UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

CARRERA: MAESTRÍA EN COMPUTACIÓN MENSIÓN SEGURIDAD INFORMÁTICA

CREACIÓN DE UN SISTEMA DE SEGURIDAD DE RECONOCIMIENTO FACIAL 3D UTILIZANDO TÉCNICAS DE INTELIGENCIA ARTIFICIAL PARA EVITAR LA SUPLANTACIÓN DE IDENTIDAD EN LA ORGANIZACIÓN ADRA ECUADOR.

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación Mención Seguridad Informática

AUTOR:

Edwin Jefferson Cárdenas Argoti

DIRECTOR:

Fabián Geovanny Cuzme Rodríguez

Ibarra, enero 2025

UNIVERSIDAD TÉCNICA DEL NORTE

DIREECIÓN DE BIBLIOTECA

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

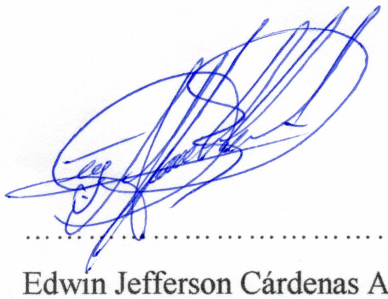
DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	0401923594		
APELLIDOS Y NOMBRES:	Cárdenas Argoti Edwin Jefferson		
DIRECCIÓN:	Av. Veintimilla y Andrés Bello		
E-MAIL:	cardenasjargoti@hotmail.com		
TELÉFONO FIJO:	0997361914	**TELÉFONO MÓVIL:**	0997361914
DATOS DE LA OBRA			
TÍTULO:	SISTEMA DE SEGURIDAD DE RECONOCIMIENTO FACIAL 3D UTILIZANDO TÉCNICAS DE INTELIGENCIA ARTIFICIAL PARA EVITAR LA SUPLANTACIÓN DE IDENTIDAD EN LA ORGANIZACIÓN ADRA ECUADOR.		
AUTOR(ES):	Cárdenas Argoti Edwin Jefferson		
FECHA:	09/01/2025		
SOLO PARA TRABAJOS DE GRADO			
PROGRAMA:	**PREGRADO**	**X POSGRADO**	
TÍTULO POR EL QUE OPTA:	Magister en Computación con Mención en Seguridad Informática		
ASESOR/DIRECTOR:	MSC. Fabián Cuzme Rodríguez		

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros; por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de esta y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 9 días del mes de enero de 2025

EL AUTOR



.....

Edwin Jefferson Cárdenas Argoti

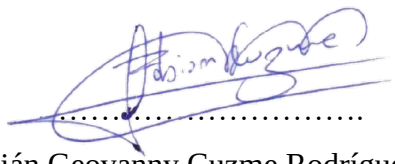
CI: 0401923594

CERTIFICACIÓN

MAGISTER FABIÁN CUZME, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Que, el presente trabajo de Titulación "SISTEMA DE SEGURIDAD DE RECONOCIMIENTO FACIAL 3D UTILIZANDO TÉCNICAS DE INTELIGENCIA ARTIFICIAL PARA EVITAR LA SUPLANTACIÓN DE IDENTIDAD EN LA ORGANIZACIÓN ADRA ECUADOR" Ha sido desarrollado por el Ingeniero Cárdenas Argoti Jefferson bajo mi supervisión.

Es todo en cuanto puedo certificar en honor de la verdad.



…….

Ing. Fabián Geovanny Cuzme Rodríguez, MsC.

C.I.

DIRECTOR

DEDICATORIA

A mi madre, cuyo amor incondicional y sacrificio han sido el pilar de mi vida. Tu apoyo constante, tus palabras de aliento y tu fe en mis sueños me han impulsado a seguir adelante, incluso en los momentos más desafiantes. Gracias por ser mi ejemplo de fortaleza y dedicación.

A mi abuelita, cuya sabiduría y cariño han dejado una huella imborrable en mi corazón. Tus historias y enseñanzas me han guiado y me han enseñado el valor de la perseverancia y el amor familiar. Eres una fuente de inspiración inagotable.

Esta tesis es un tributo a ambas, por todo lo que han hecho y continúan haciendo por mí. Sin su apoyo, este logro no habría sido posible.

Jefferson Cárdenas

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a todas las personas que han sido parte de este recorrido académico y personal.

Mi gratitud hacia Dios, guía en cada paso de este camino. Él ha sido la fuente de luz y esperanza en los momentos más difíciles, iluminando mi sendero cuando más lo necesitaba.

A mi madre, cuyo amor incondicional y sacrificio han sido el pilar de mi vida. Tu apoyo constante, tus palabras de aliento y tu fe en mis sueños me han impulsado a seguir adelante, incluso en los momentos más desafiantes. Gracias por enseñarme la importancia de la perseverancia y por siempre estar a mi lado.

A mi abuelita, cuya sabiduría y cariño han dejado una huella imborrable en mi corazón. Tus historias y enseñanzas me han guiado y me han mostrado el valor de la familia y la determinación. Eres una fuente de inspiración constante, y tu amor me ha dado la fortaleza para enfrentar cualquier obstáculo.

A mi director de tesis MsC Fabián Cuzme, por su valiosa orientación y paciencia su guía experta ha sido fundamental en el desarrollo y culminación de este proyecto, reflejando no solo su profundo conocimiento en el campo sino también su compromiso con la excelencia académica.

A mis profesores, por su guía, paciencia y compromiso. Gracias por compartir su conocimiento y por retarme a pensar de manera crítica. Cada una de sus clases ha sido una oportunidad de aprendizaje que atesoro, y su apoyo ha sido crucial en mi desarrollo académico.

Finalmente, a todos mis seres queridos, gracias por su amor y por estar siempre ahí para mí. Este logro no solo es mío, sino el resultado de un esfuerzo conjunto. Estoy profundamente agradecido por cada uno de ustedes y por el papel que han jugado en mi vida.

Jefferson Cárdenas

ÍNDICE.

