

En la fase de verificación, la muestra de voz o "expresión" se compara con una impresión de voz creada anteriormente. Para los sistemas de identificación, la expresión se compara con múltiples impresiones de voz con el fin de determinar la voz con mayor similitud.

Figura 2. Funcionamiento de un sistema de reconocimiento de voz



Fuente: *Esquema de un reconocedor de locutores, Elisabet Carcel, 9 de diciembre 2010.*

Los sistemas de reconocimiento se dividen en dos categorías: dependiente del texto y de texto independiente. La primera indica que el texto debe ser el mismo para el entrenamiento y la verificación. Un sistema dependiente del texto puede ser o bien indicaciones comunes para todos los usuarios (por ejemplo: Una frase común) o únicas. Los sistemas de texto independiente se utilizan con más frecuencia para la identificación del hablante, se requiere muy poca o ninguna cooperación por parte del hablante; En este caso el texto durante el entrenamiento y la prueba es diferente, de hecho, el entrenamiento puede ocurrir

sin el conocimiento del usuario, como en el caso de muchas aplicaciones. En las tecnologías de texto independiente no se puede comparar lo que se dijo en el entrenamiento y la verificación.

Los niveles de ruido ambiental podrían ocasionar problemas en la grabación de muestras tanto iniciales como finales. Algoritmos de reducción de ruido pueden ser empleados para mejorar la precisión, pero la aplicación incorrecta puede tener el efecto opuesto.

La extracción de datos es de gran importancia tanto para la parte de entrenamiento como para la de test. Para poder introducir los usuarios al sistema es necesario un transductor acústico-eléctrico, ya que la voz se propaga en forma de ondas y para poder extraer características es necesario transformar la presión sonora en una señal eléctrica y así poder proceder a su digitalización.

Hay factores externos al locutor como la relación señal ruido (SNR) de las muestras grabadas o la utilización de micrófonos con diferentes curvas de respuesta frecuencial que pueden influir negativamente en el resultado

2.3 ESTADO DEL ARTE

A continuación, se muestran algunos de los productos más distinguidos del mercado en el área de reconocimiento facial y de voz:

2.3.1 Certivoz. Certivoz un producto de certicámara que ha sido promovido por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia con el fin de aumentar el uso de la biometría en la industria nacional. Certivoz es aliado de Nuance, compañía “líder mundial en biometría de voz” con el cual trabajan de la mano para la prestación del servicio**.**

Figura 3. Captura de pantalla Certivoz.

Fuente: Certivoz. [Consultado el 01 de febrero del 2018]. Disponible en: https://web.certicamara.com/productos-y-servicios/servicios-de-autenticacion-biometrica-certificados/

Nuance también hace presencia en México en el banco Santander en el cual implementó la biometría de voz para sustituir los pines o contraseñas y las preguntas de seguridad en su sistema telefónico automatizado. Certivoz ofrece a los usuarios:

- Integración de firmas digitales para dar validez jurídica.
- Estampas de tiempo para garantizar la integridad de los datos.
- Detección de grabación e identificación con un 98% de certeza.

2.3.2 Checkvox. Es un producto que identifica a los usuarios mediante su voz en sólo segundos, con aplicaciones en varios sectores.

Figura 4. Captura de pantalla Checkvox

Fuente: Checkvox. [Consultado el 01 de febrero del 2018]. Disponible en: http://biometricvox.com/checkvox/

Según la empresa usan tecnología 100 % propia lo cual les permite crear soluciones a medida para cada cliente. Sus principales características o aplicaciones son:

- Identificación mediante voz.
- Desarrollo a medida.
- Control de presencia y horario.
- Integración con terceros (API).

2.3.3 True Key. True Key es un producto de Intel Security el cual permite el acceso a webs y dispositivos (tanto de escritorio como dispositivos móviles) a través de los siguientes modos:

- Reconocimiento facial
- Huella digital
- Segundo dispositivo
- Contraseña principal
- Correo electrónico
- Dispositivo de confianza

Además de esto ofrece funcionalidades adicionales como gestión de contraseñas, cifrado de datos locales y sincronización entre dispositivos.

Figura 5. Captura de pantalla True Key

Fuente: True Key. [Consultado el 01 de febrero del 2018]. Disponible en: https://www.truekey.com/es-MX

2.3.4 Selphi. Selphi es una solución diseñada por FacePhi para banca móvil, cuenta con tecnología de reconocimiento facial con las siguientes características:

- Detección de Pose +/- 15° en cada dirección
- Tolerancia a Oclusiones parciales del rostro
- Tolerancia ante cambios en barba y estilo de peinado
- Permite el uso de gafas (excepto gafas de sol)

- Altamente tolerante a cambios de iluminación
- Algoritmos de localización de rostro y ojos
- Algoritmos de codificación de características únicas e intransferibles del rostro
- El patrón facial incorpora una marca de tiempo para evitar fraudes de reutilización

Así mismo la compañía FacePhi ofrece diversas soluciones en áreas bancarias, gubernamentales y de seguridad tales como:

- Prevención de Fraudes
- Videovigilancia
- Reconocimiento en Cajeros automáticos
- Banca Online y móvil
- Verificación de firma

Figura 6. Captura de pantalla Selphi

Fuente: FacePhi. [Consultado el 01 de febrero del 2018]. Disponible en: https://www.facephi.com/en/

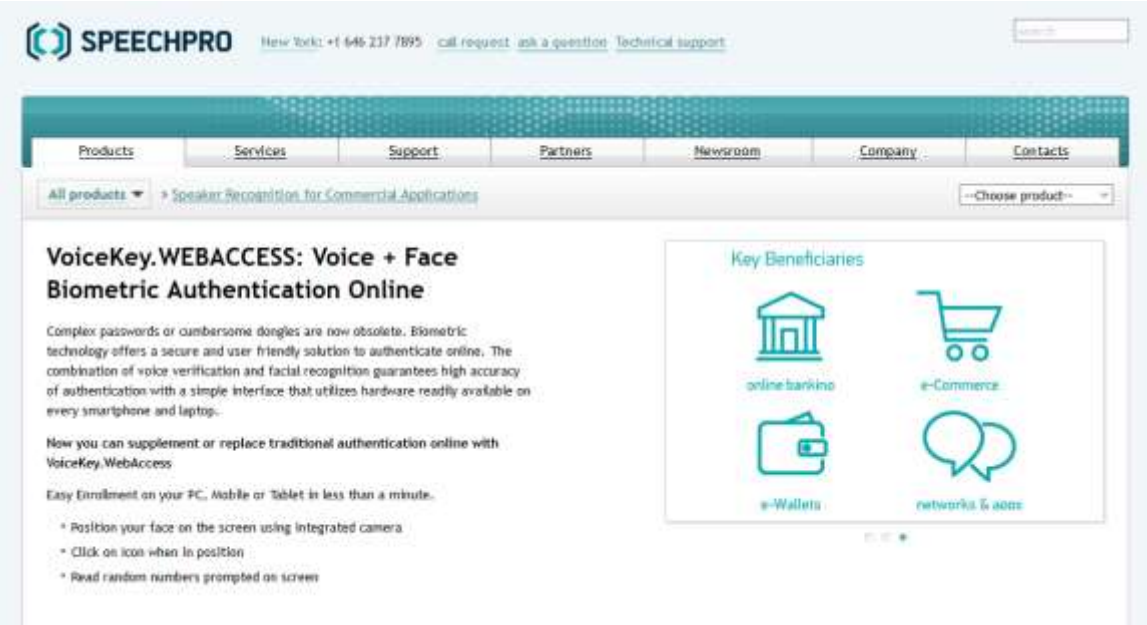
2.3.5 Voicekey.webaccess. VoiceKey.WEACCESS es un producto desarrollado por la compañía Speechpro, su característica principal es que permite la identificación de una persona en la web a través de tres métodos de verificación biométrica:

- Autenticación de voz

- Reconocimiento facial
- Detección de “vitalidad”

Su uso está adaptado a computadores, tabletas y celulares, el registro es rápido (menos de un minuto) y tiene una alta precisión debido a la fusión de biometría facial y de voz.

Figura 7. Captura de pantalla Voicekey.webaccess



Fuente: SpeechPro. [Consultado el 01 de febrero del 2018]. Disponible en: http://speechpro-usa.com/product/voice_authentication/voicekey-webaccess

2.4 HERRAMIENTAS

A continuación, se dará una introducción de cada una de las herramientas con las que se desarrolló el proyecto, así mismo se mencionan las herramientas que se tomaron en cuenta para la implementación del reconocimiento facial y de voz sobre las cuales se realizó exploración y ejecución de cada una y en base a pruebas y diferentes criterios se eligió la mejor (tanto para facial y voz) para llevar a cabo el desarrollo del módulo web de autenticación biométrica.

2.4.1 Apis. Application Programming Interface / Interfaz de programación de aplicaciones es un conjunto de subrutinas, procedimientos y métodos que ofrecen ciertas funciones que pueden ser utilizadas por otro software.[5]

2.4.2 Php. PHP (acrónimo recursivo de PHP: Hypertext Pre-processor) es un lenguaje de programación de uso general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico. Fue uno de los primeros lenguajes de programación del lado del servidor que se podían incorporar directamente en el documento HTML en lugar de llamar a un archivo externo que procese los datos. El código es interpretado por un servidor web con un módulo de procesador de PHP que genera la página web resultante.[6]

Lo que distingue a PHP de algo del lado del cliente como JavaScript es que el código es ejecutado en el servidor, generando HTML y enviándolo al cliente. El cliente recibirá el resultado de ejecutar el script, aunque no se sabrá el código subyacente que era. El servidor web puede ser configurado incluso para que procese todos los ficheros HTML con PHP, por lo que no hay manera de que los usuarios puedan saber qué se tiene debajo de la manga.

2.4.3 NetBeans. NetBeans IDE es un entorno de desarrollo - una herramienta para que los programadores puedan escribir, compilar, depurar y ejecutar programas. Está escrito en Java - pero puede servir para cualquier otro lenguaje de programación. Existe además un número importante de módulos para extender el NetBeans IDE. NetBeans IDE es un producto libre y gratuito sin restricciones de uso.[7]

---

[5] COLABORADORES DE WIKIPEDIA. Interfaz de programación de aplicaciones [En línea]. Wikipedia, La enciclopedia libre, 2018 (Recuperado en 09 de septiembre 2017). Disponible en https://es.wikipedia.org/w/index.php?title=Interfaz_de_programaci%C3%B3n_de_aplicaciones&oldid=104391567

[6] COLABORADORES DE WIKIPEDIA. PHP [En línea]. Wikipedia, La enciclopedia libre, 2018 (Recuperado en 09 de septiembre 2017). Disponible en https://es.wikipedia.org/w/index.php?title=PHP&oldid=105430889

[7] COLABORADORES DE WIKIPEDIA. PHP [En línea]. Wikipedia, La enciclopedia libre, 2018 (Recuperado en 09 de septiembre 2017). Disponible en https://es.wikipedia.org/w/index.php?title=NetBeans&oldid=105844657

NetBeans es un proyecto de código abierto de gran éxito con una gran base de usuarios, una comunidad en constante crecimiento, y con cerca de 100 socios en todo el mundo. Sun Microsystems fundó el proyecto de código abierto NetBeans en junio de 2000 y continúa siendo el patrocinador principal de los proyectos (Actualmente Sun Microsystems es administrado por Oracle Corporation).

NetBeans permite crear aplicaciones Web con PHP 5, un potente debugger integrado y además viene con soporte para Symfony un gran framework MVC escrito en php. Al tener también soporte para AJAX, cada vez más desarrolladores de aplicaciones LAMP o WAMP, están utilizando NetBeans como IDE.

2.4.4 Xammp. XAMPP es un paquete de instalación independiente de plataforma, software libre, que consiste principalmente en el sistema de gestión de bases de datos MySQL, el servidor web Apache y los intérpretes para lenguajes de script: PHP y Perl.[8]

El programa se distribuye bajo la licencia GNU y actúa como un servidor web libre, fácil de usar y capaz de interpretar páginas dinámicas. Actualmente XAMPP está disponible para Microsoft Windows, GNU/Linux, Solaris y Mac OS X.

Como ventaja frente a descargar e instalar cada componente por separado y a crear o editar sus ficheros de configuración manualmente, XAMPP sólo requiere una pequeña fracción del tiempo necesario para descargar y ejecutar un archivo ZIP, tar, exe o fkl (pudiendo encontrarse o en versión completa como en una versión más ligera, que es portable), permitiendo configurar los componentes necesarios del servidor web mediante una misma y sencilla interfaz web. XAMPP

[8] COLABORADORES DE WIKIPEDIA. XAMMP [En línea]. Wikipedia, La enciclopedia libre, 2018 (Recuperado en 09 de septiembre 2017). Disponible en https://es.wikipedia.org/w/index.php?title=XAMPP&oldid=105080893

se actualiza regularmente para incorporar las últimas versiones de Apache/MySQL/PHP y Perl. También incluye otros módulos como Open SSL y PhpMyAdmin.

2.4.5 Sql. SQL (por sus siglas en inglés Structured Query Language; en español lenguaje de consulta estructurada) es un lenguaje específico del dominio que da acceso a un sistema de gestión de bases de datos relacionales que permite especificar diversos tipos de operaciones en ellos. Una de sus características es el manejo del álgebra y el cálculo relacional que permiten efectuar consultas con el fin de recuperar, de forma sencilla, información de bases de datos, así como hacer cambios en ellas.[9]

Originalmente basado en el álgebra relacional y en el cálculo relacional, SQL consiste en un lenguaje de definición de datos, un lenguaje de manipulación de datos y un lenguaje de control de datos. El alcance de SQL incluye la inserción de datos, consultas, actualizaciones y borrado, la creación y modificación de esquemas y el control de acceso a los datos.

2.4.6 Phpmyadmin. PhpMyAdmin es una herramienta escrita en PHP con la intención de manejar la administración de MySQL a través de páginas web, utilizando Internet. Actualmente puede crear y eliminar Bases de Datos, crear, eliminar y alterar tablas, borrar, editar y añadir campos, ejecutar cualquier sentencia SQL, administrar claves en campos, administrar privilegios, exportar datos en varios formatos y está disponible en 72 idiomas. Se encuentra disponible bajo la licencia GPL Versión 2.[10]

Este proyecto se encuentra vigente desde el año 1998, siendo el mejor evaluado en la comunidad de descargas de SourceForge.net como la descarga del mes

[9] COLABORADORES DE WIKIPEDIA. PHP [En línea]. Wikipedia, La enciclopedia libre, 2018 (Recuperado en 09 de septiembre 2017). Disponible en https://es.wikipedia.org/w/index.php?title=SQL&oldid=105570196

[10] COLABORADORES DE WIKIPEDIA. PhpMyAdmin [En línea]. Wikipedia, La enciclopedia libre, 2018 (Recuperado en 09 de septiembre 2017). Disponible en https://es.wikipedia.org/w/index.php?title=PhpMyAdmin&oldid=105798509

de diciembre del 2002. Como esta herramienta corre en máquinas con Servidores Webs y Soporte de PHP y MySQL, la tecnología utilizada ha ido variando durante su desarrollo.

2.4.7 Git y github. Git (pronunciado "guit") es un software de control de versiones diseñado por Linus Torvalds, pensando en la eficiencia y la confiabilidad del mantenimiento de versiones de aplicaciones cuando éstas tienen un gran número de archivos de código fuente. Al principio, Git se pensó como un motor de bajo nivel sobre el cual otros pudieran escribir la interfaz de usuario o front end como Cogito o StGIT. Sin embargo, Git se ha convertido desde entonces en un sistema de control de versiones con funcionalidad plena.[11]

GitHub es una forja (plataforma de desarrollo colaborativo) para alojar proyectos utilizando el sistema de control de versiones Git. Utiliza el framework Ruby on Rails por GitHub, Inc. (anteriormente conocida como Logical Awesome). Desde enero de 2010, GitHub opera bajo el nombre de GitHub, Inc. El código se almacena de forma pública, aunque también se puede hacer de forma privada, creando una cuenta de pago.

2.4.8 Uml. El lenguaje unificado de modelado (UML, por sus siglas en inglés, Unified Modelling Language) es el lenguaje de modelado de sistemas de software más conocido y utilizado en la actualidad; está respaldado por el Object Management Group (OMG).[12]

2.4.9 Materialize. Es un framework de CSS que sigue la ideología de material design, el cual es un lenguaje de diseño creado y diseñado por Google, lo que

[11] COLABORADORES DE WIKIPEDIA. Git [En línea]. Wikipedia, La enciclopedia libre, 2018 (Recuperado en 09 de septiembre 2017). Disponible en https://es.wikipedia.org/w/index.php?title=Git&oldid=105649021

[12] COLABORADORES DE WIKIPEDIA. Lenguaje unificado de modelado [En línea]. Wikipedia, La enciclopedia libre, 2018 (Recuperado en 09 de septiembre 2017). Disponible en https://es.wikipedia.org/w/index.php?title=Lenguaje_unificado_de_modelado&oldid=104947251

busca unificar la experiencia de usuario en cualquier plataforma, lo que permite asegurar que el diseño va a funcionar en una amplia gama de navegadores.[13]

2.4.10 Moodle. Es una herramienta de gestión de aprendizaje, de distribución libre escrita en PHP, fue diseñada para darle la posibilidad a los educadores de crear entornos de aprendizaje en línea, permitiéndoles diseñar cursos virtuales donde pueden compartir material de apoyo, realizar exámenes virtuales, comunicar noticias o trabajos, entre muchas otras opciones.[14]

2.5 HERRAMIENTAS DE RECONOCIMIENTO VOCAL

2.5.1 VoiceIt. Es una plataforma de biometría de voz que permite construir e implementar rápidamente soluciones de seguridad. Cualquiera que sea la necesidad de integración, VoiceIt elimina los obstáculos tradicionales de entrada para proporcionar una plataforma de seguridad de voz a un costo razonable.

Sus características principales son:

- Detección de voz.
- Verificación de voz.
- Integración con diferentes lenguajes.
- Documentación de la API.
- iOS SDK and Cordova Plugin

Los lenguajes permitidos para la implementación y uso de la API son: C++, cURL, C#, Python, Perl, Go, PHP, Java, Node.JS, Ruby, Swift y Obj-c.

Esta lista se encuentra disponible en la página oficial, basta con seleccionar un lenguaje y podremos observar los métodos con los cuales podremos trabajar y un pequeño pedazo de código para la implementación de este.

