UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE CIENCIAS HUMANAS Y DE LA EDUCACIÓN

Carrera de Docencia en Informática

Modalidad: Presencial

Proyecto de Investigación previo la obtención del Título de Licenciado en Ciencias de la Educación.

Mención: Docencia en Informática

TEMA:

"RECONOCIMIENTO FACIAL APLICADO A LA AUTENTIFICACION DE USUARIOS EN CURSOS ONLINE DE LA CARRERA DE DOCENCIA EN INFORMATICA DE LA FACULTAD DE CIENCIAS HUMANAS Y DE LA EDUCACION DE LA UNIVERSIDAD TECNICA DE AMBATO"

Autor(a): Naranjo Quispe Ruth Jimena

Tutor(a): Ing. Mg. Wilma Lorena Gavilanes López

Ambato – Ecuador

2016

APROBACIÓN DEL TUTOR DEL TRABAJO DE GRADUACIÓN O TITULACIÓN

CERTIFICA:

Yo, Ing. Mg. Wilma Lorena Gavilanes López con CI: 1802624427 en calidad de Tutora del trabajo de Graduación o titulación sobre el tema "RECONOCIMIENTO FACIAL APLICADO A LA AUTENTIFICACION DE USUARIOS EN CURSOS ONLINE DE LA CARRERA DE DOCENCIA EN INFORMATICA DE LA FACULTAD DE CIENCIAS HUMANAS Y DE LA EDUCACION DE LA UNIVERSIDAD TECNICA DE AMBATO".

Desarrollado por la egresada Naranjo Quispe Ruth Jimena, considero que dicho Informe Investigativo, reúne los requisitos técnicos, científicos y reglamentarios, por lo que autorizo la presentación del mismo ante el Organismo pertinente, para que sea sometido a evaluación por parte de la Comisión calificadora designada por el H. Consejo Directivo.

TUTORA

Ing. Mg. Wilma Lorena Gavilanes López

CI: 1802624427

AUTORIA DE LA INVESTIGACION

Dejo constancia de que el presente informe es el resultado de la investigación del autor, quien en la experiencia profesional, en los estudios realizados durante la carrera, revisión bibliográfica y de campo, ha llegado a las conclusiones y recomendaciones descritas en la Investigación. Las ideas, opiniones y comentarios especificados en este informe, son de exclusiva responsabilidad de su autor.

Naranjo Quispe Ruth Jimena

C.I: 1804250940

AUTOR

CESIÓN DE DERECHOS DE AUTOR

Cedo los derechos en línea patrimoniales del presente Trabajo Final de Grado o Titulación sobre el tema: "RECONOCIMIENTO FACIAL APLICADO A LA AUTENTIFICACION DE USUARIOS EN CURSOS ONLINE DE LA CARRERA DE DOCENCIA EN INFORMATICA DE LA FACULTAD DE CIENCIAS HUMANAS Y DE LA EDUCACION DE LA UNIVERSIDAD TECNICA DE AMBATO", autorizo su reproducción total o parte de ella, siempre que esté dentro de las regulaciones de la Universidad Técnica de Ambato, respetando mis derechos de autor y no se utilice con fines de lucro.

Naranjo Quispe Ruth Jimena

C.I: 1804250940

AUTORA

AL CONSEJO DIRECTIVO DE FACULTAD DE CIENCIAS HUMANAS Y DE LA EDUCACIÓN:

La comisión de Estudio y Calificación del Informe del Trabajo de Graduación o Titulación, sobre el Tema:

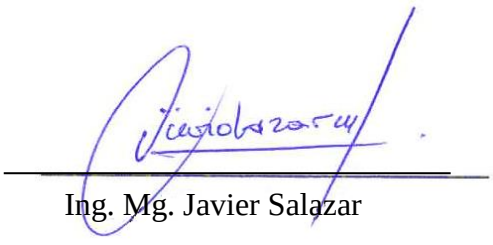
"RECONOCIMIENTO FACIAL APLICADO A LA AUTENTIFICACION DE USUARIOS EN CURSOS ONLINE DE LA CARRERA DE DOCENCIA EN INFORMATICA DE LA FACULTAD DE CIENCIAS HUMANAS Y DE LA EDUCACION DE LA UNIVERSIDAD TECNICA DE AMBATO".

Presentado por la Srta. Naranjo Quispe Ruth Jimena, egresada de la Carrera de Docencia en Informática, Promoción septiembre 2010- agosto 2015 una vez revisada y calificada la investigación, se **APRUEBA** en razón de que cumple con los principios básicos técnicos y científicos de investigación y reglamentarios.

Por lo tanto, se autoriza la presentación ante el Organismo pertinentes.

LA COMISION

Ing. Mg. Javier Sánchez
MIEMBRO



Ing. Mg. Javier Salazar
MIEMBRO

DEDICATORIA

El presente trabajo de investigación está dedicado con todo mi afecto a todos y a cada uno de los miembros de mi familia quienes supieron brindarme su apoyo en todo momento y cuando más lo he necesitado.

Por ayudarme, motivarme y nunca permitir que renuncie a mis metas y sueños impidiendo que fracase en la vida a pesar de mis errores, siempre supieron apoyarme y enseñarme que en la vida van a haber obstáculos que dificulten la llegada a mi meta.

Ruth Naranjo

AGRADECIMIENTO

Agradezco de una forma muy especial a mi madre por su cariño, comprensión y apoyo incondicional, a mi padre por siempre haberme guiado por el camino del bien, a mi hermano quien me ha apoyado con sus conocimientos para poder realizar este trabajo de investigación además a mi hijo por ser el eje fundamental en mi vida.

Con gran aprecio doy las gracias a la Facultad de Ciencias Humanas y de la Educación, por abrirme las puertas de sus establecimiento y permitir formarme profesionalmente

Doy gracias a todos mis docentes quienes supieron formarme profesional y personalmente llegando a ser más que docentes unos amigos en quienes vi un apoyo para cumplir mis metas.

Ruth Naranjo

INDICE GENERAL

ÌNDICE DE TABLAS

ÌNDICE DE GRÁFICOS

INTRODUCCIÓN

El reconocimiento facial aplicado a la autentificación de usuarios en cursos online de la carrera de docencia en informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato", es un tema de actualidad y está estructurado por los siguientes capítulos:

Capítulo 1: **El Problema**, parte con el planteamiento del problema, la contextualización macro, meso y micro para en base a esto formular en forma clara y precisa el problema, tomando como punto de partida, interrogantes, que ayudarán a interpretar por qué y para qué se desarrolla la investigación y el tipo de beneficios que se obtendrá con el presente tema de investigación. Se concluye este capítulo con el planteamiento de los objetivos generales y específicos.

Capítulo 2: **Marco Teórico,** se enfoca en el marco teórico en relación con el problema investigativo, para ello se ha con ha considerado abordar contenidos básicos sobre el reconocimiento facial y su influencia en la autentificación de usuarios en cursos online de la carrera de docencia en informática, concluyendo con el planteamiento de la hipótesis y señalamiento de variables.

Capítulo 3: **Metodología, e**xplica claramente el modelo y el proceso metodológico en la relación del trabajo, el grupo seleccionado, las características y metodologías para la selección de la muestra además se hace una descripción de los instrumentos aplicados para la recolección de datos y los pasos sugeridos para la ejecución del trabajo.

Capítulo 4. A**nálisis e interpretación de resultados**. Aquí se procede al análisis e interpretación de los resultados de las estadísticas aplicadas a los estudiantes mediante tablas y gráficos cuantitativos para la verificación de la hipótesis.

Capítulo 5. **Conclusiones y recomendaciones**. Se evidencia las conclusiones en función de los resultados obtenidos y se realizan las recomendaciones que se pueden emplear para fortalecer el proceso de la asimilación del aprendizaje de los estudiantes.

Capítulo 6. P**ropuesta**. Como parte de este informe se desarrolla y sustenta la propuesta, los datos informativos de la institución ejecutora, los antecedentes, los objetivos, el modelo operativo de la propuesta y la previsión de la evaluación.

Bibliografía. Aquí se anota todos los documentos como libros, libros electrónicos y de la web que sirven de sustento para la investigación.

Anexos. Aquí se encuentra la evidencia gráfica en la institución y además datos que servirán de sustento a la investigación.

CAPÍTULO I

EL PROBLEMA

1.1. TEMA

"RECONOCIMIENTO FACIAL APLICADO A LA AUTENTIFICACION DE USUARIOS EN CURSOS ONLINE DE LA CARRERA DE DOCENCIA EN INFORMATICA DE LA FACULTAD DE CIENCIAS HUMANAS Y DE LA EDUCACION DE LA UNIVERSIDAD TECNICA DE AMBATO"

1.2. PLANTEAMIENTO DEL PROBLEMA

1.2.1 Contextualización

Macro

En México, se ha realizado una investigación que propone un sistema de reconocimiento de rostros usando imágenes estéreo, que permiten incrementar las seguridades de reconocimiento de rostros convencionales.

Una vez que el sistema haya determinado que la imagen de entrada es un rostro real en 3D, es caracterizada y procesada independientemente usando un método de extracción de características (EC) convencional. Seguidamente se emplea un método de fusión (MF) para combinar la información obtenida en ambas imágenes. Con el fin de determinar la combinación EC-MF más adecuada, se analizaron 3 métodos de extracción de características y 3 métodos de difusión. Lo resultados obtenidos muestran que realizando la fusión de los datos extraídos mediante la transformación, antes de

pasar a la etapa de clasificación, se obtienen mejores resultados. (García Ríos, Escamilla Hernandez, Nakano Miyatake, & Pérez Meana, 2014)

También se han realizado investigaciones en Medellín, Colombia, acerca de la Extracción de puntos característicos del rostro con lo cual se ha propuesto una técnica de extracción de 22 puntos característicos del rostro, orientada a aplicaciones de antropometría. La técnica se fundamenta en la transformada wavelets-Gabor y el uso del algoritmo EBGM (Elastic Bunch Graph Matching). Este algoritmo fue modificado para que los puntos extraídos correspondan a puntos característicos del rostro, los cuales se utilizan comúnmente en medidas antropométricas faciales. Las modificaciones consisten en un conjunto de restricciones para ajustar inicialmente la ubicación de los centro de búsqueda y posteriormente para la definición de la región de la búsqueda. Los resultados mostraron que los puntos centrales del rostro presentan errores de ubicación, lo cual es consistente con las medidas en antropometría facial directa. (González & Prieto, 2010)

Meso

En Ecuador también se han realizado investigaciones acerca del reconocimiento facial. Este es el caso de la investigación realizada en la ciudad de Latacunga por la Escuela Politécnica del Ejército (López, Maranón, Erazo, & Reinoso, 2006).

En esa investigación se denota que al implementar un sistema de seguridad para los vehículos, esto ha sido de gran ayuda debido a que se tiene un control con un alto nivel de seguridad y además poder llevar una estadística de los ingresos de personal así como de los vehículos usados.

De acuerdo al párrafo anterior el acceso biométrico en donde el reconocimiento facial, es un sistema alternativo que refuerza a otros sistemas como de la huella dactilar y

clave de acceso, aumentando la confiabilidad para estos procesos de autentificación de identidad.

Micro

La educación desde hace mucho tiempo se ha venido dando de manera tradicional, por lo que es necesario poner en marcha nuevos proyectos para ayudar a mejorar el aprendizaje.

La habilidad de reconocer los rostros está ofreciendo una alternativa a las múltiples contraseñas que los usuarios de computadoras y teléfonos celulares usan y a menudo olvidan, según un artículo publicado por la revista Peer. (Telégrafo, 2014)

"Dice que existe problemas de Aprendizaje escolar cuando los docentes en su práctica docente no utilicen los medios adecuados por cumplir con los objetivos propuestos en la práctica docente" (Azcoaga, 2015).

En la Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato no se cuenta con un sistema de reconocimiento facial para la autentificación de usuarios en cursos online; los estudiantes ingresan a sus aulas virtuales de forma manual insertando un nombre de usuario y contraseña.

Árbol de problemas

1.2.2 Análisis Crítico

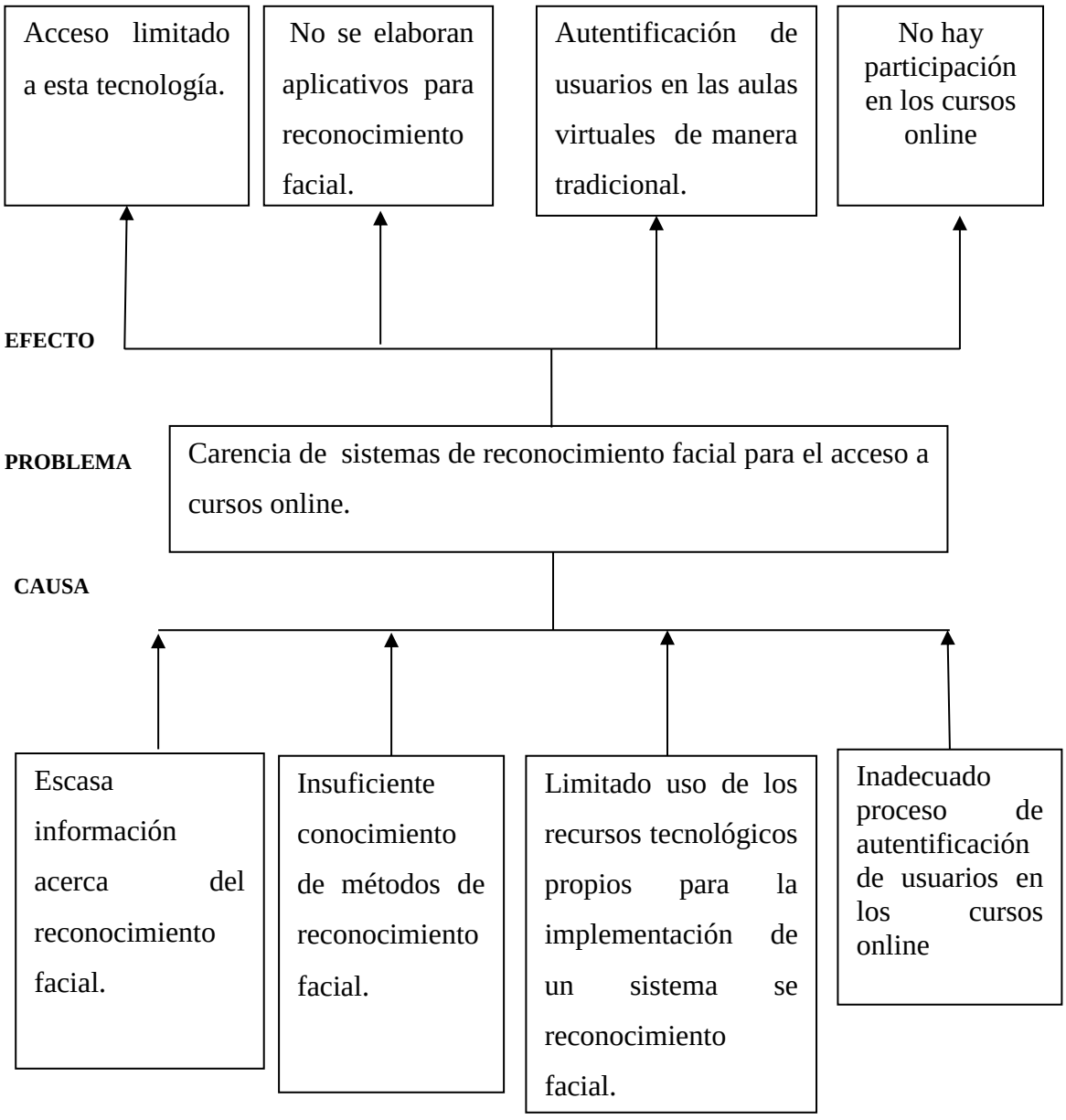


Gráfico 1. Árbol del Problema
Elaborado por: Ruth Jimena Naranjo Quispe

Luego de hacer un sondeo previo en la carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato se ha visto que se cuenta con escasa información acerca del reconocimiento facial provocado por la carencia de sistemas de reconocimiento facial para acceso a cursos online, dando como resultado un acceso limitado a esta tecnología.

El insuficiente conocimiento de métodos de reconocimiento facial, al ser este tema poco difundido por la carencia de sistemas de reconocimiento facial para el acceso a cursos online, limitan a un funcional criterio debido a que no se elaboran aplicativos para el reconocimiento facial, por la falta de dispositivos ya que éstos tienen un alto costo.

El limitado uso de los recursos tecnológicos propios para la implementación de un sistema se reconocimiento facial, por la carencia de sistemas de reconocimiento facial para el acceso a cursos online ha logrado que la autentificación de usuarios en las aulas virtuales se de una manera tradicional.

El inadecuado proceso de autentificación de usuarios en los cursos online produce carencia de sistemas de reconocimiento facial para el acceso a cursos online ocasionando que no haya participación en los cursos online, dando un ambiente poco seguro dentro de los sistemas informáticos.

1.2.3 Prognosis

En el caso de no tomar en cuenta el tema de investigación propuesto se registrará el dispendio de tiempo debido a que en la actualidad la tecnología facilita la mayor parte de los procesos, es necesario que las instituciones puedan estar a la par con estas aplicaciones, tal es así que la Facultad de Ciencias Humanas y de la Educación, utiliza todos sus recursos orientados a mejorar los procesos de formación académico profesional, tanto los docentes como los estudiantes puedan utilizar aulas virtuales

como herramientas alternativas e innovadoras de apoyo al proceso enseñanza aprendizaje y uno de sus mayores problemas es autentificar a sus usuarios para evitar suplantación de personalidad o acceso a usuarios no permitidos, se requiere contar con más recursos que fomenten y faciliten el acceso a cursos online para garantizar que el estudiante que está accediendo a ese curso sea él mismo y así evitar cualquier tipo de fraude en los cursos, uno de los aspectos que se va a mantener es que seguirá existiendo escasa información acerca del reconocimiento facial, insuficiente conocimiento de métodos de reconocimiento facial, limitado uso de los recursos tecnológicos propios para la implementación de un sistema de reconocimiento facial y por lo tanto creando inseguridad con un fácil acceso para cualquier usuario.

1.2.4 Formulación del problema

¿Cómo ayudará el proceso de Reconocimiento Facial aplicado a la Autentificación de Usuarios en cursos online de la carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato?

1.2.5 Preguntas Directrices

- ¿Qué Aplicaciones informáticas existen en el mercado para el sistema de reconocimiento facial?

- ¿Ayudará un Sistema de reconocimiento facial a una mejor autentificación en cursos online?

- ¿De qué manera ayudará el reconocimiento facial para la autentificación de usuarios?

1.2.6 Delimitación del objeto de investigación

Contenidos
Área: Tecnológico
Campo: Pedagogía- Desempeño Profesional
Aspecto: Gestión Administrativa

Espacial:

La presente investigación se llevó cabo en la carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato.

Temporal:

La investigación se realizó en el periodo comprendido entre Enero-Agosto del 2015.

1.3 JUSTIFICACIÓN

El **interés** de este proyecto pretende que los estudiantes puedan garantizar su autentificación en los cursos online y que no pueda ingresar ninguna otra persona que no sea el mismo estudiante matriculado en dicho curso.

La **Importancia teórica** de este proyecto radica en que los docentes podrán conocer a ciencia cierta quienes están ingresando al curso y cuáles son los estudiantes matriculados en el mismo con la debida autentificación facial.

La **novedad** es el uso de nuevas plataformas virtuales, ya que se fomenta el desarrollo o uso de Software libre aplicado al material educativo.

La **utilidad** radica en el uso de un Sistema de reconocimiento facial para garantizar la autentificación de los estudiantes en cursos online.

Los beneficiarios de este proyecto serán tanto los estudiantes como los docentes de la Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato.

El **Impacto Social** se refleja en el Mejoramiento de la calidad de vida, en la ampliación del número de personas que utilizarán Software educativo.

En el aspecto **económico** se pretende el incremento en la eficiencia y reducción de los costos de la elaboración de software educativo, el incremento en la **competitividad** que permitirá un mejor acceso de los estudiantes de la Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato".

En el **criterio institucional**, forjará el aprovechamiento de los recursos de software y hardware tales como el recurso del talento humano educativo.

En el **aspecto ambiental** tiene auge ya que se elimina la utilización de cuadernos y hojas contribuyendo de manera integral a la conservación de los árboles. Fortalecimiento de las actividades propias de un curso online.

Factibilidad

Es factible **económicamente** la presente investigación pues se cuenta con los recursos económicos propios del investigador quien financiará los gastos de hardware y software así como los gastos que se generen propios de la investigación, en cuanto a la adquisición de equipos de oficina en caso de ser necesario.

Tecnológicamente es factible debido a que la investigación presenta un Software innovador poco utilizado, integrado software que eliminara la espacialidad y la temporalidad por medio de aplicaciones gratuitas que podemos encontrar fácilmente en la web, lo cual permitirá el desarrollo adecuado del Sistema de reconocimiento facial para la autentificación de estudiantes en cursos online.

1.4 OBJETIVOS

1.4.1 General

Determinar la influencia del reconocimiento facial aplicado a la autentificación de los usuarios de cursos online en la Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato

1.4.2 Específicos

- Diagnosticar los recursos de autentificación que utilizan los estudiantes para el acceso a cursos online en la Carrera de Docencia en Informática.

- Fundamentar teóricamente la influencia de un Sistema de Reconocimiento facial en la autentificación de los estudiantes de cursos online en la Carrera de Docencia en Informática

- Proponer un recurso tecnológico para mejorar Sistema de Reconocimiento facial para la autentificación de cursos online en la Carrera de Docencia en Informática

CAPÍTULO II

MARCO TEORICO

2.1 ANTECEDENTES INVESTIGATIVOS

La presente investigación se basa en los siguientes antecedentes investigativos que fueron producto de una revisión bibliográfica tanto en la biblioteca de la Facultad de Ciencias Humanas y Educación y otras dependencias de la Universidad Técnica de Ambato así como en las bibliotecas virtuales y revistas digitales que hacen referencia a artículos científicos. De los cuales podemos citar las siguientes:

Gracias a las mejoras tecnológicas el diseño y desarrollo de un sistema de reconocimiento de caras, cada día es más utilizado, labores que tradicionalmente eran realizadas por seres humanos, son ahora realizadas por sistemas automatizados.

Una de las actividades que pueden automatizarse y que ha cobrado gran importancia, es la capacidad de establecer la identidad de los individuos. En relación con esta tarea se están desarrollando grandes avances en distintos campos como la biometría, reconocimiento de patrones, procesado y clasificación de imágenes (Gámez Jiménez, 2009)

La motivación general que ha guiado este proyecto ha sido profundizar en el estudio de las técnicas que permiten realizar un reconocimiento automático de caras e implementar un sistema que realice esta tarea.

Se ha desarrollado un Sistema de Reconocimiento de Caras que resuelve la detección de la cara dentro de la imagen, la extracción de características y finalmente

el reconocimiento del individuo. Todo ello se ha implementado utilizando Matlab. (Gámez Jiménez, 2009)

En este proyecto se han utilizado imágenes estáticas en color. Se ha trabajado con las imágenes en el espacio de color RGB (aunque también se utiliza el YcbCr para la creación de mapas y ojos) y con su transformación en escala de grises. Se pretende conseguir de esta manera una mayor información acerca de las imágenes para poder facilitar el reconocimiento (Gámez Jiménez, 2009).

Esta investigación de acuerdo a lo anteriormente mencionado, se manifiesta que ha sido de mucha importancia debido a que el sistema biométrico para la autentificación por medios alternativos se basa o fundamenta en la imagen digital facial estática, además se debe tomar en cuenta que las imágenes deben ser tomadas con mucho cuidado porque puede influenciar diferentes factores como las luz, posición acercamiento entre otras para que el sistema resulte eficaz.

El reconocimiento automático de caras se profundizó en el estudio del algoritmo EBGM el cual utiliza descriptores de Gabor locales. Para ello se partió de una implementación en lenguaje de programación C/C++ existente. Se logró mejorar el desempeño de dicha implementación, así como también, superar el desempeño del algoritmo original.

Se realizó estudio distintas formas de mejorar la implementación del algoritmo considerado. Entre ellas, se destaca un estudio estadístico para compensar la potencia de los descriptores locales de Gabor con el objetivo de aplicarlos al Reconocimiento de Caras. Los buenos resultados obtenidos remarcan la importancia de las conclusiones. (Aguerrebere, Capdehourat, Delbracio, & Mateu, http://iie.fing.edu.uy, s.f.)