ÍNDICE DE TABLAS.

ÍNDICE DE FIGURAS.

RESUMEN

Este trabajo de titulación presenta el desarrollo de un sistema de seguridad de reconocimiento facial 3D, utilizando técnicas de inteligencia artificial, diseñado para prevenir la suplantación de identidad en la organización ADRA Ecuador, que brinda apoyo social a personas en situación de vulnerabilidad. El objetivo es automatizar los procesos manuales que tradicionalmente se emplean para controlar la suplantación de identidad y evitar la repetición de ayudas destinadas a otros beneficiarios en los centros de asistencia social.

El proyecto se estructura en cinco fases, siguiendo la metodología estandarizada por la norma IEEE 15288. La primera fase implica un análisis detallado de la organización para identificar y establecer los requisitos específicos del software, lo cual fundamenta el diseño y la definición de la arquitectura del sistema. A continuación, se procede a la fase teórica y luego a la fase metodológica. La cuarta fase abarca el desarrollo, que incluye la codificación del sistema y su implementación en el servidor proporcionado por la empresa. Finalmente, la etapa de verificación y validación garantiza el correcto funcionamiento del sistema y la optimización de las tareas gestionadas.

Los resultados obtenidos tras la implementación del sistema cumplen con las expectativas de la organización, mostrando una mejora significativa en la eficiencia de los procesos de verificación de personas vulnerables. Este trabajo no solo optimiza las operaciones internas de ADRA Ecuador, sino que también establece un precedente en la aplicación de inteligencia artificial en el reconocimiento facial.

Palabras claves: Inteligencia artificial, Reconocimiento facial 3D, Sistema de seguridad, Suplantación de identidad, Automatización, Metodología IEEE15288, Optimización de operaciones.

ABSTRACT

This degree work presents the development of a 3D facial recognition security system, using artificial intelligence techniques, designed to prevent identity theft in the ADRA Ecuador organization, which provides social support to people in vulnerable situations. The objective is to automate the manual processes that are traditionally used to control identity theft and avoid the repetition of aid intended for other beneficiaries in social assistance centers.

The project is structured in five phases, following the methodology standardized by the IEEE 15288 standard. The first phase involves a detailed analysis of the organization to identify and establish the specific requirements of the software, which bases the design and definition of the architecture of the system. Next, we proceed to the theoretical phase and then to the methodological phase. The fourth phase covers development, which includes coding the system and its implementation on the server provided by the company. Finally, the verification and validation stage guarantees the correct functioning of the system and the optimization of the managed tasks.

The results obtained after the implementation of the system meet the expectations of the organization, showing a significant improvement in the efficiency of the verification processes for vulnerable people. This work not only optimizes ADRA Ecuador's internal operations, but also sets a precedent in the application of artificial intelligence in facial recognition.

Keywords: Artificial intelligence, 3D facial recognition, Security system, Identity theft, Automation, IEEE15288 Methodology, Operations optimization.

CAPITULO I – ANTECEDENTES

1.1. Tema.

Creación de un sistema de seguridad de reconocimiento facial 3d utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la organización adra Ecuador.

1.2. El Problema

El reconocimiento facial mediante cámaras de video está en estado de perfeccionamiento a nivel mundial ya que se están realizando nuevas investigaciones a nivel mundial por lo que es un tema que se encuentra en desarrollo y con el paso del tiempo se lo está mejorando; a nivel nacional se han estado realizando prácticas dentro de las universidades y algunas empresas comprometidas con la tecnología (Pérez, 2022); la Organización ADRA es una Organización no Gubernamental que se encarga del bienestar de las personas de bajos recursos económicos y para su mejor funcionamiento, requiere de la automatización y control fácil del personal para brindar una mayor seguridad en el desarrollo de las funciones diarias que la fundación realiza.

El problema radica en la organización y selección de sectores vulnerables para llegar con las ayudas comunitarias dependiendo del sector, la organización se encarga primero de realizar un estudio de campo para verificar a las personas más vulnerables para generar un registro y asistirlas después, luego se debe organizar un sitio específico para que las personas beneficiarias vayan, se reúnan e ingresen ordenadamente para recibir los aportes que la organización ADRA tiene para su bienestar.

Al no existir un control inteligente de quienes ingresan y salen, generalmente otras personas que no están registradas acceden a ayudas no correspondidas, por lo que algunas personas que más necesitan deben quedarse sin ayuda, ya que la organización calcula el volumen de las ayudas comunitarias mediante el registro generado en la primera visita de campo.

Para evitar estos problemas, la organización ADRA busca una solución contundente para evitar la suplantación de identidad de las personas registradas mediante un control inteligente; así se podrá evitar el acceso de personas no relacionadas con la organización y las ayudas comunitarias llegarán a las personas registradas en visitas previas.

1.3. Objetivos.

1.3.1. Objetivo General.

Implementar un sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios.

1.3.2. Objetivos Específicos:

- Realizar una investigación bibliográfica sobre sistemas de seguridad de reconocimiento facial en 3D y cómo evitar la suplantación de identidad aplicando técnicas de Inteligencia Artificial.
- Diagnosticar la situación actual de la Organización ADRA Ecuador en lo referente al control y registro del personal y usuarios beneficiarios de ayuda humanitaria en la ciudad de Tulcán.
- Desarrollar un sistema de seguridad de reconocimiento facial en 3D para detectar el rostro de las personas usando Inteligencia Artificial para la Organización ADRA Ecuador.
- Evaluar la eficiencia que tiene el sistema de seguridad de reconocimiento facial respecto a la suplantación de identidad en la Organización ADRA Ecuador.

1.4. Alcance.

La Organización ADRA de la ciudad de Tulcán ha tenido pérdida de recursos materiales y económicos, debido principalmente al robo de identidad por lo que se requiere de la presencia de cámaras con sistemas de reconocimiento facial en 3D mediante Técnicas de Inteligencia Artificial con el fin de registrar a todos los trabajadores y usuarios para dar un seguimiento personalizado de cada persona que recibe beneficios de la Organización con el fin de evitar la suplantación de identidad por parte de personas sospechosas y verificar los datos estadísticos de todas las ayudas que se brinda y la población beneficiada; por lo que, en el presente proyecto se realizará el proceso de codificación facial y sus respectivas pruebas de funcionamiento para reconocer a cada persona mediante la captura de su rostro.