[13] MATERIALIZECSS. About Materialize [En línea]. Materializecss, 2018 (Recuperado en 13 de septiembre 2017). Disponible en http://materializecss.com/about.html
[14] COLABORADORES DE WIKIPEDIA. Moodle [En línea]. Wikipedia, La enciclopedia libre, 2018 (Recuperado en 09 de septiembre 2017). Disponible en https://es.wikipedia.org/w/index.php?title=Moodle&oldid=105837357

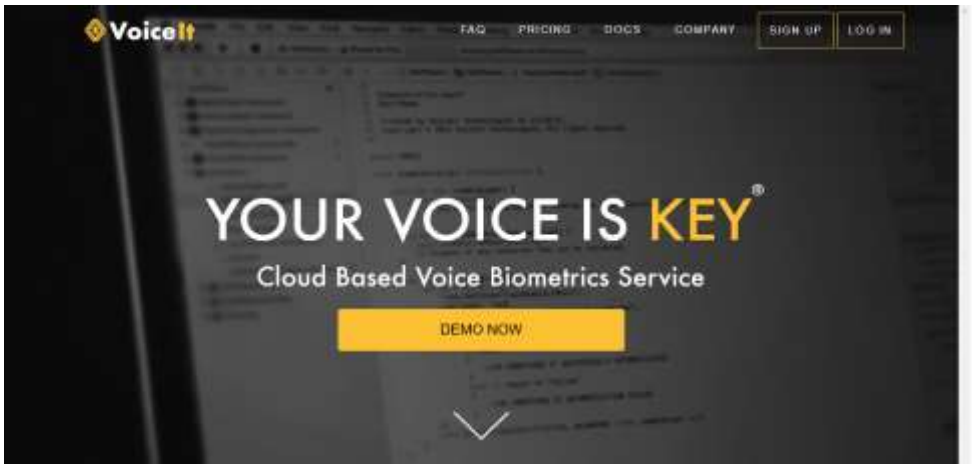
Para empezar a trabajar con la API es necesario el developerID al cual es posible acceder mediante registro, este nos permite trabajar con la API y hacer llamadas o interactuar con la misma gratuitamente por un periodo de un mes.

Todas las respuestas dadas por la API son en formato JSON, en el cual se nos informa del tipo de operación y sobre el resultado de esta. Con dichas respuestas es posible tomar decisiones para trabajar en nuestro proyecto.

Las mayores ventajas de VoiceIt son: la facilidad de su implementación, la amplia opción de lenguajes disponibles sobres los cuales se puede hacer el desarrollo y la plataforma a nuestra disposición sobre la cual se puede administrar información de los usuarios, ver el historial de la actividad e incluso oír los audios cargados por cada usuario.

Todo esto sumado a la opción de la prueba gratuita durante un periodo de un mes facilita no solo la implementación sino las pruebas del servicio y nos permite llegar a estimar que se podría hacer con las herramientas que están a nuestra disposición, esto con el fin de hacer un análisis antes de tomar una decisión sobre un pago por los servicios de dicha plataforma.

Figura 8. Captura de pantalla VoiceIt



Fuente: VoiceIt. [Consultado el 01 de febrero del 2018]. Disponible en: http://voiceit.io/

Los costos del servicio son los siguientes:

Cuadro 1. Costos del servicio de la API de VoiceIt

PLAN	DESCRIPCIÓN	COSTO EN USD	COSTO EN COP
Silencioso (Silence)	Ilimitado por 30 días	0	0
Susurro (Whisper)	1 - 10.000 Llamadas por mes	$0,025 por llamada	$70,17 por llamada
Hablar (Speak)	10.001 - 75.000 Llamadas por mes	$0,02 por llamada	$ 56,13 por llamada
Gritar (Shout)	Sobre 75.000 Llamadas por mes	Mediante contacto	Mediante contacto

Fuente: VoiceIt. [Consultado el 01 de febrero del 2018]. Disponible en: https://voiceit.io/pricing

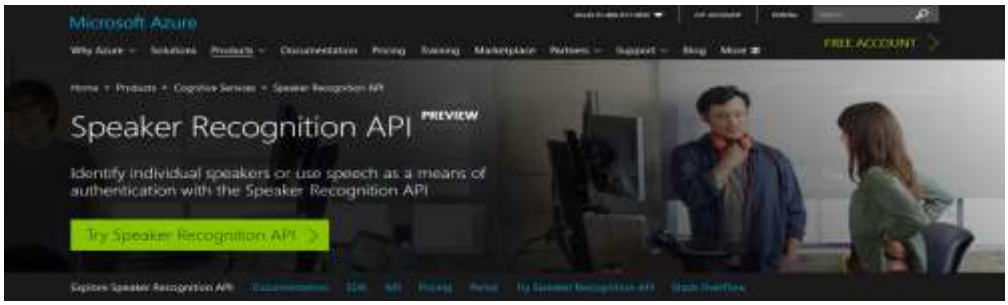
Cada llamada tiene un valor de 0,025 centavos de dólar, por lo tanto 40 llamadas a la API tendrían un costo de 1 dólar. Esto dependiendo del plan contratado el cual reduce los costos según la cantidad de llamadas en el mes.

Estas llamadas incluyen desde el registro de usuarios en la plataforma hasta la autenticación de usuarios, en general todo lo que implique llamadas al servidor de autenticación biométrica será tenido en cuenta en el momento del cobro.

2.5.2 Microsoft Speaker Recognition. Microsoft Speaker Recognition API es una herramienta que se puede utilizar en diversas aplicaciones para potenciar una verificación inteligente e identificar si el orador es quien dice ser.

La API se puede utilizar para determinar la identidad de un hablante desconocido. El audio de la voz desconocida se compara contra un grupo de hablantes seleccionados, y en el caso de que haya encontrado una coincidencia, se devuelve la identidad del hablante.

Figura 9. Captura de pantalla Microsoft Speaker Recognition



Fuente: Microsoft Azure. [Consultado el 01 de febrero del 2018]. Disponible en: https://azure.microsoft.com/en-us/services/cognitive-services/speaker-recognition/

Sus características principales son:

- Detección de voz.
- Verificación de voz.
- Integración con diferentes lenguajes.
- Documentación de la API.

Al igual que con el uso de otras APIs Microsoft Speaker Recognition devuelve la respuesta de sus operaciones en un JSON el cual trae información del tipo de operación ejecutada y el estado de esta con lo cual podemos tomar distintas decisiones para el desarrollo de nuestro proyecto.

Figura 10. Ejemplo de resultados de la herramienta Microsoft Speaker Recognition

Fuente: Microsoft Azure. [Consultado el 01 de febrero del 2018]. Disponible en: https://azure.microsoft.com/en-us/services/cognitive-services/speaker-recognition/

En la anterior imagen podemos ver un ejemplo de la identificación por medio de la voz y la respuesta que arroja la API en JSON, este ejemplo se encuentra en la página principal de Speaker Recognition API, donde además encontramos un demo de verificación en el cual se nos permite agregar tres grabaciones y verificar nuestra identidad por medio de esta.

Uno de los mayores inconvenientes del uso de esta herramienta es su integración, ya que, aunque la herramienta cuenta buena documentación sobre el uso de esta, se encuentran pocos ejemplos de implementación o ayuda para el desarrollador en el momento de la integración. Por esto y más cuestiones técnicas como la petición del "*Binary data"* del archivo de audio a usar, se dificulta más el trabajo con dicha API y se hace tedioso cualquier tipo de pruebas.

En cuanto a costos Microsoft ofrece diferentes rangos de precios:

Cuadro 2. Costos del servicio de la API de Microsoft

Número de transacciones	**Costo en USD (por 1000 transacciones)**	**Costo en COP (por 1000 transacciones)**
0 - 50.000	$5	$ 14.033,35
50.001 - 100.000	$4,50	$ 12.630,02
100,001 - 250,000	$4	$ 11.226,68
250,001 - 500,000 $3.50	$3,50	$ 9.823,35
> 500,000	$3	$ 8.420,01

Fuente: Microsoft Azure. [Consultado el 01 de febrero del 2018]. Disponible en: https://azure.microsoft.com/en-us/pricing/details/cognitive-services/speaker-recognition-api/

Además de estos precios, se puede conectar a la API de manera gratuita para realizar pruebas básicas. Los precios mostrados en la tabla corresponden a cada 1000 transacciones por mes, lo cual varía dependiendo del uso de la herramienta.

2.5.3 VeriSpeak. VeriSpeak a diferencia de las demás herramientas mencionadas hasta el momento es un SDK (kit de desarrollo de software) el cual nos ofrece diferentes posibilidades si comparamos con las APIs, la más importante sería el desarrollo de una herramienta local o en línea la cual no dependa únicamente de una plataforma o proveedor lo cual nos daría más libertad a la hora de trabajar y comercializar el producto.

Este SDK desarrollado por *Neurotechnology* que además proporciona algoritmos y productos de desarrollo de software para reconocimiento biométrico de huellas dactilares, cara, iris, reconocimiento de voz y palma, visión basada en computadora y reconocimiento de objetos a empresas de seguridad.

Figura 11. Captura de pantalla VeriSpeak

Fuente: Neurotechnology. [Consultado el 01 de febrero del 2018]. Disponible en: http://www.neurotechnology.com/verispeak.html

La tecnología de identificación de voz VeriSpeak está diseñada para desarrolladores e integradores de sistemas biométricos. El algoritmo de

reconocimiento de locutor dependiente del texto garantiza la seguridad del sistema comprobando la autenticidad de la voz y la frase. Las plantillas de huella vocal pueden combinarse en modos 1 a 1 (verificación) y 1 a muchos (identificación).

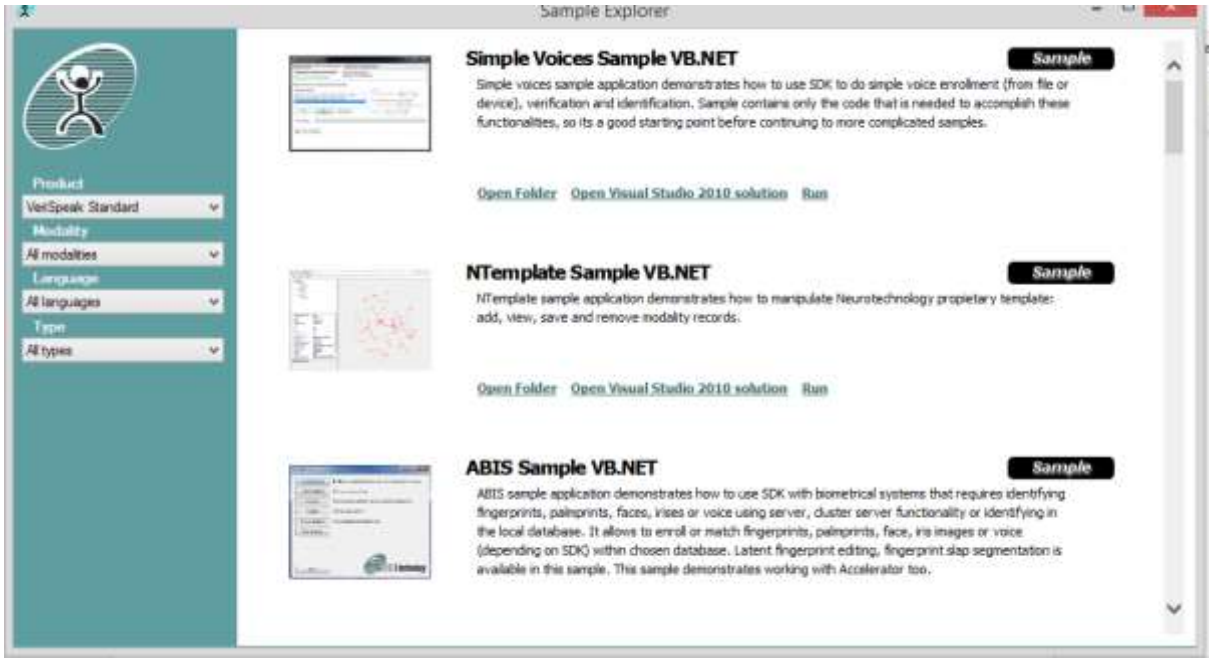
Entre sus características principales se destaca:

- El algoritmo dependiente del texto evita el acceso no autorizado con una voz de usuario grabada previamente.
- Autenticación de dos factores mediante la comprobación de la biometría de voz y autenticidad de frase.
- Los micrófonos regulares y los teléfonos inteligentes son adecuados para grabar voces de usuario.
- Disponible como un SDK multiplataforma que admite varios lenguajes de programación.
- Precios razonables, licencias flexibles y soporte al cliente gratuito.

Al igual que las herramientas mencionadas anteriormente, el SDK de veriSpeak posee una versión de Trial por un periodo de 30 días en el que se incluyen ejemplos de ejecución para cada una de las funcionalidades del SDK, entre ellas VeriSpeak.

Esta versión de trial con sus ejemplos puede ser descargada de la página oficial de *neurotechnology* e instalada en cualquier equipo en donde se quieran ejecutar los ejemplos disponibles.

Figura 12. Ejemplos de la herramienta VeriSpeak



Fuente: VeriSpeak software - Biometric technology demo applications. [consultado el 10 de diciembre del 2017]. Disponible en: http://www.neurotechnology.com/download.html

En la imagen anterior podemos ver el explorador de ejemplos en donde encontramos diferentes ejecutables para cada uno de los SDKs disponibles, entre estos VeriSpeak. El ejemplo disponible permite guardar unas voces por medio del micrófono o por medio de archivos pregrabados y posteriormente verificar o identifican una de estas voces.

En cuanto a costos veriSpeak ofrece dos modelos de licencias, una para la versión estándar y otra para la versión extendida.

Cuadro 3. Costos de la herramienta VeriSpeak.

Versión SDK	**Costo en EUR**	**Costo en COP**
Estándar	339.00	$ 1’172.054,83
Extendida	859.00	$ 2’969.897,06

Fuente: Neurotechnology. [Consultado el 01 de febrero del 2018]. Disponible en: http://www.neurotechnology.com/prices-verispeak.html

Las licencias estándar y extendida varían en la cantidad de componentes y opciones disponibles para el desarrollo. Un SDK a diferencia de una API no tiene interacción alguna con un servidor externo y permite el desarrollo de cualquier herramienta integrando la tecnología de reconocimiento, dicho software ejecutará todo localmente o en el lado del usuario lo cual da más control sobre el desarrollador y abre un poco más las opciones de aplicación para esta tecnología. Por otro lado, la licencia posee un costo fijo el cual hay que considerar si realmente se quiere trabajar con dicha herramienta, este valor contrasta un poco al valor del uso de las API el cual solo depende de las llamadas o interacciones con la plataforma haciendo que el costo para una cantidad baja de operación sea relativamente bajo.

2.6 HERRAMIENTAS DE RECONOCIMIENTO FACIAL

2.6.1 Amazon Rekognition. Amazon Rekognition es un servicio que facilita la adición de análisis de imágenes en aplicaciones. Con Rekognition se pueden detectar objetos, escenas y caras en imágenes. También es posible buscar y comparar rostros e identificar contenido inapropiado. Sus características principales son:

- Detección de objetos y escenas.
- Moderación de imágenes.
- Análisis facial.
- Comparación de rostros.
- Reconocimiento facial.
- Administración vía API, Consola o línea de comandos.
- Seguridad administrativa.
- Privacidad de datos.
- Documentación de la API.

Con esta herramienta se tiene la posibilidad de integrar diferentes servicios ofrecidos por Amazon, entre estos se encuentra Amazon S3, que es un servicio de almacenamiento en la nube en donde se alojarán todas las imágenes que sean analizadas por la API.

Figura 13. Captura de pantalla Amazon Rekognition

Fuente: Amazon Web Services. [Consultado el 01 de febrero del 2018]. Disponible en: https://aws.amazon.com/es/rekognition/

Amazon Rekognition tiene soporte para diversos lenguajes de programación entre los que se encuentran: Android, JavaScript, iOS, Java, .Net, Node.js, PHP, Ruby y Python. Además, cuenta con una gran documentación y ejemplos, lo que facilita empezar o adaptar cualquier proyecto con la API.

Al igual que otras herramientas Amazon Rekognition genera los resultados en formato JSON, lo que permite tener los datos de forma ordenada y de fácil acceso, así mismo, Amazon cuenta con diferentes funciones preestablecidas, como detectar rostros, comparar, rostros, detectar texto, buscar rostros, entre muchas otras.

Amazon Web Services ofrece un año de prueba gratis, donde se podrán usar diferentes servicios, en los que se incluye Amazon Rekognition, después de este

periodo se prueba se empezará a realizar un cobro por el uso de los servicios, los costos son los siguientes:

Cuadro 4. Costos de la herramienta Amazon Rekognition

Capa de análisis de imágenes	Precio en USD por 1000 imágenes procesadas	Precio en COP por 1000 imágenes procesadas*
Primer millón de imágenes procesadas al mes	$1,00	$2.777,7778
Siguientes 9 millones de imágenes procesadas al mes	$0,80	$2.222,2222
Siguientes 90 millones de imágenes procesadas al mes	$0,60	$1666,6666
Más de 100 millones de imágenes procesadas al mes	$0,40	$1111,1111
Al realizar la inscripción por primera vez, los nuevos usuarios hacen parte de la capa gratuita de AWS donde podrán analizar un máximo de 5000 imágenes al mes sin ningún costo, durante los primeros 12 meses.		

Fuente: Amazon Web Services. [Consultado el 01 de febrero del 2018]. Disponible en: https://aws.amazon.com/es/rekognition/pricing/

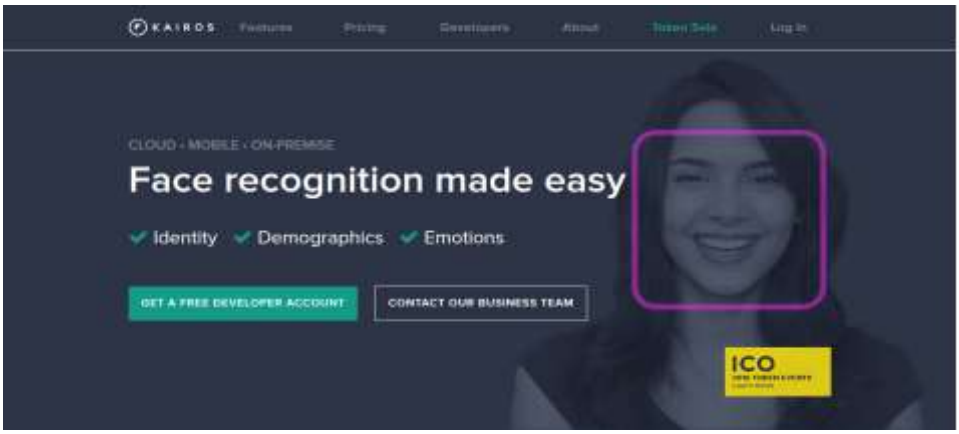
2.6.2 Kairos. Kairos es una empresa de inteligencia artificial especializada en el reconocimiento facial. A través de la visión por computadora y machine learning, Kairos puede reconocer caras en videos, fotos y en el mundo real. Sus características principales son:

- Detección de rostros.
- Identificación de rostros.
- Verificación de rostros.
- Detección de emociones.