Por otro lado, se desarrolló un Sistema de Reconocimiento de Caras, que resuelve la adquisición de la imagen, la detección de la cara, la extracción de características y finalmente el reconocimiento facial. Siendo utilizado este sistema biométrico de autentificación facial como prototipo en un lenguaje de alto nivel, pero con código libre para su modificación parcial o total debido a que se estructura en función de módulos independientes.

Este tema aporta significativamente en la investigación ya que este sistema de reconocimiento, está orientado a una aplicación de control de acceso, utilizando como característica biométrica la imagen del rostro de una persona y podríamos usar como guía para la investigación y desarrollo del sistema de conocimiento facial orientado para la autentificación en cursos online. (Aguerrebere, Capdehourat, Delbracio, & Mateu, http://iie.fing.edu.uy, s.f.)

El diseño e implementación de una herramienta de detección facial influye positivamente en la detección de rostros, esto es una necesidad en la actualidad para varias aplicaciones como la de video conferencia, indexación y sobre todo de video vigilancia.

Su importancia crece con la consideración que es la primera etapa en un sistema de reconocimiento de rostro. La gran apariencia del objeto rostro, hace que su detección sea considerada una tarea difícil para el reconocimiento de patrones (García Chang, 2009)**.**

Siguiendo el criterio de los párrafos anteriores se manifiesta que se logró el objetivo principal establecido en el principio de esta tesis que es el desarrollo de un sistema de detección facial. Muchos métodos de detección de rostro comparten las mismas técnicas y algoritmos de reconocimiento de patrones y análisis de imágenes a pesar que los tres últimos apuntan aplicaciones distintas.

Combinar la detección de rostro con la detección del ojo para mejorar la clasificación no resulta siempre eficaz. Al contrario puede empeorar los resultados además de aumentar el tiempo de computación y perder uno de los puntos clave de esta técnica que es su respuesta en tiempo real.

Podemos rescatar de esta investigación que con este método se consigue detectar el rostro en tiempo real. La investigación tiene un papel importante durante el proceso de enseñanza aprendizaje ya que mediante las aulas virtuales se intenta vincular a los estudiantes de forma activa y reflexiva con la tecnología TIC's para facilitar el aprendizaje en los estudiantes donde se permita una comunicación entre estudiantes y docentes en un entorno de aprendizaje virtual y privado.

2.2 FUNDAMENTACIÓN FILOSÓFICA

La investigación se encuentra enmarcada dentro del paradigma constructivista, porque enfoca, conceptualiza y analiza una problemática educativo y plantea una alternativa de solución, ya que el presente proyecto orienta sus esfuerzos al desarrollo de un sistema de reconocimiento facial orientado a la autentificación de estudiantes en cursos online, debiendo ser un proceso de aprendizaje que debe valorar y estimular el pensamiento crítico y ético y la consecuente formación de la responsabilidad del estudiante que precisa aprender a tomar decisiones y tener el valor para asumirlas.

2.3 FUNDAMENTACIÓN TECNOLÓGICA

Como consecuencia del desarrollo tecnológico, en la actualidad se plantean nuevas exigencias y necesidades, este criterio se fundamenta holísticamente para lograr una alfabetización tecnológica y científica, así se construirá una nueva cultura tecnológica. Resulta interesante contemplar a la tecnología durante el proceso de enseñanza-aprendizaje. Logrando concebir a la enseñanza desde la perspectiva de una racionalidad

práctica científica, permitiendo la construcción de un conocimiento que logre relacionar los modelos científicos con la realidad.

2.4 FUNDAMENTACIÓN LEGAL

El presente trabajo de investigación se basa en las siguientes leyes: La Constitución Política Del Ecuador 2008

Capítulo segundo. Derechos del buen vivir. Sección cuarta. Cultura y Ciencia.

Art. 22.- Las personas tienen derecho a desarrollar su capacidad creativa, al ejercicio digno y sostenido de las actividades culturales y artísticas, y a beneficiarse de la protección de los derechos morales y patrimoniales que les correspondan por las producciones científicas, literarias o artísticas de su autoría.
Art. 25.- Las personas tienen derecho a gozar de los beneficios y aplicaciones del progreso científico y de los saberes ancestrales.

Título VII. Régimen del buen vivir. Sección octava. Ciencia, tecnología, innovación y saberes ancestrales

Artículo 385 numeral 3: Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

Artículo 387: Será responsabilidad del Estado:

Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo.

Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica, y potenciar los saberes ancestrales, para así contribuir a la realización del buen vivir, al sumakkawsay.

Asegurar la difusión y el acceso a los conocimientos científicos y tecnológicos, el usufructo de sus descubrimientos y hallazgos en el marco de lo establecido en la Constitución y la Ley.

Garantizar la libertad de creación e investigación en el marco del respeto a la ética, la naturaleza, el ambiente, y el rescate de los conocimientos ancestrales.
Reconocer la condición de investigador de acuerdo con la Ley.

2.5 CATEGORÍAS FUNDAMENTALES

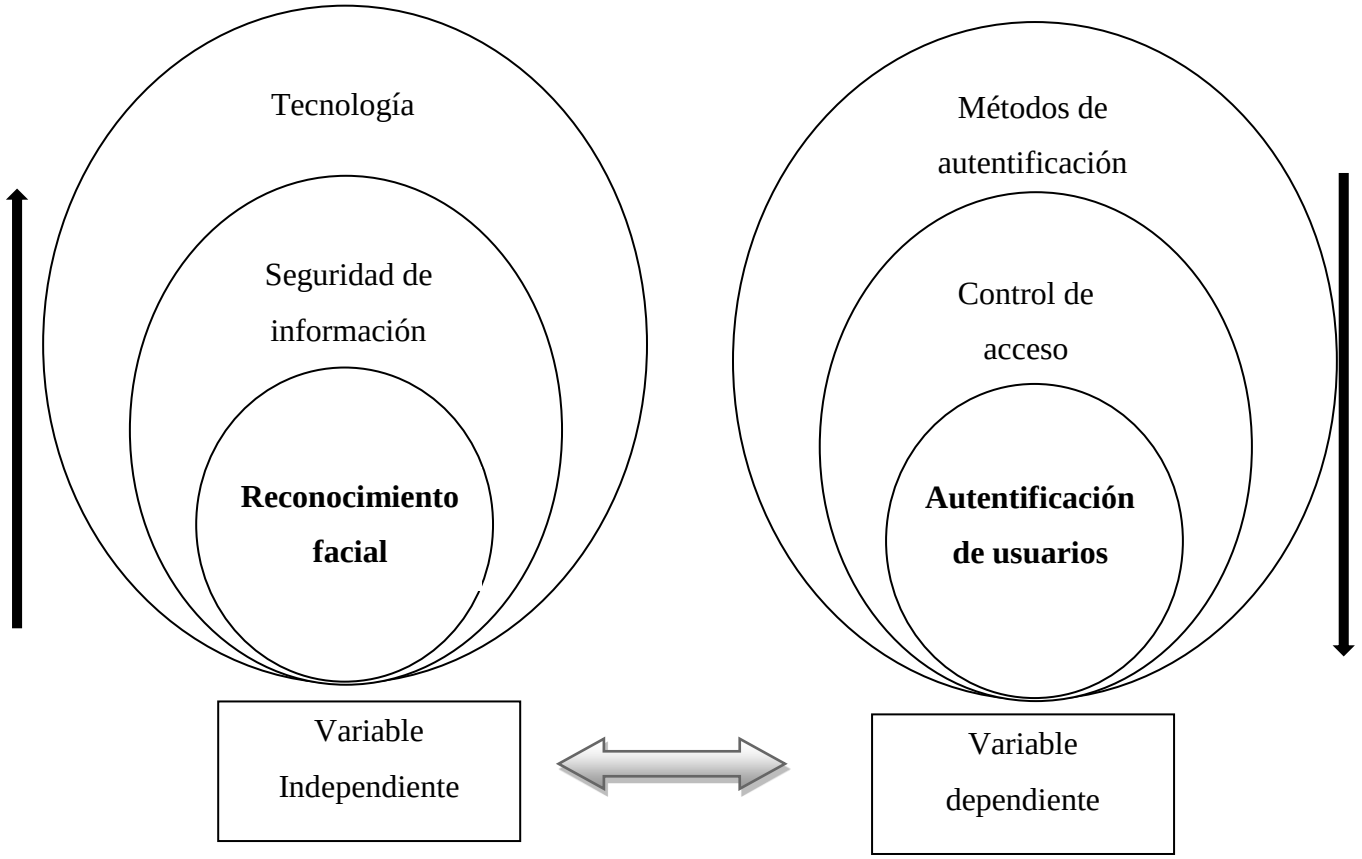


Gráfico 2. Categorías Fundamentales
Elaborado por: Ruth Jimena Naranjo Quispe

2.6 CONSTELACIÓN DE VARIABLES

Variable Independiente: Reconocimiento facial

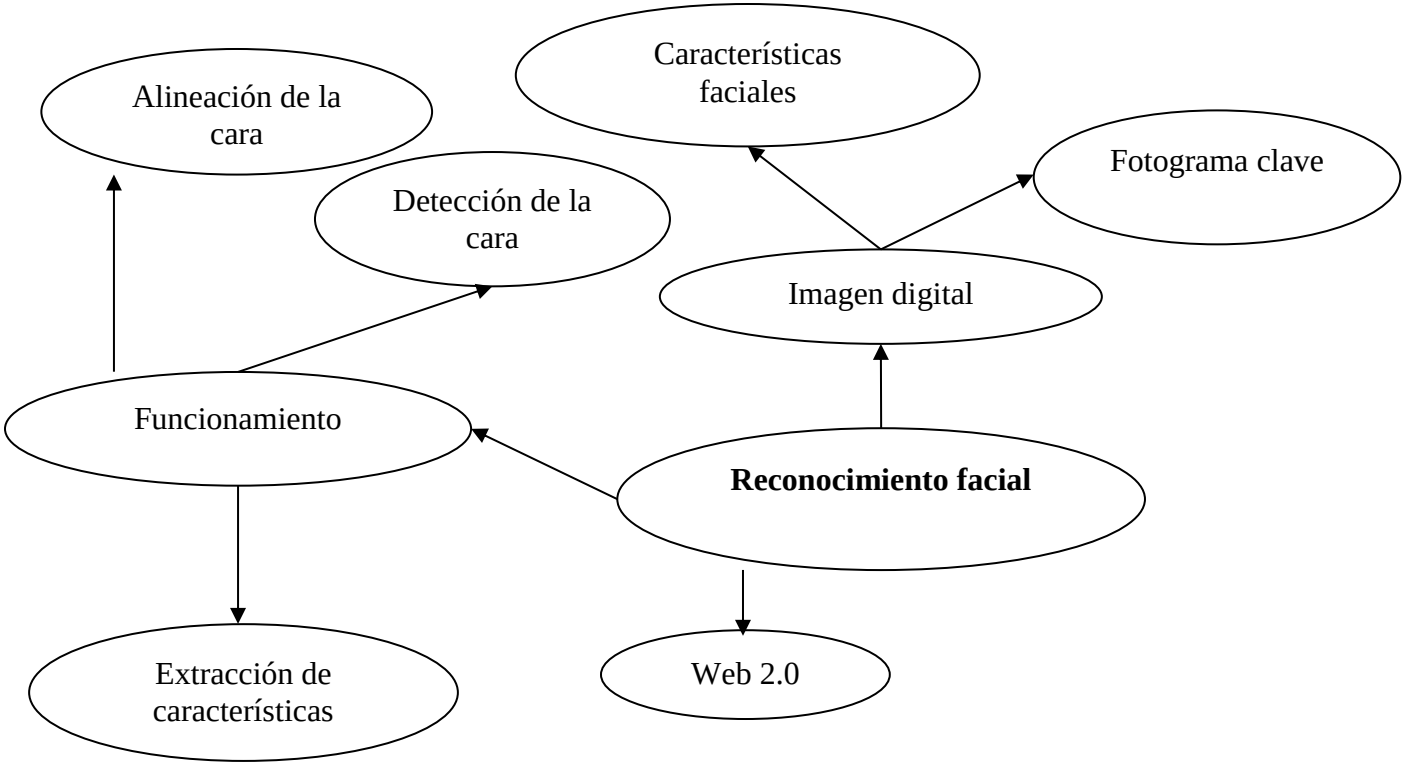


Gráfico 3. Variable Independiente
Elaborado por: Ruth Jimena Naranjo Quispe

Variable Dependiente: Autentificación de usuarios

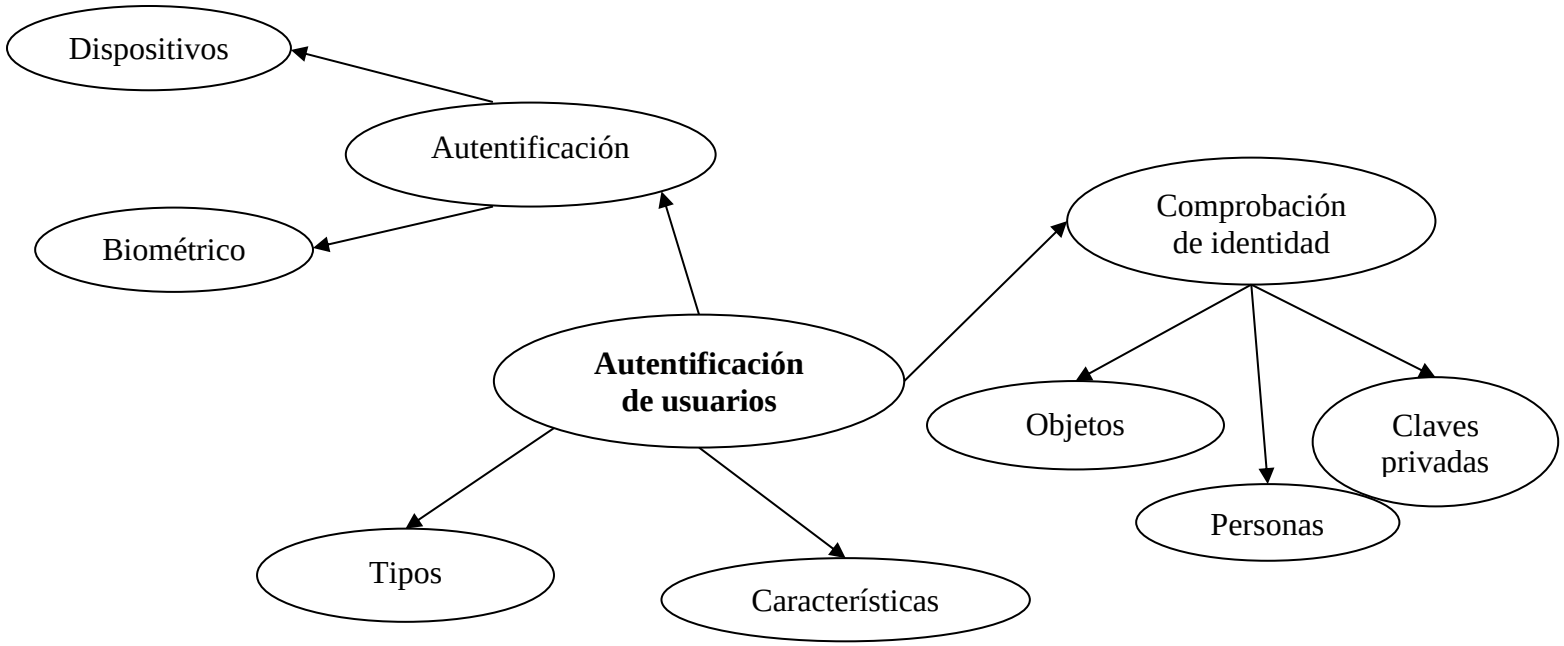


Gráfico 4. Variable Dependiente
Elaborado por: Ruth Jimena Naranjo Quispe

VARIABLE INDEPENDIENTE

TECNOLOGÍA

La tecnología se define usualmente como el conjunto de herramientas hechas por el hombre, como los medios eficientes para un fin, o como el conjunto de artefactos materiales. Pero la tecnología también contiene prácticas instrumentales, como la creación, fabricación y uso de los medios y las máquinas; incluye el conjunto material y no-material de hechos técnicos; está íntimamente conectada con las necesidades institucionalizadas y los fines previstos a los cuales las tecnologías sirven. (Werner, LA TECNOLOGÍA: SUS FORMAS Y LAS DIFERENCIAS DE LOS MEDIOS, 2001)

De acuerdo a la cita anterior, en la era en la que vivimos estamos constantemente rodeados de tecnología, como ejemplo se puede consultar en internet, realizar llamadas, enviar emails, por tanto facilita la vida del ser humano ya sea para ser más eficaces en nuestro trabajo, todo esto permite llegar a obtener una educación significativa de calidad y dejando atrás el método tradicional.

La Web 2.0

El término Web 2.0 fue acuñado por el americano Dale Dougherty de la editorial O'Reilly Media durante el desarrollo de una conferencia en el año 2004. El término surgió para referirse a nuevos sitios web que se diferenciaban de los sitios web más tradicionales englobados bajo la denominación Web 1.0. La característica diferencial es la participación colaborativa de los usuarios. Un ejemplo de sitio web 1.0 sería la Enciclopedia Británica donde los usuarios pueden consultar en línea los contenidos elaborados por un equipo de expertos. Como alternativa web 2.0 se encuentra la Wikipedia en la cual los usuarios que lo deseen pueden participar en la construcción de sus artículos. Poco tiempo después, en el año 2005, Tim O'Reilly definió y ejemplificó el concepto de Web 2.0 utilizando el mapa conceptual elaborado por Markus Angermeier (Intef, s.f.).

De acuerdo al párrafo anterior se manifiesta que la Web social dentro de la historia de redes sociales se le conoce como de segunda generación, siendo características de las mismas: Usabilidad, economía, diseño, estandarización, remezclabilidad, convergencia y participación.

Educación virtual

Sobre educación virtual en Ecuador, no se puede hablar demasiado, las experiencias de las Instituciones Universitarias Ecuatorianas han sido escasas ya sea por las condiciones tecnológicas del país como por la demanda casi inexistente de educación mediada por tecnologías.

Es necesario diferenciar entre educación virtual o en línea en la que el desarrollo de los programas es completamente a través de las Nuevas Tecnologías de la Información y Comunicaciones (NTIC´s) y educación a distancia tradicional o semipresencial con apoyo de las NTIC´s.

En Ecuador la aplicación de tecnologías en el desarrollo de programas académicos inició en el año 1999 y se fortaleció en los años posteriores, para en el año 2002 ya contar con ofertas de formación continuada y de pregrado completamente en línea (Torres , Diagnóstico de la Educación Virtual en Ecuador, 2002).

De acuerdo a la cita anterior en el Ecuador los educadores y estudiantes, con el cambio constante de paradigma en el proceso de enseñanza aprendizaje existe el constante e innovador método de educación por medio de la web, rompiendo la espacialidad y temporalidad, características de la educación virtual.

Edmodo

Según (Garza, PLATAFORMA EDMODO, 2012): “EDMODO, una plataforma social privada para Educación.

El empleo de esta red social nos facilita la interacción a través de las respuestas de los estudiantes, de los comentarios y de las exposiciones que realizan en las diferentes actividades cada uno de los miembros de los diferentes grupos que realicen"

De acuerdo a la cita anterior, EDMODO es una plataforma virtual interactiva que en la actualidad tiene mucha acogida por facilidad de uso debido a que no se necesita la instalación de ningún programa y basta ingresar a la página web de Edmodo e inmediatamente comenzar a utilizarlo.

Moodle

Moodle es un software diseñado para ayudar a los educadores a crear cursos en línea de alta calidad y entornos de aprendizaje virtuales. Tales sistemas de aprendizaje en línea son algunas veces llamados VLEs (Virtual Learning Environments) o entornos virtuales de aprendizaje.

La palabra Moodle originalmente es un acrónimo de Modular Object-Oriented Dynamic Learning Environment (Entorno de Aprendizaje Dinámico Orientado a Objetos y Modular).

Una de las principales características de Moodle sobre otros sistemas es que está hecho en base a la pedagogía social constructivista, donde la comunicación tiene un espacio relevante en el camino de la construcción del conocimiento. Siendo el objetivo generar una experiencia de aprendizaje enriquecedora (Entornos educativos, 2015)**.**

Qué es una Tutoría en Línea

Una Tutoría en Línea en Perseptia es una sesión sincrónica de aprendizaje en la web en donde interactúan un estudiante y un facilitador de Perseptia de manera escrita, verbal, y visual en un aula virtual de aprendizaje. El objetivo de esta sesión

interactiva es desarrollar habilidades en un tema específico de las Matemáticas que le permitan al estudiante un desempeño eficaz y eficiente en dicho tema. (Perseptia, 2016)

SEGURIDAD DE INFORMACIÓN

Seguridad de la información: distintas formas y estados de los datos
Para conocer la diferencia principal con la seguridad de la información, revisemos otros conceptos interesantes que nos permitirán tener el contexto general. De acuerdo con la Real Academia Española (RAE), la seguridad se define como "libre o exento de todo peligro, daño o riesgo". Sin embargo, se trata de una condición ideal, ya que en la realidad no es posible tener la certeza de que se pueden evitar todos los peligros (Mendoza, Ciberseguridad o seguridad de la información, 2015)

"Seguridad" apunta a una condición ideal, ya que no existe la certeza de que se pueden evitar todos los peligros. Su propósito es reducir riesgos hasta un nivel aceptable para los interesados. El propósito de la seguridad en todos sus ámbitos de aplicación es reducir riesgos hasta un nivel que sea aceptable para los interesados en mitigar amenazas latentes. En un sentido amplio, por seguridad también se entienden todas aquellas actividades encaminadas a proteger de algún tipo de peligro (Mendoza, Ciberseguridad o seguridad de la información, 2015)

Sin embargo, la información puede encontrarse de diferentes maneras, por ejemplo en formato digital (a través de archivos en medios electrónicos u ópticos), en forma física (ya sea escrita o impresa en papel), así como de manera no representada - como pueden ser las ideas o el conocimiento de las personas. En este sentido, los activos de información pueden encontrarse en distintas formas.
Además, la información puede ser almacenada, procesada o transmitida de diferentes maneras: en formato electrónico, de manera verbal o a través de mensajes escritos o impresos, por lo que también es posible encontrarla en diferentes estados. (Mendoza, Ciberseguridad o seguridad de la información, 2015)

La información requiere de medidas de protección adecuadas de acuerdo con su importancia y criticidad, y éste es precisamente el ámbito de la seguridad de la información por lo tanto, sin importar su forma o estado, la información requiere de medidas de protección adecuadas de acuerdo con su importancia y criticidad, y éste es precisamente el ámbito de la seguridad de la información (Mendoza, Ciberseguridad o seguridad de la información, 2015).

Recordemos que la seguridad en cómputo se limita a la protección de los sistemas y equipos que permiten el procesamiento de la información, mientras que la seguridad informática involucra los métodos, procesos o técnicas para el tratamiento automático de la información en formato digital, teniendo un alcance mayor, ya que incluye la protección de las redes e infraestructura tecnológica.

Por ejemplo y con base en las definiciones, cuando se busca proteger el hardware, redes, software, infraestructura tecnológica o servicios, nos encontramos en el ámbito de la seguridad informática o ciberseguridad. Cuando se incluyen actividades de seguridad relacionadas con la información que manejan las personas, seguridad física, cumplimiento o concientización nos referimos a seguridad de la información (Mendoza, Ciberseguridad o seguridad de la información, 2015)

Principales diferencias entre ciberseguridad y seguridad de la información.

Luego de revisar los conceptos, es posible identificar las principales diferencias y por lo tanto conocer cuándo aplicar un concepto u otro. En primer lugar, resaltamos que la seguridad de la información tiene un alcance mayor que la ciberseguridad, puesto que la primera busca proteger la información de riesgos que puedan afectarla, en sus diferentes formas y estados (Mendoza, Ciberseguridad o seguridad de la información, 2015).

Por el contrario, la ciberseguridad se enfoca principalmente en la información en formato digital y los sistemas interconectados que la procesan, almacenan o transmiten, por lo que tiene un mayor acercamiento con la seguridad informática. Además, la seguridad de la información se sustenta de metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos, que soportan la idea de protección en las distintas facetas de la información; también involucra la aplicación y gestión de medidas de seguridad apropiadas, a través de un enfoque holístico (Mendoza, Ciberseguridad o seguridad de la información, 2015).