El contexto temático del problema es la Inteligencia Artificial para reconocer los rostros de cada beneficiaria de la Organización ADRA de la ciudad de Tulcán que se encuentre registrada en la base de datos.

Al no tener un sistema inteligente de reconocimiento facial en 3D impide registrar de forma automática a las personas que asisten a los sitios de beneficencia comunal; al no registrar a los usuarios de la Organización no se puede obtener un registro general para la realización de cuadros estadísticos que permiten una mejor comprensión de las comunidades más necesitadas; al no conocer los lugares con mayor índice de pobreza no se puede saber hacia dónde ir a brindar ayuda con mayor frecuencia.

La modalidad de estudio aplica enfoques cualitativos y cuantitativos, y se encarga de aplicar seguridad usando Inteligencia Artificial para cumplir con la hipótesis: Mejora de la seguridad mediante un sistema de reconocimiento facial en 3D, aplicando la Inteligencia Artificial.

1.5. Justificación.

El presente proyecto de investigación presenta una gran importancia ya que la Organización ADRA requiere que el control de usuarios sea en tiempo real ya que es complicado pasar lista a cada uno de los beneficiarios y la mejor forma es utilizar la Inteligencia Artificial para el reconocimiento de los rasgos faciales de cada persona y de esta forma acceder directamente a su información y registrar su asistencia; se realizará un aporte tecnológico en el área del conocimiento ya que el presente sistema dejará un precedente para que se realicen posteriores investigaciones que tengan como base el presente proyecto por lo que la ciudad de Tulcán tendrá una institución que manejará este tipo de sistema lo cual es un avance dentro de la comunidad; la realización del sistema de reconocimiento facial es un inicio para la automatización de otros sectores que permitan mejorar la calidad de vida agilizando procesos que se realizan diariamente (ADRA, 2012).

Con la implementación de un sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA de la ciudad de Tulcán aplicado al control y registro del personal y usuarios beneficiarios, se debe tener en cuenta la privacidad de las personas al ser vigiladas sin permiso por lo que para evitar posibles conflictos legales, en la primera visita en donde se registrará a las personas vulnerables se les hará firmar un acta en dónde ellos accedan y se comprometan a estar en constante vigilancia por las cámaras dentro del

sitio y así con la firma de compromiso no puedan demandar a la organización por violación a su privacidad.

La línea de investigación en la que se encuentra el presente proyecto es desarrollo, aplicación de software y cyber security (Seguridad Cibernética).

CAPITULO II – FUNDAMENTACIÓN TEÓRICA

2.1. Antecedentes.

En la Provincia del Carchi existen proyectos desarrollados que tienen cierta referencia con respecto a la propuesta y sirven de base para el desarrollo del presente proyecto; entre ellos se destacan: “Sistema de visión artificial para la detección de aglomeración de personas en un semáforo” realizado por (Jiménez, 2018) de la Universidad Nacional de Loja cuyo objetivo es verificar aglomeraciones en ciertos lugares cercanos a un semáforo; “Sistema informático de visión artificial para mejorar la gestión del parqueadero de la Uniandes Tulcán” realizado por (Vizcaino, 2018) cuyo objetivo es organizar los vehículos que ingresan al parqueadero; “Sistema informático con visión artificial para evitar el robo de vehículos en la empresa Seguros Olímpicos de la ciudad de Tulcán” realizado por (Ruano, 2022) cuyo objetivo es evitar el robo de vehículos dentro de la ciudad de Tulcán.

2.2. Sistema Informático.

Permite el procesamiento y transmisión de información de una manera rápida y concisa, de esta manera las personas pueden transmitir datos o información a través de esta parte fundamental conocida como sistema informático.

Se define como sistema de información a un conjunto de programas que están relacionados entre sí y permiten administrar la información mediante el empleo de la computadora; como cualquier sistema, es un conjunto de funciones interrelacionadas, hardware, software y de Recursos Humanos. El sistema informático utiliza un conjunto de dispositivos que se usan para programar y almacenar programas y bases de datos. (Blanco, 2008).

El sistema informático ordena la información usando bases de datos para parametrizar y administrar los datos, todo mediante hardware, software y, sobre todo, el recurso humano para transmitir información de forma ordenada y almacenar datos y programas. Hoy es fundamental, ya que las personas almacenan mucha información cada día que pasa por lo que los sistemas de almacenamiento son muy importantes.

2.2.1. Componentes.

El sistema informático presenta componentes importantes para operar al ordenador, el sistema operativo es fundamental para que uno cumpla con sus funciones básicas.

Componente físico: Es el hardware del sistema informático, el computador y sus componentes internos como memorias, CPU, los periféricos de entrada y salida, etc., y todo aquel dispositivo que se conecte a este hardware.

Componente lógico: Proporciona la capacidad y la potencia de procesamiento para que un sistema informático funcione, este componente es el software del sistema informático, la documentación, los datos que procesa y gestiona; el software es el que se requiere para almacenar, procesar y distribuir los datos que se registran en el mismo.

Componente humano: Está formado por los usuarios, es decir las personas que utilizan los componentes lógicos y físicos, son los encargados del soporte y mantenimiento técnico. (Sejal, 2018).

Un sistema informático presenta características útiles para transmitir la información orientada para que usuarios y operadores puedan realizar. Se deben considerar las funciones que permite realizar cada componente como físico lógico y humano, indispensables ya que dependen del anterior para sus procesos y funciones.

2.3. Visión Artificial.

La Visión Artificial es una disciplina en desarrollo, que apunta a construir modelos computacionales de las funcionalidades visuales en humanos, que trabaja mediante el procesamiento de imágenes la cual se capta en los colores básicos (RGB) rojo, verde y azul los cuales son captados mediante dispositivos que disponen de cámaras (Contaval, 2016).