- Detección de edad.
- Detección de género.
- Detención multi-facial.
- Detección de etnicidad.
- Documentación de la API.

Kairos ofrece realizar un cambio radical en nuestros proyectos con la ayuda de estas características, con las cuales se pueden maximizar el valor de los recursos digitales tales como videos o imágenes, permitiendo etiquetar personas y realizar una búsqueda rápida de un individuo específico, así mismo promete mejorar la seguridad usando reconocimiento facial de alta calidad.

Figura 14. Costos de la herramienta Amazon Rekognition



Fuente: Kairos. [Consultado el 01 de febrero del 2018]. Disponible en: https://www.kairos.com/

Kairos ofrece su servicio a través de SDK y API, el primer método está orientado a desarrollos que no necesiten conexión a internet como un sistema de acceso a un inmueble o ingreso a un dispositivo de forma local, el segundo se enfoca más en desarrollo en entornos web.

Ambos tipos de servicios cuentan con una gran documentación y ejemplos, la API de Kairos puede ser integrada en diferentes lenguajes de programación, tales como: PHP, Python, Ruby, Node.js, JavaScript, PHP, Python y .NET.

La API genera los resultados en formato JSON, donde se almacenan la cantidad de rostros encontrados, sus atributos, estimaciones de edad, género, etnia entre otros, la posición de los rasgos importantes, la rotación del rostro y la confidencialidad de detección.

Cuadro 5. Costos herramienta Kairos

Plan	Descripción	Costo en USD mensual	Costo en COP mensual
Personal+	API:	$500	$1’388.888,89
Business	API:	$3000	$8’333.333,33
Enterprise	API y SDK:	Personalizado	Personalizado

Fuente: Kairos. [Consultado el 01 de febrero del 2018]. Disponible en: https://www.kairos.com/pricing

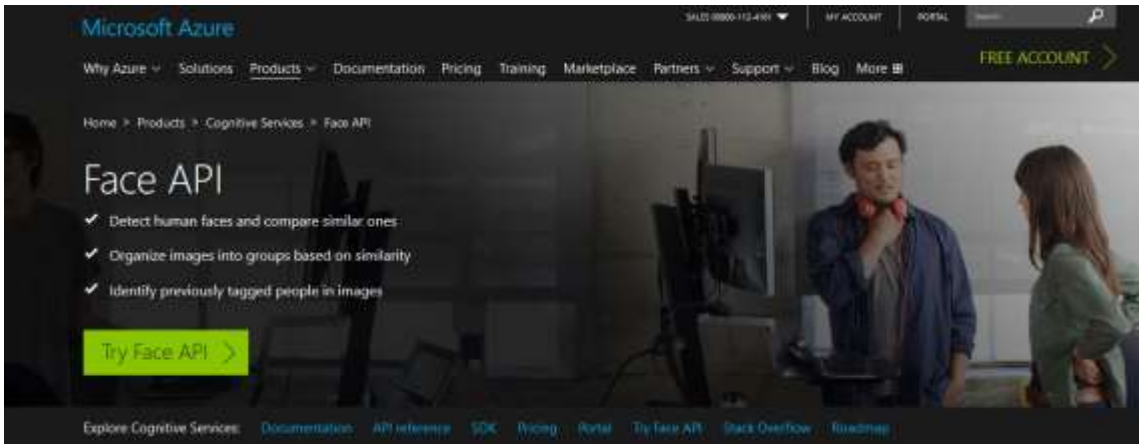
2.6.3 Microsoft - Face API. Microsoft Cognitive Service APIs, es un conjunto de soluciones mediante APIs, divididas en áreas como visión, habla, lenguaje y conocimiento.

En el área de visión se encuentra Face API, sus características principales son:

- Detección de rostros.
- Verificación de rostros.
- Identificación de rostros.
- Búsqueda similar de rostros.
- Detección de edad.
- Detección de género.
- Agrupación de rostros.
- Análisis de video en tiempo casi real.
- Documentación de la API.

La respuesta de esta API retorna la información en formato JSON y muestra datos como, pose de la cara, confidencialidad de detección, aproximación de emociones detectadas, edad estimada del rostro, género estimado, entre otros.

Figura 15. Captura de pantalla Microsoft - Face API



Fuente: Microsoft Azure. [Consultado el 01 de febrero del 2018]. Disponible en: https://azure.microsoft.com/en-us/services/cognitive-services/face/

Algunos de los lenguajes soportados para la integración del api son: PHP, Python, Ruby, JavaScript, C#, Curl, Java y Obj-C; En la página de documentación se pueden encontrar guías y ejemplos en cada uno de los lenguajes anteriormente nombrados.

Microsoft cuenta con este y más servicios en la plataforma Azure, donde cada servicio tiene un costo base diferente, para el caso de Microsoft Face API los precios son los siguiente:

Cuadro 6. Costos de la herramienta Microsoft Face API

Plan	**Características**	**Precio en USD por cada 1000 transacciones**	**Precio en COP por cada mil transacciones**
Free	Hasta 20 transacciones por minuto	30000 transacciones gratuitas al mes	30000 transacciones gratuitas al mes
Standard	Entre 0 y 1’000.000	$1,50	$4.166,6666

	transacciones		
Standard	Entre 1’000.001 y 5’000.000	$1,10	$3.055,5555
Standard	Entre 5’000.001 y 20’000.000 transacciones	$0,65	$1.805,5555
Almacenamiento de rostros	Almacenamiento de imágenes con un tamaño de hasta 4MB cada una	$0,5	$1.388,8888

Fuente: Microsoft Azure. [Consultado el 02 de febrero del 2018]. Disponible en: https://azure.microsoft.com/en-us/pricing/details/cognitive-services/face-api/

2.6.4 OpenCV. OpenCV es una biblioteca libre de visión artificial originalmente desarrollada por Intel. Desde que apareció su primera versión alfa en el mes de enero de 1999, se ha utilizado en infinidad de aplicaciones. Desde sistemas de seguridad con detección de movimiento, hasta aplicaciones de control de procesos donde se requiere reconocimiento de objetos. Esto se debe a que su publicación se da bajo licencia BSD, que permite que sea usada libremente para propósitos comerciales y de investigación con las condiciones en ella expresadas.

Figura 16. Captura de pantalla OpenCV

Fuente: OpenCV. [Consultado el 01 de febrero del 2018]. Disponible en: https://opencv.org/

Cabe mencionar que se hará un estudio de las herramientas y se optará por API o SDK, posteriormente se dará paso a las pruebas de las herramientas escogidas y se seleccionará una en la cual se basará el desarrollo, una vez hecha dicha selección se procederá a desarrollar el escenario de prueba, el prototipo del módulo de autenticación y posteriormente el enlace entre estos dos últimos.

2.7 COMPARACIÓN Y ELECCIÓN DE HERRAMIENTAS DE IDENTIFICACIÓN BIOMÉTRICA

A continuación, se muestra una tabla comparativa entre las diferentes herramientas de reconocimiento biométrico, tendremos en cuenta varios factores que serán fundamentales para el desarrollo del módulo, entre los más importantes encontramos el costo de la herramienta y la facilidad de implementación:

Herramientas de reconocimiento facial:

Cuadro 7. Comparación de herramientas de reconocimiento facial

	Amazon	**Kairos**	**Microsoft**	**OpenCV**
Tipo de herramienta	API	API/SDK	API	Librería
Documentación	Alta	Media	Media	Alta
Licencia	Por llamadas o transacción	Suscripción	Por llamadas o transacción	BSD
Costos por imagen	$1 USD Por cada 1000 imágenes	$500 /mes	$1,5 USD Por cada 1000 imágenes	NA
Periodo de prueba	12 meses	Indefinido	12 meses	NA
Restricción periodo de prueba	5000 imágenes al mes	1500 imágenes al día	$200 USD en crédito	NA
Lenguajes soportados	Android, JavaScript, iOS, Java, .net, Node.js, Php, Ruby, Python.	PHP, Python, Ruby, JavaScript, .Net, Node.js	C#, Curl, Java, JavaScript, Php, Python, Ruby.	C++, C, Python
Facilidad de implementación	Fácil	Medio	difícil	difícil
Almacenamiento de imágenes	Nube	Local	Local	Local

Características añadidas	Múltiples objetivos, género, edad, pose, etiquetas, análisis de video, texto, emociones.	Múltiples objetivos, género, edad, etnia, análisis de video, emociones.	Múltiples objetivos, género, edad, emociones.	Múltiples objetivos, género, edad.

Teniendo en cuenta los anteriores factores se ha decidido trabajar con la herramienta Amazon Rekognition, ya que es la más fácil de implementar en lenguajes de programación orientados al desarrollo web y posee la más amplia documentación, así mismo, tiene muchas características añadidas que pueden ser útiles para posteriores versiones del proyecto, agregado a esto, durante el periodo de prueba también se tiene acceso a Amazon S3, que es una herramienta de almacenamiento que será sumamente útil a la hora de guardar las imágenes analizadas.

Herramientas de reconocimiento vocal:

Cuadro 8. Comparación de herramientas de reconocimiento vocal

	VoiceIt	**Microsoft Speaker recognition**	**VeriSpeak**
Tipo de herramienta	API	API	SDK
Documentación	Alta	Media	Media
Licencia	Por llamadas o transacción	Por llamadas o transacción	Suscripción
Costos por llamada a la API o suscripción (SDK)	$0.025 USD Por cada llamada a la API	por cada 1000 llamadas 5 dólares, disminuye dependiendo de la cantidad de transacciones	€ 339 Versión estándar o € 859 versión extendida.
Periodo de prueba	1 meses	1 mes	1 mes
Lenguajes de programación soportados	C Sharp, VB.net, C++, Python, Perl, Go, PHP, Java, Node.JS, Ruby, Swift, Obj-C	PHP, Python, Ruby, JavaScript, C#, Curl, Java, Obj-C	C, C++, C#, Visual basic.net, Java
Facilidad de implementación	Fácil	Medio	difícil

Almacenamiento de audios	Nube	Nube	Local
Características añadidas	Buen soporte, diferentes métodos ya preestablecidos, diferentes idiomas soportados para la autenticación, posibilidad de añadir la frase de autenticación a nuestro gusto.	La API se puede usar para determinar la identidad de un hablante desconocido	Las plantillas de huella vocal pueden combinarse en modos 1 a 1 (verificación) y 1 a muchos (identificación). Permite el desarrollo de una herramienta local o en línea.

En base a la tabla anterior y a diferentes pruebas para evaluar cada una de las opciones disponibles para el desarrollo del proyecto se eligió una de estas herramientas.

Elegimos VoiceIt por su facilidad para acceder a su periodo de prueba, por su documentación bien explicada para cada uno de los lenguajes la cual detalla los pasos para la integración de la API, por la gran variedad de lenguajes aceptados y finalmente por la sencillez, pero eficacia de su sistema el cual no exige muchos requisitos a la hora de enviar un audio o hacer una llamada a la plataforma.

En el caso de Microsoft Speaker recognition tuvimos demasiados problemas para poder probar la herramienta pues el audio requería un formato específico y por falta de documentación se dificulta obtener ese formato además la documentación no detalla cómo realizar una llamada a la API lo cual hace más difícil entender su funcionamiento. Algo similar sucedió con VeriSpeak pues pone

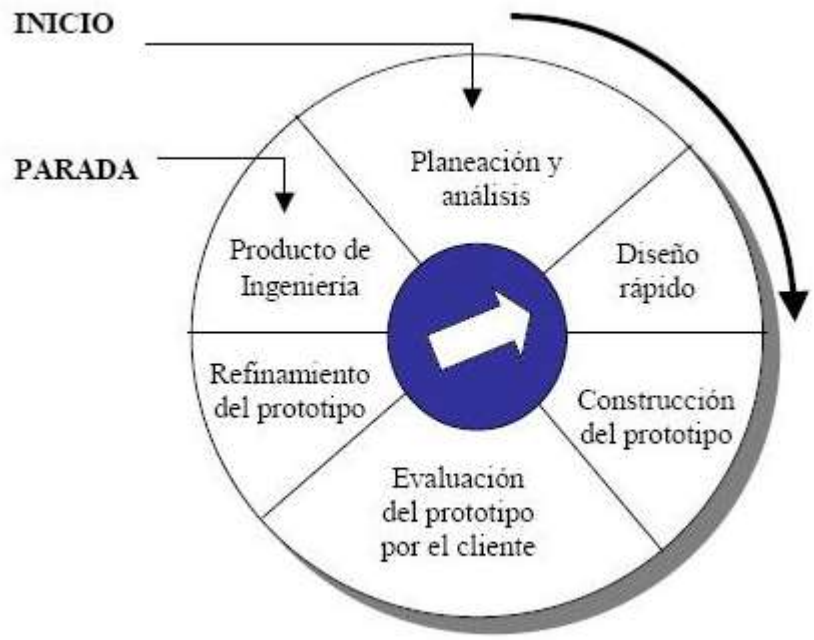
a nuestra disposición un demo, pero no detalla el funcionamiento de este ni de la herramienta.

2.8 METODOLOGÍA

En la ingeniería de software, una metodología de desarrollo de software también conocida como metodología de desarrollo de sistemas es la división del trabajo de desarrollo de software en distintas fases (o etapas) que contienen actividades con la intención de una mejor planificación y gestión.

Modelo de desarrollo evolutivo

Figura 17. Fases del desarrollo evolutivo



Fuente: Zachman, John A. El modelado de las empresas: la arquitectura de Zachman. Zachman Institute for Framework Advancement. Estados Unidos, 1999.

Para el desarrollo de este proyecto se utilizará el modelo de desarrollo evolutivo o prototipado evolutivo. El modelo de desarrollo evolutivo se basa en la creación

de prototipos o versiones incompletas del programa que se está desarrollando. Un prototipo comúnmente expone aspectos o características del software final pero que pueden cambiar durante el desarrollo e incluso no ser iguales en el producto final.[15]

El prototipo tiene varios beneficios: el diseñador de software y el desarrollador puede obtener información relevante de cada uno de los prototipos, principalmente en las etapas iniciales del proyecto. Se pueden realizar comparaciones para comprobar si el software cumple con las especificaciones planteadas. También permite tener una idea de las estimaciones iniciales y si los plazos pactados inicialmente realmente se cumplen.

Este modelo es útil cuando el cliente conoce los objetivos o requisitos generales para el software, también ofrece un mejor enfoque cuando el responsable del desarrollo del software está inseguro de la eficacia de un algoritmo, de la adaptabilidad de un sistema operativo, permite la reutilización del código.

A pesar de que tal vez surjan problemas, este modelo suele ser un paradigma efectivo para la ingeniería del software. La clave es definir las reglas del juego desde el principio.

[15] COLABORADORES DE WIKIPEDIA. Modelo de prototipos [En línea]. Wikipedia, La enciclopedia libre, 2018 (Recuperado en 09 de septiembre 2017). Disponible en https://es.wikipedia.org/w/index.php?title=Modelo_de_prototipos&oldid=103882276

3. ESPECIFICACIÓN DE REQUISITOS

3.1 ESPECIFICACIÓN DE REQUISITOS

Esta sección tiene como propósito definir las especificaciones funcionales, no funcionales y del sistema para la implementación de un módulo web que permita la identificación de usuarios de cursos virtuales a través de reconocimiento biométrico facial y de voz.

Se realizará el diseño y desarrollo del prototipo de módulo web y su ejecución mediante un escenario de prueba (emulador de aula virtual).

El módulo permitirá el ingreso de todos los involucrados al aula virtual (escenario de prueba) verificando sus características biométricas faciales y de voz, en caso de que la autenticación por los métodos biométricos sea fallida el usuario podrá ingresar por medio de contraseña.

El módulo por sí solo no será un gestor de aulas virtuales, ya que las funciones del sistema sólo abarcan el registro y autenticación biométrica de usuarios, los cuales serán redirigidos a las aulas virtuales en las que están inscritos.

El principal beneficio del módulo será la versatilidad otorgada a los usuarios a la hora de autenticarse, ya que para lograrlo bastará capturar las características faciales y vocales a través de la cámara web y el micrófono respectivamente, en caso de que no se tengan estos dispositivos o haya fallos con la autenticación biométrica se da la posibilidad de ingreso por contraseña.
[Se plantea como meta la integración del módulo con aulas virtuales en Moodle, la plataforma más famosa para la creación y administración de cursos.]

Cada usuario tendrá un perfil específico para que su interacción con el módulo sea correcta.

Usuario: Su rol en el sistema consiste en ingresar al aula virtual mediante el módulo de autenticación biométrica, para conseguir esto es necesario realizar el registro como participante con sus datos personales, posteriormente se dará la información para realizar el registro de datos biométricos, procedimiento que será dirigido por el administrador del módulo. Debe tener conocimientos básicos de navegación por páginas web, su educación no puede ser definida.

Administrador: Usuario con gran conocimiento del módulo con capacitación previa por parte de los desarrolladores, encargado de manejar el módulo y realizar el registro biométrico de los demás usuarios de forma presencial para así confirmar su identidad.

3.2 FUNCIONALIDADES

- **Toma de datos personales:** A través de un formulario se adquirirán los datos personales de los usuarios.
- **Toma de datos biométricos:** El administrador de manera presencial y mediante la cámara y el micrófono adquirirá las características faciales y de voz de los usuarios.
- **Registro de usuarios:** Se almacenará la información de los usuarios en una base datos, que a su vez se conecta con el aula virtual.
- **Autenticación biométrica:** Se verificará la identidad de la persona que intenta ingresar al sistema**.**
- **Redirección al aula virtual:** Una vez autenticado el usuario será redirigido al aula virtual la que está vinculado.
- **Ingreso por contraseña:** Se dará la opción de realizar el ingreso al aula virtual mediante contraseña en caso de que la autenticación biométrica falle o no se tengan los dispositivos para la toma de las características biométricas.
- **Verificación de intentos fallidos:** Todo usuario tendrá un número máximo de intentos a la hora de autenticarse ya sea por biometría o contraseña.