Por lo tanto, sin importar los límites de cada concepto, el objetivo principal es proteger la información, independientemente de que ésta pertenezca a una organización o si se trata de información personal, ya que nadie está exento de padecer algún riesgo de seguridad.

Ahora que conocemos la definición de cada término y su alcance, podemos utilizarlos haciendo las distinciones correspondientes, pues seguramente seguiremos aplicando el concepto. Con los avances tecnológicos que se incorporan cada vez más a nuestra vida cotidiana, la dependencia a la tecnología aumenta, y en consecuencia lo hace la necesidad de aplicar la ciberseguridad. (Mendoza, Ciberseguridad o seguridad de la información, 2015)

Reconocimiento Facial

El reconocimiento facial es una herramienta que se utiliza para verificar si las personas son quienes realmente dicen que son y ha adquirido mucha importancia con la aparición de Internet, donde los fraudes son comunes. Pero la mayoría de los reconocedores faciales requieren que el usuario esté delante de la pantalla 'posando' y esperando a que se le tome la foto (Reizabal, 2015).

La tecnología de reconocimiento facial no es algo nuevo, y existen a muchas definiciones e interpretaciones de su terminología. Por ello conviene definirla claramente en el contexto del presente Dictamen. Imagen digital:

Una imagen digital es una representación bidimensional de una imagen en forma digital. No obstante, los últimos avances en tecnología de reconocimiento facial requieren la inclusión de imágenes tridimensionales, además de las imágenes estáticas y en movimiento (es decir, fotografías y videos grabados y en directo).

Reconocimiento facial: El reconocimiento facial es el tratamiento automático de imágenes digitales que contienen las caras de personas a fines de identificación, autenticación/verificación o categorización de dichas personas. El proceso de reconocimiento facial está compuesto por una serie de subprocesos diferenciados:

a) **Obtención de la imagen:** Es el proceso de captar la cara de una persona y convertirla en formato digital (la imagen digital). En un servicio en línea y móvil, la imagen puede haberse obtenido en un sistema diferente, por ejemplo, haciendo una fotografía con una cámara digital que, a continuación, se transfiere a un servicio en línea.

b) **Detección de la cara:** En este proceso se detecta la presencia de una cara dentro una imagen digital y se marca la zona.

c) **Normalización:** Es el proceso de atenuar las variantes entre las regiones faciales detectadas, por ejemplo, convirtiéndolas en dimensiones estándar, rotándolas o alineando las distribuciones de los colores.

d) **Extracción de características:** Es el proceso de aislar y extraer las características reproductibles y distintivas de la imagen digital de una persona. La extracción de características puede ser holística, basada en las características o una combinación de ambos métodos. El conjunto de características clave puede almacenarse en una plantilla para ser comparado posteriormente.

e) **Registro:** Cuando una persona se somete por primera vez a un determinado sistema de reconocimiento facial, la imagen y/o la plantilla pueden almacenarse como registro para comparaciones posteriores.

f) **Comparación:** Es el proceso de medir la similitud existente entre un conjunto de características (la muestra) y otro registrado previamente en el sistema. Los principales objetivos de la comparación son la identificación y la autenticación/verificación. Un tercer objetivo de la comparación es la categorización, que consiste en extraer las características de una imagen de una persona a fin de clasificarla en una o varias categorías generales (edad, sexo, color de la ropa, etc.). Un sistema de categorización no tiene por qué tener un proceso de registro (Jacob, 2012).

VARIABLE DEPENDIENTE

Autenticación de usuarios

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.
Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación (Segu.info, 2009).

Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:
Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc (Segu.info, 2009).

Algo que la persona posee: por ejemplo una tarjeta magnética.
Algo que el individuo es y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz (Segu.info, 2009).

Algo que el individuo es capaz de hacer: por ejemplo los patrones de escritura.
Para cada una de estas técnicas vale lo mencionado en el caso de la seguridad física en cuanto a sus ventajas y desventajas. Se destaca que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también, los más costosos por lo dificultosos de su implementación eficiente (Segu.info, 2009).

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina "single login" o sincronización de passwords (Segu.info, 2009).

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos. (Segu.info, 2009)

De acuerdo a lo mencionado anteriormente se manifiesta que es necesario que los usuarios adopten medidas de seguridad utilizando medios de autentificación de usuario de los que disponen sus ordenadores personales.

1. Técnicas de identificación y autenticación La identificación digital forma parte indisoluble de la mayoría de servicios en Internet y las TIC. Por ejemplo, para colgar un vídeo en un servidor, se pide que el usuario esté dado de alta en el servicio y se identifique para poder llevar a cabo la publicación del contenido. Por otra parte, para utilizar una red social, es preciso que el usuario esté registrado. Asimismo, los contactos de esta red también deben estar convenientemente identificados. Para realizar acciones tan variadas como hacer un pago mediante tarjeta de crédito, utilizamos esta misma tarjeta para identificarnos. O bien para hacer gestiones bancarias a través de Internet, lo primero que haremos es especificar quién somos. Esta identificación digital puede ser relativamente sencilla. Basta con disponer de un nombre de usuario, usar como identificador la dirección de correo electrónico o, en el caso de un pago, usar el número de tarjeta de crédito. Ahora bien, para la mayoría de servicios, además de la identificación digital, es necesaria una autenticación de esta identidad. (Martínez, Identificación autenticación y control de acceso, s.f.)

Esquema de un sistema de autentificación.

Vamos a empezar por definir un diagrama para realizar la autentificación de usuario en unas páginas web, que nos servirá para programar luego las páginas ajustándose al diagrama.

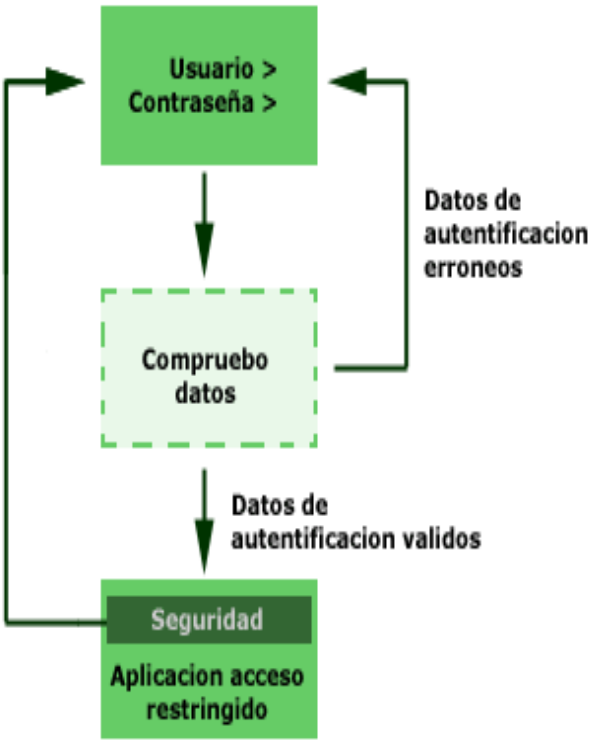


Gráfico 5. Esquema de un sistema de autentificación
Elaborado por: Ruth Jimena Naranjo Quispe

En la imagen anterior podemos ver el diagrama, que empieza por la página donde se pide un usuario y contraseña para acceder a la aplicación de acceso restringido.

Los datos de autentificación (usuario y contraseña escritos en la página inicial) se envían a la página dibujada con línea de puntos, que se encarga de hacer una comprobación de dichos datos del usuario. Según los datos de autentificación, se re direcciona al navegador a la página de la aplicación restringida, en caso de que sean correctos, o a la página donde volver a escribir el usuario/contraseña, en caso de que sean incorrectos. Esta página la he dibujado con línea de puntos porque no es una página donde se pare el navegador para nada, sino que sólo es una página de paso que re direcciona a un sitio u otro dependiendo de los datos que reciba.

La aplicación de acceso restringido, aparte de mostrar las funcionalidades que queríamos proteger con usuario contraseña, debe de realizar unas comprobaciones de seguridad para saber si se ha pasado con éxito el proceso de autentificación o si se está intentando acceder de manera no permitida a esa página. Esta comprobación

la he dibujado como una capa con color verde más oscuro sobre la página de la aplicación. Si no se satisface dicha comprobación (el usuario no se ha autentificado correctamente) se vuelve a la página donde escribir el usuario y la contraseña. (Álvarez, Funcionamiento del sistema de autentificación en PHP, 2002)

CONTROL DE ACCESO

La definición más generalizada de un sistema de control de acceso hace referencia al mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos. Básicamente encontramos sistemas de controles de acceso en múltiples formas y para diversas aplicaciones. Por ejemplo, encontramos sistemas de controles de acceso por software cuando digitamos nuestra contraseña para abrir el correo, otro ejemplo es cuando debemos colocar nuestra huella en un lector para encender el PC. Estos casos, son ejemplos que permiten el acceso a datos. Sin embargo, nuestro enfoque en la seguridad electrónica está relacionado al acceso de recursos, en nuestro caso, apertura de una puerta, un torniquete o una talanquera por ejemplo. (Villegas, ¿ Qué es un Sistema de Control de Acceso ?, 2009)

Claro está, que la definición que interesa debe estar dada en términos de seguridad electrónica:

Un sistema de control de acceso es un sistema electrónico que restringe o permite el acceso de un usuario a un área específica validando la identificación por medio de diferentes tipos de lectura (clave por teclado, tags de proximidad o biometría) y a su vez controlando el recurso (puerta, torniquete o talanquera) por medio de un dispositivo eléctrico como un electroimán, cantonera, pestillo o motor (Villegas, ¿ Qué es un Sistema de Control de Acceso ?, 2009)

Básicamente los controles de acceso se clasifican en dos tipos:
Sistemas de Control de Acceso Autónomos
Sistemas de Control de Acceso en Red

Los Sistemas de Control de Acceso Autónomos son sistemas que permiten controlar una o más puertas, sin estar conectados a un PC o un sistema central, por lo tanto, no guardan registro de eventos. Aunque esta es la principal limitante, algunos controles de acceso autónomos tampoco pueden limitar el acceso por horarios o por grupos de puertas, esto depende de la robustez de la marca. Es decir, los más sencillos solo usan el método de identificación (ya sea clave, proximidad o biometría) como una "llave" electrónica (Villegas, ¿ Qué es un Sistema de Control de Acceso ?, 2009)

Los Sistemas de Control de Acceso en Red son sistemas que se integran a traves de un PC local o remoto, donde se hace uso de un software de control que permite llevar un registro de todas las operaciones realizadas sobre el sistema con fecha, horario, autorización, etc. Van desde aplicaciones sencillas hasta sistemas muy complejos y sofisticados según se requiera. (Villegas, ¿ Qué es un Sistema de Control de Acceso ?, 2009)

Ejemplo de un Sistema de Control de Acceso en Red:

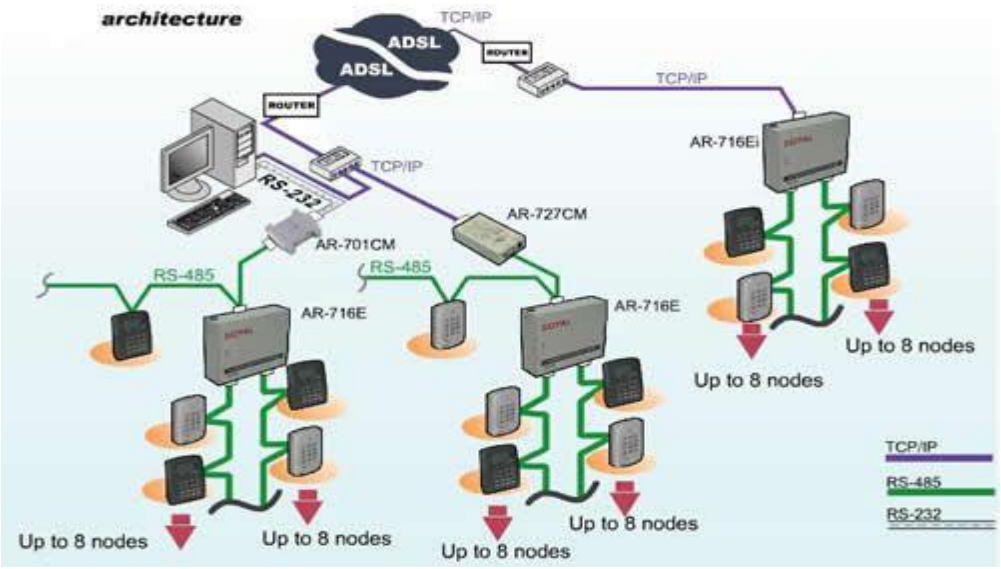


Gráfico 6. Sistema de Control de Acceso en
Elaborado por: Ruth Jimena Naranjo Quispe

MÉTODOS DE AUTENTIFICACIÓN

Perspectiva de los métodos de autenticación multifactor y de la evolución de los llaveros token a los teléfonos inteligentes.

Más vieja que la propia web, la autenticación de múltiples factores es un método de tecnología de seguridad de TI que requiere que la gente proporcione múltiples formas de identificación o de información para confirmar la legitimidad de su identidad para una transacción en línea o con el fin de tener acceso a una aplicación corporativa. El objetivo de los métodos de autenticación multifactorial es aumentar la dificultad con la que un adversario puede explotar el proceso de inicio de sesión para vagar libremente por las redes personales o corporativas y así comprometer equipos de cómputo con el fin de robar información confidencial, o algo peor.

En pocas palabras, la autenticación multifactorial toma algo que sólo cada usuario posee (una huella digital, la impresión de voz, un llavero token, un código de seguridad, o una pieza de software en un teléfono inteligente) y lo combina con otro factor, algo que el usuario sabe (tal como el diálogo habitual de inicio de sesión de usuario/contraseña) para demostrar que él o ella es legítimamente quien dice ser (Strom, 2016)

La autenticación de múltiples factores antes se llamaba autenticación de dos factores, pero hoy en día hay muchos factores diferentes que se pueden emplear para la seguridad adicional, por lo que ha prevalecido la nomenclatura de la primera sobre la segunda. Muchos en TI probablemente recuerdan los escáneres biométricos de mano que asegura muchos puntos de entrada a un centro de datos como si fuera su primer roce con este tipo de dispositivos.

Tokens AMF: De los llaveros a los smartphones

Para los empleados móviles, los generadores de contraseñas de un solo uso que vienen en forma de llaveros con una pequeña pantalla LCD y un botón se pusieron de moda originalmente durante los primeros días de la autenticación de múltiples

factores, hace más de una década. Cuando un usuario pulsa el botón, la pantalla en el llavero muestra una secuencia de números durante 30 segundos. El usuario debe escribir exactamente esta secuencia dentro de ese período de tiempo en la aplicación o recurso al que trata de acceder (Strom, 2016)

Los códigos de acceso generados por los llaveros se verifican contra un servidor ubicado en la red de la empresa para asegurar que coincidan. Este servidor ejecuta los procesos de gestión de identidad, establece diversas políticas de seguridad y conecta los tokens con las tiendas de directorio de usuario, como Active Directory o RADIUS.

Si una secuencia de número introducido coincide, el usuario tiene permiso de acceso. Si no, él o ella deben comenzar de nuevo, presionando el botón en el llavero para generar un nuevo código de acceso general (Strom, 2016).

Aunque estos tokens estaban bien como una solución multifactorial en ese entonces y, de hecho, todavía se utilizan en algunos sectores, los llaveros hoy se consideran una tecnología un poco anticuada. No son perfectos, tampoco: Tomemos, por ejemplo, el sofisticado ataque de phishing llamado Emmental (por el queso suizo) que se utilizó a principios de este año y que combina un certificado falsificado con un ataqueman-in-the-middle en un inicio de sesión con autenticación de dos factores (Strom, 2016).

Llevar el registro de los tokens o los llaveros también es engorroso, y un usuario tal vez no tenga el token requerido a la mano cuando necesite iniciar sesión en algún lugar. Además, está la carga adicional de tener que desactivar o terminar el acceso del usuario cuando éste deja la empresa, o si se pierde un llavero.

¿La respuesta a estos problemas? Teléfonos inteligentes.
Diversas aplicaciones de teléfonos inteligentes se han construido para generar las mismas contraseñas de un solo uso como llaveros, y pueden ayudar a aliviar los problemas anteriormente mencionados. Y, conforme Apple y Google añadan

sensores de huellas digitales a sus teléfonos, el segundo factor puede ir más allá de simples contraseñas numéricas de un solo uso hacia el reconocimiento de la copia digital de la huella digital de un usuario a través de un escáner incorporado en un teléfono inteligente (Strom, 2016)

Otros tipos de factores secundarios habilitados por los teléfonos inteligentes y otros dispositivos móviles incluyen el uso de mensajes de texto SMS, correos electrónicos y cámaras para escanear un código QR que aparece en la página web cuando se trata de iniciar sesión en una aplicación o recurso, o realizar una transacción.

El creciente atractivo de la autenticación de múltiples factores como las contraseñas se han vuelto inseguras, las herramientas multifactoriales han ampliado su uso desde el núcleo original de los trabajadores de TI a casi todo el mundo en muchas grandes empresas, sobre todo cuando se está consumiendo información personal. También han ido más allá de las herramientas iniciales de gestión de identidades y ahora también son productos comunes de inicio único de sesión (Strom, 2016)

Seguridad informática en la era del cómputo de nube.

Además de todo esto, con la proliferación de los servicios Web basados en la oferta de software como servicio (SaaS) y el número de contraseñas reutilizadas, los métodos de autenticación multifactorial se han vuelto más importantes y han ampliado su atractivo para las PyMEs. Además, empresas de la talla de Facebook, LinkedIn, Twitter, Gmail, Apple y muchos otros proveedores han adoptado estas herramientas para asegurar sus propios inicios de sesión (Strom, 2016).

Si las empresas aún no se han involucrado en el uso y soporte de herramientas multifactoriales, encontrarán que se requiere un poco de esfuerzo para configurarlas y desplegarlas. Las herramientas tienen un montón de piezas móviles y las empresas necesitarán especialistas de diferentes partes de su organización de TI para

coordinar y configurar la infraestructura y conseguir que los accesos protegidos funcionen correctamente (Strom, 2016).

Aunque las más nuevas herramientas de autenticación de factores múltiples son un poco más fáciles de manejar, todavía implican un cierto esfuerzo de integración. En ese sentido, algunos de estos productos incluyen varios agentes de software que pueden proteger a las VPN, servidores de SharePoint, Outlook Web App y servidores de bases de datos, por ejemplo.

Por último, un desarrollo relativamente reciente ha movido los servidores multifactoriales tradicionales basados en sitio hacia hardware en la nube. La mayoría de los proveedores de soluciones de múltiples factores ofrecen ambas opciones, y observan que los clientes eligen los despliegues fuera del sitio más que nunca gracias a la flexibilidad que la nube genera en términos de apoyo y gestión (Strom, 2016).

El costo de los modelos de precios de la autenticación multifactorial, los costos típicos para el despliegue de soluciones de autenticación de múltiples factores son unos pocos dólares al mes, por token. Sin embargo, esto puede llegar a múltiples decenas de miles de dólares por año para las empresas que tienen una gran cantidad de usuarios o tokens, o ambos (Strom, 2016)

El panorama se complica con la forma en que cada proveedor tiene una manera diferente para calcular el precio de la línea de fondo: hay descuentos por cantidad, descuentos plurianuales y tarifas de soporte 24x7. Algunos cobran sobre una base por token (con diferentes tarifas para tokens de hardware o software), mientras que otros lo hacen sobre una base por usuario o por servidor. Otros tienen precios de componentes añadidos o capas de integración (Strom, 2016).

Ciertamente, las herramientas de autenticación de factores múltiples valen la molestia, sobre todo porque el número de exploits de contraseñas sigue aumentando y acapara los titulares. Las empresas necesitan mejores formas de proteger la

información de acceso de los usuarios más allá de la simple combinación usuario/contraseña (Strom, 2016).

Una encuesta rápida del panorama actual pone de relieve cómo se está utilizando la tecnología de autenticación de múltiples factores en cada vez más lugares. Basta con mirar el número de despliegues por varios servicios de medios sociales y SaaS para consumidores. La combinación de un robusto panorama de productos de autenticación multifactor y la conciencia del usuario sobre la importancia de una sólida autenticación de los usuarios significa que tal vez nunca ha habido un momento más favorable para que las empresas consideren la autenticación de múltiples factores (Strom, 2016).

2.7 HIPÓTESIS

El proceso de reconocimiento facial incide en la autentificación de usuarios en cursos online de la carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato.

2.8 SEÑALAMIENTO DE VARIABLES

Variable Independiente: Reconocimiento Facial

Variable Dependiente: Autentificación de Usuarios

CAPÍTULO III

METODOLOGIA DE LA INVESTIGACIÓN

3.1 ENFOQUE

La presente investigación se basa en un enfoque cualitativo, ya que ayudará a los estudiantes a adquirir y desarrollar conocimientos y habilidades que faciliten su proceso de formación. "Utiliza la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación" (Fernandez, 2006), este enfoque analiza la autentificación facial para cursos online, como formación integral de los estudiantes con competencias tecnológicas.

Es cuantitativa por que busca las causas de los hechos que generan el problema, en forma que se puede tabular, contabilizar por medio de un proceso que requiere de cálculos matemáticos y de la interpretación estadística de los datos y sus resultados.

3.2 MODALIDAD BÁSICA DE LA INVESTIGACIÓN

De Campo

La investigación tendrá la modalidad de campo porque se estará en contacto con el problema, con los involucrados como son los estudiantes, maestros y usuarios de la Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato y en el lugar mismo de la investigación

Investigación Bibliográfica

Porque se ha investigado en libros, textos, artículos científicos e internet. Esta forma de investigación ayuda al propósito del tema planteado, para ampliar y profundizar los diferentes enfoques, teorías, conceptualizaciones y criterios de los diferentes autores; además es importante apoyarnos en fuentes primarias y secundarias para explicar de manera teórica y científica el proceso de investigación.

3.3 NIVEL O TIPO DE INVESTIGACIÓN

Exploratoria.- Se describe las características del problema con el contexto Investigado a nivel exploratorio en una acción preliminar que nos permitirá reconocer e indagar para tener una idea general del objeto de investigación, es un estudio poco estructurado.

Descriptiva.- El nivel descriptivo que se orienta a determinar cómo se manifiesta el problema, cuando se busca especificar las cualidades importantes para analizar los componentes del fenómeno estudiado que se apoyaran en criterios de clasificación de los datos del nivel anterior, tomando en cuenta que es un nivel de investigación de medición precisa y requiere de conocimientos suficientes para realizar comparaciones entre los fenómenos o problemas que producen algún malestar dentro de la institución.

Explicativa.- Al final se propenderá a llegar al nivel explicativo con el estudio minuciosamente estructurado en la propuesta de solución al problema.

3.4 POBLACIÓN Y MUESTRA

La investigación se desarrolló en los predios de Huachi Loreto de la Universidad Técnica de Ambato en la Facultad de Ciencias Humanas y de la Educación, con los estudiantes de la Carrera de Docencia en Informática.

Para ello se ha tomado una muestra referente a la población existente relacionada a estudiantes, la misma que asciende a 96 usuarios que se detallan en el siguiente cuadro, a quienes se les aplicará las encuestas.