La Visión Artificial se enfoca con imágenes digitalizadas; es decir usa escala de grises con ello obtiene un mayor reconocimiento al momento de exponerlo frente a una persona u objeto.

2.3.1. Procesamiento de imágenes.

El procesamiento de imágenes ya sea dirigido al algoritmo de patronos binarios locales o Viola & Jones siguen un patrón que se encuentra ya establecido permitiendo de esta manera capturar la imagen de entrada y posteriormente pasa a ser digitalizada, este proceso presenta los siguientes parámetros: captura, procesamiento y visualización de

imágenes y video en tiempo real que permiten la visualización de grandes cantidades de datos; las principales aplicaciones que se desarrollan con IoT y Visión Artificial pueden ser implementadas en educación, medicina, edificios inteligentes, sistemas de vigilancia de personas y vehículos, entre otros. Este tipo de aplicaciones mejoran la calidad de vida de los usuarios, sin embargo, para su desarrollo se requiere una infraestructura que permita la convergencia de diferentes protocolos y dispositivos, pero de manera especial que puedan manejar las diferentes fases de la adquisición de imágenes. (UTE, 2024).

2.4. Algoritmos para la codificación facial.

El software de detección facial sirve para verificar si una fotografía cualquiera contiene o no uno o varios rostros de personas, este tipo de software es importante para la realización de proyectos que requieran este tipo de características como son la captura de imágenes y procesamiento de imágenes, generalmente se lo realiza por categorización binaria mediante clasificadores que permite minimizar errores; para este tipo de reconocimiento es necesario que el algoritmo minimice errores frecuentes como lo son los falsos positivos y negativos para que el código de programación tenga un rendimiento aceptable; este proceso requiere una codificación numérica que sea exacta ya que debe ser capaz de diferenciar rostros humanos de objetos. (Pérez, 2022).

2.4.1. Algoritmo de Viola & Jones.

Se usa para detectar rostros humanos a partir de una imagen, donde el sistema toma imágenes faciales y no faciales como entrada, y luego se iniciará la fase de entrenamiento en la que el sistema detecta el rostro. En fase de formación se incluyen dos tipos de conjuntos como son: el conjunto de imágenes positivas y el conjunto de imágenes negativas, las imágenes positivas se refieren a imágenes con rostros y en lo que es imágenes negativas se refiere a las imágenes sin rostro; en la fase de formación, se recogen todas las características que son relacionadas con las imágenes de rostro y todas estas características se almacenan en un archivo el que es comparado mediante los clasificadores en cascada. (Jones, 2018).

El algoritmo de Viola & Jones tiene cuatro etapas las cuales son:

2.4.1.1. Características de tipo Haar Cascade.

Haar Cascade es el nombre del algoritmo de reconocimiento de patrones visuales en imágenes; las características de tipo Haar Cascade son combinaciones de rectángulos del mismo tamaño, adyacentes horizontal o verticalmente, como se muestra en la figura 3. Los rectángulos en negro representan zonas con una contribución positiva; mientras que, los rectángulos blancos representan zonas con una contribución negativa al filtro o resultado final.

Las características tipo Haar están compuestas por tres características las cuales son: dos rectángulos, tres rectángulos, cuatro rectángulos (horizontal – vertical). De esta forma se puede observar los tipos de características Haar las cuales están aplicadas al rostros y ojos relacionadas a dos y tres rectángulos con ello se logra comparar la intensidad de la zona asignada, el resultado del filtro es la diferencia de los pixeles de una imagen tanto de la zona negra como blanca. (Jones, 2018).

2.4.1.2. Imagen integral.

Viola & Jones usaron una representación de imagen llamada imagen integral, también conocida como tabla de área sumada, para determinar la presencia o ausencia de cientos de características similares a Haar en cada ubicación de imagen, para realizar el cálculo se determina un punto x, y; que se establece su valor en la suma de los pixeles ubicados por encima y a su izquierda de dicho punto incluyéndose, convirtiendo la imagen original en una imagen integral (Jones, 2018).

2.4.1.3. Impulso adaptativo.

El impulso adaptativo es capaz de elegir entre un gran conjunto de filtros, las características Haar, para seleccionar en cada momento cuál de ellos se ajusta mejor, para que se clasifiquen satisfactoriamente los diferentes elementos que vamos a clasificar.

En este procedimiento se obtiene después de algunas iteraciones, donde se prueba los clasificadores de Haar para cada una de las muestras, un clasificador que separa entre muestras positivas y muestras negativas; primeramente, se genera una detección con algún clasificador, donde los elementos mal clasificados aumentan su tamaño, para que el siguiente clasificador que intervenga, de más importancia a que, la clasificación de los elementos con mayor tamaño sea la correcta. (Jones, 2018).

2.4.1.4. Cascada de clasificadores.

Se describe al algoritmo para construir una cascada de clasificadores que logra un mayor rendimiento de detección mientras reduce radicalmente el cálculo negativo de dicha imagen, la idea clave es que, si son más pequeños los clasificadores, más se pueden construir clasificadores eficientes e impulsados que rechacen muchas de las imágenes negativas mientras detecta casi todas las instancias positivas; los clasificadores más simples rechazan la mayoría de las imágenes en cambio los clasificadores complejos son llamados para lograr bajo falsos positivos. (Jones, 2018).

Las etapas en la cascada se construyen mediante entrenamiento de clasificadores utilizando impulsos adaptivos, comenzando con una de dos características del clasificador fuerte, se puede obtener un filtro facial eficaz ajustando al umbral del clasificador fuerte para minimizar falsos negativos.

2.4.2. Algoritmo patrón binario local.

Durante los últimos años, patrones binarios locales (LBP) han despertado un interés referente al procesamiento de imágenes y visión artificial. LBP es un método no paramétrico que resume las estructuras locales de las imágenes de manera eficiente comparando cada píxel con píxeles adyacentes. Las propiedades más importantes de LBP son: su tolerancia a la iluminación monotónica y su simplicidad computacional. LBP se propuso para análisis de texturas, ya que es potente para describir las estructuras locales.