- **Eliminación de usuarios:** El administrador tendrá la posibilidad de eliminar usuarios que hayan presentado fallas reiteradas a la hora de autenticarse.
- **Eliminación de huellas biométricas:** El administrador podrá eliminar las huellas de cualquier usuario.
- **Actualización de huellas biométricas:** El administrador serpa capaz de actualizar las huellas biométricas que se hayan tomado de manera errada o estén presentando problemas durante la autenticación de usuarios.
- **Listar usuarios:** El administrador podrá listar todos los usuarios registrados con los datos más relevantes.
- **Búsqueda de usuarios:** El administrador tendrá la capacidad de buscar un usuario mediante el correo electrónico con el que se registró.
- **Visualización de huellas biométricas:** Al seleccionar un usuario específico, el administrador será capaz de visualizar las huellas vocales y la huella facial que se encuentran enlazadas a dicho usuario.
- **Habilitar/Inhabilitar usuarios:** El administrador podrá suspender a los usuarios que hayan pasado un límite de intentos determinados, estos usuarios tendrán que contactarse con el administrador para verificar las huellas biométricas y así reactivar la cuenta.

3.3 CASOS DE USO

Definición de casos de uso. Los casos de uso se crean para refinar un conjunto de requisitos de acuerdo con una función o tarea. En lugar de la tradicional lista de requisitos que quizá no trate de forma directa el uso de la solución, los casos de uso reúnen requisitos comunes basados en el tipo de función u objetivo. Los casos de uso definen qué harán los usuarios o funciones en la solución y un proceso empresarial define cómo realizarán esas funciones.[16]

[16] COLABORADORES DE WIKIPEDIA. Caso de uso [En línea]. Wikipedia, La enciclopedia libre, 2018 (Recuperado en 09 de septiembre 2017). Disponible en https://es.wikipedia.org/w/index.php?title=Caso_de_uso&oldid=105447584

Los diagramas de casos de uso sirven para especificar la comunicación y el comportamiento de un sistema mediante su interacción con los usuarios y/u otros sistemas. O lo que es igual, un diagrama que muestra la relación entre los actores y los casos de uso en un sistema.

Se le llama actor a toda entidad externa al sistema que guarda una relación con éste y que le demanda una funcionalidad. Esto incluye a los operadores humanos, pero también incluye a todos los sistemas externos, además de entidades abstractas, como el tiempo.

Un caso de uso debe:

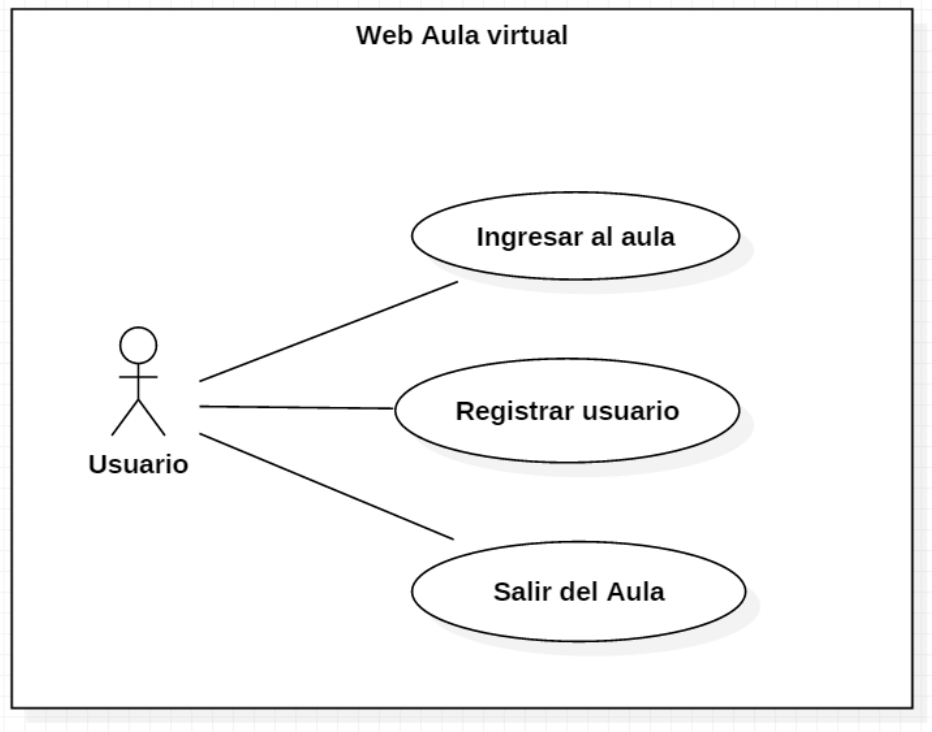
- Describir una tarea del negocio que sirva a una meta de negocio.
- Tener un nivel apropiado del detalle.
- Ser bastante sencillo como que un desarrollador lo elabore en un único lanzamiento.

Los casos de uso pueden ser útiles para establecer requisitos de comportamiento, pero no establecen completamente los requisitos funcionales ni permiten determinar los requisitos no funcionales. Los casos de uso deben complementarse con información adicional como reglas de negocio, requisitos no funcionales, diccionario de datos que complementen los requisitos del sistema.

Diagramas de caso de uso:

Cuadro 9. Caso de uso ingreso al aula virtual

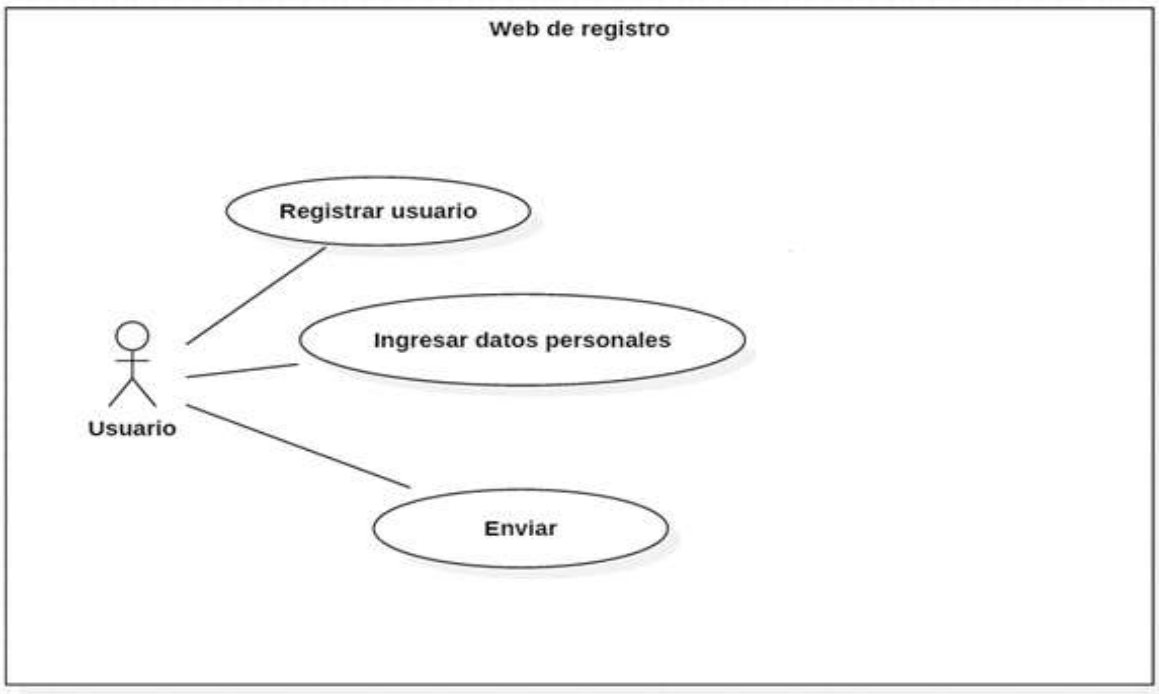
CASO DE USO: Ingreso al aula virtual



Descripción:	En el anterior diagrama se muestran las opciones de interacción que tiene el usuario en su ingreso al aula virtual, entre ellas está Ingresar al aula siempre y cuando el usuario se haya registrado previamente. Además de la opción de ingreso también podrá realizar el registro en donde se tomarán sus datos y posteriormente su información biométrica para así poder realizar comparación y verificación en caso de autenticación biométrica. Esto presentado en un entorno Web el cual brindará un acceso sencillo. La última acción presentada en caso de que el usuario no quiera ingresar ni registrarse es la opción de salir de la página.
Actores principales:	Visitantes, Estudiantes, Tutores.

Flujo de eventos:	Encontrándose en la página: 1. El usuario ve la opción de ingreso y de registro. 2. El usuario se registra o ingresa. 3. ¿El usuario se registra? SI: Ingresa sus datos personales y posteriormente registra su información biométrica. NO: Si el usuario no se registra ni ingresa al aula puede salir de la misma.
Condiciones de entrada:	Haberse registrado previamente o registrarse en el momento para luego agregar su información biométrica.
Condiciones de salida:	Ninguna, si el usuario desea puede salir de la página en cualquier momento.

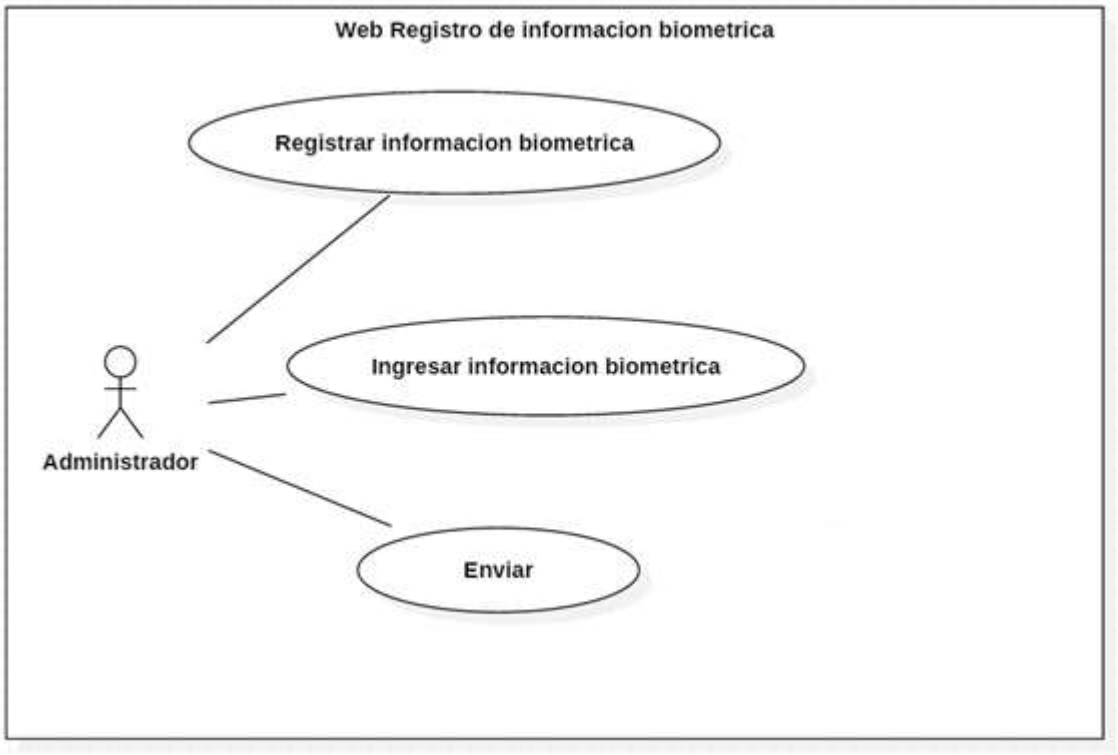
Cuadro 10. Caso de uso registro de usuario

CASO DE USO: Registro de usuario


Descripción:	En el anterior diagrama se muestran las opciones en el momento del registro en el aula y los datos necesarios para el mismo. Una vez ingresada la información necesaria el usuario podrá registrarse en la plataforma.
Actores principales:	Visitantes y Estudiantes.
Flujo de eventos:	Encontrándose en la página: 1. El usuario ingresa al registro. 2. El usuario digita la información requerida. 3. ¿El usuario se registra? SI: Su información es almacenada para su posterior ingreso a la plataforma NO: Si el usuario no se registra puede salir página.
Condiciones de entrada:	No haberse registrado antes para poder realizar el registro satisfactoriamente.
Condiciones de salida:	Ninguna

Cuadro 11. Caso de uso registro de información biométrica

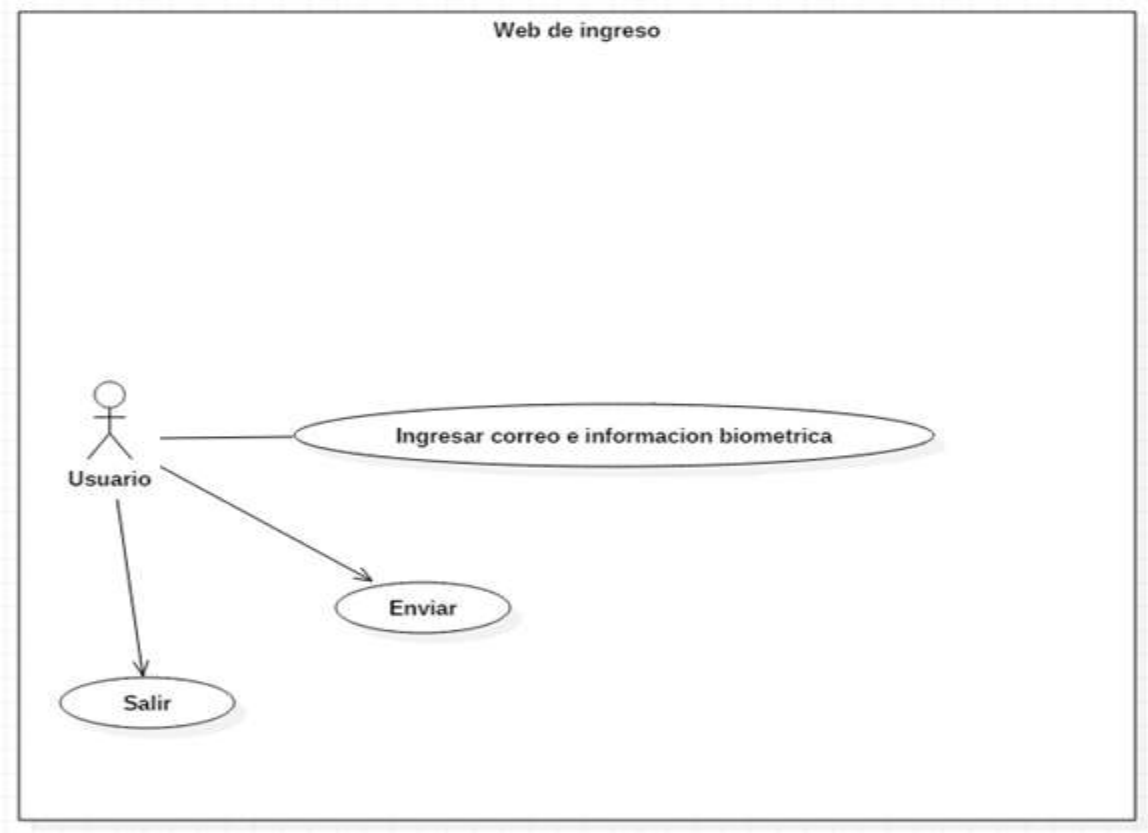
CASO DE USO: Registro información biométrica



Descripción:	El administrador que fue registrado previamente tiene acceso a la opción de registrar la información biométrica de cualquier usuario. Este registro se realiza sencillamente con el correo de cada usuario y los archivos correspondientes a su información biométrica.
Actores principales:	Administrador
Flujo de eventos:	Encontrándose en la página: 1. El administrador ingresa al registro de información biométrica. 2. El usuario autoriza la toma sus características biométricas. 3. Los archivos son enviados y se crea la huella biométrica correspondiente.

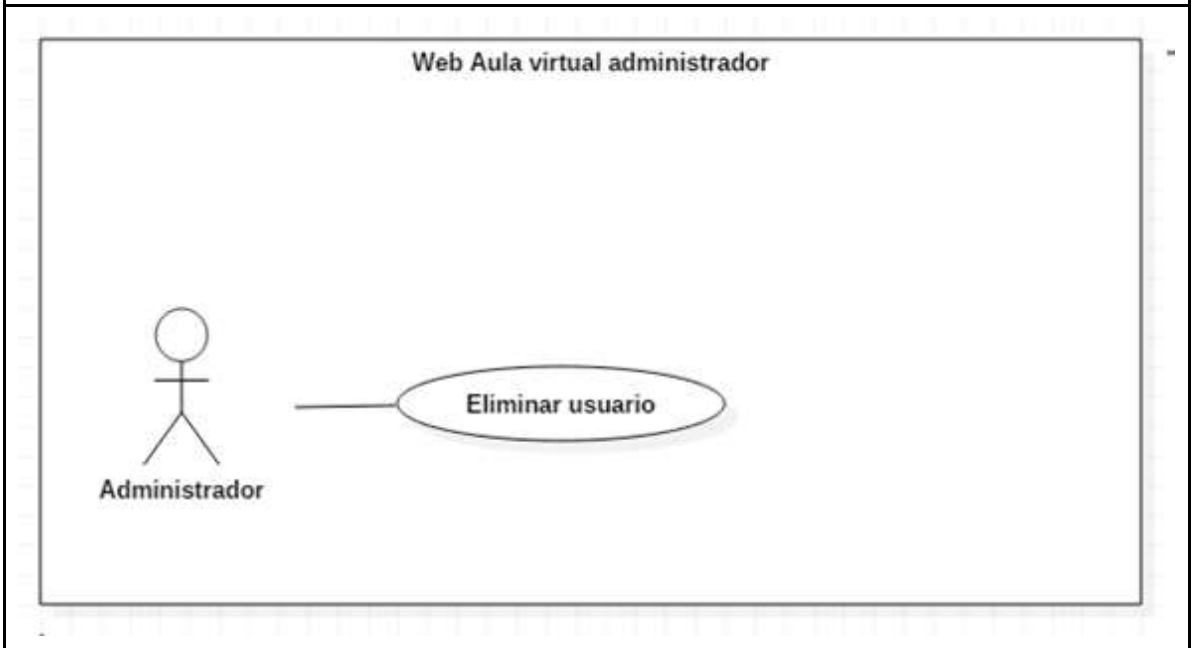
Condiciones de entrada:	Que usuario o estudiante se haya registrado previamente.
Condiciones de salida:	Ninguna

Cuadro 12. Caso de uso ingreso por autenticación biométrica

CASO DE USO: Ingreso por autenticación biométrica	
	
Descripción:	El usuario ya después de haber registrado su información biométrica podrá ingresar al sistema usando sus rasgos biométricos.
Actores principales:	Usuario