Carrera de Docencia en Informática	**Estudiantes**
Primero	28
Segundo	-
Tercero	-
Cuarto	-
Quinto	17
Sexto	-
Séptimo	16
Octavo	18
Noveno	-
Décimo	17
Total	**96**

Tabla 1: Población y muestra
Elaborado por: Ruth Jimena Naranjo Quispe

3.5 OPERACIONALIZACIÓN DE VARIABLES

Variable Independiente: Reconocimiento facial

CATEGORIZACIÓN	CATEGORIAS	INDICADORES	ITEMS	TECNICAS/ INSTRUMENTOS
El reconocimiento facial es el tratamiento automático de imágenes digitales que para un buen funcionamiento debe seguir deferentes técnicas o algoritmos contienen las caras de personas a fines de identificación, autenticación/verificación o categorización de dichas personas.	Reconocimiento facial Imagen Digital Funcionamiento Técnicas o algoritmos	Herramienta tecnológica Características faciales. Fotograma clave Detección de la cara Alineación de la cara Extracción de características. Reconocimiento Técnicas 3D Holísticas Locales y geométricas.	¿Utiliza usted un curso online? ¿Le gustaría que en su curso online la autentificación sea por medio de reconocimiento facial? ¿Ha usado usted algún sistema de reconocimiento facial? ¿Considera usted que para el correcto funcionamiento de un sistema de reconocimiento facial es importante al alineación de la cara? ¿Considera usted que es necesario el uso de técnicas 3D en las aulas virtuales?	Técnica: Encuesta Instrumento: Cuestionario

Cuadro 2. Operacionalización: Variable Independiente
Elaborado por: **Ruth Jimena Naranjo Quispe**

Variable Dependiente: Autentificación de usuarios

CATEGORIZACIÓN	CATEGORIAS	INDICADORES	ITEMS	TECNICAS/ INSTRUMENTOS
La **autenticación** es la comprobación de la identidad de una persona o de un objeto, por tanto es importante que los usuarios adopten medidas de seguridad de redes de datos ya que por medio de éstas y de diferentes métodos de autentificación se llega a la comprobación de la identidad.	Autentificación de usuarios Seguridad de datos y redes Métodos Comprobación de identidad	Identidad Persona Claves privadas Autentificación Autorización Contraseñas Dispositivos Biométricos	¿Usted usaría un Sistema de reconocimiento facial para la comprobación de su identidad? ¿Considera usted que para mejorar la seguridad de datos es recomendable usar un sistema de reconocimiento facial? ¿Cuál de estos métodos ha utilizado usted para autentificarse al momento del ingreso a las aulas virtuales? Manual () Biométrico () Dispositivos () ¿Conoce usted algún dispositivo que contenga un sistema de autentificación? Considera usted que el uso de un sistema de reconocimiento facial mejoraría la autentificación en los cursos online.	Técnica: Encuesta Instrumento: Cuestionario

Cuadro 3: Operacionalización: Variable Dependiente
Elaborado por: Ruth Jimena Naranjo Quispe.

3.6 PLAN DE RECOLECCIÓN DE INFORMACIÓN

La recolección de datos que servirá para el proceso de investigación se hará con diferentes técnicas e instrumentos que ayudará a recopilar información referente a la inclusión educativa de los estudiantes con discapacidad visual.

Para recolectar la información se utilizará una encuesta a los estudiantes de la Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato.

Nº	Preguntas	Respuestas
1	¿Para qué?	Para alcanzar los objetivos de la investigación
2	¿A qué personas u objetos?	Estudiantes de la Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato
3	¿Sobre qué aspecto?	Autentificación en cursos online
4	¿Quién? ¿Quiénes?	Ruth Jimena Naranjo Quispe
5	¿Cuándo?	Periodo académico 2014 - 2015.
6	¿Lugar de recolección de la información?	Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato
7	¿Cuántas veces?	
8	¿Qué técnicas de recolección?	Encuesta estructurada. Entrevista
9	¿Con qué?	Cuestionario.
10	¿En qué situación?	Favorable porque existe la colaboración por parte de la comunidad educativa.

Cuadro 4: Plan de recolección de información
Elaborado por: Ruth Jimena Naranjo Quispe

3.7 PLAN DE PROCESAMIENTO DE LA INFORMACIÓN

- Diseño de materiales de recolección de Información.
- Aplicación de la encuesta.
- Revisión crítica de la información recogida, es decir, se hará la limpieza de la información defectuosa: contradictoria, incompleta, no pertinente, etc.
- Tabulación o cuadros según variables de cada hipótesis: manejo de información, estudio estadístico de datos para presentación de resultados.
- Representaciones gráficas.
- Análisis e interpretación de resultados.
- Análisis de los resultados estadísticos, destacando tendencias o relaciones fundamentales de acuerdo con los objetos e hipótesis.
- Interpretación de resultados, con apoyo del marco teórico, en el aspecto pertinente.
- Comprobación de hipótesis.
- Establecimiento de conclusiones y recomendaciones.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 ANÁLISIS DE LOS RESULTADOS

De conformidad al proyecto de investigación se aplicó la encuesta a 96 estudiantes de la Facultad de Ciencias Humanas y de la Educación, teniendo prioridad con los estudiantes de la Carrera de Docencia en Informática.

4.1.1 ENCUESTA A ESTUDIANTES

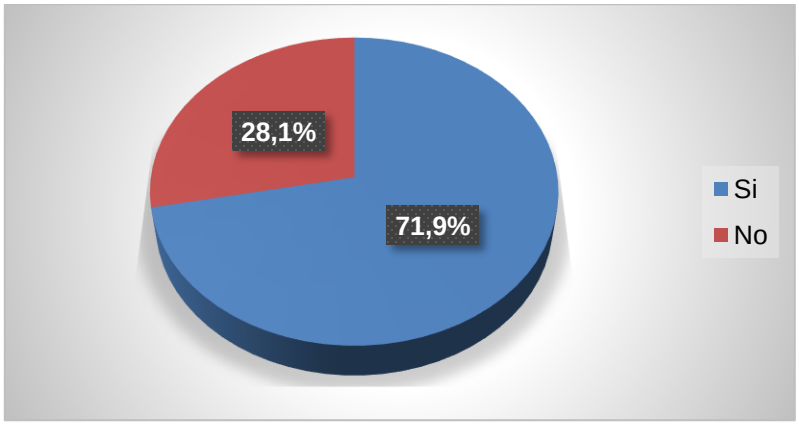
Pregunta Nº 1. ¿Utiliza usted un curso online?

Cuadro 5.Utilización de cursos online

Alternativas	Frecuencia	Porcentaje
Si	69	71,9
No	27	28,1
TOTAL	96	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 6. Utilización de cursos online



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

El 71,9% de los estudiantes encuestados han confirmado que utilizan un curso online, mientras que un 28,1% afirma que no utiliza un curso online.

Interpretación:

Se puede evidenciar que la mayoría de los estudiantes han utilizado alguna vez o utilizan actualmente un curso online, lo que determina que los estudiantes si utilizan medios tecnológicos para realizar consultas e investigaciones en las bibliotecas virtuales, a diferencia que unos pocos prefieren utilizar medios tradicionales por desconocer del tema.

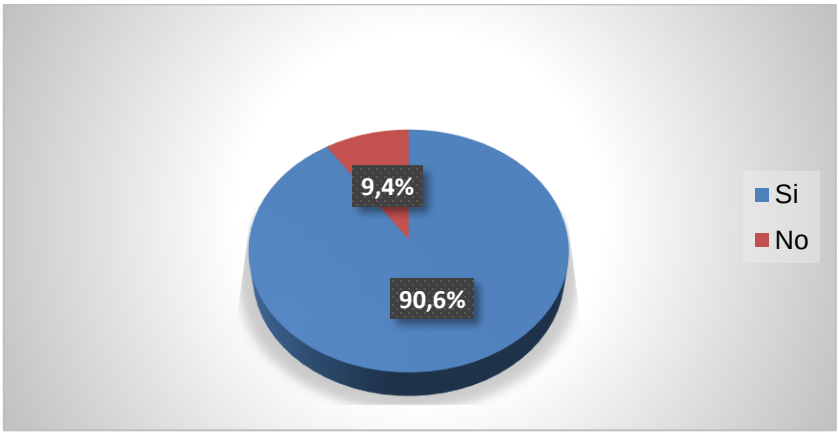
Pregunta Nº 2. ¿Le gustaría que en su curso online la autentificación sea por medio de reconocimiento facial?

Cuadro 6. Preferencia de autentificación en curso online

Alternativas	Frecuencia	Porcentaje
Si	87	90,6
No	9	9,4
TOTAL	96	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 7. Preferencia de autentificación en curso online



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

Respecto a la Pregunta 2, el 90,6% de los estudiantes encuestados aseguran que les gustaría que en su curso online la autentificación sea por medio de reconocimiento facial; mientras que el 9,4% piensan que no les gustaría que en su curso online la autentificación sea por medio de reconocimiento facial.

Interpretación:

Se puede determinar que a la mayoría de los estudiantes les gustaría que en su curso online la autentificación sea por medio de reconocimiento facial, debido a que la tecnología es un medio seguro de autentificación y de acceso rápido, en un mundo globalizado todos deben conocer estos medios tecnológicos porque en cualquier aspecto de la vida se va tener que utilizar estos medios tecnológicos como en un banco o aeropuertos que ya se utiliza y cada día este tipo de autentificación es más común en cursos online.

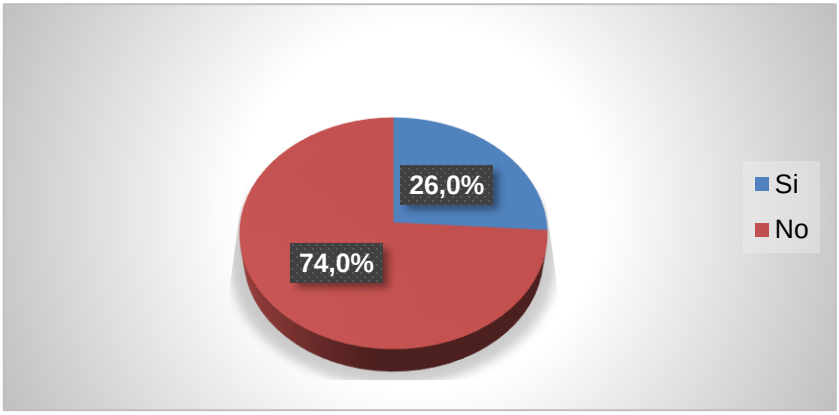
Pregunta Nº 3. ¿Ha usado usted algún sistema de reconocimiento facial?

Cuadro 7. Utilización del Sistema de reconocimiento facial

Alternativas	Frecuencia	Porcentaje
Si	25	26,0
No	71	74,0
TOTAL	96	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 8. Utilización del Sistema de reconocimiento facial



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

De los estudiantes encuestados, el 26% afirma que alguna vez ha usado algún tipo de sistema de reconocimiento facial, mientras que el 74% ha manifestado que no han utilizado ningún tipo de sistema de reconocimiento facial.

Interpretación:

Se puede manifestar que la mayoría de los estudiantes encuestados no han utilizado un sistema de reconocimiento facial, en tanto que unos pocos si han utilizado alguna vez, por lo tanto se determina el desconocimiento de este medio de autentificación por medios tecnológicos e innovadores, en los cursos virtuales se generaliza el reconocimiento facial para la autentificación de identificación y de registro, de ahí se evidencia la falta de actualizarse en estas nuevas tecnologías por el cambio de paradigmas en los medios informáticos online.

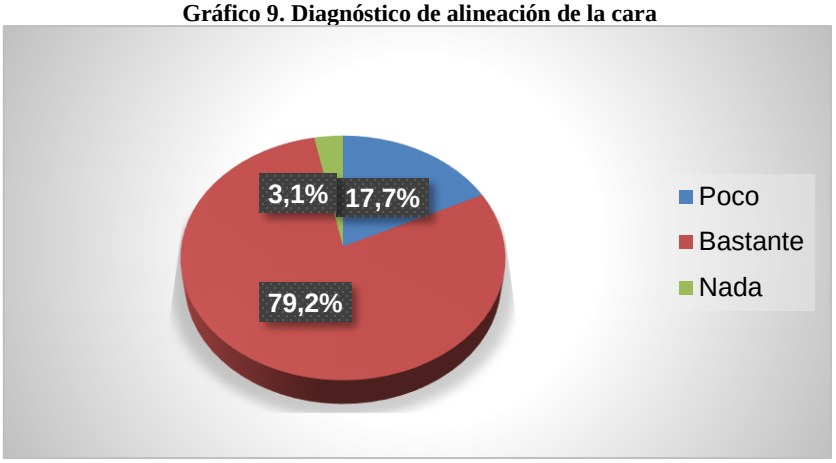
Pregunta Nº 4. ¿Considera usted que para el correcto funcionamiento de un sistema de reconocimiento facial es importante al alineación de la cara?

Cuadro 8. Diagnóstico de alineación de la cara

Alternativas	Frecuencia	Porcentaje
Poco	17	17,7
Bastante	76	79,2
Nada	3	3,1
TOTAL	96	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 9. Diagnóstico de alineación de la cara



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

Referente a la Pregunta 4, podemos notar que el 79,2% de los encuestados afirman que para el correcto funcionamiento del reconocimiento facial es bastante importante la alineación de la cara, en tanto un 7% considera que es poco importante, y al mismo tiempo el 3,1% de los encuestados piensan que no es importante la alineación de la cara para el reconocimiento facial.

Interpretación:

Se puede afirmar que la mayoría de los estudiantes encuestados han coincidido en que para el correcto funcionamiento de un sistema de reconocimiento facial es bastante importante la alineación de la cara, en tanto unos pocos consideran que es poco importante, y otro grupo más pequeño de los encuestados afirman que no es importante la alineación de la cara para un sistema de reconocimiento facial, al ser una variable bastante importante y al ser un sistema sensible a los mínimos cambios es necesario tener en consideración, además de ser muy metódico y cuidadoso al realizar el registro en la autentificación.

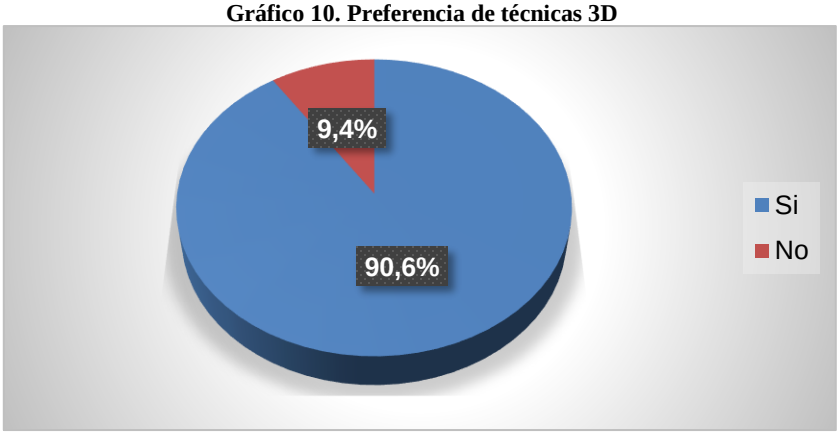
Pregunta Nº 5. ¿Considera usted que es necesario el uso de técnicas 3D en las aulas virtuales?

Cuadro 9. Preferencia de técnicas 3D

Alternativas	Frecuencia	Porcentaje
Si	87	90,6
No	9	9,4
TOTAL	96	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 10. Preferencia de técnicas 3D



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

El 90,6% de los estudiantes encuestados consideran que es necesario el uso de técnicas 3D en las aulas virtuales, mientras que el 9,4% restante afirman que no es necesario en uso de técnicas 3D en las aulas virtuales.

Interpretación:

Se determina que la mayoría de los estudiantes consideran que es necesario el uso de técnicas de 3D en las aulas virtuales, en tanto unos pocos opinan que no es necesario el uso de técnicas 3D en las aulas virtuales, siendo una herramienta imprescindible en la autentificación facial debido a que es un método de registro online.

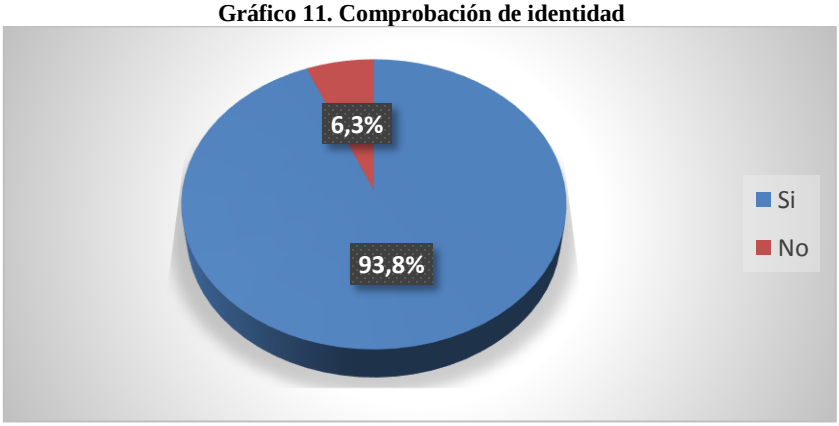
Pregunta Nº 6. ¿Usted usaría un Sistema de reconocimiento facial para la comprobación de su identidad?

Cuadro 10. Comprobación de identidad

Alternativas	Frecuencia	Porcentaje
Si	90	93,8
No	6	6,3
TOTAL	96	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 11. Comprobación de identidad



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

Con los valores obtenidos en la Pregunta 6, el 93,8% de los estudiantes encuestados afirman que si usarían un sistema de reconocimiento facial para la comprobación de su identidad, mientras que el restante 6,3% mencionaron que no usarían un sistema de reconocimiento facial para la comprobación de su identidad.

Interpretación:

Se puede deducir que la mayoría de los estudiantes encuestados si usarían un sistema de reconocimiento facial para la comprobación de su identidad, mientras que en menor cantidad manifestaron que no usarían un sistema de reconocimiento facial para la comprobación de su identidad, debido a que el registro es un poco complicado y demoroso, mientras que el resto de alumnos piensan que se deben acostumbrar a este tipo de autentificación.

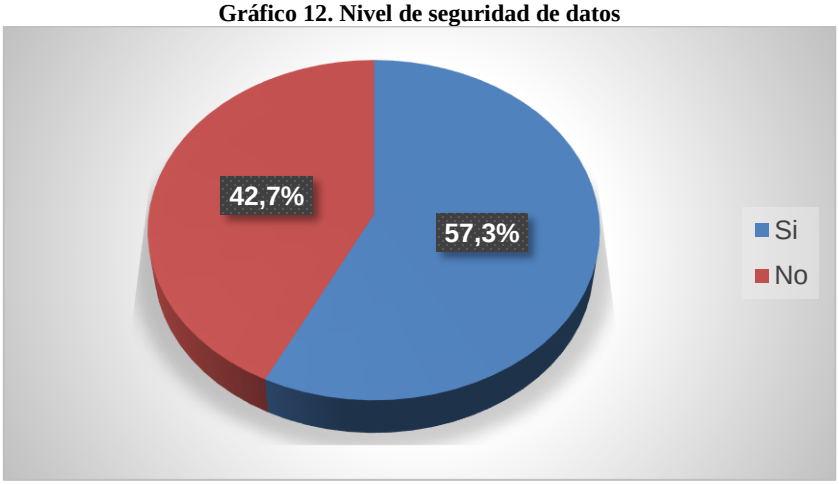
Pregunta Nº 7. ¿Considera usted que para mejorar la seguridad de datos es recomendable usar un sistema de reconocimiento facial?

Cuadro 11. Nivel de seguridad de datos

Alternativas	Frecuencia	Porcentaje
Si	55	57,3
No	41	42,7
TOTAL	96	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 12. Nivel de seguridad de datos



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

El 57,3% de los encuestados consideran que si es recomendable el uso de un sistema de reconocimiento facial para mejorar la seguridad de datos, en tanto el otro 42,7% supone que no es recomendable el uso de un sistema de reconocimiento facial para mejorar la seguridad de datos.

Interpretación:

Se puede determinar que un poco más de la mitad de los estudiantes encuestados consideran que si es recomendable el uso de un sistema de reconocimiento facial para mejorar la seguridad de datos, mientras que otro grupo considera que no es recomendable el uso de un sistema de reconocimiento facial para mejorar la seguridad de datos, tomando en cuenta que sería muy difícil violar la seguridad de autentificación fácil, debido a que cada rostro es diferente porque existe mucha diferencia entre uno y otro rostro y esto se refleja en una matriz algorítmica única para cada persona.

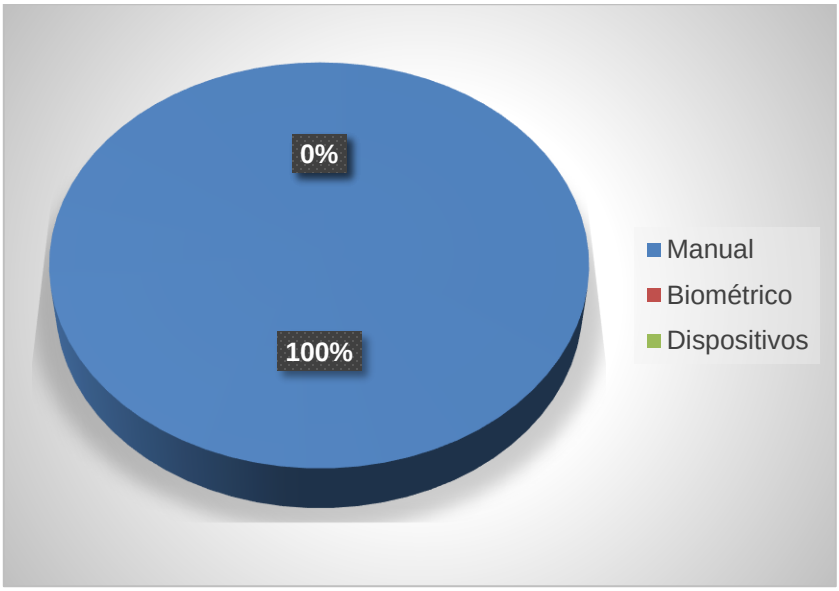
Pregunta Nº 8. ¿Cuál de estos métodos ha utilizado usted para autentificarse al momento del ingreso a las aulas virtuales?

Cuadro 12. Elección de Métodos de autentificación

Alternativas	Frecuencia	Porcentaje
Manual	96	100,0
Biométrico	0	0,0
Dispositivos	0	0,0
TOTAL	96	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 13. Elección de Métodos de autentificación



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

Con respecto a la Pregunta 8, el 100% de los estudiantes encuestados afirman que él método que han usado para autentificarse al momento del ingreso a las aulas virtuales ha sido el método manual.

Interpretación:

Se puede determinar que todos los estudiantes encuestados han usado el método manual al momento de la autentificación en sus aulas virtuales, es decir por medio de una clave, la misma que cualquier informático puede violar dicha seguridad por medio de software de ahí la necesidad de medios de autentificación innovadores y novedosos como lo es el reconocimiento facial.

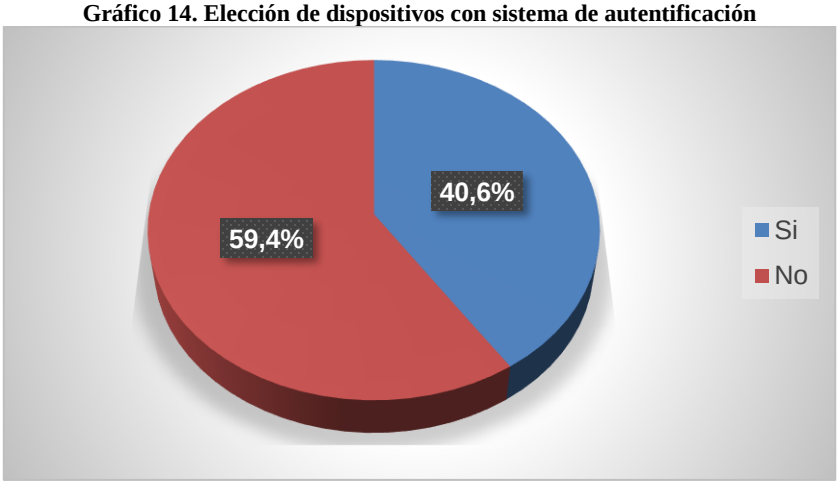
Pregunta Nº 9. ¿Conoce usted algún dispositivo que contenga un sistema de autentificación?

Cuadro 13. Elección de dispositivos con sistema de autentificación

Alternativas	Frecuencia	Porcentaje
Si	39	40,6
No	57	59,4
TOTAL	96	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 14. Elección de dispositivos con sistema de autentificación



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

Respecto a la Pregunta 9, se observa que un 59,4% de los estudiantes encuestados aseguran que no conocen ningún dispositivo que contenga un sistema de autentificación, mientras el otro 40,6% afirman que si conocen dispositivos que contienen un sistema de autentificación.

Interpretación:

Se puede verificar que la mayoría de los estudiantes encuestados afirman que no conocen un dispositivo con un sistema de autentificación, mientras que otro grupo de es los encuestados manifestaron que si conocen dispositivos con un sistema de autentificación, este particular se debe a que las empresas y unidades educativas utilizan muy poco dispositivos biométricos o tecnológicos, tal vez por desconocimiento o por no innovarse.