Ha sido ampliamente explotado en muchas aplicaciones, por ejemplo, análisis de imagen, recuperación de imagen y vídeo, modelado de entorno, inspección visual, y teledetección. El análisis de imagen facial basado en LBP ha sido uno de los más populares y exitosos en los últimos años. (Troya, 2016).

2.4.3. Algoritmo de enfoque basado en características elásticas.

El algoritmo EBGM es un buen algoritmo porque es único en relación con los demás ya que percibe los rostros y contrasta sus partes; en segundo lugar, los resultados son buenos en relación con diferentes algoritmos evaluados en las pruebas.

Presenta código abierto ampliado que incorpora cuatro algoritmos de referencia y una disposición de los dispositivos y secuencias de comandos que se pueden utilizar para evaluar la ejecución del algoritmo de reconocimiento facial. (STACKPOINTERS, 2018)

2.5. Selección del algoritmo para el análisis facial del proyecto.

Para la selección del algoritmo de reconocimiento facial a utilizar se han analizado tres tipos de código y se los ha clasificado en tres ítems los cuales son:

- Resolución.
- Dato temporal.
- Rasgos de algoritmo.

A continuación, en la Tabla 1 se muestran las características de cada algoritmo.

Tabla 1.

Selección de algoritmo de reconocimiento facial.

Algoritmo	Características	Ventajas	Desventajas
Viola & Jones	Archivos HAAR, imagen adaptativa en cascada	Análisis de fotogramas con cualquier cámara	Depende de la clasificación de Haar Cascade
Patrón Binario	Codificación binaria del rostro	El rostro se distingue mediante código binario	Requiere cámara de alta resolución y super computador
Características Elásticas	Movimiento pendular, red con rejillas de 8 y 16 slots	Actúa con el movimiento del video captado	Requiere cámara de alta resolución y super computador

Nota. Esta tabla muestra 3 algoritmos dedicados al reconocimiento facial.

En el ítem de resolución es evidente que, por su bajo costo de procesamiento y utilización de memoria, el algoritmo de Viola & Jones es el más concreto para la realización del presente sistema ya que analiza la imagen en fotogramas que es considerable y válido para la realización del proyecto.

En el ítem de dato temporal, se puede verificar que los 3 algoritmos son similares por lo que en este punto cualquier algoritmo es una buena opción para sistema.

En el ítem de rasgos el algoritmo que mejor se adapta al ambiente del reconocimiento facial de rostros en tiempo real es el algoritmo de Viola & Jones, puesto que va a interactuar directamente con el rostro del usuario a cierta distancia para verificar sus rasgos faciales permitiendo una adaptación oportuna al cambio de iluminación y entorno.

2.6. Seguridad Ciudadana.

La realización del presente estudio parte de una comprensión de la violencia que va más allá del análisis patológico de las conductas individuales y se concibe a partir de un marco temático que entiende como lo que es: un tipo particular de relación social en la que intervienen, al menos, dos clases de actores que, como forma de resolver el conflicto de sus intereses diferentes, hacen o intentan hacer daño, en términos físicos o psicológicos. El informe tiene como objeto central el estudio de la seguridad ciudadana; lo cual implica poner énfasis en la calidad de vida de la población, en los derechos y deberes de las personas (ciudadanía) y en el conjunto de las distintas fases y expresiones de la violencia.

La definición de la seguridad ciudadana, como objeto de conocimiento y actuación, implica un avance y un redireccionamiento de la problemática; primero, porque se refiere a una violencia en particular (social); y, segundo, porque tiene que ver con la totalidad del proceso de la violencia, pero desde una connotación con carga positiva (seguridad) y no negativa (violencia). (Palomeque, 2018).

El concepto de seguridad ciudadana contiene a la violencia, pero no se agota en ella. Esto plantea diferencias con el concepto de seguridad nacional o pública, centrado en la acción del Estado; mientras que la seguridad ciudadana busca promover los derechos y responsabilidades de la población, dentro del campo público y privado, lo que conlleva la necesidad de un Estado Social de Derecho que garantice la efectividad plena de la libertad.

La violencia es un fenómeno complejo de carácter multicausal y plural. Es multicausal porque es producida por una variedad de factores y con la participación de diversos actores, y es plural porque no existe una única violencia, sino múltiples violencias; por la

multicausalidad del fenómeno se debe definir un marco de aproximación que considere los factores estructurales (por ejemplo: desigualdad, ingobernabilidad), institucionales (impunidad, ineficiencia), y situacionales (porte de armas, consumo de alcohol); por su característica plural, cada tipo de violencia requiere ser tratada con una estrategia particular. Desde la perspectiva de la seguridad ciudadana, se reconoce que existen múltiples violencias (políticas, económicas y sociales) y distintas fases de violencia (percepción, prevención, control), y que ambas son el resultado de relaciones sociales específicas. Pero no solo que hay distintos tipos de violencia, sino que éstos se expresan de forma diferenciada, según el lugar, el momento, la sociedad y la cultura.

El tratamiento de la violencia también requiere de un enfoque de externalidad, debido a los impactos económicos que ella produce en el conjunto de la sociedad: producción, presupuesto, salud, turismo, banca, comercio, etc. (Armijos & Pontón, 2019).

El estudio realizado por FLACSO – Sede Ecuador, se orienta principalmente a analizar el tema de la violencia social o común, la cual está referida a las relaciones sociales e interpersonales de convivencia y cotidianidad, en las que tanto los agresores como los agredidos no siempre tienen una actitud encaminada hacia la violencia. Se caracteriza por ser difusa y ubicua, y comprende desde aquellos casos que se relacionan con problemas biológicos y psicológicos a los que surgen de ciertas interacciones entre personas, y de éstas con sus ambientes concretos.