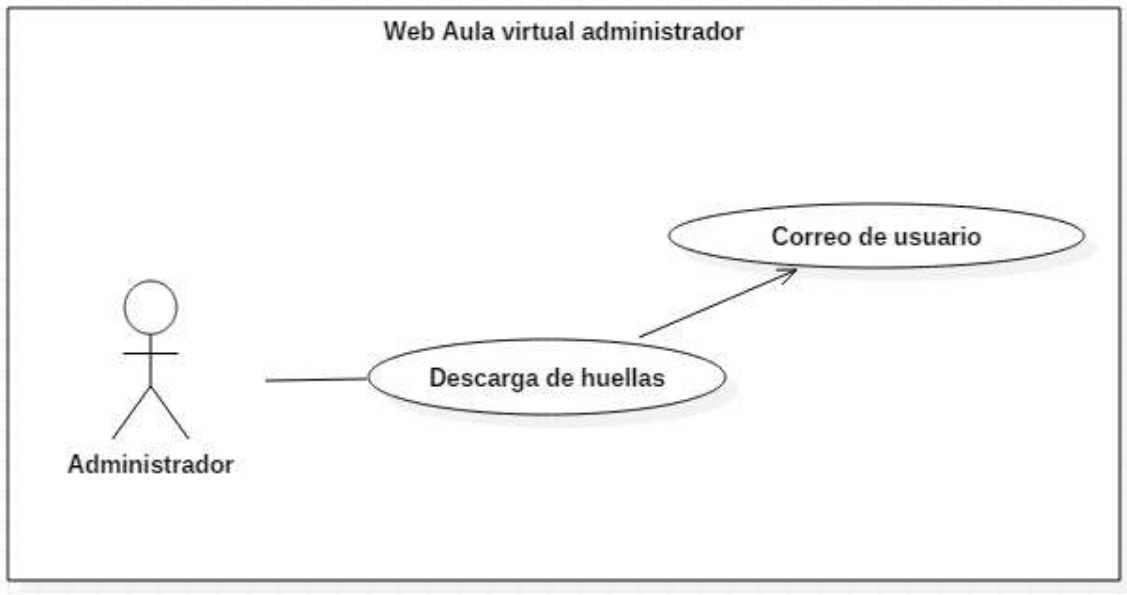
Flujo de eventos:	Encontrándose en la página: 1. El usuario ingresa su correo con el fin de iniciar sesión 2. El usuario autoriza la toma sus características biométricas. 3. Los archivos son enviados y se crea la huella biométrica correspondiente.
Condiciones de entrada:	Que usuario o estudiante se haya registrado previamente.
Condiciones de salida:	Ninguna

Cuadro 13. Caso de uso Eliminación de usuarios

CASO DE USO: Eliminación de usuarios	
	
Descripción:	El administrador puede eliminar usuarios de la plataforma con solo agregar el correo de ese usuario a eliminar.
Actores principales:	Administrador

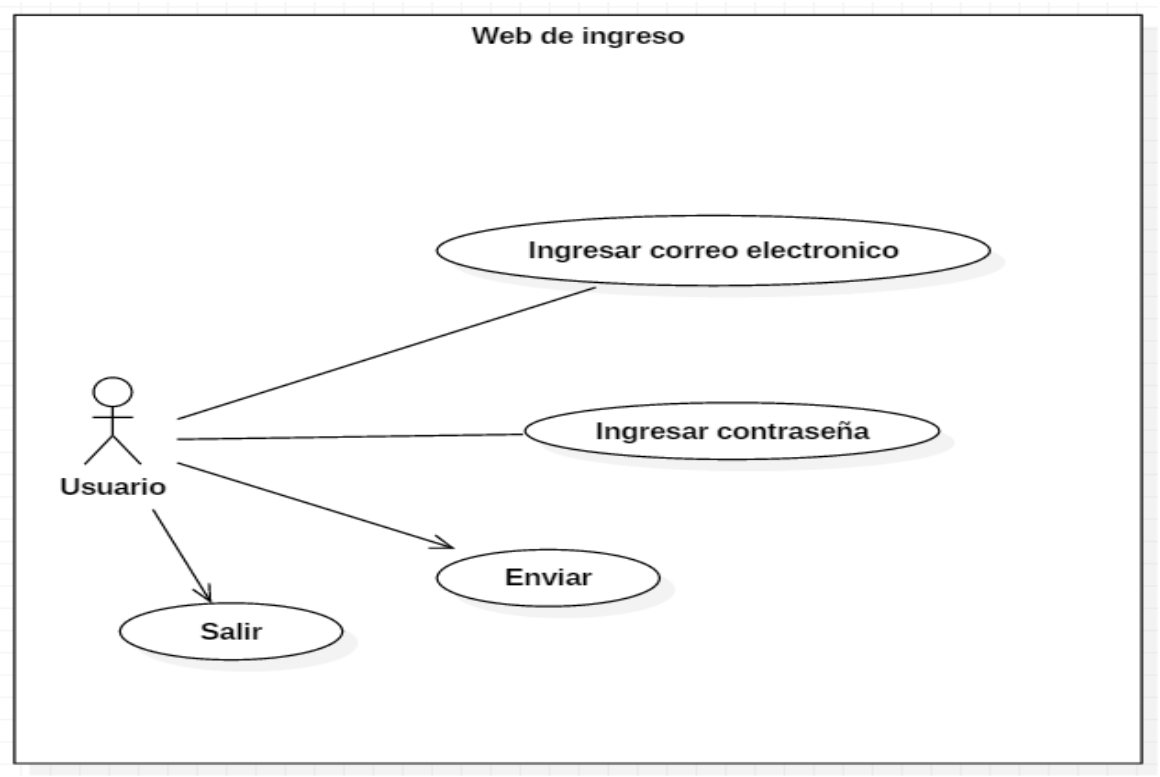
Flujo de eventos:	Encontrándose en la página: 1. El administrador tiene la opción de eliminar un usuario. 2. El administrador agrega el correo del usuario a eliminar.
Condiciones de entrada:	Que usuario o estudiante se haya registrado previamente.
Condiciones de salida:	Que el administrador haya ingresado a la plataforma con sus credenciales. Deberá cerrar sesión y posteriormente salir.

Cuadro 14. Caso de uso descarga de huellas biométricas

CASO DE USO: Descarga de huellas biométricas	
	
Descripción:	El administrador puede descargar las huellas biométricas de un usuario ya sea para verificar su identidad o integridad.
Actores principales:	Administrador

Flujo de eventos:	Encontrándose en la página: 1. El administrador además de la opción de eliminar un usuario podrá descargar sus huellas biométricas 2. El administrador agrega el correo del usuario
Condiciones de entrada:	Que usuario o estudiante se haya registrado previamente.
Condiciones de salida:	Que el administrador haya ingresado a la plataforma con sus credenciales. Deberá cerrar sesión y posteriormente salir.

Cuadro 15. Caso de uso Ingreso por contraseña

CASO DE USO: Ingreso por contraseña	
	
Descripción:	En caso tal de que surja alguna falla de hardware o en la toma de los rasgos biométricos el usuario podrá ingresar al sistema

	haciendo uso de la contraseña que él asignó en el momento del registro.
Actores principales:	Usuario
Flujo de eventos:	Encontrándose en la página: 1. El usuario ingresa su correo con el fin de iniciar sesión 2. El usuario selecciona la opción de ingresar por contraseña. 3. El usuario ingresa la contraseña que estableció al momento del registro.
Condiciones de entrada:	-Que usuario o estudiante se haya registrado previamente. -Fallo en el ingreso por métodos biométricos.
Condiciones de salida:	Ninguna.

4. DISEÑO

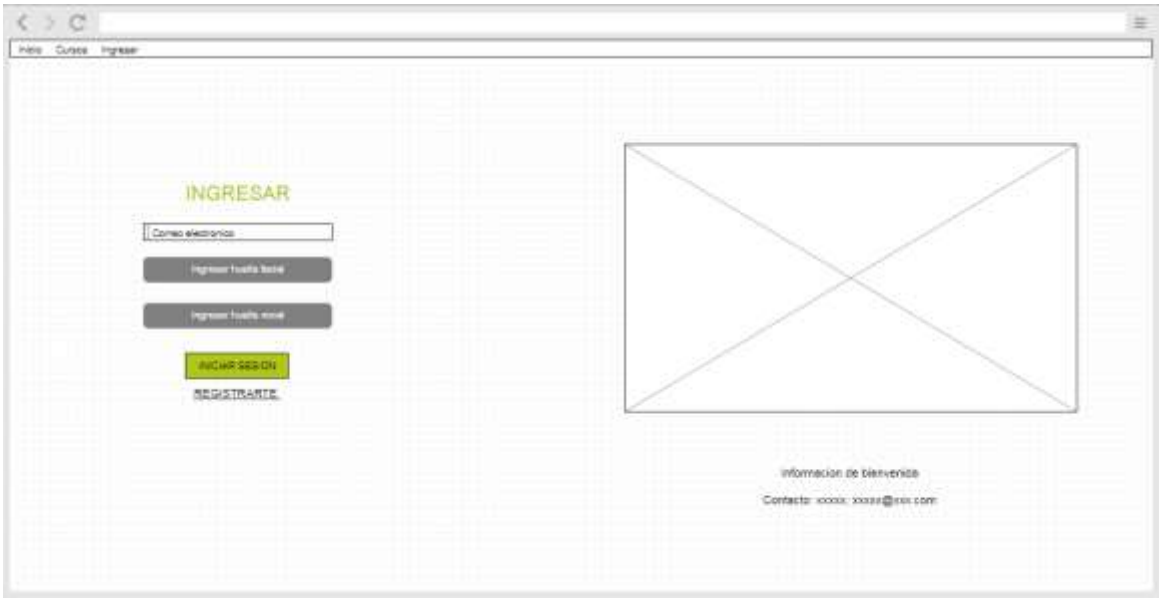
4.1 PROTOTIPOS DE INTERFAZ DE USUARIO

En base a los requerimientos y la idea previa que se tiene de cómo funcionará el módulo de ingreso dentro del aula virtual se podría dar forma a la interfaz gráfica del módulo con el fin de mostrar cómo será el aspecto de este y como podrá interactuar el usuario con las opciones disponibles, las cuales ya han sido especificadas.

Para el desarrollo de los prototipos es necesario elegir una herramienta de prototipado rápido en el ámbito UX (User experience design). Entre estas herramientas están: pidoco, balsamiq y Macromedia Fireworks entre otros. En este caso usaremos pidoco.

Prototipo página de Ingreso a la plataforma. En esta pantalla el usuario podrá tanto iniciar sesión como registrarse, además se mostrará cierta información básica sobre el módulo y la funcionalidad de este.

Figura 18. Prototipo de baja fidelidad de la página principal del módulo



Prototipo de registro. En esta pantalla el usuario podrá realizar el registro en el módulo, el usuario debe estar registrado previamente en el aula virtual, en ese caso Moodle (escenario de prueba sobre el cual se simula dicha aula virtual).

Inicialmente solo se solicitarán los datos básicos del usuario, la información biométrica será tomada posteriormente por el administrador con lo cual se espera mayor autenticidad y seguridad en la toma de datos.

Figura 19. Prototipo de baja fidelidad de la página de registro

Una vez realizado el registro será mostrado un mensaje en el cual se informará al usuario el paso a seguir para el registro de sus datos biométricos.

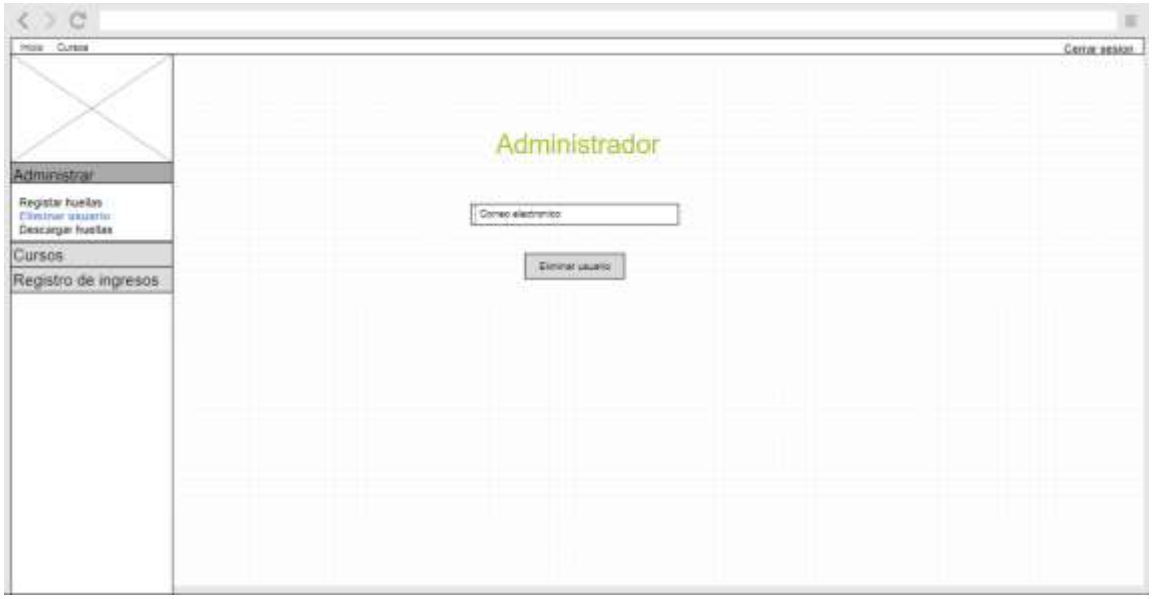
Figura 20. Prototipo de baja fidelidad del mensaje de registro exitoso

Registro de huella biométrica. El administrador tendrá acceso a diferentes opciones entre ellas el registro de huellas biométricas las cuales deben realizarse en presencia de este. El rol de administrador será asignado desde el momento del registro de este directamente desde la base de datos.

Figura 21. Prototipo de baja fidelidad de la página de inicio del administrador

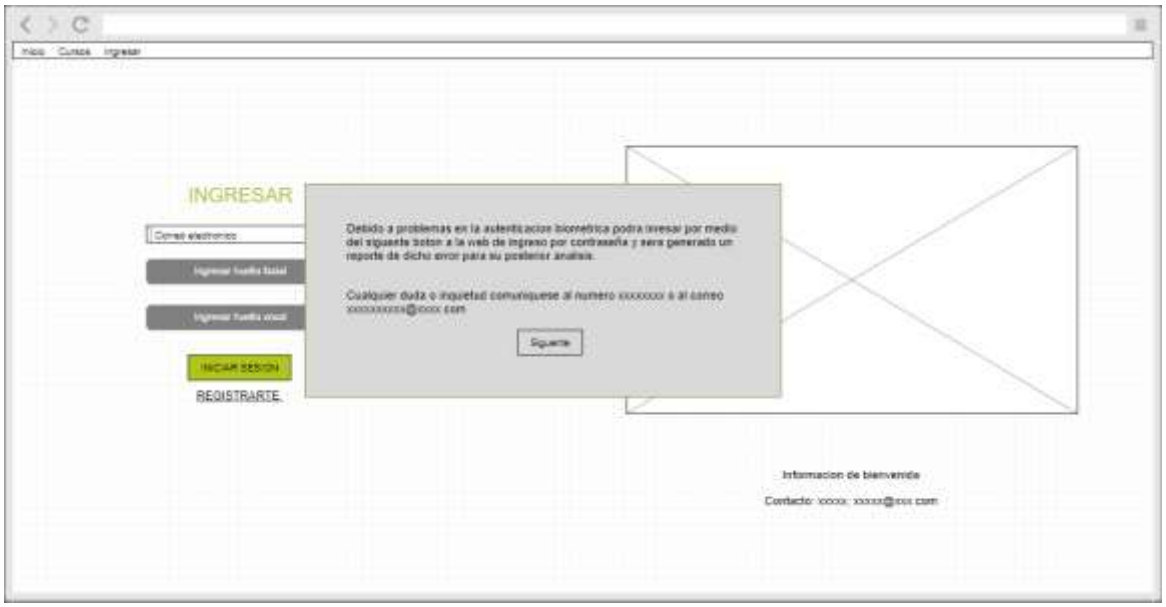
Eliminación de usuarios. En esta opción se podrán eliminar usuarios del módulo de autenticación tan solo con su correo electrónico, también se podrá no solo eliminar el usuario sino cada una de sus huellas o incluso actualizarlas desde la misma página.

Figura 22. Prototipo de baja fidelidad de la página de eliminación de usuarios



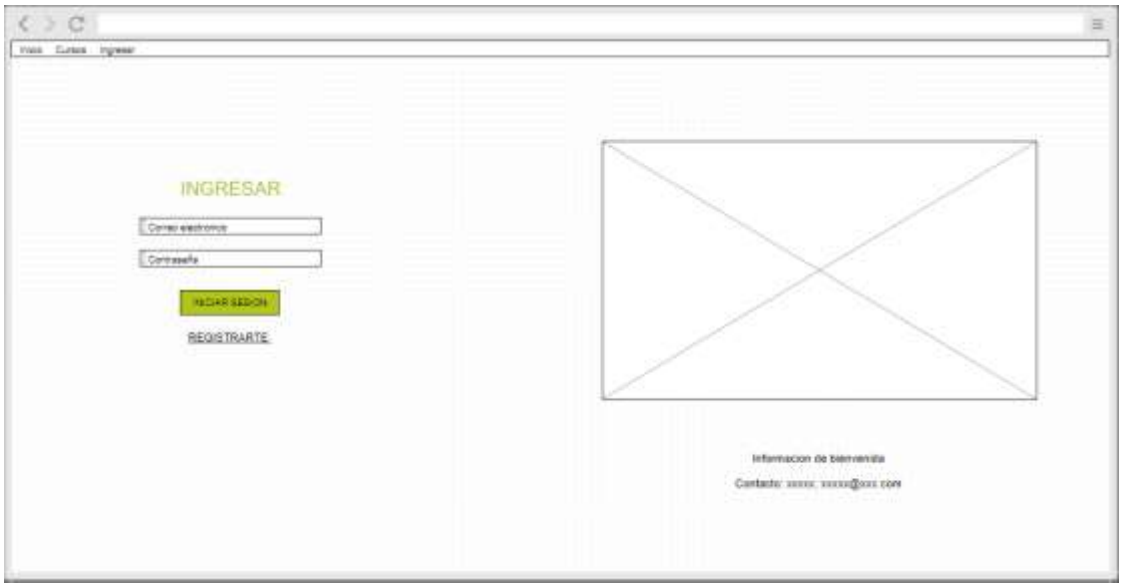
Información de fallo reconocimiento biométrico. En caso de tres fallos en el ingreso al sistema se plantea la opción de ingreso por contraseña además se informará al usuario y administrador sobre dicho fallo y los datos de contacto para la actualización de sus huellas si es necesario.