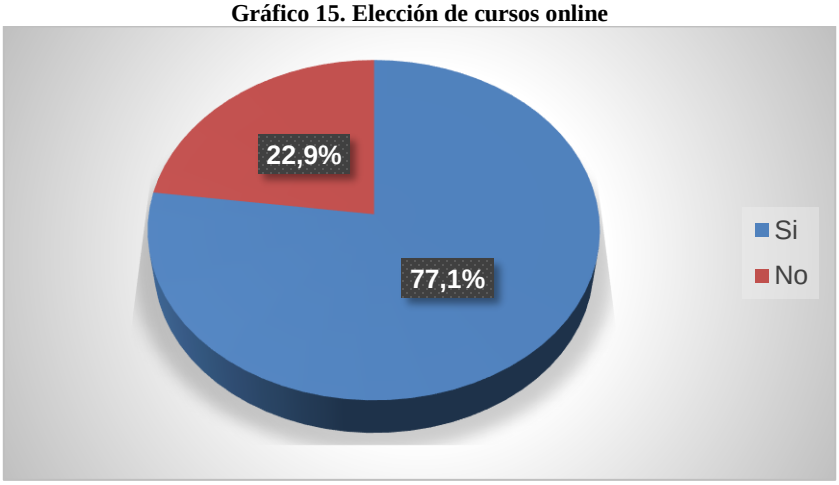
Pregunta Nº 10. Considera usted que el uso de un sistema de reconocimiento facial mejoraría la autentificación en los cursos online.

Cuadro 14. Elección en cursos online

Alternativas	Frecuencia	Porcentaje
Si	74	77,1
No	22	22,9
TOTAL	96	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 15. Elección de cursos online



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

De los valores obtenidos para la Pregunta 10, se determina que el 77,1% de los estudiantes encuestados consideran que el uso de un sistema de reconocimiento facial mejoraría la autentificación en los cursos online, y el 22,9% restante considera que el uso de reconocimiento facial no mejoraría la autentificación en los cursos online.

Interpretación:

Se puede identificar que la mayoría de los estudiantes encuestados consideran que con el uso de un sistema de reconocimiento facial mejoraría la autentificación en los cursos online, mientras que otro grupo pequeño de los estudiantes encuestados opinan que el uso de reconocimiento facial no mejoraría la autentificación en los cursos online. Pero en definitiva el avance tecnológico no se puede detener y por ende los estudiantes deben adquirir estas competencias informáticas para estar al mismo nivel de otras instituciones educativas de elite, por considerarse el reconocimiento facial como algo muy complicado existe cierta oposición a la aplicación de innovadoras sistemas de autentificación.

4.1.2 ENCUESTA A DOCENTES

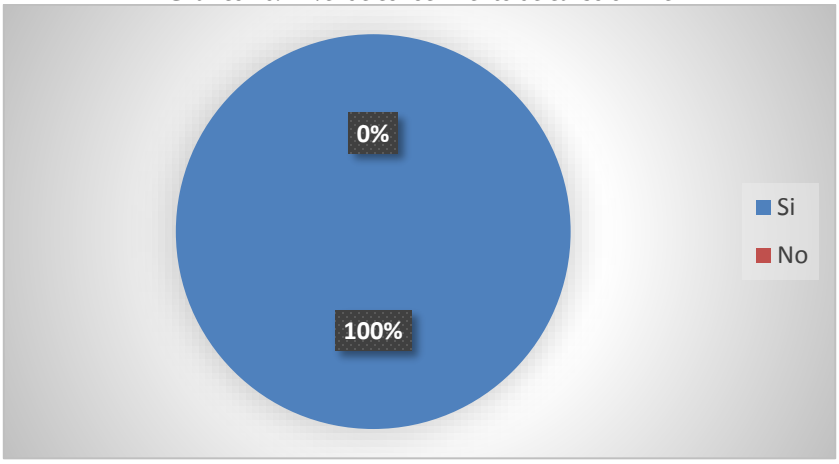
Pregunta Nº 1. ¿Utiliza usted un curso online?

Cuadro 15. Nivel de conocimiento de curso online

Alternativas	Frecuencia	Porcentaje
Si	9	100%
No	0	0,0
TOTAL	9	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 16. Nivel de conocimiento de curso online



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

El 100% de los docentes encuestados indican que utilizan los cursos online.

Interpretación:

Se puede evidenciar que todos los docentes encuestados han utilizado o utilizan un curso online, debido que han utilizado el software como el Moodle y el nuevo Edmodo

que presenta mejores facilidades y herramientas y es netamente virtual y online, es decir es un nuevo sistema de educación a distancia por medio de la web.

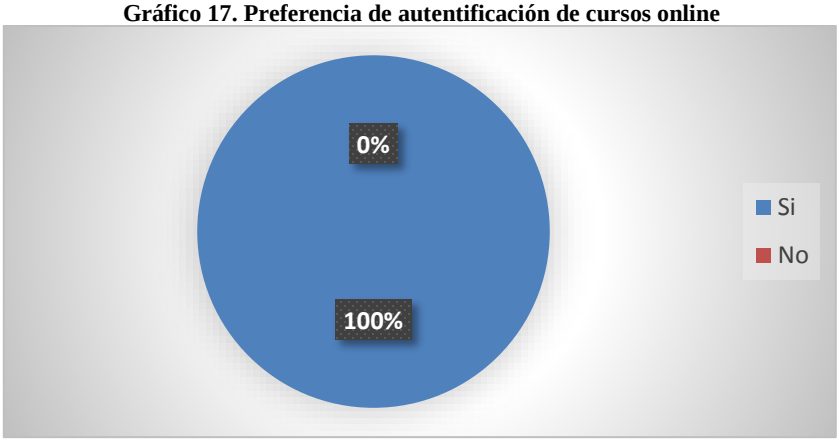
Pregunta Nº 2. ¿Le gustaría que en su curso online la autentificación sea por medio de reconocimiento facial?

Cuadro 16. Preferencia de autentificación de cursos online

Alternativas	Frecuencia	Porcentaje
Si	9	9,4
No	0	0,0
TOTAL	9	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 17. Preferencia de autentificación de cursos online



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

El 100% de los docentes encuestados afirman que si usarían la autentificación por medio de reconocimiento facial.

Interpretación:

Se puede determinar que todos los docentes encuestados afirman que les gustaría que en un curso online la autentificación sea por medio de reconocimiento facial. Debido a

que creen que es un método novedoso y además le gustaría conocer acerca de esta tecnología. Están convencidos que el registro por medio de claves a los usuarios ya es un método obsoleto y muy vulnerable.

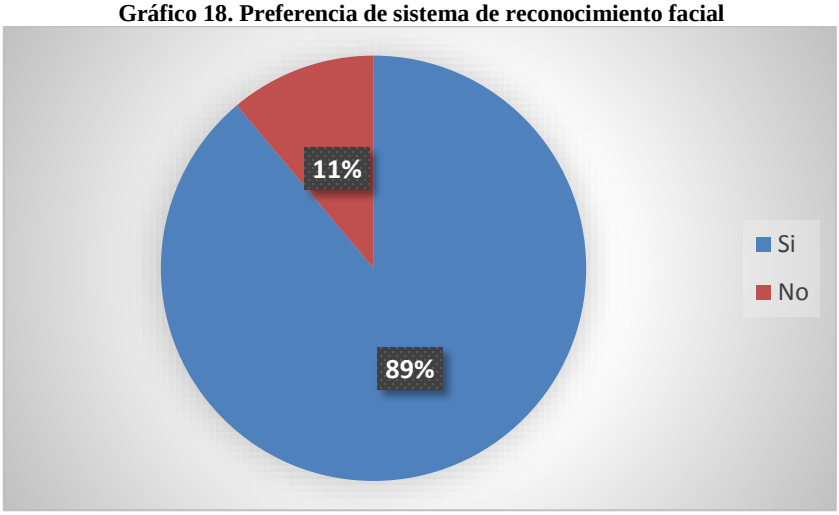
Pregunta Nº 3. ¿Ha usado usted algún sistema de reconocimiento facial?

Cuadro 17. Preferencia de sistema de reconocimiento facial

Alternativas	Frecuencia	Porcentaje
Si	8	89
No	1	11
TOTAL	9	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 18. Preferencia de sistema de reconocimiento facial



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

De los docentes encuestados, el 89% afirma que alguna vez ha usado algún tipo de sistema de reconocimiento facial, mientras que el 11% ha manifestado que no han utilizado ningún tipo de sistema de reconocimiento facial.

Interpretación:

Se puede determinar que la mayoría de los estudiantes encuestados no han utilizado un sistema de reconocimiento facial porque no saben como hacerlo, en tanto unos pocos si han utilizado alguna vez un sistema de reconocimiento facial, debido a existen muy pocas instituciones de que disponen de esta tecnología.

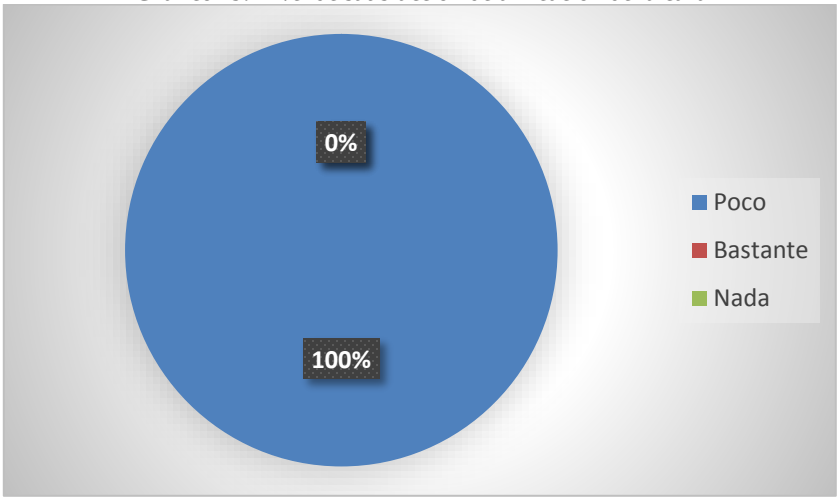
Pregunta Nº 4. ¿Considera usted que para el correcto funcionamiento de un sistema de reconocimiento facial es importante al alineación de la cara?

Cuadro 18. Nivel de satisfacción de alineación de la cara

Alternativas	Frecuencia	Porcentaje
Altamente	9	100%
Poco	0	0,0
Nada	0	0,0
TOTAL	9	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 19. Nivel de satisfacción de alineación de la cara



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

Podemos notar que el 100% de los docentes encuestados afirman que para el correcto funcionamiento de un sistema de reconocimiento facial es altamente importante la alineación de la cara.

Interpretación:

Se puede afirmar que todos los docentes encuestados han coincidido en que para el correcto funcionamiento de un sistema de reconocimiento facial es altamente importante la alineación de la cara, debido que al ser un sistema que utiliza muchas variables en el algoritmo es necesario tomar en cuenta además otras variables como luz, fisonomía, posición, distancia entre otros.

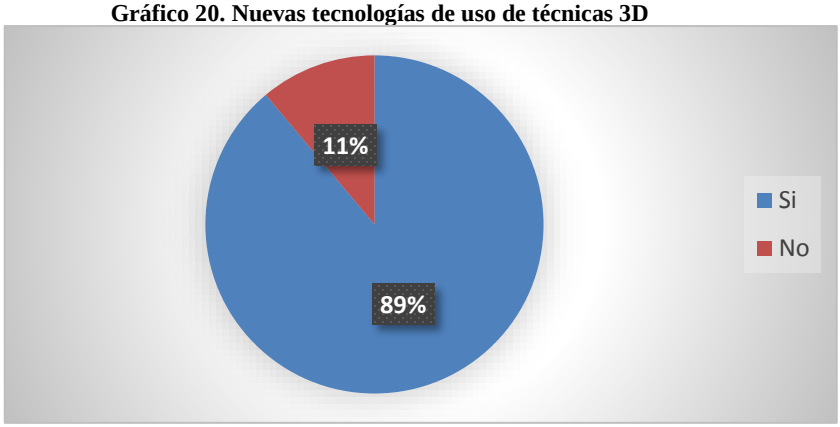
Pregunta Nº 5. ¿Considera usted que es necesario el uso de técnicas 3D en las aulas virtuales?

Cuadro 19. Nuevas tecnologías de uso de técnicas 3D

Alternativas	Frecuencia	Porcentaje
Si	8	89
No	1	11
TOTAL	9	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 20. Nuevas tecnologías de uso de técnicas 3D



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

El 89% de los docentes encuestados consideran que es necesario el uso de técnicas 3D en las aulas virtuales, mientras que el 11% restante afirman que no es necesario en uso de técnicas 3D en las aulas virtuales.

Interpretación:

Se puede determinar que la mayoría de los docentes encuestados consideran que es necesario el uso de técnicas de 3D en las aulas virtuales por considerarlo un método novedoso, en tanto unos pocos opinan que no es necesario, porque son tecnologías nunca utilizadas en nuestro medio y desconocen del sistema y les parece complicada.

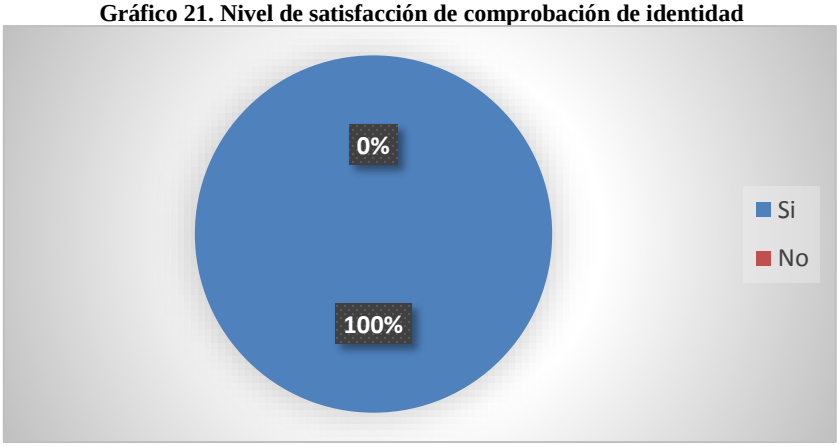
Pregunta Nº 6. ¿Usted usaría un Sistema de reconocimiento facial para la comprobación de su identidad?

Cuadro 20. Nivel de satisfacción de comprobación de identidad

Alternativas	Frecuencia	Porcentaje
Si	9	100
No	0	0,0
TOTAL	9	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 21. Nivel de satisfacción de comprobación de identidad



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

El 100% de los estudiantes encuestados afirman que si usarían un sistema de reconocimiento facial para la comprobación de su identidad.

Interpretación:

Se puede deducir que todos los docentes encuestados si usarían un sistema de reconocimiento facial para la comprobación de su identidad, esto radica que es un medio de registro online para autentificación de identidad.

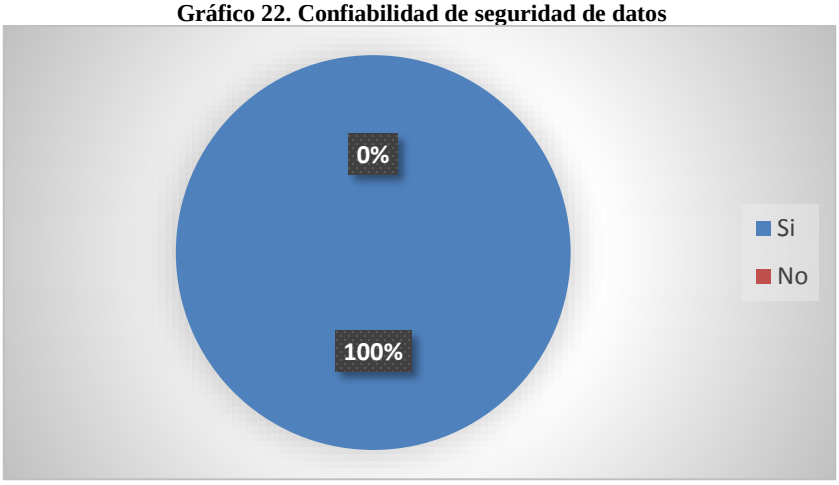
Pregunta Nº 7. ¿Considera usted que para mejorar la seguridad de datos es recomendable usar un sistema de reconocimiento facial?

Cuadro 21. Confiabilidad de seguridad de datos

Alternativas	Frecuencia	Porcentaje
Si	9	100%
No	0	0,0
TOTAL	9	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 22. Confiabilidad de seguridad de datos



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

El 100% de los encuestados consideran que si es recomendable el uso de un sistema de reconocimiento facial para mejorar la seguridad de datos.

Interpretación:

Se puede determinar que todos de los docentes encuestados consideran que si es recomendable el uso de un sistema de reconocimiento facial para mejorar la seguridad de datos y de esta manera determinar los usuarios autorizados sin la necesidad de digitar una clave, por medio del programa realizado en Matlab utilizando un algoritmo matemático comparando las variables biométricas para eliminar los falsos positivos.

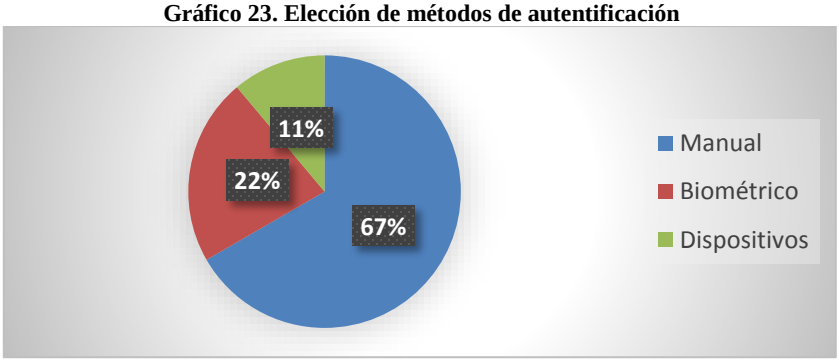
Pregunta Nº 8. ¿Cuál de estos métodos ha utilizado usted para autentificarse al momento del ingreso a las aulas virtuales?

Cuadro 22. Elección de métodos de autentificación

Alternativas	Frecuencia	Porcentaje
Manual	6	67
Biométrico	2	22
Dispositivos	1	11
TOTAL	9	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 23. Elección de métodos de autentificación



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

El 100% de los docentes encuestados el 67% afirman que él método que han usado para autentificarse al momento del ingreso a las aulas virtuales ha sido el método manual, el 22% el método Biométrico y el 11% ha utilizado otros dispositivos.

Interpretación:

Se puede determinar que la mayoría de los docentes encuestados han usado el método manual al momento de la autentificación en sus aulas virtuales, mientras que unos pocos si han utilizado alguna ocasión métodos biométricos y otros métodos, pero todos coinciden que es un método innovador.

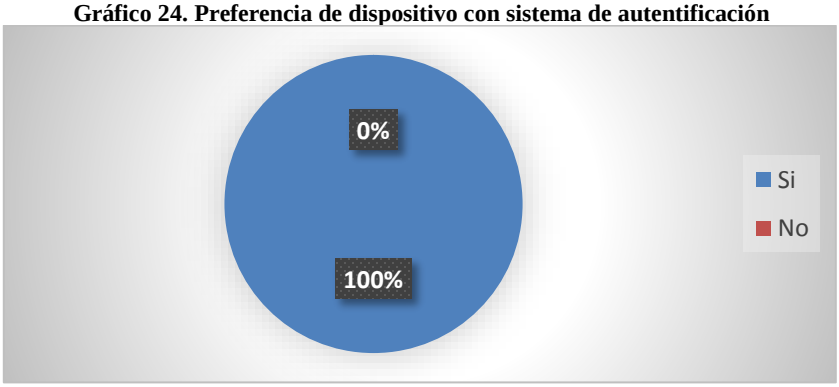
Pregunta Nº 9. ¿Conoce usted algún dispositivo que contenga un sistema de autentificación?

Cuadro 23. Preferencia de dispositivo con sistema de autentificación

Alternativas	Frecuencia	Porcentaje
Si	9	100
No	0	0,0
TOTAL	9	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 24. Preferencia de dispositivo con sistema de autentificación



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

El 100% de los docentes encuestados aseguran que si conocen un dispositivo que contenga un sistema de autentificación.

Interpretación:

Se puede verificar que todos los docentes encuestados afirman que conocen un dispositivo con un sistema de autentificación, como dispositivos biométricos, pero el de reconocimiento facial no lo ha utilizado y además piensan que es un tipo de autentificación actual e ingenioso.

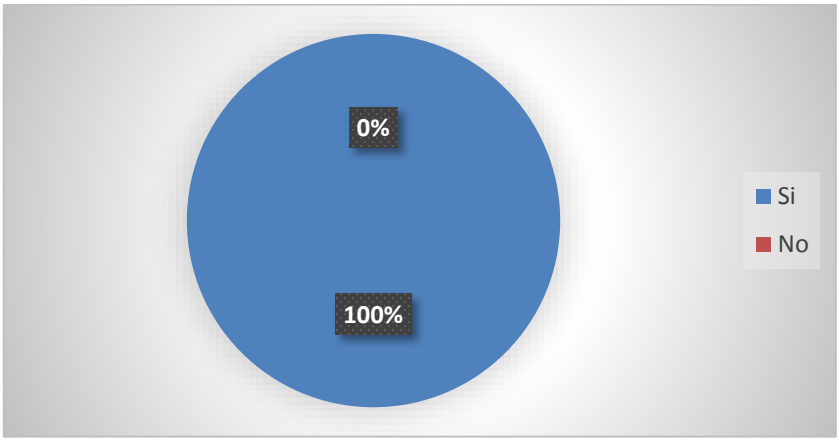
Pregunta Nº 10. Considera usted que el uso de un sistema de reconocimiento facial mejoraría la autentificación en los cursos online.

Cuadro 24. Satisfacción autentificación en los cursos online

Alternativas	Frecuencia	Porcentaje
Si	9	100
No	0	0,0
TOTAL	9	100%

Fuente: Encuesta estructurada
Elaborado por: Ruth Jimena Naranjo Quispe

Gráfico 25. Satisfacción autentificación en los cursos online



Elaborado por: Ruth Jimena Naranjo Quispe

Análisis:

El 100% de los docentes encuestados consideran que el uso de un sistema de reconocimiento facial mejoraría la autentificación en los cursos online.

Interpretación:

Se puede identificar que todos los docentes encuestados consideran que con el uso de un sistema de reconocimiento facial mejoraría la autentificación en los cursos online, para potenciar la seguridad que ofrece una simple contraseña. Algunas computadoras ya incorporan tecnología biométrica de fábrica, lo que implica que valdría la pena si se aprovecha como es debido por medio de cámara web integrada en una computadora pueden convertirse en hardware para reconocimiento facial, ya que el software implementa un potente algoritmo de reconocimiento biométrico.

4.2 VERIFICACIÓN DE LA HIPÓTESIS

Para verificar la hipótesis se utiliza el método del chi cuadrado, que es una herramienta estadística que facilitara saber si se rechaza la hipótesis negativa H0 y si se acepta la hipótesis alternativa H1.

Hipótesis

El Reconocimiento Facial incide en la Autentificación de usuarios en cursos online de la carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato.

Variable Independiente

Reconocimiento Facial

Variable Dependiente

Autentificación de usuarios

4.2.1 Planteamiento de la Hipótesis

H_0: El Reconocimiento Facial **NO** incide en la autentificación de usuarios en cursos online de la carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato

H_1: El Reconocimiento Facial **SI** incide en la autentificación de usuarios en cursos online de la carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato

4.2.2 Selección del Nivel de Significación

Para la verificación hipotética se utilizará el nivel de significación; **α = 95%**

4.2.3 Descripción de la población.

Para este trabajo de investigación no se ha tomado muestra, sino que trabajamos con el total de la población compuesta por los estudiantes y docentes de la Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato.

4.2.4 Especificación del Estadístico

Se trata de un cuadro de contingencia de 2 filas por 2 columnas con la aplicación de la siguiente fórmula estadística.

$$X^2 = \frac{\sum(O - E)^2}{E}$$

X^2 = Chi cuadrado

$\sum$ = Sumatoria

O = Frecuencias Observadas

E = Frecuencias Esperadas

Las filas hacen referencia a las preguntas, en este caso se han tomado 2 preguntas que son las más relevantes de la encuesta, y las columnas que hacen referencia a la alternativa de cada pregunta, en este caso las alternativas son **Sí** y **No.**

4.2.5 **Especificación de las Zonas de Aceptación y Rechazo**

gl=(f-1)(c-1)

gl = Grados de Libertad

c = columnas, las columnas es el número de alternativas que tiene las preguntas, en este caso 2, “si” y “no”.

f = filas, el número de filas son las preguntas que se involucran dentro de las variables, en este caso existe una para la variable dependiente y una para la variable independiente, en total 2 preguntas.

gl=(f-1)(c-1)
gl=(2-1)(2-1)
gl=(1)(1)
gl=(1), con este grado de libertad, el chi cuadrado tabulado es:

Con un nivel de significación de 95% y 1 grado de libertad el valor de X^2 tabular es 3,84.