2.7. Sistema de Automatización.

Se define un sistema (máquina o proceso) automatizado capaz de reaccionar automáticamente (sin intervenir el operario) ante los cambios que se producen en él, realizando las acciones adecuadas para cumplir la función para la que se diseñó.

Es un sistema en bucle cerrado, donde se procesa la información sobre los cambios del proceso captada por los sensores, dando lugar a las acciones necesarias, implementadas físicamente sobre el proceso mediante los actuadores. Este sistema de control se comunica con el operador, recibe consignas de funcionamiento, como marcha, paro, cambio de características de producción, etc. y comunicando información sobre el estado del proceso (para la supervisión del correcto funcionamiento). Se denomina automatismo al sistema completo, aunque con este término se refiere al sistema de control, ya que produce

automáticamente las acciones sobre el proceso a partir de la información captada por los sensores. Las señales de entrada y de salida pueden ser de cualquier tipo; sin embargo, el concepto tradicional de automatismo se utiliza para sistemas de eventos discretos (también llamados sistemas secuenciales) en los que esas señales son binarias, es decir, solo pueden tomar 2 valores, activa o inactiva (estos valores suelen representarse como un 1 ´o un 0). En ese caso el sistema de control implementa el algoritmo de lógica binaria que relaciona los valores que van tomando en cada instante las entradas (1 ´o 0) con los valores que deben ir tomando en cada instante las salidas (también 1 o 0) para que el sistema funcione adecuadamente.

2.7.1. Clasificación Tecnológica.

En función de la tecnología empleada para la implementación del sistema de control, se puede distinguir entre automatismos cableados y automatismos programados. Automatismos cableados. Se implementan por medio de uniones físicas entre los elementos que forman el sistema de control (por ejemplo, contactores y relés unidos entre sí por cables eléctricos). La estructura de conexionado entre los distintos elementos da lugar a la función lógica que determina las señales de salida en función de las señales de entrada. Se pueden distinguir tres tecnologías diferentes: Fluídica (neumática o hidráulica). Eléctrica (relés o contactores). Electrónica estática (puertas lógicas y biestables). Los inconvenientes fundamentales de los automatismos cableados son: Ocupan mucho espacio. Son muy poco flexibles. La modificación o ampliación es difícil. Solo permiten funciones lógicas simples. No sirven para implementar funciones de control o de comunicación complejas. Las ventajas de los automatismos cableados son: Pueden ser muy robustos. Bajo coste para sistemas muy sencillos. Es una tecnología muy fácil de entender por cualquier operario. En general se puede afirmar que los automatismos cableados solo tienen utilidad para resolver problemas muy sencillos (por ejemplo, un arranque estrella triángulo de un motor de inducción). (Herrera, 2023).

Automatismos programados. Se implementan mediante un programa ejecutado en un microprocesador. Las instrucciones de este programa determinan la función lógica que relaciona las entradas y las salidas. Se pueden distinguir 3 formas de implementación: Autómata programable industrial. Hoy por hoy es el que más se utiliza en la industria. Es un equipo electrónico programable en un lenguaje específico, diseñado para controlar en tiempo real y en ambiente de tipo industrial procesos secuenciales. Se utilizan para el

control de máquinas y procesos. Ordenador (PC industrial). Cada vez se utilizan más. Son ordenadores compatibles con los PC de sobremesa en cuanto a software, pero cuyo hardware está especialmente diseñado para ser robusto en entornos industriales. Microcontrolador. Son circuitos integrados (“chips”) programables, que incluyen en su interior un microprocesador y la memoria y los periféricos necesarios. Para utilizarlos, normalmente se diseña una tarjeta electrónica específica para la aplicación, que incluye el propio microcontrolador y los circuitos electrónicos de interfaz necesarios para poder conectarse a los sensores y actuadores.

Se utilizan sobre todo para sistemas de control de máquinas de las que se van a fabricar muchas unidades, de forma que la reducción de coste por el número de unidades fabricadas justifica la mayor dificultad (y mayor coste) del diseño.

Las ventajas más importantes de los automatismos programados son:

- Permiten una gran flexibilidad para realizar modificaciones o ampliaciones.
- Permiten implementar funciones de control y de comunicación complejas.
- Ocupan poco espacio.

Los inconvenientes respecto de los sistemas cableados son fundamentalmente el mayor coste (solo si el sistema es muy sencillo), la menor robustez y la mayor complejidad de la tecnología. Sin embargo, estos inconvenientes cada vez lo son menos, pues el coste se reduce continuamente, cada vez se diseñan equipos más robustos, y los sistemas de programación son cada vez más sencillos. En resumen, se puede afirmar que la tecnología programada (y en especial los autómatas programables) es superior a la tecnología cableada, salvo en automatismos que sean extremadamente simples. (Miyashiro, 2017).

La naturaleza física de las señales de entrada y salida depende de la tecnología del automatismo. Por ejemplo, un automatismo puramente neumático tiene como entradas señales de presión de aire, y dan como salida señales de presión de aire. Lo más habitual en la industria son los automatismos de naturaleza eléctrica (cableados o programados). En este caso las señales de entrada y de salida son señales eléctricas. Los sensores se encargarán de convertir las magnitudes físicas en señales eléctricas, mientras los actuadores transforman las señales eléctricas en acciones físicas sobre el proceso.

2.7.2. Seguridad en los Automatismos.

Un aspecto importante en la implementación de automatismos es la seguridad. Esta se debe tener en cuenta de dos formas. Por una parte, se debe definir la secuencia de operaciones del proceso para garantizar siempre la seguridad de los operarios. Por ejemplo, una prensa en la que el operario introduce una chapa para después darle al pulsador de marcha. La secuencia del automatismo debería permitir la puesta en marcha de la prensa solo cuando el operario pulsa de forma simultánea dos pulsadores separados. De esta forma se garantiza que las dos manos quedan fuera de la prensa cuando ésta actúa. Tener en cuenta la seguridad en la secuencia del automatismo no es; sin embargo, suficiente, ya que si por alguna razón falla el sistema de control pueden producirse situaciones de peligro. (Palomeque, 2018).