Figura 23. Prototipo de baja fidelidad del mensaje de fallo por ingreso biométrico



Ingreso por contraseña. La página de ingreso por contraseña permitirá el ingreso a la plataforma de la misma forma que el ingreso por biometría. Es añadida en caso de que se presente un error en el ingreso biométrico ya sea por hardware (mala calidad de la cámara o del micrófono) o por problemas en las huellas registradas en el sistema previamente.

Figura 24. Prototipo de baja fidelidad de la página de ingreso por contraseña



Descarga y actualización de huellas. Las huellas podrán ser descargadas individualmente y actualizadas de ser necesario.

Figura 25. Prototipo de baja fidelidad de la pantalla de búsqueda de huellas

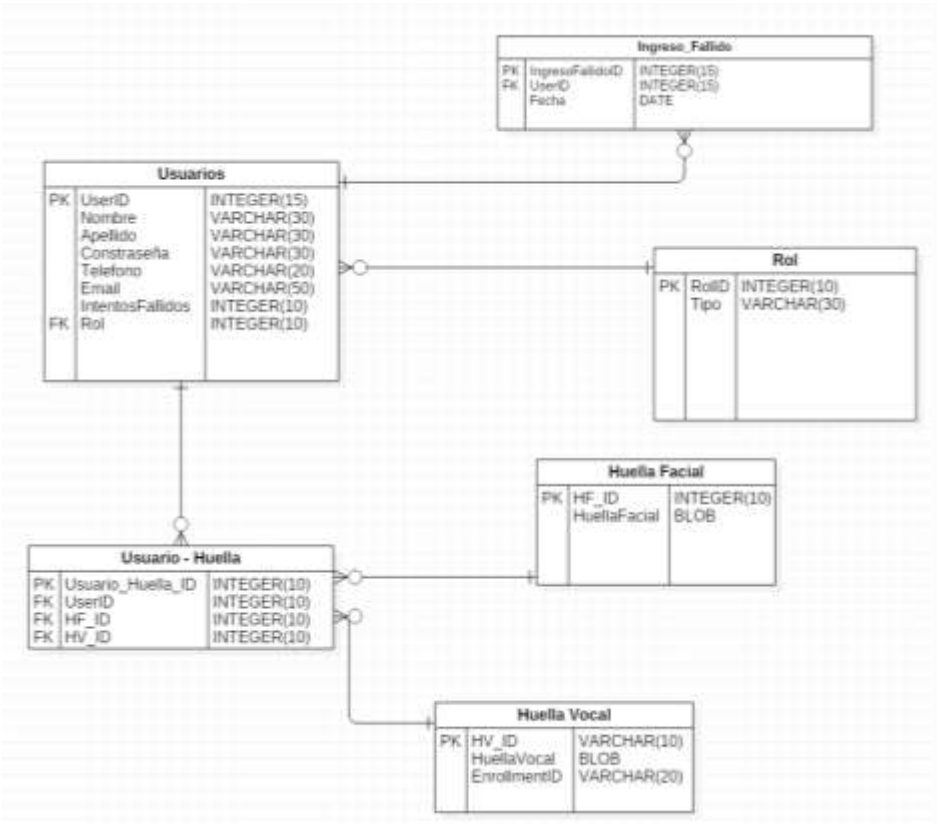
4.2 DISEÑO E IMPLEMENTACIÓN DEL MODELO ENTIDAD RELACIÓN

En este capítulo se presenta el modelo entidad relación que fue utilizado para que la creación de la base de datos fuera más adecuada y eficiente, además se encuentra una descripción de las entidades más importantes.

La base de datos de este proyecto está conformada por aquellas entidades requeridas para el proceso de evaluación de usabilidad, experiencia de usuario (UX) y gestión de los usuarios que se lleva a cabo en esta aplicación.

Se diseñó una base de datos de acuerdo con los requisitos del módulo de autenticación la cual cuenta con las tablas que veremos a continuación.

Figura 26. Base de datos



A continuación, se realizará una descripción de las entidades más importantes que se pueden observar en el diagrama de entidad-relación, que se presentaron anteriormente:

- Entidad Usuario: Esta entidad almacena la información básica requerida para cada usuario, diferenciándolos por un tipo de usuario (Participante, profesor, administrador). Su llave primaria es un identificador de usuario, y es usada como foránea por varias entidades que se relacionan directamente con la entidad en mención.

- Entidad Rol: Es la entidad encargada de definir el tipo de usuario para todos los usuarios registrados en la base de datos.

- Usuario Huella: es la entidad encargada de asignar una o varias combinaciones de huellas (facial y vocal) a un usuario específico, con el

fin de evitar la “***redundancia***” debido a que a un usuario no se le puede relacionar directamente con la entidad huella facial o vocal. Para esto esta tabla relaciona las entidades usuario, huella vocal y huella facial mediante llaves foráneas.

- Huella Facial: Es la entidad que contiene el archivo de la huella facial (imagen) y le asigna un identificador único.

- Huella Vocal: Es la entidad que contiene el archivo de la huella vocal (audio) y le asigna un identificador único.

5. DESCRIPCIÓN DEL SISTEMA

Esta sección comprende la descripción detallada del sitio web obtenido como resultado de este proyecto, así como una visión de sus interfaces y la descripción de cada una de ellas.

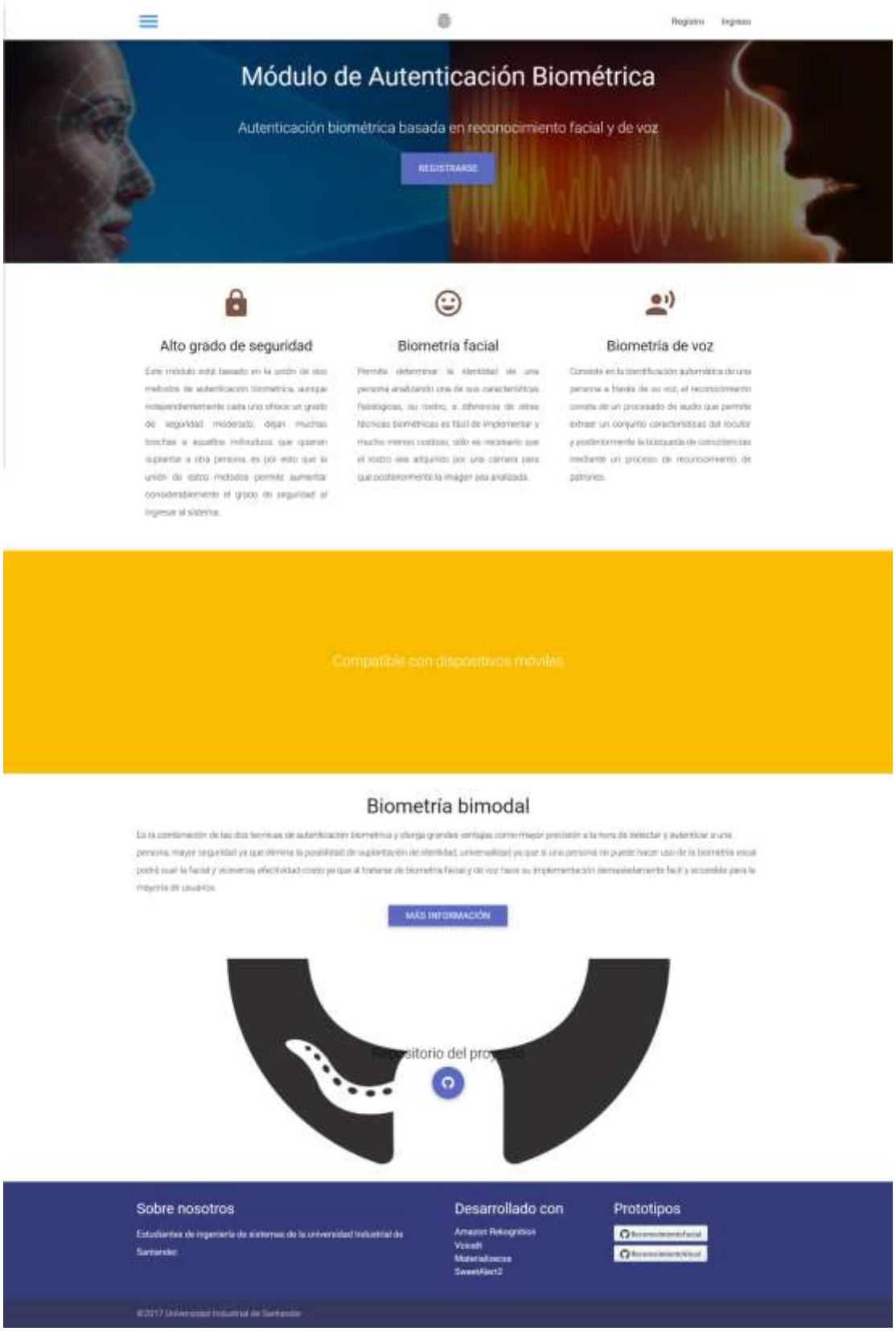
El sitio resultante es el **módulo de autenticación biométrica** el cual nos permite el ingreso a una plataforma determinada por medio de la biometría facial y de voz. Este sitio es un prototipo con el cual se quiere mostrar los beneficios de la autenticación biométrica y la seguridad que esta otorga para el ingreso de usuarios al sistema.

A continuación, se presentarán cada una de las pantallas del sistema y se dará una descripción detallada de las funcionalidades.

5.1 PANTALLA DE INICIO

Esta es la primera pantalla a la que usuarios tendrán acceso, en esta se expone toda la información relacionada con modulo e información adicional sobre los métodos de autenticación biométrica usados en este, así mismo cuenta con los enlaces que redirigen a las páginas de registro e ingreso, adicionalmente también incluyen enlaces a los repositorios de GitHub, donde se pueden encontrar los diferentes prototipos realizados durante la elaboración del módulo y los prototipos individuales para cada método de autenticación biométrica.

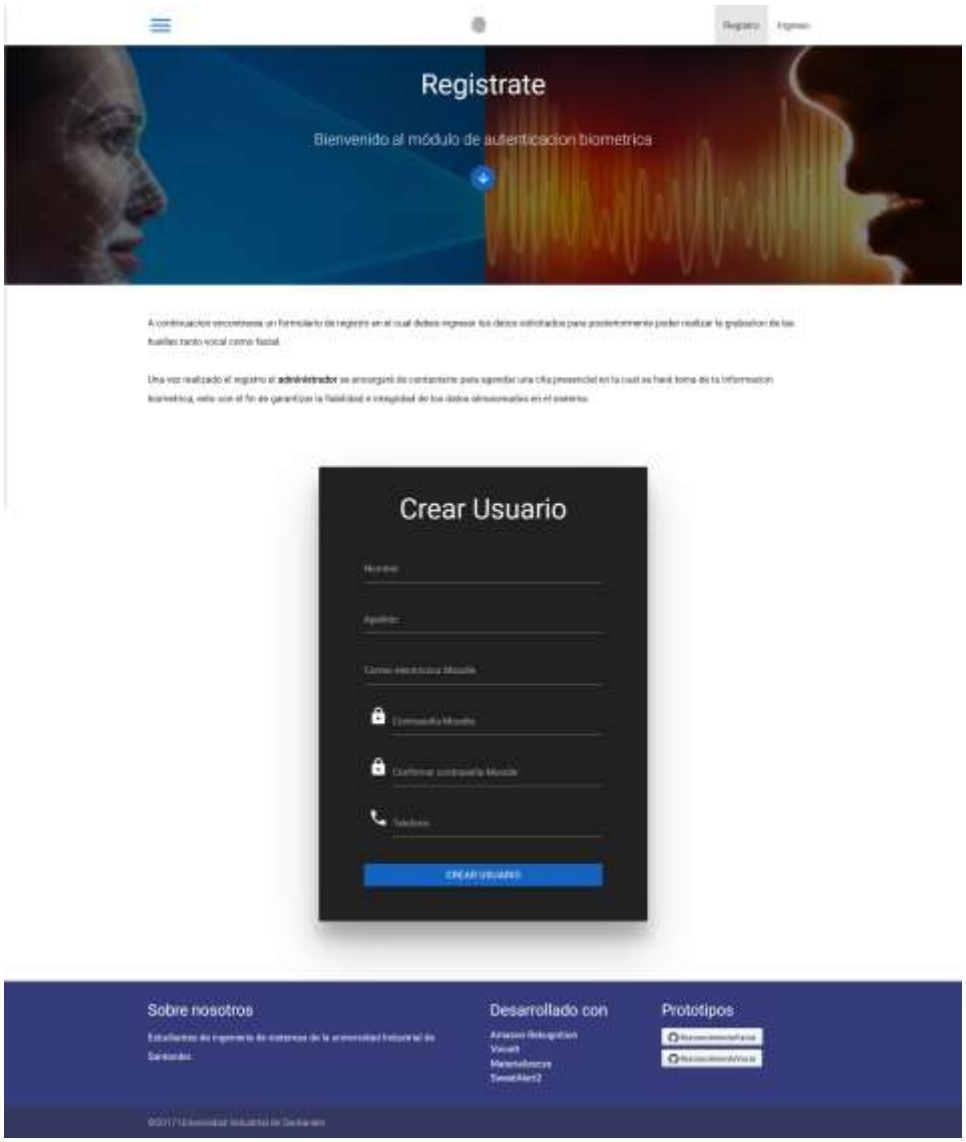
Figura 27. Pantalla de inicio



5.2 PANTALLA DE REGISTRO

En esta pantalla el usuario tiene la posibilidad de llenar un formulario con sus datos personales, dichos datos son necesarios para realizar el registro del usuario en la base de datos, existe un único requisito y este es que el usuario ya se encuentre registrado en Moodle, esto para garantizar que solo se puedan registrar usuarios pertenecientes a los cursos virtuales ya existentes en la plataforma de Moodle.

Figura 28. Pantalla de registro



5.3 PANTALLA DE INGRESO POR BIOMETRÍA

Esta sección del módulo es la encargada de capturar la información biométrica para realizar la autenticación de usuarios que intentan entrar al sistema, para esto es necesario que el usuario que intenta ingresar este registrado y que el administrador del módulo haya almacenado sus datos biométricos; En esta pantalla se le pide llenar un formulario al usuario donde este tiene que ingresar su correo con el cual está registrado en el sistema, su huella vocal y su huella facial, para estos dos ultimo datos es indispensable que el usuario cuente con un micrófono y cámara web respectivamente.

Figura 29. Pantalla de ingreso por biometría

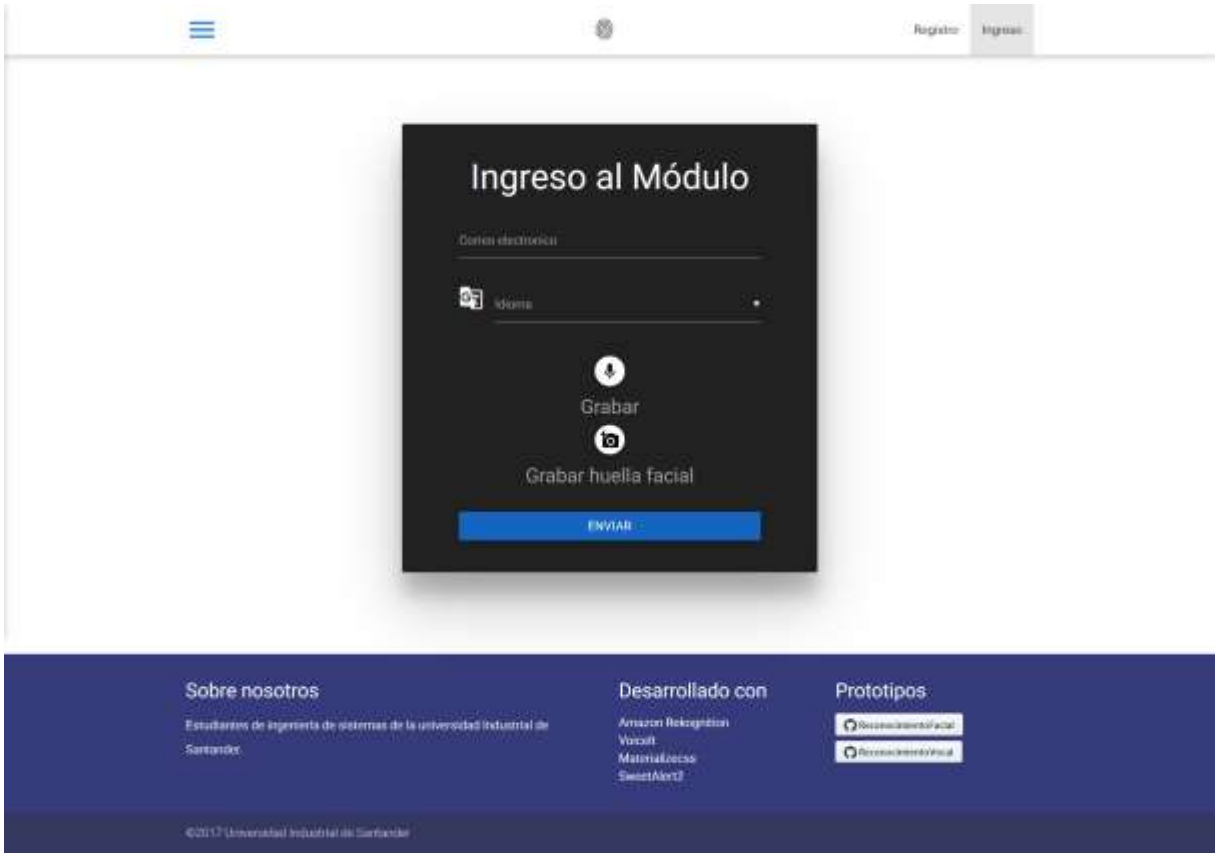


Figura 30. Pantalla de captura de huellas vocales

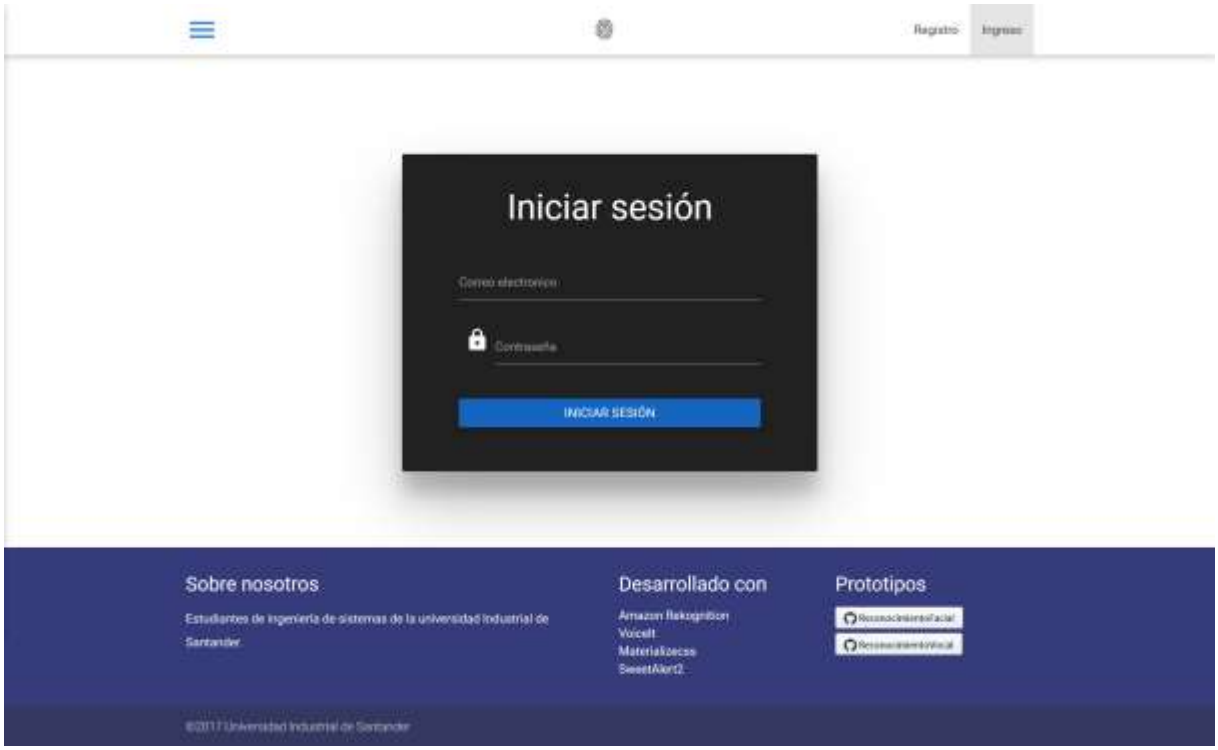
Figura 31. Pantalla de captura de huella facial

5.4 PANTALLA DE INGRESO POR CONTRASEÑA

Esta pantalla es la alternativa que se le da al usuario solo en caso de que haya fallado 3 veces el ingreso por biometría, esto con el fin de que no se le niegue con completo el acceso al sistema y el usuario pueda ingresar usando la contraseña previamente registrada, ya que es muy factible que el reconocimiento

facial o vocal fallen por diferentes motivos, tales como hardware, cambios físicos del usuario, fallos en la API, entre otros. Si el usuario falla la autenticación biométrica e ingresa con contraseña quedará el registro en la base de datos para que el administrador del módulo tome medidas al respecto.