4.2.6 Campana de Gauss

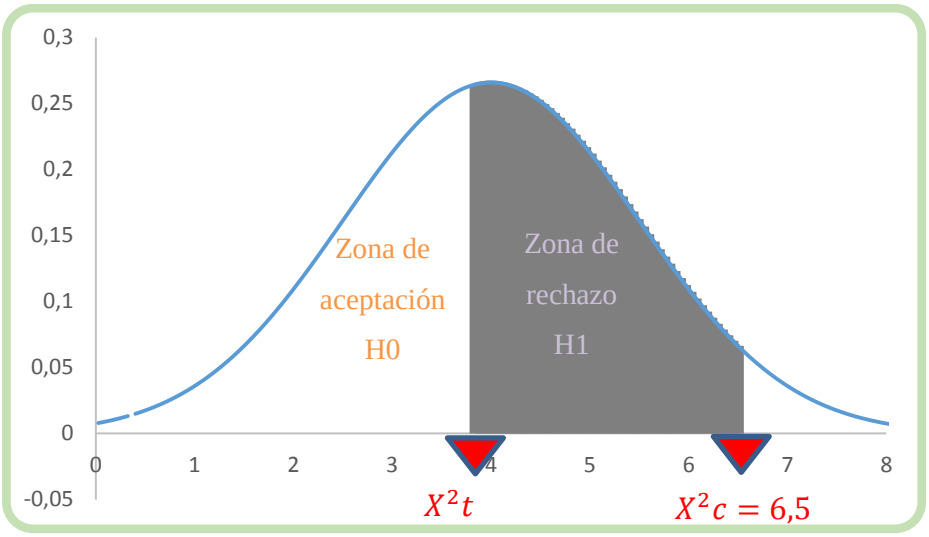


Gráfico 26. Campana de Gauss
Elaborado por: Ruth Jimena Naranjo Quispe

4.2.7 Recolección de Datos y Cálculos Estadísticos

Para el cálculo y elaboración de las frecuencias observadas se tomará en consideración las preguntas más relevantes de la lista de cotejo, las mismas que el problema tuvo un mayor grado de incidencia.

Datos obtenidos a partir de la investigación.

Frecuencias Observadas

Nº	Preguntas	Alternativas		Total
		Si	No	
2	¿Le gustaría que en su curso online la autentificación sea por medio de reconocimiento facial?	87	9	96
10	Considera usted que el uso de un sistema de reconocimiento facial mejoraría la autentificación en los cursos online.	74	22	96
SUBTOTAL		161	31	192

Cuadro 25. Frecuencias Observadas
Elaborado por: Ruth Jimena Naranjo Quispe

Frecuencias esperadas

El cálculo de las frecuencias esperadas es el resultado de la multiplicación del valor total de las filas por el valor total de las columnas y finalmente dividido por el valor general o total.

Cuadro 26. Frecuencias esperadas

Frecuencias esperadas	
161*96/192	80.5
31*96/192	15.5
TOTAL	**96**

Elaborado por: Ruth Jimena Naranjo Quispe

Frecuencias Esperadas

Nº	Preguntas	Alternativas		Total
		Si	No	
2	¿Le gustaría que en su curso online la autentificación sea por medio de reconocimiento facial?	80.5	15.5	96
3	¿Ha usado usted algún sistema de reconocimiento facial?	80.5	15.5	96
SUBTOTAL		161	31	192

Cuadro 27. Frecuencias Esperadas
Elaborado por: Ruth Jimena Naranjo Quispe

Cálculo del Chi Cuadrado de Estudiantes

$$x^2 = \sum \frac{(O-E)^2}{E}$$

Simbología:
X^2= Chi cuadrado
∑= Sumatoria
O= Frecuencias observadas
E= Frecuencias esperadas
(0-E)2/E= Frecuencias observadas - Frecuencias esperadas al cuadrado divido por las frecuencias esperadas.

Cuadro 28. Cálculo del Chi cuadrado

O	E	(O-E)	(0-E)2	*(0-E)2/E*
87	80.5	6.5	42.25	0.52
9	15.5	-6.5	42.25	2.73
74	80.5	-6.5	42.25	0.52
22	15.5	6.5	42.25	2.73
				6.50

Elaborado por: Ruth Jimena Naranjo Quispe

Regla de decisión.

Una vez obtenido el resultado del Chi cuadrado se afirma lo siguiente:

$$X^2c = 6.50 > X^2t = 3.84$$

De acuerdo a la teoría, entonces se procede a rechazar la hipótesis nula y por lo tanto se acepta la hipótesis positiva.

CONCLUSIÓN

Para 1 grado de libertad a un nivel de significancia 0.05 se obtiene en la tabla $X^2t = 3,84$ y como el valor del $X^2c = 6,50$ se encuentra fuera de la región de aceptación, entonces se rechaza la hipótesis nula Ho por lo que se acepta lo hipótesis alternativa H1 que dice:

H_1: El Reconocimiento Facial **SI** incide en la Autentificación de usuarios en cursos online de la carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Del trabajo realizado se ha tomado en cuenta los resultados de las preguntas de la encuesta y la comprobación de la hipótesis, para llegar a las siguientes conclusiones:

La influencia del reconocimiento facial aplicado a la autentificación de los usuarios de cursos online en la Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato, después de finalizar el tema investigado, se realza la necesidad de este criterio tecnológico, claramente direccionada a la consolidación de fijación de saberes del pensamiento significativo

Los docentes y estudiantes de la carrera no han seguido un curso online de autentificación por medio de reconocimiento facial. El 90,6% de los estudiantes encuestados aseguran que les gustaría que en su curso online la autentificación sea por medio de reconocimiento facial; mientras que el 9,4% piensan que no les gustaría que en su curso online la autentificación sea por medio de reconocimiento facial.

Por medio de las encuestas se determina que el 77,1% de los estudiantes consideran que el uso de un sistema de reconocimiento facial mejoraría la autentificación en los cursos online, y el 22,9% restante considera que el uso de reconocimiento facial no mejoraría la autentificación en los cursos online.

Actualmente los datos en la institución son vulnerables, existe poca seguridad en cuanto a la confidencialidad de los mismos, no existe un sistema para controlar el

ingreso de usuarios a los cursos online en la institución por ende los datos están expuestos.

La gran mayoría de los docentes y estudiantes utilizan actualmente cursos online mediante autenticación manual. Existe desconocimiento en los estudiantes sobre los dispositivos que permiten la autentificación facial.

5.2 RECOMENDACIONES

Fundamentar teóricamente las competencias holísticas de dispositivos biométricos para la autentificación facial.

Plantear un aula virtual que permita la autentificación de usuarios mediante reconocimiento facial y proponer un curso online de la autentificación enfocado al reconocimiento facial.

Socializar en los docentes y estudiantes de la carrera cursos online de autentificación por medio de reconocimiento facial para eliminar medios de autentificación caducos y de esta manera conocer otro método alternativo online.

Desarrollar una guía didáctica para el proceso de reconocimiento facial para la autentificación de usuarios en cursos online de la carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato.

CAPÍTULO VI

PROPUESTA

TEMA

Sistema de Reconocimiento facial utilizando Matlab.

6.1 DATOS INFORMATIVOS

Institución Ejecutora: Universidad Técnica de Ambato.
Beneficiarios: Estudiantes de la Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato.
Ubicación: Universidad Técnica de Ambato
Cantón: Ambato
Provincia: Tungurahua
Dirección del Establecimiento: Campus Huachi. Av. Los Chasquis y Río Guayllabamba.
Tiempo estimado para la ejecución: Abril-Septiembre 2016
Inicio: Abril 2016 **Fin:** Septiembre 2016
Responsable: Ruth Jimena Naranjo Quispe
Costo: $ 700

6.2 ANTECEDENTES DE LA PROPUESTA

En el presente trabajo de investigación se plantea dar solución al problema, la necesidad de que los docentes y estudiantes se capaciten en reconocimiento facial aplicado a la autentificación de usuarios en cursos online de la Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de

Ambato" por lo que se propone realizar un Sistema de Autentificación de usuarios utilizando Matlab.

El resultado de la encuesta demuestra que la aplicación de un Sistema de Autentificación de usuarios utilizando Matlab, por parte de los maestros y estudiantes durante el proceso enseñanza, da a conocer que la mayor parte de estudiantes desconocen del tema pero a la vez presenta un gran interés, ya que facilitará los resultados de aprendizaje esperados en la resolución de estos indicativos.

6.3 JUSTIFICACIÓN

El propósito de la propuesta es que se convierta en un documento de consulta ya que del tema investigado existe muy poca información debido a que es innovador y relativamente nuevo en la Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato.

La importancia de esta propuesta se fundamenta en que los estudiantes tienen el compromiso de aprender y los docentes desean capacitarse en estas innovadoras técnicas para promover estudiantes exitosos.

La originalidad se basa en que anteriormente no se ha propuesto en la Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato la aplicación de las técnicas para la autentificación de usuarios en cursos online por medio de reconocimiento facial.

Los beneficiarios directos son los docentes y estudiantes ya que existirá un eficiente uso de la aplicación de las técnicas para la autentificación de usuarios en cursos online por medio de reconocimiento facial, es decir soluciones concretas para mejorar el rendimiento académico de los estudiantes en la Carrera de Docencia en Informática

de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato.

6.4 OBJETIVOS

6.4.1 Objetivo General

Utilizar Matlab como recurso de reconocimiento facial para autentificación de rostros de usuarios.

6.4.2 Objetivos Específicos

- Fundamentar teóricamente un sistema de Autentificación de usuarios utilizando Matlab.

- Utilizar rutinas de programación en Matlab para generar procesos de reconocimiento facial.

- Realizar pruebas de funcionamiento de las rutinas de programación usadas en Matlab para reconocimiento facial.

6.5 ANÁLISIS DE FACTIBILIDAD

El tema del estudio investigativo junto con la propuesta planteada posee características positivas que pretende reforzar y modificar conductas de los estudiantes frente al proceso de enseñanza-aprendizaje, debido a que es muy importante la autentificación de usuarios utilizando Matlab.

La factibilidad se basa en el interés que presentan los estudiantes y docentes de la Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato y en el sustento científico que posee el trabajo investigativo. Además, no existen otros trabajos similares en la institución, resultando inédito.

6.6 FUNDAMENTACIÓN CIENTÍFICA

El sistema de autentificación de usuarios utilizando Matlab ayuda a "reconocimiento facial en cursos online de la Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato", debido a que motiva la utilización de medios informáticos para lograr optimizar los cursos online por medio de reconocimiento facial.

¿Qué es un sistema de reconocimiento facial?

Los humanos a menudo utilizan los rostros para reconocer individuos y los avances en las capacidades de computación en las últimas décadas, ahora permiten reconocimientos similares en forma automática. Los algoritmos de reconocimiento facial anteriores usaban modelos geométricos simples, pero el proceso de reconocimiento actualmente ha madurado en una Ciencia de Sofisticadas representaciones matemáticas y procesos de coincidencia. Importantes avances e iniciativas en los pasados diez a quince años han propulsado a la tecnología de reconocimiento facial al centro de la atención (Bíometria, 2016).

Se puede definir a un sistema de reconocimiento facial como un sistema de identificación mediante un análisis de características fisiológicas extraídas de una imagen para luego ser comparadas con una base de datos y finalmente mostrar los resultados.

Ventajas

Las características físicas y de comportamiento son mucho más difíciles de falsificar que los métodos de identificación tradicionales. Mientras un criminal podría obtener una contraseña en forma ilegal, conseguir las huellas dactilares de un usuario sería mucho más complicado. Además, al contrario de lo que sucede con los documentos de identidad o tarjetas de identificación tradicionales, no puedes perder tus características físicas, proporcionando el mantenimiento más rentable para la empresa u organización y la tecnología más conveniente para los usuarios (Grossman, Ventajas de reconocimiento facial, s.f.)

Entre las ventajas podemos encontrar las siguientes:

- Es un sistema que puede ser utilizado para el control y vigilancia ya que es muy discreto.

- Se puede controlar el sistema desde cualquier computador.

- Es un sistema confiable ya que es mucho más difícil falsificar estos métodos de autentificación.

Desventajas

Las máquinas de identificación biométrica son más costosas que las tradicionales. Además, algunos usuarios pueden rechazar la biometría en su conjunto, viéndola como una invasión de la privacidad. Otra desventaja es que las máquinas de identificación biométrica no siempre son totalmente precisas. Por ejemplo, es probable que un individuo con un resfriado no pueda identificarse por un dispositivo de uso de la voz y la gente que aumenta o baja de peso puede, de repente, perder el

acceso a un lugar protegido por un sistema de identificación de rasgos faciales (Grossman, Ventajas de reconocimiento facial, s.f.)

Se puede observar que también existen desventajas significativas en el uso de un sistema de reconocimiento facial, entre ellas tenemos:

- Los dispositivos para la identificación biométrica son costosos.
- No todos los dispositivos pueden llegar a ser precisos.
- En un sistema de reconocimiento facial influyen considerable los factores ambientales, como la iluminación.
- Un sistema de reconocimiento facial debe estar constantemente actualizado, para poder mantener la precisión ya que a medida que el ser humano envejece afecta nuestro aspecto, especialmente el rostro.

Matlab

Millones de ingenieros y científicos de todo el mundo usan MATLAB para analizar y diseñar los sistemas y productos de transformación de nuestro mundo.

MATLAB es en los sistemas de seguridad activa del automóvil, nave espacial interplanetaria, los dispositivos de vigilancia de la salud, las redes eléctricas inteligentes y las redes celulares LTE. Se utiliza para el aprendizaje automático, procesamiento de señales, procesamiento de imágenes, visión por ordenador, las comunicaciones, las finanzas computacionales, diseño de control, robótica, y mucho más (MATLAB, 2016).

Características del entorno

Características principales de Matlab.

Lenguaje de alto nivel para la computación científica y de ingeniería.

Entorno de escritorio sintonizado para la exploración iterativa, el diseño y la resolución de problemas.

Los gráficos para la visualización de datos y herramientas para la creación de parcelas personalizados.

Aplicaciones para el ajuste de la curva, la clasificación de datos, análisis de señales, y muchas otras tareas específicas de dominio.

Complemento de cajas de herramientas para una amplia gama de aplicaciones de ingeniería y científicas.

Herramientas para la creación de aplicaciones con interfaces de usuario personalizadas

Interfaces para C / C ++ , Java ™ , .NET , Python® , SQL , Hadoop® y Microsoft® Excel®.

Opciones de implementación libres de regalías para el intercambio de programas de MATLAB con los usuarios finales (MATLAB, 2016).

DESARROLLO DE LA PROPUESTA

El proceso de identificación facial utilizando Matlab con el método eigenfaces está compuesto por dos partes:

Detección

Comprende la localización de una o varias caras dentro de una imagen.

El reconocimiento

Consiste en la comparación de la cara detectada y la el rostro guardado en la base de datos.

Estos procesos de detección y reconocimiento facial están fuertemente condicionados por la posición y orientación de la cara del usuario con respecto a la cámara y las condiciones ambientales como la iluminación en el momento de realizar la detección.

En lo que se refiere al programa aparece una ventana en la cual está el título, luego tenemos otra sección donde van a ir dos ventanas en las cuales se ubicaran cada foto, luego podemos observar cuatro botones:

Capturar rostro.- al presionar este botón, la cámara se enciende y captura una foto. Es necesario ubicarnos bien frente de la cámara.

Procesar Rostro.- Se realiza la comparación entre la captura y las fotos de la base de datos. Se puede visualizar una pequeña pantalla donde se muestra el rostro procesado.

Cargar rostro.- Se sube la foto de una base de datos predefinida.

Procesar rostro cargado.- Se realiza la comparación de los rostros en la base predefinida y la que se desea comparar.

Detalle de cómo trabaja la base de datos.

La base de datos creada en la carpeta **bin** dentro de Matlab en el disco C, almacena fotografías previamente agregadas, o a su vez al momento de la captura del rostro, se guarda también una foto con un nombre específico dentro de esta carpeta.

En la detección de la cara hay una cara en la imagen, sin identificarla, luego se realiza alineación del rostro en donde se determina las características faciales las mismas que serán procesadas por medio de algoritmos matemáticos en donde se subdivide en una serie de matrices continuas para normalizarlas en una base de datos.

Toda esto se va almacenado en una base de datos direccionada, como como ya mencionamos anteriormente se sugiere debe estar dentro del programa y específicamente en la carpeta BIN.

Como se hace el reconocimiento facial.

Las imágenes del rostro a procesar se graba en espacio definidos de cada característica del rostro uno a continuación del otro, como se mencionó anteriormente estas matrices se almacenan en por medio de algoritmos numéricos en una base de datos. Se debe destacar que para un fácil procesamiento facial es recomendable realizarla en una escala de grises para definir de una mejor manera las facciones significativas llamadas eigenfaces, las cuales se denominan vectorialmente los eigenvectors, los mismo que se encargan de dividir el rostro en vectores matemáticos y se realiza la sumatoria de los

vectores sectorizados de la facción para ser comparados de una base de datos predefinida con el rostro a ser comparado.

Análisis de Componentes Principales (PCA - Principal Component Analysis).
La normalización de los ingenvectores de entre varios métodos se utilizó el más generalizado aunque no sea el más fácil (P.C.A.) en donde predominan las dimensiones de las distancias de las características del rostro tomando en cuenta que distancia existe las mismas así como también la posición dentro del rostro, además se debe tomar en cuenta las condiciones de la carga del reconocimiento facial sea la más adecuada tomando en cuenta la iluminación y la posición del rostro sea fija.

Aquí se presenta el desarrollo de lo anteriormente mencionado:
Se hace correr el programa:

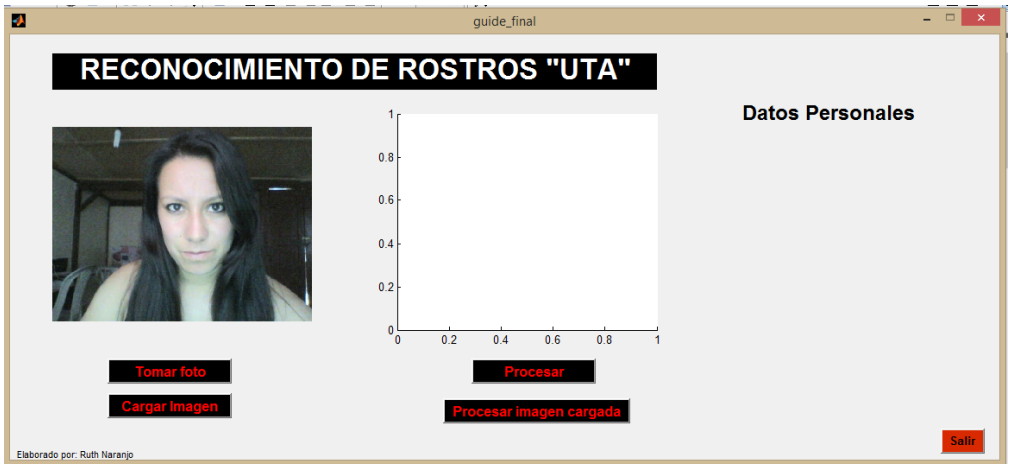


Gráfico 27. Reconocimiento de rostro

Se escoge tomar foto y se procede a capturar la fotografía.

Gráfico 28. Reconocimiento

Una vez capturada la fotografía, presionamos el botón Procesar y el programa hace una búsqueda de la foto más parecida a la que tomamos en un inicio, muestra como resultado, la fotografía almacenada en el programa y los datos personales de dicha persona.

El siguiente procedimiento es:

Cargar Rostro

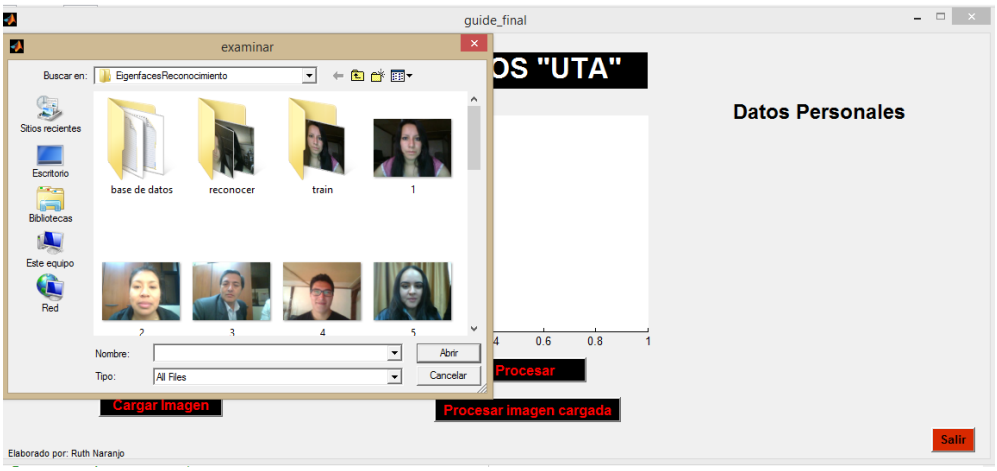


Gráfico 29. Cargar rostro

Como se observa en la pantalla luego de cargar foto aparece el explorador que se debe direccionar a la base de fotos y escogemos una foto a ser comparada.

Gráfico 30. Coteja

Aquí se coteja entre las dos fotos y como se observa, nos muestra de igual manera la fotografía que tenemos almacenada en el programa, además de los datos personales.

Cabe resaltar que debido a que existen muchas condicionantes de diferentes tipos la captura de imágenes debe ser en las mismas condiciones de luz, acercamiento de rostro, ubicación entre otras.

6.7 METODOLOGÍA MODELO OPERATIVO

Cuadro 29. Modelo Operativo

FASES	OBJETIVOS	ACTIVIDADES	RECURSOS	RESPONSABLE
Diseño	Identificar estrategias para aplicar el sistema de reconocimiento facial utilizando Matlab.	Selección de contenidos	Humanos Materiales Económicos	Investigador
Socialización	Socializar a los docentes y estudiantes el sistema de reconocimiento facial en la solución de situaciones prácticas académicas.	Presentación de la propuesta a los docentes y estudiantes de la institución	Humanos Materiales Económicos	Docentes Investigador
Aplicación	Aplicar el sistema de reconocimiento facial en la solución	Aplicación de la propuesta en la institución	Humanos Materiales Económicos	Investigador
Evaluación	Evaluar los resultados	Evaluación de la propuesta en la institución	Humanos Materiales Económicos	Docentes Investigador

Elaborado por: Ruth Jimena Naranjo Quispe

6.8 ADMINISTRACIÓN

El reconocimiento facial aplicado a la autentificación de usuarios en cursos online se aplicara en la carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato", aquí se capacitara al personal para que adquiera competencias sobre el software del reconocimiento facial.

Estará a cargo de la administración de redes de Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato conjuntamente con la investigadora quien realizará cambios y ajustes necesarios para mejorar la aplicación.

Como es una entidad pública dentro de su organigrama jerárquico reposara en la Administración de Redes de la facultad para su posterior administración.

6.8.1. Recursos:

Institucionales: Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato

Humanos: Docentes, estudiantes de la Carrera de Docencia en Informática de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato e investigadora.

Materiales: Computadora, internet, hojas de papel bond, infocus, impresora, taxi, carpeta, memory, impresiones.