Según el nivel de riesgo puede requerirse utilizar en la implementación una tecnología adecuada que garantice la seguridad. Por ejemplo, si el automatismo se implementa mediante un autómata programable y se quiere garantizar que la apertura de una puerta produzca la parada instantánea de la máquina, no basta con definir la secuencia para que así sea, sino que hay que utilizar un interruptor y un relé de seguridad que corte la alimentación de la máquina independientemente del autómata programable que la controla. La tecnología utilizada en la implementación del automatismo deberá considerar la seguridad, pudiendo requerirse elementos especiales para realizar alguna de sus funciones.

2.8. Tecnologías Digitales.

Desde fines de los años ochenta, la revolución digital ha transformado la economía y la sociedad. Primeramente, se desarrolló una economía conectada, caracterizada por la masificación del uso de Internet y por el despliegue de redes de banda ancha. Luego, se desarrolló una economía digital resultado de la expansión del uso de plataformas digitales como modelos de negocios de oferta de bienes y servicios. Y ahora se avanza hacia una economía digitalizada que basa sus modelos de producción y consumo en la incorporación de tecnologías digitales en todas las dimensiones económicas, sociales y medioambientales. (CEPAL, 2018).

Como resultado de la adopción y de la integración de tecnologías digitales avanzadas (redes móviles de quinta generación (5G), Internet de las cosas (IoT), computación en la

nube, inteligencia artificial, analítica de grandes datos, robótica, entre otros), se está pasando de un mundo hiperconectado a un mundo digitalizado en las dimensiones económicas y sociales. En ese mundo conviven y se fusionan la economía tradicional - con sus sistemas organizativos, productivos y de gobernanza - con la economía digital - con sus innovaciones en los modelos de negocios, la producción, la organización empresarial y la gobernanza. Esto da lugar a un nuevo sistema digitalmente entrelazado en el que se integran e interactúan modelos de ambos mundos, dando lugar a ecosistemas complejos que están en proceso de adecuación organizativa, institucional y normativa. Estas dimensiones del desarrollo digital están en permanente evolución, en un proceso sinérgico que tiene efectos en las actividades a nivel de la sociedad, del aparato productivo y del estado.

Esto hace que el proceso de transformación digital sea altamente dinámico y complejo y, por ende, es un desafío para las políticas públicas ya que demanda una adecuación permanentemente y un enfoque sistémico del desarrollo nacional. En ese marco, las redes 5G viabilizarán la convergencia de las telecomunicaciones y las tecnologías de la información, cambiando la estructura y la dinámica del sector, al tiempo que la adopción de tecnologías digitales y de inteligencia artificial –en tanto tecnologías de propósito general– marca una nueva etapa, la de la economía digitalizada.

A nivel de la sociedad, la disrupción digital genera cambios en los modelos de comunicación, interacción y consumo que se reflejan en una mayor demanda de dispositivos, software con más funcionalidades, servicios de computación en la nube y de tráfico de datos, así como de habilidades digitales básicas para la utilización de las tecnologías asociadas. A su vez, la economía digital representa para los consumidores la posibilidad de acceder a información y conocimientos de toda índole en diversos formatos, así como a bienes y servicios, y a formas de consumo no presenciales más ágiles. La evolución hacia la economía digitalizada permitiría satisfacer a los consumidores con productos inteligentes, en muchos casos asociados a servicios avanzados con un alto grado de personalización. Todo esto significa un aumento en el bienestar del consumidor, acompañado de una reconfiguración de las habilidades digitales necesarias para realizar un consumo digital más avanzado y enfrentar las nuevas demandas laborales resultado de los nuevos modelos de producción; por otro lado, las nuevas formas de consumo se asocian con beneficios potenciales derivados de la

reducción de la materialización y de decisiones medioambientales más sostenibles, en la medida que se basen en más y mejor información (por ejemplo, la relacionada con la huella ambiental de un producto) o recompensen prácticas más inocuas con el medioambiente. (Sejal, 2018).

El desarrollo de la economía digital ha llevado a un cambio radical de la propuesta de valor de los bienes y servicios, al reducir los costos de transacción e intermediación, y explotar la información proveniente de los datos que se generan e intercambian en las plataformas digitales. Estos modelos habilitados digitalmente propician la generación y la captura de datos que, al ser procesados y analizados con herramientas inteligentes, permiten mejorar los procesos de decisión y optimizar la oferta. Ello da lugar a una mayor agilidad en los procesos operativos, a la segmentación de mercados y a la personalización y la transformación de productos.

Los datos y el conocimiento digitalizado se convierten en un factor estratégico de producción (CEPAL, 2016). Todo ello conlleva la necesidad de realizar cambios normativos en una diversidad de materias, desde la regulación del sector de las telecomunicaciones hasta los ámbitos del comercio, pasando por políticas de competencia y de protección de datos y ciberseguridad.

2.9. Inteligencia Artificial ANI (IA Limitada).

Es un sistema que puede llevar a cabo tareas programadas, esto se debe a que tiene una combinación de memoria limitada; en la actualidad, la mayor parte de las aplicaciones de inteligencia artificial corresponden a esta categoría.

La IA limitada o ANI es una forma de inteligencia artificial que se enfoca en realizar tareas específicas de manera eficiente y precisa, a diferencia de la IA general (AGI) o de la superinteligencia artificial (ASI), que buscan imitar la capacidad cognitiva del ser humano en su totalidad, la ANI está diseñada para realizar tareas específicas en un campo de conocimiento limitado; es decir, la ANI utiliza algoritmos y técnicas de aprendizaje automático para analizar grandes cantidades de datos para tomar decisiones precisas y automatizadas.

2.9.1. Principales usos de la ANI.

En términos generales, se podría decir que la IA limitada es parte de nuestra vida diaria en muchos aspectos; a continuación, se mencionan algunos de los principales ejemplos de sus usos:

- *Los sistemas de imagen y de reconocimiento facial.* En la actualidad, gracias a estos mecanismos de inteligencia artificial limitada, las empresas como Google o Facebook son capaces de identificar de manera automática a las personas que aparecen en una fotografía.