Figura 32. Pantalla de ingreso por contraseña



5.5 PANTALLA DE INICIO DEL ADMINISTRADOR

Una vez el administrador sea autenticador biometría o contraseña, este ingresará al módulo donde verá un mensaje de bienvenida y se le presentará un menú de opciones en esta pantalla, así mismo se muestra información relacionada al módulo en general y el enlace al repositorio de GitHub donde tiene a disposición el código fuente.

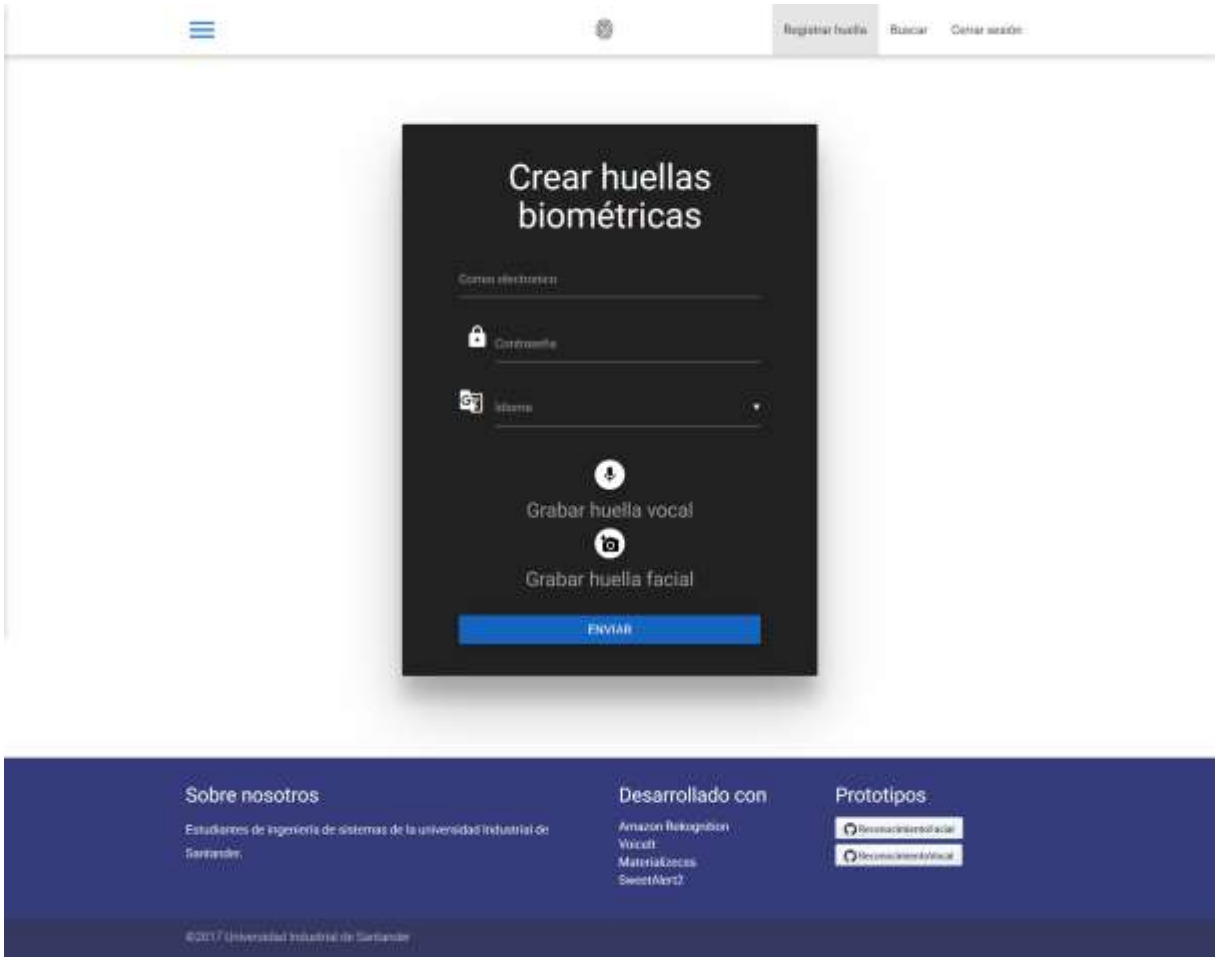
Figura 33. Pantalla de inicio del administrador

5.6 REGISTRO DE HUELLAS BIOMÉTRICAS

Esta sección del módulo es solo accesible por el administrador del módulo, ya que este de manera presencial verificará la identidad de los usuarios y los guiará en el proceso de captura de sus huellas biométricas, esto usando un formulario donde el usuario tiene que ingresar el correo con el cual se encuentra registrado

en el módulo y su respectiva contraseña, así mismo se le pedirá registrar la huella vocal y facial.

Figura 34. Pantalla de registro de huellas biométricas



5.7 PANTALLA DE BÚSQUEDA

En está pantalla el administrador tendrá la posibilidad de listar los usuarios que están registrados en el módulo, de igual manera se hace posible la búsqueda de un usuario en particular a partir del correo electrónico con el que está registrado, una vez se haya buscado el usuario el administrador podrá visualizar si tiene huellas biométricas y de ser así se darán las opciones de actualizarlas, eliminarlas o eliminar el usuario completamente de la base datos.

Además, los usuarios tendrán un contador de intentos fallidos y un estado el cual se podrá cambiar desde la misma página. Este estado estará en Inactivo hasta el momento del registro de huellas.

Figura 35. Pantalla de búsqueda

Figura 36. Vista de un usuario sin huellas registradas

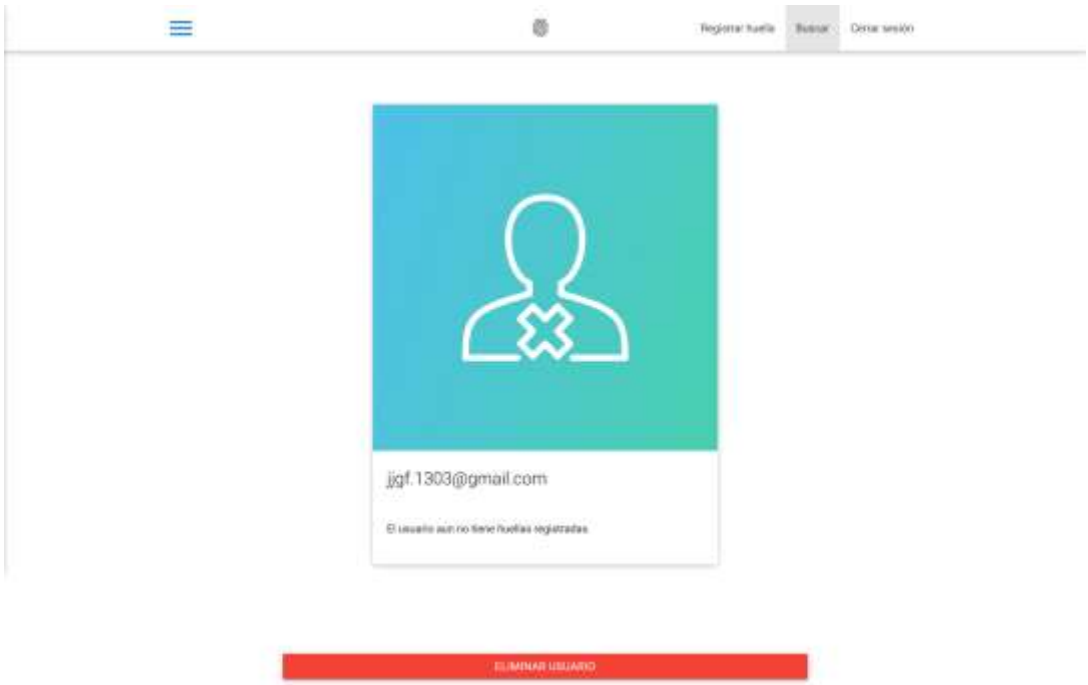
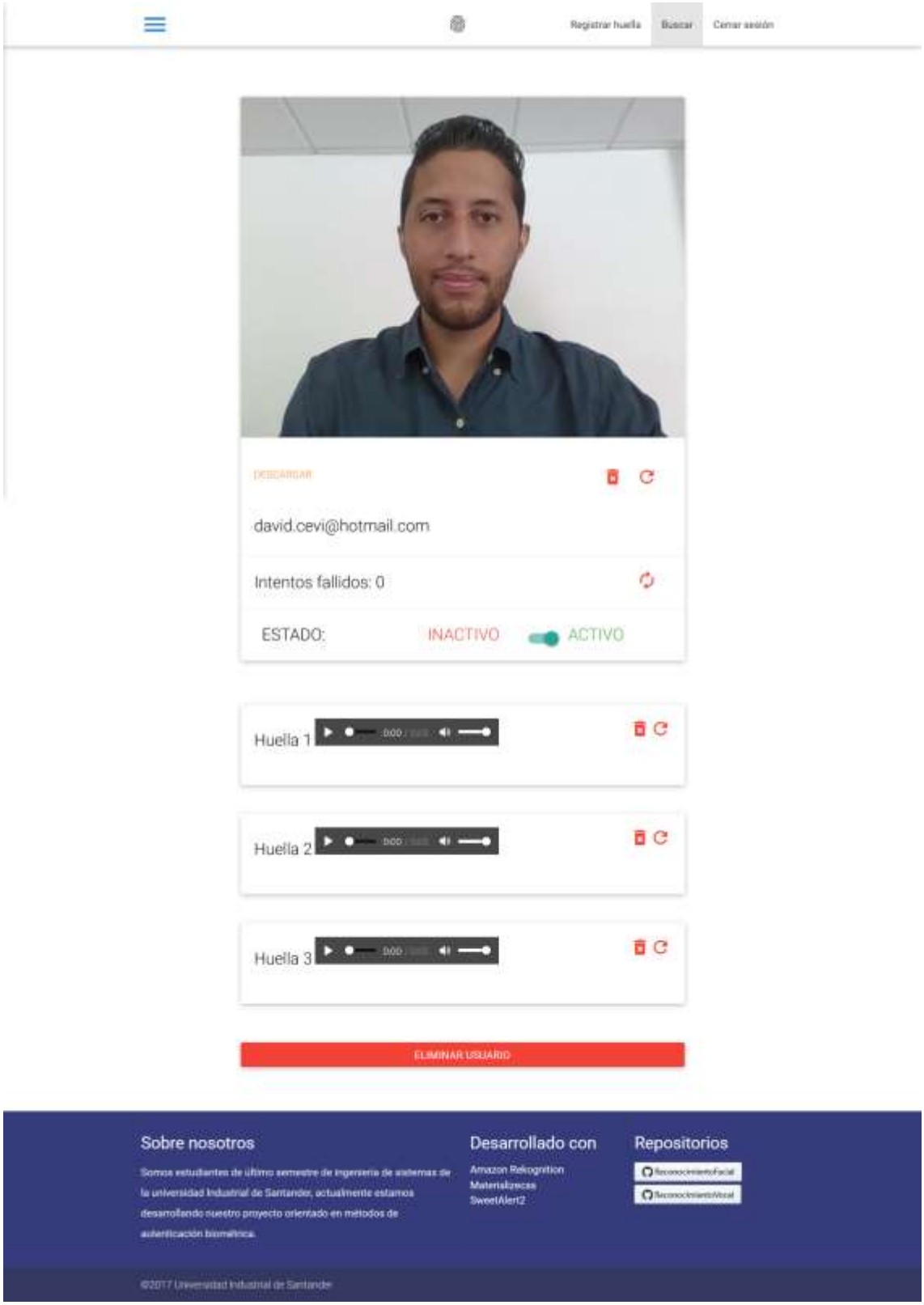


Figura 37. Vista de un usuario con huellas registradas



6. PRUEBAS

6.1 PRUEBAS DE SEGURIDAD

Las pruebas de seguridad son realizadas con el fin de evaluar la calidad del producto y garantizar la integridad de los datos que se manejan en la aplicación. Esto con el fin de brindar información a los interesados sobre la calidad y seguridad de la aplicación

6.1.1 Owasp. OWASP (acrónimo de Open Web Application Security Project, en inglés 'Proyecto abierto de seguridad de aplicaciones web') es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.[17]

Los documentos con más éxito de OWASP incluyen la Guía OWASP y el ampliamente adoptado documento de autoevaluación OWASP Top 10.

OSWAP Top 10 es un documento de los diez riesgos de seguridad más importantes en aplicaciones web según OWASP, esta lista se publica y actualiza cada tres años por dicha organización.

- A1 Inyección
- A2 Pérdida de autenticación y gestión de sesiones.
- A3 Exposición de datos sensibles
- A4 Entidades Externas de XML (XXE)
- A5 Violación de control de acceso
- A6 Configuración de seguridad incorrecta
- A7 Secuencia de comandos en sitios cruzados (XSS)
- A8 Deserialización insegura

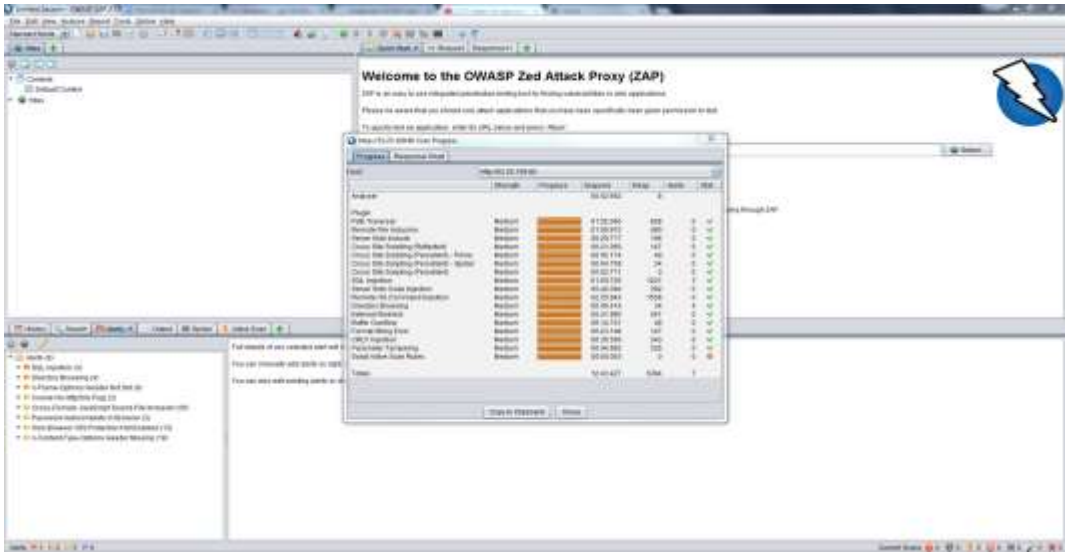
[17] COLABORADORES DE WIKIPEDIA. Open Web Application Security [En línea]. Wikipedia, La enciclopedia libre, 2018 (Recuperado en 29 de septiembre 2017). Disponible en https://es.wikipedia.org/w/index.php?title=Open_Web_Application_Security_Project&oldid=104353232

- A9 Utilización de componentes con vulnerabilidades conocidas
- A10 Monitoreo y registro insuficiente

6.1.2 Owasp zap. OWASP Zap es una herramienta disponible para Linux, Windows y Mac desarrollada dentro del Open Web Application Security Project. Esta herramienta nos permite realizar múltiples pruebas de penetración (SQLi, XSS, Descubrimiento de ficheros, etc.) en aplicaciones Web de una forma muy sencilla. [18]

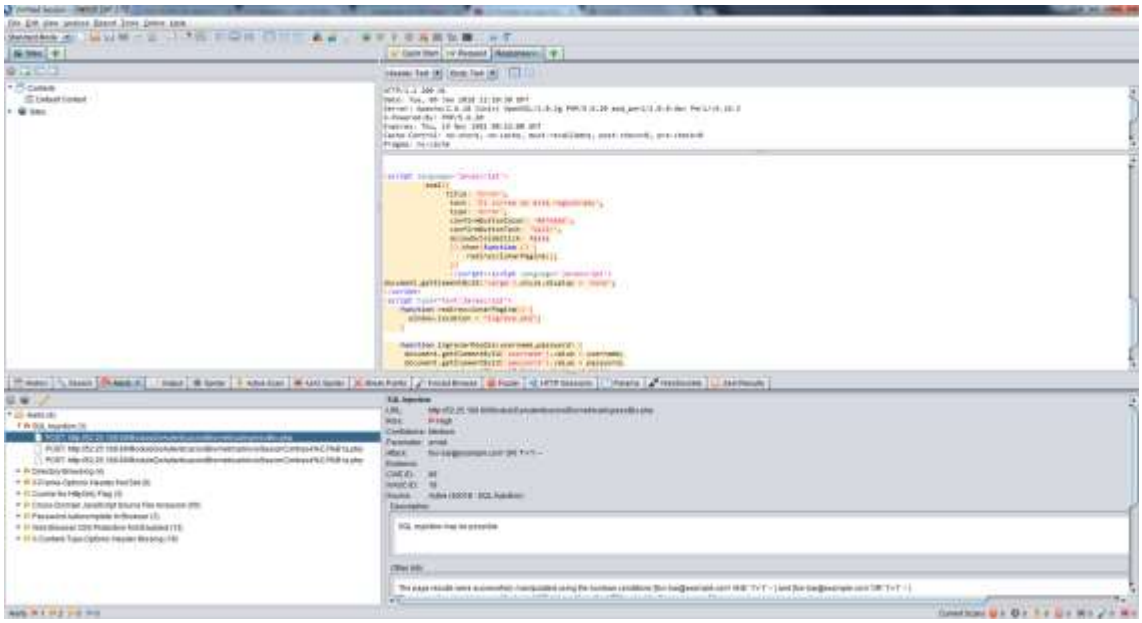
Está escrita en lenguaje JAVA y es multiplataforma lo que permite utilizarla prácticamente sobre cualquier sistema operativo, orientada a encontrar vulnerabilidades del OWASP Top 10, en sus últimas versiones está traducida al español y puede ser utilizada como Proxy permitiéndole al usuario interceptar tráfico de datos y manipularlo para comprobar el comportamiento de la aplicación web escaneada.