6.8.2. Económicos, Presupuesto y Financiamiento

Cuadro 30. Económicos. Presupuesto y Financiamiento

Rubros de Gastos	**Valor**
1. Personal de Apoyo	$200,00
2. Adquisición de Equipos	$50.00
3. Material de Escritorio	$30.00
4. Material Bibliográfico	$40.00
5. Transporte	$130.00
6. Impresiones.	$250.00
TOTAL	**$700.00**

Elaborado por: Ruth Jimena Naranjo Quispe

6.9 PREVISIÓN DE LA EVALUACIÓN

Cuadro 31. Previsión de la evaluación

Preguntas Básicas	**Explicación**
¿Quiénes solicitan la evaluación?	Estudiantes, docentes de la FCHE.
¿Por qué evaluar?	Para conocer los resultados obtenidos a partir de la aplicación de la propuesta
¿Para qué evaluar?	Obtener datos reales sobre la efectividad del Sistema de Reconocimiento facial utilizando Matlab.
¿Qué evaluar?	La eficacia que demostró la propuesta como solución o un factor de disminución al problema.
¿Quién evalúa?	Investigador Docentes
¿Cuándo evaluar?	Permanentemente
¿Cómo evaluar?	Observación
¿Con qué evaluar?	Fichas de observación Notas de usuarios
¿En qué situación?	En el Sistema de Reconocimiento facial utilizando Matlab

Elaborado por: Ruth Jimena Naranjo Quispe

BIBLIOGRAFÍA

Aguerrebere, C., Capdehourat, G., Delbracio, M., & Mateu, M. (s.f.). *http://iie.fing.edu.uy*. Obtenido de http://iie.fing.edu.uy/~gcapde/trabajos/aguara/descargas/resumen_aguara.pdf

Aguerrebere, C., Capdehourat, G., Delbracio, M., & Mateu, M. (s.f.). *http://iie.fing.edu.uy*. Obtenido de http://iie.fing.edu.uy/~gcapde/trabajos/aguara/descargas/resumen_aguara.pdf

Álvarez, M. Á. (19 de 12 de 2002). *Funcionamiento del sistema de autentificación en PHP*. Obtenido de http://www.desarrolloweb.com/articulos/1007.php

Álvarez, M. Á. (2010). *http://www.desarrolloweb.com.* Obtenido de http://www.desarrolloweb.com/articulos/1007.php

Asamblea Constituyente. (2008). *Constitucion de la Republica del Ecuador*. Obtenido de Constitucion de la Republica del Ecuador: http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf

Azcoaga, J. E. (27 de 5 de 2015). *Proceso de la investigación*. Obtenido de www.neurociencia.cl/dinamicos/articulos/961150-rcnp2014v9ne2-8.pdf

Bíometria. (2016). *Reconocimiento facial*. Obtenido de http://www.biometria.gov.ar/metodos-biometricos/facial.aspx

Bíometria. (31 de 07 de 2016). *Reconocimiento facial*. Obtenido de http://www.biometria.gov.ar/metodos-biometricos/facial.aspx

Borghello, C. (2009). *Seguridad Lógica - Identificación y Autentificación*. Obtenido de http://www.segu-info.com.ar/logica/identificacion.htm

Entornos educativos. (2015). *¿Qué es Moodle?* Obtenido de http://www.entornos.com.ar/moodle

Fernandez, C. (2006). Mexico: Mc. Graw-Hill Interamericana, Metodología de la Investigación.

Gámez Jiménez, C. V. (Abril de 2009). *http://e-archivo.uc3m.es.* Obtenido de http://e-archivo.uc3m.es/bitstream/handle/10016/5831/PFC_CarmenVirginia_Gamez_Jimenez.pdf?sequence=1

García Chang, M. E. (Junio de 2009). *http://itzamna.bnct.ipn.mx.* Obtenido de http://itzamna.bnct.ipn.mx/dspace/bitstream/123456789/6111/1/DISENOIMPLEMFACIAL.pdf

García Ríos, E., Escamilla Hernandez, E., Nakano Miyatake, M., & Pérez Meana, H. (2014). Sistema de Reconocimiento de Rostros usando Visión Estéreo. *Scielo*.

Garza, A. (09 de 10 de 2012). *PLATAFORMA EDMODO*. Obtenido de http://plataformaedmodo.blogspot.com/2012/10/concepto-edmodo.html

Garza, A. (2015). *PLATAFORMA EDMODO*. Obtenido de http://plataformaedmodo.blogspot.com/2012/10/concepto-edmodo.html

González, A., & Prieto, F. (2010). Extracción de puntos característicos del rostro para medidas antropométricas. *Scielo*.

Grossman, J. (7 de 7 de 2016). *Ventajas de reconocimiento facial*.

Grossman, J. (s.f.). *Ventajas de reconocimiento facial*. Obtenido de http://www.ehowenespanol.com/cuales-son-ventajas-desventajas-identificacion-biometrica-info_89194/

Intef. (7 de 12 de 2015). *Concepto de Web 2.0*. Obtenido de http://www.ite.educacion.es/formacion/materiales/155/cd/modulo_1_Iniciacionblog/concepto_de_web_20.html

Intef. (s.f.). *Concepto de Web 2.0*. Obtenido de http://www.ite.educacion.es/formacion/materiales/155/cd/modulo_1_Iniciacionblog/concepto_de_web_20.html

Jacob, K. (22 de Marzo de 2012). *ec.europa.eu.* Obtenido de http://ec.europa.eu/justice/data-protection/index_en.htm

López Martínez, M., & Acosta Rodríguez, J. (2004). *Introducción a Matlab*. Obtenido de http://www.esi2.us.es/~mlm/RAN/ManualMatlabRAN.pdf

López, M. (2015). *Introducción a Mathlab*. Obtenido de http://www.esi2.us.es/~mlm/RAN/ManualMatlabRAN.pdf

López, R., Maranón, F., Erazo, G., & Reinoso, S. (2006). *Sistema de seguridad mediante reconocimiento facial para la puesta en marcha de un Chevrolet Super Carry de la empresa Soon Burguer*. Obtenido de COBUEC: http://repositorio.espe.edu.ec/bitstream/21000/7009/1/AC-ESPEL-MAI-0428.pdf

Martínez, A. (s.f.). *Identificación autenticación y control de acceso*. Obtenido de https://www.exabyteinformatica.com/uoc/Dactiloscopia/Identidad_digital/Identidad_digital_(Modulo_1).pdf

Martínez, A. (s.f.). *Identificación autenticación y control de acceso*. Obtenido de https://www.exabyteinformatica.com/uoc/Dactiloscopia/Identidad_digital/Identidad_digital_(Modulo_1).pdf

MATLAB. (2016). *MATLAB*. Obtenido de http://www.mathworks.com/products/matlab/index.html

Mendoza, M. (15 de 06 de 2015). *Ciberseguridad o seguridad de la información*. Obtenido de http://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

Mendoza, M. (18 de 06 de 2015). *Ciberseguridad o seguridad de la información*. Obtenido de https://www.uv.mx/infosegura/general/conocimientos_ciberseguridad-2/

Perseptia. (2015). *Tutorías en Línea*. Obtenido de http://www.perseptia.com/math/es/node/13

Perseptia. (2016). *Tutorías en Línea*. Obtenido de http://www.perseptia.com/math/es/node/13

Reizabal, M. (6 de Mayo de 2015). Reconocimiento facial 'online'. *Dirio Vasco*.

Segu.info. (2009). *Seguridad Lógica - Identificación y Autentificación*. Obtenido de http://www.segu-info.com.ar/logica/identificacion.htm

Strom, D. (2016). *Introducción a los métodos de autenticación* . Obtenido de http://searchdatacenter.techtarget.com/es/consejo/Introduccion-a-los-metodos-de-autenticacion-multifactor-en-la-empresa

Telégrafo. (30 de Junio de 2014). Tecnología. *El reconocimiento Facial se muestra como una alternativa a las contraseñas*.

Torres , J. (2002). *Diagnóstico de la Educación Virtual en Ecuador*. Obtenido de http://unesdoc.unesco.org/images/0014/001404/140469s.pdf

Torres , J. (02 de 2002). *Diagnóstico de la Educación Virtual en Ecuador*. Obtenido de http://unesdoc.unesco.org/images/0014/001404/140469s.pdf

Unesco. (2010). *Datos Mundiales de Educación. VII Ed.* Obtenido de Datos Mundiales de Educación: http://www.ibe.unesco.org/fileadmin/user_upload/Publications/WDE/2010/pdf-versions/Ecuador.pdf

Villegas, J. (27 de 2 de 2009). *¿ Qué es un Sistema de Control de Acceso ?* Obtenido de http://www.tecnoseguro.com/faqs/control-de-acceso/%C2%BF-que-es-un-control-de-acceso.html

Villegas, J. (22 de 2 de 2009). *¿ Qué es un Sistema de Control de Acceso ?* Obtenido de https://www.tecnoseguro.com/faqs/control-de-acceso/%C2%BF-que-es-un-control-de-acceso.html

virtuales, E. (2015). *¿Qué es Moodle?* Obtenido de http://www.entornos.com.ar/moodle

Werner, R. (2001). *LA TECNOLOGÍA: SUS FORMAS Y LAS DIFERENCIAS DE LOS MEDIOS*. Obtenido de http://www.ub.edu/geocrit/sn-80.htm

Werner, R. (15 de 01 de 2001). *LA TECNOLOGÍA: SUS FORMAS Y LAS DIFERENCIAS DE LOS MEDIOS*. Obtenido de http://www.ub.edu/geocrit/sn-80.htm

ANEXOS

Anexo 1: CUESTIONARIO APLICADO A DOCENTES Y ESTUDIANTES

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE CIENCIAS HUMANAS Y DE LA EDUCACIÓN
CARRERA DE DOCENCIA EN INFORMÁTICA
ENCUESTA ESTUDIANTES Y DOCENTES

Objetivo: Recabar información para la investigación acerca del uso de un sistema de reconocimiento facial aplicado a la autentificación de usuarios en curos online.

Indicaciones: Lea detenidamente cada ítem y conteste con toda seriedad (Marcar con una **X** la alternativa correcta para usted) sus respuestas ayudaran a realizar la investigación con toda seriedad.

1. ¿Utiliza usted un curso online?

   Si ( ) No ( )

2. ¿Le gustaría que en su curso online la autentificación sea por medio de reconocimiento facial?

   Si ( ) No ( )

3. ¿Ha usado usted algún sistema de reconocimiento facial?

   Si ( ) No ( )

4. ¿Considera usted que para el correcto funcionamiento de un sistema de reconocimiento facial es importante al alineación de la cara?

   Poco ( ) Bastante ( ) Nada ( )

5. ¿Considera usted que es necesario el uso de técnicas 3D en las aulas virtuales?

   Si ( ) No ( )

6. ¿Usted usaría un Sistema de reconocimiento facial para la comprobación de su identidad?

Si ( ) No ( )

7. ¿Considera usted que para mejorar la seguridad de datos es recomendable usar un sistema de reconocimiento facial? Si respuesta es afirmativa, explique el por qué.

Si ( ) No ( )

Porqué?

.....
.....

8. ¿Cuál de estos métodos ha utilizado usted para autentificarse al momento del ingreso a las aulas virtuales?

Manual ( ) Biométrico ( ) Dispositivos ( )

9. ¿Conoce usted algún dispositivo que contenga un sistema de autentificación?

Si ( ) No ( )

10. Considera usted que el uso de un sistema de reconocimiento facial mejoraría la autentificación en los cursos online.

Si ( ) No ( )

GRACIAS POR SU COLABORACION

Anexo 2: TABLA DE CHI CUADRADO

Ji cuadrada/ chi cuadrada /χ^2

Grados libertad	0,1	0,05	0,025	0,01	0,005
1	2,71	3,84	5,02	6,63	7,88
2	4,61	5,99	7,38	9,21	10,60
3	6,25	7,81	9,35	11,34	12,84
4	7,78	9,49	11,14	13,28	14,86
5	9,24	11,07	12,83	15,09	16,75
6	10,64	12,59	14,45	16,81	18,55
7	12,02	14,07	16,01	18,48	20,28
8	13,36	15,51	17,53	20,09	21,95
9	14,68	16,92	19,02	21,67	23,59
10	15,99	18,31	20,48	23,21	25,19
11	17,28	19,68	21,92	24,73	26,76
12	18,55	21,03	23,34	26,22	28,30
13	19,81	22,36	24,74	27,69	29,82
14	21,06	23,68	26,12	29,14	31,32
15	22,31	25,00	27,49	30,58	32,80
16	23,54	26,30	28,85	32,00	34,27
17	24,77	27,59	30,19	33,41	35,72
18	25,99	28,87	31,53	34,81	37,16
19	27,20	30,14	32,85	36,19	38,58
20	28,41	31,41	34,17	37,57	40,00
21	29,62	32,67	35,48	38,93	41,40
22	30,81	33,92	36,78	40,29	42,80
23	32,01	35,17	38,08	41,64	44,18
24	33,20	36,42	39,36	42,98	45,56
25	34,38	37,65	40,65	44,31	46,93
26	35,56	38,89	41,92	45,64	48,29
27	36,74	40,11	43,19	46,96	49,65
28	37,92	41,34	44,46	48,28	50,99
29	39,09	42,56	45,72	49,59	52,34
30	40,26	43,77	46,98	50,89	53,67
40	51,81	55,76	59,34	63,69	66,77
50	63,17	67,50	71,42	76,15	79,49
60	74,40	79,08	83,30	88,38	91,95
70	85,53	90,53	95,02	100,43	104,21
80	96,58	101,88	106,63	112,33	116,32
90	107,57	113,15	118,14	124,12	128,30
100	118,50	124,34	129,56	135,81	140,17

Anexo 3: Manual de Usuario

INTRODUCCIÓN

MATLAB es un programa de computación que sirve para solucionar algoritmos aritméticos con su principal herramienta como lo es las matrices que pueden procesar problemas muy complejos como es el caso del reconocimiento facial, el determinado programa presenta una serie de herramientas que facilita al usuario utilizar para dar soluciones gráficas en 2D Y 3D.

Matlab es un programa intuitivo como para poder realizar un pequeño sistema de reconocimiento facial y no requiere que seamos muy conocedores en su uso.

Para poder realizar el reconocimiento facial se necesitan de dos partes principales, la primera es la detección de rostros; la segunda es la identificación de la cara.

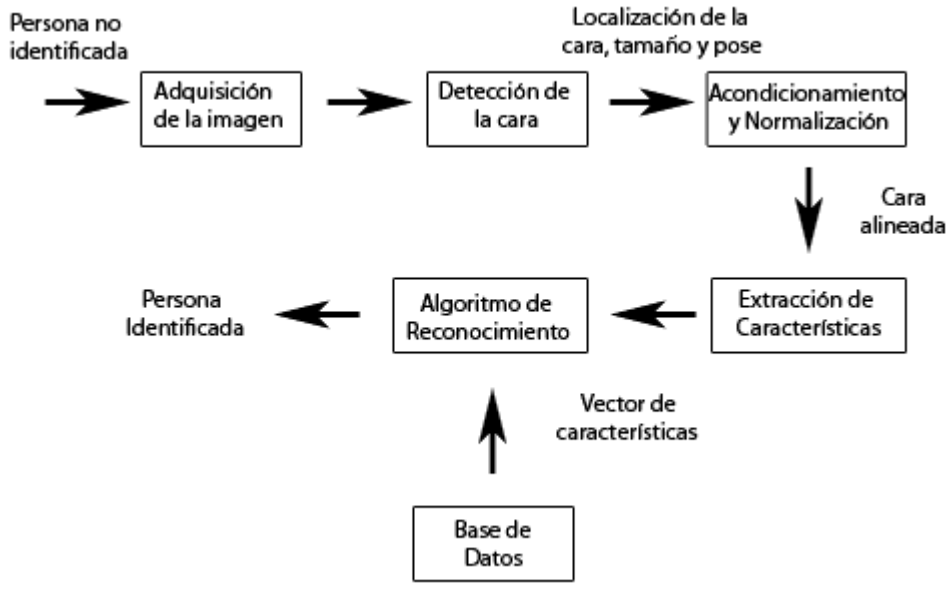


Gráfico 31. Detección de rostro

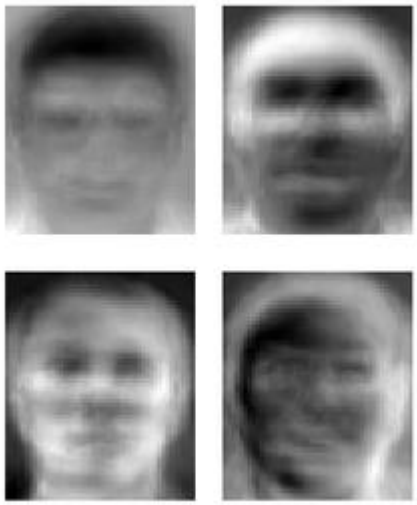


Gráfico 32. Escala de grises

Autocara (Eigenfaces)

Se denomina autocara a las características faciales como son las distancias que existe entre los ojos y pupilas así como también la posición de los otros componentes del rostro entre los que tenemos nariz, boca, labios los que se pueden denominar componentes de cada rostro.

Las autocaras es base de las características faciales básica que por medio de la algebra lineal va a ser utilizada para para entrenar, ya que en la sumatoria de Eigenvectores y realizar la comparación se evaluara cuanto se parece el rostro conocido con el rostro a procesar por medio de los eigenfaces entre las distancias euclídeas para ser más eficiente y reducir las probalidades de error.

El programa está realizado con código abierto de tal manera que en función de la necesidad del usuario puede ser modificado tanto la interfaz gráfica como el proceso de selección, tomando en cuenta la distancia euclídea del eigenface de la foto de la base de datos, realizando la autentificación facial, rechazándola o aceptándola.

Manual de ingreso al programa

Busco el archivo guide_final, en este caso lo he guardado en una carpeta en el escritorio.

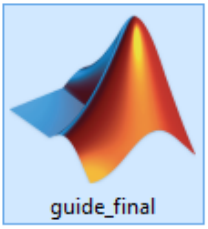


Gráfico 33. Abrir Programa

Una vez abierto el programa visualizaremos la siguiente pantalla.

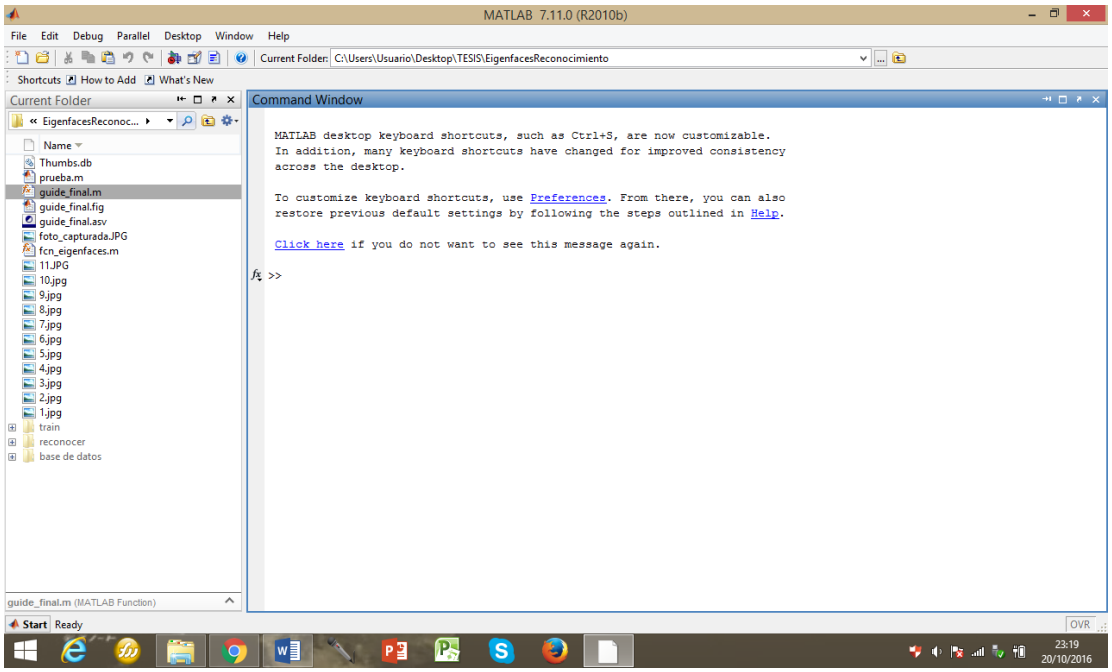


Gráfico 34. Ver Programa

Aquí podemos ver los archivos que están guardados en el programa, debemos escoger gui_final para poder visualizar el corrido del programa.

Aparece el programa en Matlab

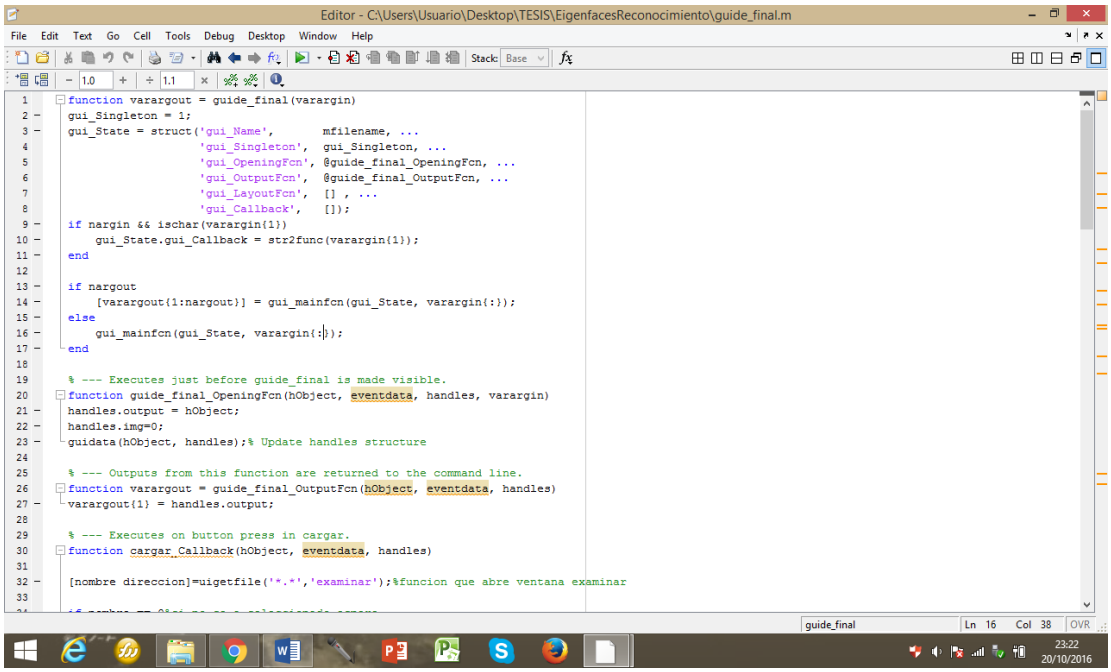


Gráfico 35. Programa de Matlab

Como podemos ver, se muestra el interfaz donde hemos realizado la programación, en la parte superior tenemos el botón de ejecutar, presionamos y el programa se mostrará de la siguiente manera.

Gráfico 36. Botó Ejecución

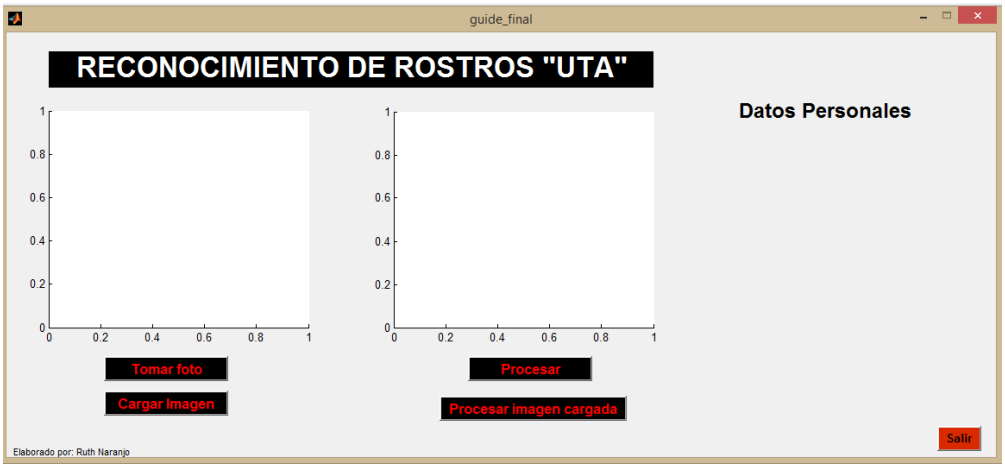


Gráfico 37. Ejecución

Podemos ver ya el programa ya listo y en completo funcionamiento.

Aparece una ventana con 2 recuadros, el del lado izquierdo para la foto capturada o la foto cargada del sistema y el recuadro del lado derecho para el resultado del cotejo de las fotografías.

En la parte inferior podemos observar que tenemos 4 botones.

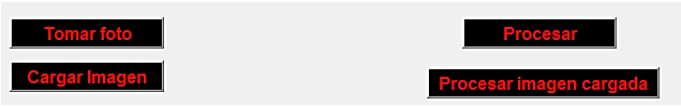


Gráfico 38. Botones

Tomar foto: que sirve para encender la cámara y automáticamente capturar una fotografía en tiempo real.

Procesar: con éste botón procesamos la imagen que hemos capturado con la cámara.

Cargar Imagen: que sirve para cargar una fotografía previamente capturada y guardada.

Procesar imagen cargada: utilizado para procesar la imagen que estamos cargando desde el computador.

1. Con el botón **tomar foto**, capturamos una fotografía con la cámara del computador.
2. Esta fotografía se guarda automáticamente con el nombre de foto_capturada en la carpeta creada para este programa, dentro de ésta se ubica la capeta train y reconocer que es donde se encuentra nuestra base de datos de fotografías, esta foto se debe renombrar por un número si así lo deseamos, las fotos deben ser tomadas recordando que la ubicación del rostro frente a la cámara es muy importante, además de la luminosidad que tengamos ya que éste factor influye considerablemente al momento de procesar para el cotejo de las fotografías.

3. Una vez capturada la fotografía, el programa recorta la imagen, capturando así únicamente le rostro de la persona que se ha fotografiado. Mostrando este resultado en una ventana auxiliar.

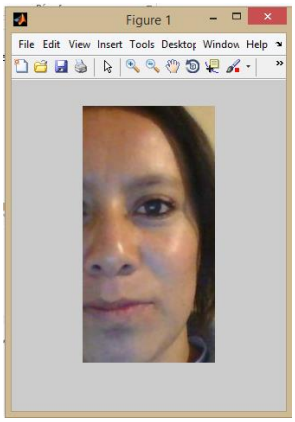


Gráfico 39. Foto capturada

4. Ahora que se ha guardado y procesado la fotografía, presionamos el botón procesar, con el cual se realizará el cotejo de la fotografía capturada con la que tenemos en la base de datos del programa.

5. Una vez procesada la imagen, se muestran los resultados. Se visualiza el rostro más parecido que encuentre el programa, además de los datos personales correspondientes a la persona que ha sido fotografiada.

Gráfico 40. Resultado

6. A la vez nos muestra una ventana más grande llamada **Figure 2** con el rostro que corresponde a la persona fotografiada.

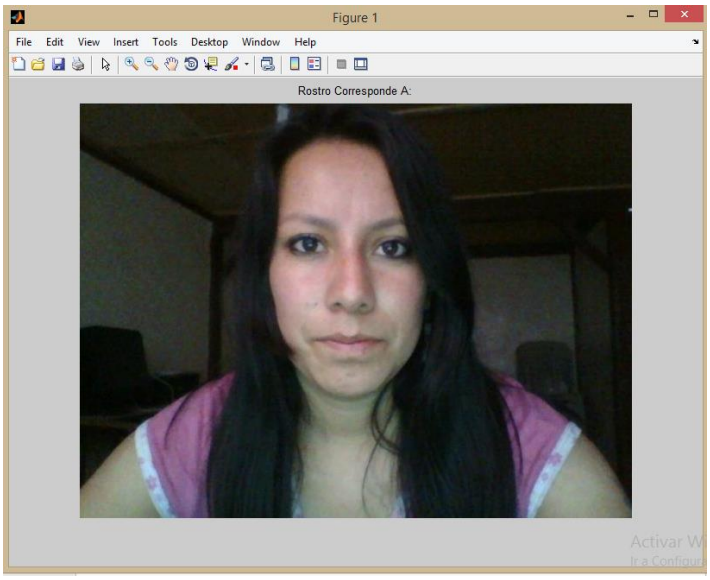


Gráfico 41. Rostro ganador

7. Luego tenemos el botón de cargar imagen.

Gráfico 42. Cargar imagen

8. Se da clic en este botón y aparece el explorador donde se escoge la foto a ser comparada. En este caso existe una carpeta llamada **reconocer**, en la que podemos encontrar varias fotografías de diferentes personas con distintos gestos. Constan al menos 2 fotografías de cada persona.

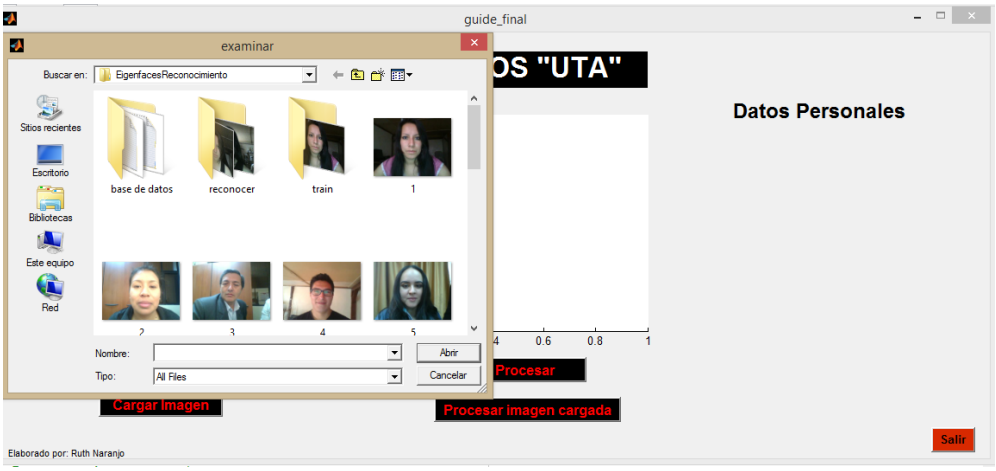


Gráfico 43. Examinar

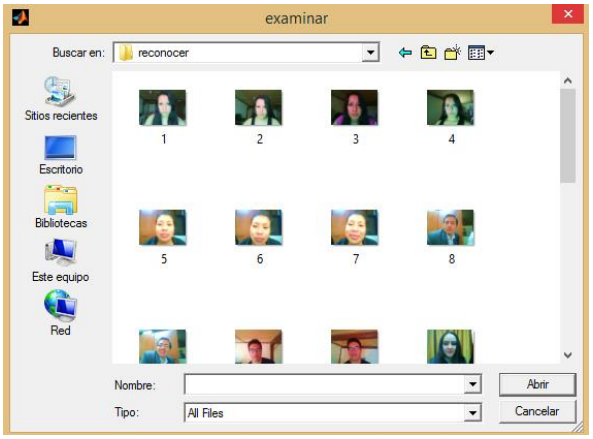


Gráfico 44. Fotografías personas

9. Escogemos una de las fotografías que tenemos, damos clic en aceptar y la imagen que hayamos escogido se habrá ubicado en el recuadro del lado izquierdo, como observamos en la siguiente imagen.

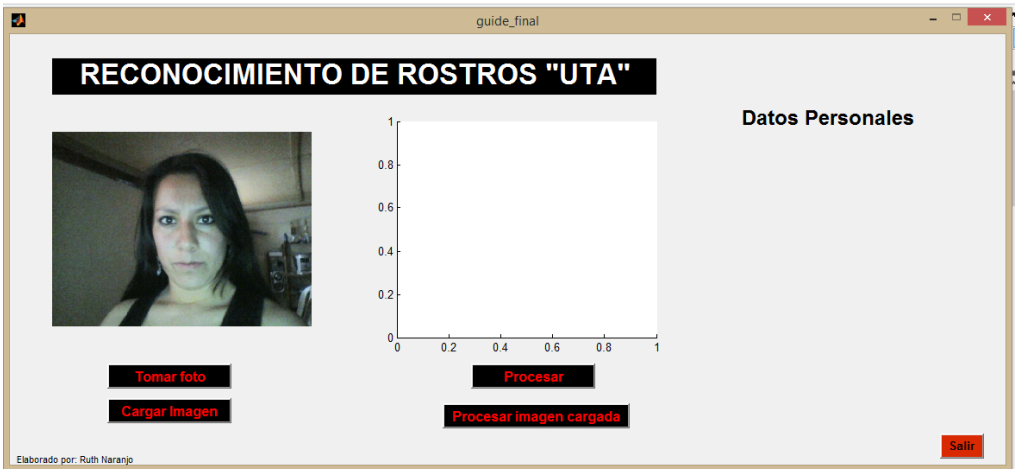


Gráfico 45. Imagen cargada

10. Ahora podemos dar clic en el botón **Procesar imagen cargada**, donde nos mostrará el rostro cotejado más parecido al de la fotografía que seleccionamos.

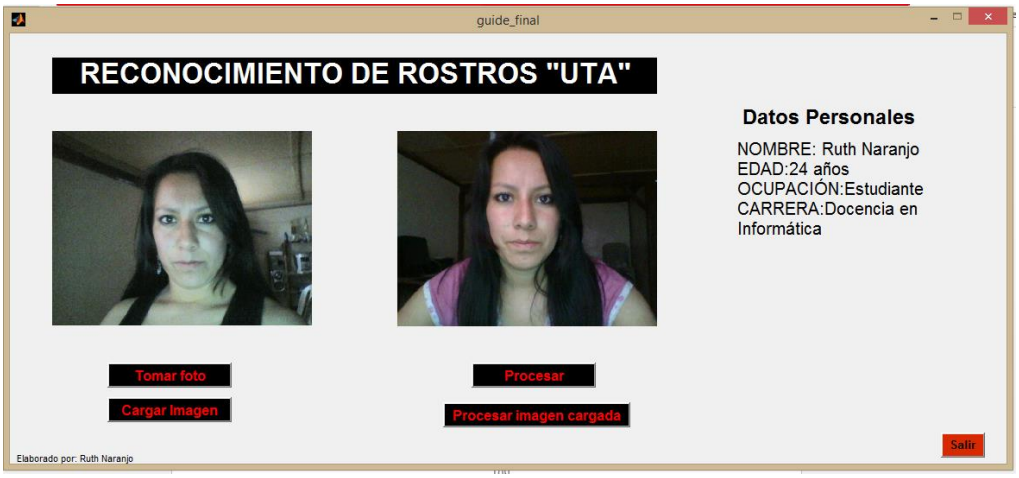


Gráfico 46. Cotejo

Como se observó el cotejo de imágenes ha sido exitoso, mostrando así el rostro de la persona más parecida al rostro de la imagen seleccionada, además también se puede observar los datos personales.

Otro ejemplo de este proceso.

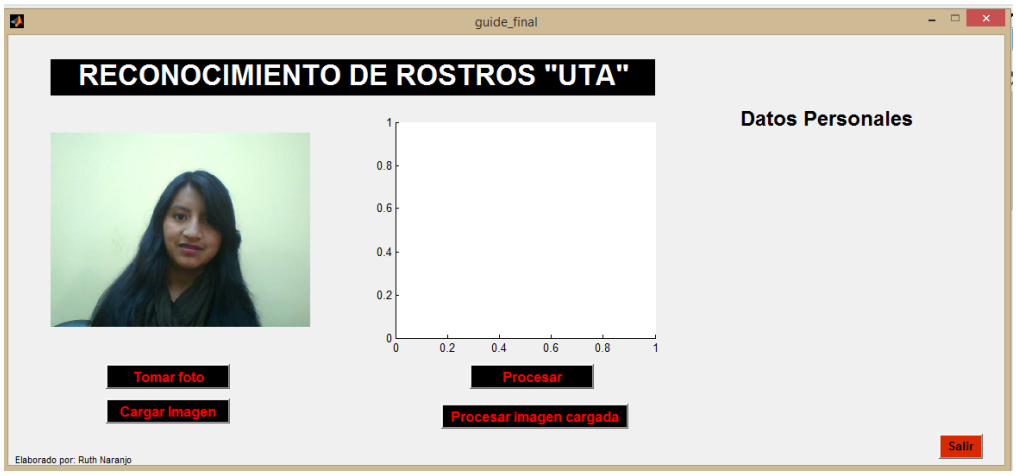


Gráfico 47. Ejemplo 1

Gráfico 48. Resultado 1

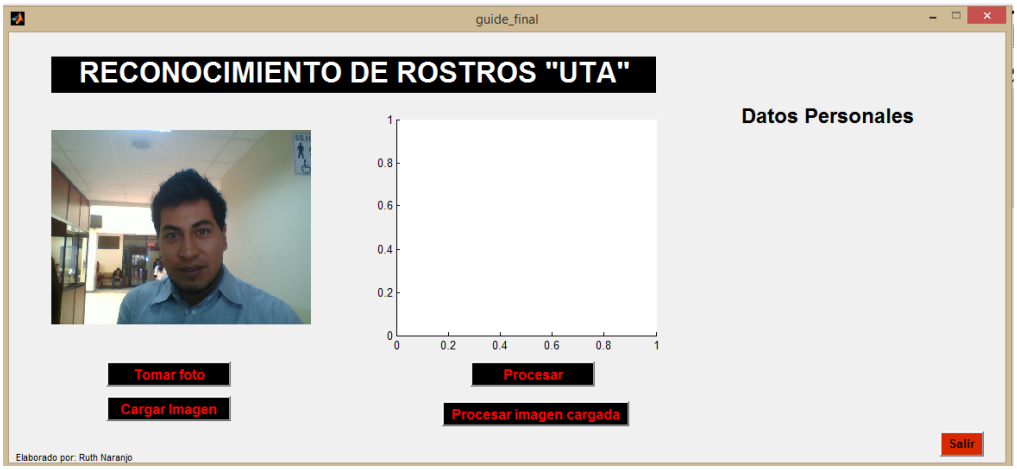


Gráfico 49. Ejemplo 2

Gráfico 50. Resultado 2

11. Finalmente tenemos un botón llamado **Salir.**

Gráfico 51. Salir

12. Al dar clic en éste botón, nos mostrará un mensaje donde nos pregunta si deseamos o no salir del programa.

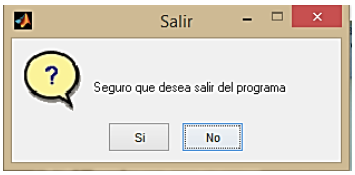


Gráfico 52. Opciones

13. En caso que seleccionemos la opción **Si**, saldremos del programa y se cerrará a ventana del corrido.

14. En cambio si seleccionamos la opción **No**, seguiremos en la ventana del corrido del programa donde podemos seguir experimentando el reconocimiento de rostros en Matlab.

Anexo 4: Código del sistema

Código donde se programa el reconocimiento facial usando la función eigenfaces

```
function[foto_ganadora,nombre_foto_ganadora]=fcn_eigenfaces(imagen_e
ntrada,path_train_folder)


%% +++++tratamiento train+++++
input_dir=path_train_folder;
dimension_mormalizada=[64 48];%normalizacion de las imagenes

nombre_archivos= dir(fullfile(input_dir,'*.jpg'));%guarda la ruta de
los archivos
numero_imagenes=numel(nombre_archivos);%cantidad de imagenes en la
estructura

%++++++++++++++++++++++++ representacion de imagenes en
vectores++++++++++

campo_vectorial=[];%conjunto de caras vacio

for n=1:numero_imagenes
    filename=fullfile(input_dir,nombre_archivos(n).name);
    img=imread(filename);%leo imagen a convectir como vector
    %img=rgb2gray(img);%paso imagenes a grises
    imagenGris=uint8(zeros(size(img,1),size(img,2)));

for i=1:size(img,1)
      for j=1:size(img,2)

imagenGris(i,j)=0.2989*img(i,j,1)+0.5870*img(i,j,2)+0.1140*img(i,j,3
);
      end
end
    img=im2double(imagenGris); %paso imagen a double

    if n==1%campo vectorial inicializado

campo_vectorial=zeros(prod(dimension_mormalizada),numero_imagenes);
    end
    img=imresize(img,dimension_mormalizada);%normalizacion de imagen
    campo_vectorial(:,n)=img(:);%campo vectorial de caras
end

%+++calculo de la media covarianza y el pca eigen vectors+
media_caras=mean(campo_vectorial,2);%media calculada
rep=repmat(media_caras,1,numero_imagenes);%replica de las medias
para cada imagen
```

```
informacion_importante_entrenamiento=campo_vectorial-rep;%calculo
estadistico de la covarianza info mas importantes

[evectors,score]=princomp(campo_vectorial');%componentes
principales,forma canonica reducida

num_eigenvectors=17;%eigenvectors sin ruido
disp(size(evectors));
evectors= evectors(:,1:num_eigenvectors);%eigenvectors sin ruido

features= evectors'* informacion_importante_entrenamiento; %
proyeccion de los vectores caracteristicos

%% imagen test

imaen_in=imagen_entrada;
imaen_in=imresize(imaen_in,dimension_mormalizada);%normaliza imagen

%imaen_in=rgb2gray(imaen_in);%trabaja con una capa grises
imagenGris2=uint8(zeros(size(imaen_in,1),size(imaen_in,2)));

for i=1:size(imaen_in,1)
      for j=1:size(imaen_in,2)

imagenGris2(i,j)=0.2989*imaen_in(i,j,1)+0.5870*imaen_in(i,j,2)+0.114
0*imaen_in(i,j,3);
      end
end
imaen_in=im2double(imagenGris2);%pasa datos a double
%se calcula la similaridad de entrada con cada de las imagenes en la
%carpeta

feature_vec=evectors'*((imaen_in(:)- media_caras));
similarity_score= arrayfun(@(n)1/ (1+norm(features(:,n)-
feature_vec)),1:numero_imagenes);

% encuentra la imagen con mayor similidad
[match_score,match_1x]= max(similarity_score);

% muestrea el resultado

nombre_foto_ganadora=nombre_archivos(match_1x).name;
foto_ganadora=imread(nombre_foto_ganadora);
```

Código con que se realiza la identificación del rostro, el recorte de la fotografía capturada y el cotejo tanto de la fotografía capturada como la seleccionada desde el computador.

```
function varargout = guide_final(varargin)
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @guide_final_OpeningFcn, ...
                   'gui_OutputFcn',  @guide_final_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end

% --- Executes just before guide_final is made visible.
function guide_final_OpeningFcn(hObject, eventdata, handles,
varargin)
handles.output = hObject;
handles.img=0;
guidata(hObject, handles);% Update handles structure

% --- Outputs from this function are returned to the command line.
function varargout = guide_final_OutputFcn(hObject, eventdata,
handles)
varargout{1} = handles.output;

% --- Executes on button press in cargar.
function cargar_Callback(hObject, eventdata, handles)

[nombre direccion]=uigetfile('*.*','examinar');%funcion que abre
ventana examinar

if nombre == 0%si no se a seleccionado espere
    return
end
imagen_cargada=imread(fullfile(direccion,nombre));%lectura de imagen

handles.img=imagen_cargada;%guardo la imagen para ser usada en otros
botones
guidata(hObject,handles);%actualizo el handles

axes(handles.axes1);
```

```
imshow(imagen_cargada)

% --- Executes on button press in tomarfoto.
function tomarfoto_Callback(hObject, eventdata, handles)
global vid
vid=videoinput('winvideo',1, 'YUY2_640x480' ); % se declara el
dispositivo de captura
foto=getsnapshot(vid);% captura lo que ve la camara en escala Ycbr
foto=ycbcr2rgb(foto); % se convierte a rgb
extension = '.JPG'; %  guardo la extension de la foto capturada
filename = strcat('foto_capturada', extension); % se colocar nombre
a la foto capturada
imwrite(uint8(foto),filename);% se guarda la foto capturada
axes(handles.axes1);
imshow(foto);

% --- Executes during object creation, after setting all properties.
function texto_CreateFcn(hObject, eventdata, handles)
if ispc && isequal(get(hObject,'BackgroundColor'),
get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end

% --- Executes on button press in salir.
function salir_Callback(hObject, eventdata, handles)
boton_salida = questdlg('Seguro que desea salir del
programa','Salir','Si','No','No')
if strcmp(boton_salida,'No')%si no sedea salir, continue
    return;
end
close all% si desea salir cierre todo


% --- Executes on button press in Procesar.***********
function Procesar_Callback(hObject, eventdata, handles)
foto=imread('foto_capturada.jpg');%foto capturada
recorte=imcrop(foto,[250 110 152 296]);
figure;imshow(recorte)
[foto_ganadora,nombre_foto_ganadora]=fcn_eigenfaces(recorte,'.\train
');
axes(handles.axes2);
imshow(foto_ganadora);
if (strcmp('1.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Ruth Naranjo
EDAD:24 años OCUPACIÓN:Estudiante CARRERA:Docencia en Informática');
elseif (strcmp('2.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Vanessa Córdova
EDAD:28años OCUPACIÓN:Estudiante CARRERA:Docencia en Informática');
elseif (strcmp('3.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Javier Salazar
EDAD:45años OCUPACIÓN:Docente    CARRERA:Docencia en Informática');
elseif (strcmp('4.jpg', nombre_foto_ganadora))
```

```
    set(handles.text9,'string','NOMBRE: Fabricio Mora
EDAD:25 años OCUPACIÓN:Conserje  DEPENDENCIA:Fcaultad Ciencias
Humanas y de la Educación');
elseif (strcmp('5.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Gabriela Alvarez
EDAD:25años OCUPACIÓN:Secretaria DEPENDENCIA:Facultad Ciencias
Humanas y de la Educación');
elseif (strcmp('6.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Jeaneth Bejarano
EDAD:26años OCUPACIÓN:Secretaria DEPENDENCIA:Facultad Ciencias
Humanas y de la Educación');
elseif (strcmp('7.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Gabriela Cholota
EDAD:23años OCUPACIÓN:Estudiante CARRERA:Educación Básica');
elseif (strcmp('8.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Norma Punina
EDAD:42años OCUPACIÓN:Secretaria DEPENDENCIA:Facultad Ciencias
Humanas y de la Educación');
elseif (strcmp('9.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Maricela Chimbolema
EDAD:27años OCUPACIÓN:Estudiante CARRERA:Docencia en Informática');
elseif (strcmp('10.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Iván Villacís
EDAD:25años OCUPACIÓN:Estudiante CARRERA:Docencia en Informática');
elseif (strcmp('11.JPG', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Amable Tisalema
EDAD:25años OCUPACIÓN:Estudiante CARRERA:Docencia en Informática');
end

figure;imshow(foto_ganadora);title('Rostro Corresponde A:')

% --- Executes on button press in procesar_cargada.***********
function procesar_cargada_Callback(hObject, eventdata, handles)

[foto_ganadora,nombre_foto_ganadora]=fcn_eigenfaces(handles.img,'.\t
rain');
axes(handles.axes2);
imshow(foto_ganadora);

if (strcmp('1.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Ruth Naranjo
EDAD:24 años OCUPACIÓN:Estudiante CARRERA:Docencia en Informática');
elseif (strcmp('2.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Vanessa Córdova
EDAD:28años OCUPACIÓN:Estudiante CARRERA:Docencia en Informática');
elseif (strcmp('3.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Javier Salazar
EDAD:45años OCUPACIÓN:Docente    CARRERA:Docencia en Informática');
elseif (strcmp('4.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Fabricio Mora
EDAD:25 años OCUPACIÓN:Conserje  DEPENDENCIA:Fcaultad Ciencias
Humanas y de la Educación');
elseif (strcmp('5.jpg', nombre_foto_ganadora))
```

```
    set(handles.text9,'string','NOMBRE: Gabriela Alvarez
EDAD:25años OCUPACIÓN:Secretaria DEPENDENCIA:Facultad Ciencias
Humanas y de la Educación');
elseif (strcmp('6.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Jeaneth Bejarano
EDAD:26años OCUPACIÓN:Secretaria DEPENDENCIA:Facultad Ciencias
Humanas y de la Educación');
elseif (strcmp('7.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Gabriela Cholota
EDAD:23años OCUPACIÓN:Estudiante CARRERA:Educación Básica');
elseif (strcmp('8.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Norma Punina
EDAD:42años OCUPACIÓN:Secretaria DEPENDENCIA:Facultad Ciencias
Humanas y de la Educación');
elseif (strcmp('9.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Maricela Chimbolema
EDAD:27años OCUPACIÓN:Estudiante CARRERA:Docencia en Informática');
elseif (strcmp('10.jpg', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Iván Villacís
EDAD:25años OCUPACIÓN:Estudiante CARRERA:Docencia en Informática');
elseif (strcmp('11.JPG', nombre_foto_ganadora))
    set(handles.text9,'string','NOMBRE: Amable Tisalema
EDAD:25años OCUPACIÓN:Estudiante CARRERA:Docencia en Informática');
end
```