Figura 38. Pruebas realizadas por el software OWASP ZAP



[18] OWASP. OWASP Zed Attack Proxy Project [En línea]. Owasp, 2016 (Recuperado en 29 de septiembre 2017). Disponible en https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Figura 39. Resultado de pruebas en el software OWASP ZAP 2



Las pruebas que se llevaron a cabo al sitio (Modulo De Autenticación Biométrica) el cual se encuentra alojado en una instancia de una máquina virtual en Amazon EC2 (http://52.25.189.80) arrojaron los resultados en las imágenes mostradas anteriormente.

Entre estas se destacan las alertas por SQL Injection de las cuales se dejan capturas, estas alertas no representan mayor riesgo pues, aunque se presenta la advertencia, la autenticación e ingreso al módulo no fue exitoso además dicha autenticación depende directamente de la respuesta de la autenticación facial y vocal la cual se da mediante llamadas a dos servicios independientes.

Gracias a esta prueba se pudo verificar que hacía falta bloquear el acceso a ciertas carpetas del directorio que alojan imágenes y audios que son útiles para el correcto funcionamiento del módulo. Una vez realizada la prueba se procedió a bloquear el acceso a dichas carpetas y a corregir los errores de seguridad presentes en el módulo.

6.2 TABLA DE PRUEBAS DE INGRESO POR BIOMETRÍA

Para la prueba de ingreso por biometría participaron varios usuarios los cuales hicieron uso de diferentes dispositivos, esto para comprobar qué tanto varía la fiabilidad de autenticación cuando se ingresa en un dispositivo diferente del que se hizo el registro de huellas biométricas.

Cabe recordar que cada API tiene definido un grado de confidencialidad predefinido, para el caso de la API de reconocimiento facial, retornara que un rostro es similar a otro solo si estos tienen un grado de similitud mayor o igual al 80%, para la API de reconocimiento vocal el valor preestablecido es de un 87%, aunque estos valores son editables se realizaron las pruebas con los valores por defecto para validar la confidencialidad de cada herramienta.

Cuadro 16. Pruebas de ingreso por biometría

Usuario (10 intentos c/u)	**dispositivo registro**	**dispositivo ingreso**	**resultado autenticación facial (promedio)**	**resultado autenticación vocal (promedio)**	**Tiempo de respuesta (promedio)**	**Resultado final**
1	Lenovo T460 (Portátil)	Lenovo T460 (Portátil)	99%	90%	2.289s	Exitoso
1	Lenovo T460 (Portátil)	Lenovo G40-70 (Portátil)	98%	60.4%	2.250s	Fallido

1	Lenovo T460 (Portátil)	Moto g5 plus (smartphone)	91%	79%	2.228s	Fallido
2	Lenovo T460 (Portátil)	Lenovo T460 (Portátil)	100%	90%	2.743s	Exitoso
2	Lenovo T460 (Portátil)	Lenovo G40-70 (Portátil)	99%	76.8%	2.498s	Fallido
2	Lenovo T460 (Portátil)	Moto g5 plus (smartphone)	91%	89%	2.731s	Exitoso
3	Acer E3-111 (Portátil)	Acer E3-111 (Portátil)	100%	90%	2.327s	Exitoso
3	Acer E3-111 (Portátil)	Lenovo T460 (Portátil)	99%	73.6%	2.249s	Fallido
3	Acer E3-111 (Portátil)	Moto g5 plus (smartphone)	96%	87%	2.701s	Exitoso

Se llevo a cabo la verificación del correcto funcionamiento del módulo con el fin de garantizar que se cumple con los requisitos y los casos de uso establecidos anteriormente.

Para ello se realizaron una serie de pruebas en cada una de las funcionalidades en donde se ingresaron los datos necesarios para poder ejecutar y validar cada una de las opciones disponibles. Estas pruebas fueron realizadas en varias ocasiones para así realizar las mejoras necesarias en el prototipo y llegar al producto final.

6.3 PRUEBAS FUNCIONALES

Una prueba funcional está basada en la revisión, retroalimentación y ejecución de las funcionalidades previamente diseñadas. Son un proceso de control de calidad que consiste en asegurar el cumplimiento de un sistema o componente con requerimientos funcionales.

El objetivo principal de las pruebas funcionales es analizar el producto terminado y determinar si hace todo lo que debería hacer y si lo hace correctamente. Las pruebas se hacen mediante el diseño de modelos de prueba que buscan evaluar cada una de las opciones con la que cuenta el sistema.

A partir de estas pruebas se realizaron las respectivas correcciones a las diferentes falencias encontradas. Los resultados de las pruebas realizadas para verificar la funcionalidad de cada módulo se presentan en los siguientes cuadros.

Resultado de las pruebas a la interfaz de Inicio (Producto Final)

Cuadro 17. Pruebas de interfaz de inicio

Caso de prueba	Resultado
Prueba de ingreso a la página principal del módulo de autenticación, a través del enlace temporal biouis.tk.	Acceso a la página de forma correcta, evidencias en el capítulo 5 o en el enlace alternativo http://52.25.189.80.
Inscripción de un usuario por medio de la página de registro, teniendo en cuenta	Registro exitoso, cumpliendo los requisitos preestablecidos.

que el usuario se debe encontrar previamente registrado en el escenario de prueba Moodle.	
Ingreso al módulo a través de autenticación biométrica y redirección al escenario de prueba Moodle.	Ingreso verificado, evidencias en la sección 6.3.
Prueba de ingreso alternativo por contraseña y redirección al escenario de prueba Moodle.	Redirección correcta a la página de ingreso por contraseña al errar 3 veces el ingreso por biometría e ingreso por contraseña exitoso.

Resultado de las pruebas a la interfaz de Administrador (Producto Final)

Cuadro 18. Pruebas de interfaz de administrador

Caso de prueba	**Resultado**
Prueba de ingreso como usuario con rol de administrador.	Ingreso y visualización de la página de administrador exitoso, evidencias en la sección 5.5.
Prueba de la opción de búsqueda y verificación de la tabla de usuarios.	Opción de búsqueda verificada, evidencias en la sección 5.7.
Prueba de selección de un usuario específico, visualización de sus datos personales y huellas biométricas.	Prueba realizada con éxito, visualización de usuario con y sin huellas. Evidencias en la sección 5.7.
Prueba de eliminación, actualización y descarga de las huellas de un usuario especifico de manera individual y eliminación del usuario del módulo.	Verificación exitosa de las opciones mencionadas, capturas en la sección 5.7.

Prueba de registro de huellas biométricas por parte del administrador a usuarios previamente registrado en el módulo.	Registro de huellas realizado con éxito, captura de un usuario con huellas en la sección 5.6
Prueba de bloqueo de usuario en caso de error durante el ingreso al módulo y validación de la opción de reactivación por parte del administrador.	Bloqueo verificado exitosamente y opción de reactivación verificada. Evidencias de la opción de reactivación en la sección 5.7.

6.4 CUADRO DE CUMPLIMIENTO DE OBJETIVOS

En la siguiente tabla se presenta cada uno de los objetivos establecidos para este proyecto y el nivel de avance correspondiente para cada uno de ellos.

Cuadro 19. Cumplimiento de objetivos

OBJETIVO GENERAL		
Diseño y desarrollo de prototipo de módulo web en el que los usuarios puedan ser identificados por reconocimiento biométrico (facial y de voz) y ejecución mediante un escenario de prueba (emulador de aula virtual).		
OBJETIVO ESPECIFICO	**AVANCE**	**EVIDENCIA**
Elaboración del Documento de especificación de requisitos del módulo de autenticación biométrica y del escenario de prueba.	100%	Ver capítulo 3.

Elaboración de una tabla comparativa y selección de las herramientas de biometría facial y de voz a usar en el módulo de autenticación.	100%	Ver sección 2.7.
Diseño del módulo de autenticación biométrica que permita: ● Crear y gestionar el banco de huellas faciales y el banco de huellas vocales para el reconocimiento biométrico. ● Verificar la identidad de un usuario a partir de sus características biométricas faciales y de voz. ● Proporcionar la información requerida para la adecuada toma de los datos biométricos.	100%	Ver capítulo 4, en el capítulo 5 se da evidencia del ingreso por biometría y en la sección 6.2 se presenta una tabla en donde muestran las pruebas de ingreso y sus resultados.
Diseño del escenario de prueba del módulo de autenticación biométrica, esto es un emulador de aula virtual que permita:		

• Registro del usuario-estudiante con sus datos personales e información biométrica (huella facial y vocal) usando la cámara y el micrófono. • Brindar al usuario una alternativa de autenticación en caso de fallo en la autenticación biométrica (por causas de hardware, fallas en el servidor o plataforma).	100%	Ver capítulo 4, evidencia del resultado de la implementación en el capítulo 5.
Implementación del módulo de autenticación biométrica y del escenario de prueba.	100%	Ver capítulo 5, en este se presenta una descripción e imagen de cada una de las pantallas del módulo.
Ejecución de pruebas para evaluar la usabilidad y rendimiento del módulo software.	100%	Ver capítulo 6, en donde se presentan las diferentes pruebas y verificaciones realizadas.

.

CONCLUSIONES

En este proyecto se desarrolló un prototipo de módulo software que busca autenticar usuarios, más específicamente estudiantes, que están registrados en aulas o cursos virtuales en plataformas tales como Moodle, estos obtienen acceso a través de autenticación biométrica basada en reconocimiento facial y de voz.

El uso de técnicas de autenticación biométrica para la verificación de la identidad de usuarios se ha convertido durante los últimos años en una de las opciones de autenticación que más auge ha ganado, sin embargo, en muchas ocasiones su implementación se hace costosa y complicada, por lo que se determina que la integración de reconocimiento facial y de voz realizada en este proyecto ha sido una opción acertada, ya que hace posible su uso desde la mayoría de computadores y dispositivos móviles que se encuentran hoy en día en el mercado.

El desarrollo de este proyecto permitió a los autores realizar una comparación entre diferentes herramientas de reconocimiento facial y de voz, entre las que se encontraban SDKs, librerías y APIs, siendo estas últimas las más adecuadas para el desarrollo web y las más fáciles de implementar, no obstante, son herramientas de uso comercial que a pesar de tener unos periodos de prueba amplios, pueden volverse muy costosos dependiendo del número de llamadas a la API, de igual manera el uso de estas herramientas hacen que cualquier proyecto sea dependiente de ellas y de la calidad de su servicio.

A pesar de que en algunos casos se cree que el uso de métodos biométricos es completamente seguro e infalible, durante el desarrollo del proyecto se evidenció que es posible engañar al sistema de reconocimiento facial de manera individual usando una imagen del usuario al que se trata de suplantar y poniéndola en frente de la cámara, así mismo, el sistema de reconocimiento vocal puede ser burlado al usar una grabación con buena calidad de algún usuario diciendo la

frase de seguridad, a pesar de esto, se concluye que al solicitar de manera conjunta las características biométricas facial y vocal, se crea un sistema de reconcomiendo bimodal que hace del módulo un sistema mucho más fiable y mitiga el riesgo de suplantación de usuarios.

Se realizaron una serie de pruebas que determinaron el correcto funcionamiento del módulo software y el cumplimiento de los requerimientos preestablecidos, dichas pruebas también evidenciaron una falencia al usar la herramienta de reconocimiento vocal que provocaba que la mayoría de intentos de autenticación realizados en un dispositivo diferente del que se grabaron los datos biométricos fallaran, esto se debe a que la calidad de las grabaciones de las huellas vocales varían dependiendo del hardware usado durante su captura.

La optimización y versatilidad con la que se han venido creando dispositivos inteligentes, en conjunto con nuevas tecnologías como el internet de las cosas y las técnicas de reconocimiento biométrico, han demostrado que estamos cambiando la manera como interactuamos, no solo con ordenadores o dispositivos móviles, sino también con todo tipo de objetos y lugares, razón por la cual se infiere que el estudio y desarrollo de aplicaciones con estas tecnologías debe ser incentivado en mayor medida, para así dar soluciones a todo tipo de retos existentes en los diferentes sectores sociales, económicos y educativos.

RECOMENDACIONES

Alojar el módulo en un dominio que cuente con certificado https, ya que algunos navegadores impiden el correcto funcionamiento del sistema sin dicho certificado.

Se recomienda hacer uso de dispositivos que cuenten con micrófonos y cámaras de calidad para obtener mejores resultados durante el proceso de captura y autenticación de las huellas biométricas.

Se sugiere implementar procedimientos de autenticación que permitan a los usuarios acceder a plataformas diferentes a Moodle, tales como Single Sign-On.

Dada la gran cantidad de herramientas existentes para el desarrollo de software orientado al reconocimiento facial y de voz, se recomienda explorar alternativas a las APIs para así trasladar el sistema a otras áreas de aplicación tales como autenticación de usuarios en dispositivos locales, acceso a establecimientos, entre muchas otras.

BIBLIOGRAFÍA

AMAZON WEB SERVICES. “Amazon Rekognition - Documentation”. [En línea]. (Recuperado en agosto del 2017.) Disponible en: https://aws.amazon.com/rekognition/resources/?nc1=f_ls.

APACHE FRIENDS. “FAQs”. [En línea]. (Recuperado en septiembre 2017.) Disponible en: https://www.apachefriends.org/faq_windows.html.

BRUEGGE, Bernd y DUTOIT, Allen. “Object-Oriented Software Engineering Using UML, Patterns, and Java”. Boston: Prentice Hall, tercera edición, 2010. ISBN 978-0-13-606125-0.

CARRERA, Marcelo. “Proyectos tecnológicos - modelo de desarrollo prototipado”. [Internet]. (Recuperado en septiembre 2017.) Disponible en: http://www.imaginar.org/iicd/tus_archivos/LLL/docs/5_laboratorios.pdf.

DEMAREE, David. “Git for humans”. Nueva York: A book apart, 2016. ISBN 978-1-9375573-9-3.

GITHUB, “GitHub Guides”. [En línea]. (Recuperado en agosto 2017.) Disponible en: https://guides.github.com/.

ISO 25000. “Calidad del producto software”. [En línea]. (Recuperado en agosto 2017.) Disponible en: http://www.iso25000.com/.

JAIN, Anil; BOLLE, Ruud y PANKANTI, Sharath. “Biometrics: Personal Identification in Networked Society”. Nueva York: Springer,2006. ISBN 978-0-387-32659-7.

MATERIALIZECSS. “Getting Started”. [En línea]. (Recuperado en septiembre 2017.) Disponible en: http://materializecss.com/getting-started.html.

MOODLE. “Moodle docs”. [En línea]. (Recuperado en junio 2017.) Disponible en: https://docs.moodle.org/34/en/Main_page

MYSQL, “MySQL Documentation”. [En línea]. (Recuperado en septiembre 2017.) Disponible en: https://dev.mysql.com/doc/.

NETBEANS, “Community Documentation”. [En línea]. (Recuperado en agosto 2017.) Disponible en: https://netbeans.org/community/commdocs.html.

OWASP. “OWASP Zed Attack Proxy Project”. [En línea]. (Recuperado en noviembre 2017.) Disponible en: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project.

PHP, “Documentation”. [En línea]. (Recuperado en agosto 2017.) Disponible en: http://php.net/docs.php.

PHPMYADMIN, “PhpMyAdmin Documentation”. [En línea]. (Recuperado en septiembre 2017.) Disponible en: https://www.phpmyadmin.net/docs/.

SAHOO, Soyuj y PRASANNA, Mahadeva. “Bimodal Biometric Person Authentication Using Speech and Face Under Degraded Condition”. National Conference on Communications (NCC), Bangalore, 2011, p. 1-5.

TAPIADOR, Marino y SIGÜENZA, Juan. “Tecnologías biométricas aplicadas a la seguridad”. Madrid: RA-MA, 2005. ISBN 978-84-7897-636-2.

VIRDEE-CHAPMAN, Ben. “What's the Difference Between an API and a SDK?”. [En línea]. 24 de febrero 2017. (Recuperado en junio 2017.) Diponible en: https://www.kairos.com/blog/what-s-the-difference-between-an-api-and-a-sdk

VOICEIT. “PHP API Guide”. [En línea]. (Recuperado en septiembre 2017.) Disponible en: https://voiceit.io/apidocs.

WIKIPEDIA, THE FREE ENCYCLOPEDIA. “Biometría”. [En línea]. (Recuperado en junio 2017.) Disponible en: https://es.wikipedia.org/wiki/Biometría