- *Los chatbots y asistentes conversacionales.* Los asistentes virtuales son modelos de lenguaje creados con inteligencia artificial limitada; entre ellos, podemos mencionar a Google, Siri, Alexa y, al más reciente, ChatGPT., en esta categoría, también se incluyen los chatbots de servicio al cliente.

- *Los vehículos autónomos.* Otra de las aplicaciones de ANI más comunes, hoy en día, son los vehículos autónomos o semiautónomos; por ejemplo, algunos de los autos de Tesla, los drones o barcos.

- *Los modelos de mantenimiento predictivo.* Estos modelos recopilan datos de máquinas y; con base a ello, son capaces de predecir cuándo las mismas pueden fallar; de esta forma, los usuarios cuentan con la ventaja de recibir una alerta de manera anticipada.

- *Los motores de recomendación.* Esta tecnología de inteligencia artificial limitada está; además, preparada para poder predecir el contenido que un usuario puede buscar o por el cual puede tener alguna preferencia.

2.9.2. Beneficios de usar la IA limitada

Como ya se ha mencionado, los sistemas de inteligencia artificial limitada solo consiguen hacer aquellas tareas para las que han sido diseñados; sin embargo, también tienen la característica de aprendizaje automático o machine learning, ya que los desarrolladores construyen un primer modelo, al cual lo entrenan; posteriormente, el algoritmo tiene un proceso de aprendizaje, este se lleva a cabo mediante la predicción de resultados; en este

sentido, tiene la capacidad de analizar millones de datos; por ejemplo, un sistema de inteligencia artificial limitada desarrollado para diagnosticar el cáncer a partir de imágenes de rayos X o ultrasonido.

Este mecanismo tendrá mayor precisión que un radiólogo con grandes capacidades, esto se debe a la capacidad que posee esta tecnología para procesar imágenes de un modo mucho más rápido; para concluir, se puede decir que la inteligencia artificial limitada o ANI es una forma de inteligencia artificial que se enfoca en realizar tareas específicas de manera precisa y eficiente con capacidad cognitiva limitada, se utiliza ampliamente en diferentes sectores para automatizar los procesos y mejorar la eficiencia en la toma de decisiones.

2.10. Software.

Un lenguaje de programación es un conjunto de reglas gramaticales tanto sintácticas como semánticas que instruyen a que un ordenador o dispositivo se comporte de una cierta manera; cada lenguaje de programación tiene un vocabulario, un conjunto único de palabras clave que sigue a una sintaxis especial para formar y organizar instrucciones del computador. Para el desarrollo del presente proyecto se utilizarán lenguajes para reconocimiento facial como son: OpenCV para reconocimiento facial, Visual Studio como lenguaje frontal y SQL Server para base de datos.

2.10.1. Open CV.

Es un software que está orientado al desarrollo de aplicaciones de reconocimiento de imágenes, estos software actualmente son conocidos herramientas para el desarrollo de visión artificial, lo cual es de gran importancia ya que permite reconocer los rasgos fisiológicos que presenta una persona y así generar aplicaciones que administren y diferencien los diferentes estados de ánimo de una persona mediante un escaneo o relieve en 3D; esta librería ofrece varios algoritmos que son capaces de reconocer rasgos de personas, animales, cosas y hasta paisajes con el fin de orientarlos a la realidad aumentada (OpenCV, 2019).

2.10.2. Visual Studio.

Microsoft Visual Studio es un entorno de desarrollo integrado para sistemas operativos Windows, soporta múltiples lenguajes de programación, tales como C++, C#, Visual

Basic .NET, F#, Java, Python, Ruby y PHP, al igual que entornos de desarrollo web, como ASP.NET MVC, Django, etc., a lo cual hay que sumarle las nuevas capacidades online bajo Windows Azure en forma del editor Mónaco. (Roblesdo, 2012).

Visual Studio permite a los desarrolladores crear sitios y aplicaciones web, así como servicios web en cualquier entorno que soporte la plataforma .NET; así, se pueden crear aplicaciones que se comuniquen entre estaciones de trabajo, páginas web, dispositivos móviles, dispositivos embebidos y consolas, entre otros.

2.11. Metodología de Cascada para desarrollo de Software.

Para la presentación del proyecto, se aplicó como metodología el modelo de Cascada para desarrollo de software, el mismo que tiene las siguientes etapas:

- **Análisis:** Se analizan las necesidades propias del sistema. También se analizan las decisiones estructuradas por realizar, que son decisiones donde las condiciones, condiciones alternativas, acciones y reglas de acción podrán determinarse.

- **Diseño:** Se usa la información recolectada con anterioridad y se elabora el diseño lógico de sistemas de información, esta etapa también incluye el diseño de los archivos o la base de datos que almacenará aquellos datos requeridos por quien toma las decisiones en la organización.

- **Implementación:** Dentro de las técnicas estructuradas para el diseño y documentación del software se tienen: el método HIPO, los diagramas de flujo, los diagramas Nassi-Schneiderman, los diagramas Warnier-Orr y el pseudocódigo es aquí donde se transmite al programador los requerimientos de programación.

- **Verificación:** Todo sistema de información debe probarse antes de ser utilizado, ya que el costo es menor si se detectan los problemas antes de que entre en funcionamiento.

- **Validación:** Esta es la última etapa del desarrollo del sistema, esto incluye el adiestramiento que el usuario requerirá. Uno de los criterios fundamentales que debe satisfacerse, es que el futuro usuario utilice el sistema desarrollado. (Arsitega, 2021).

2.12. Marco Legal.

En Ecuador el artículo 66, numeral 19 de la Constitución de la República, establece que el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

Al amparo de esta norma, la Dirección Nacional de Registros Públicos (Dinarp) trabajó en la propuesta del proyecto de Ley de Protección de Datos Personales, ya que una Ley de Protección de Datos Personales es necesaria en un mundo hiperconectado, pues habilita la confianza digital.

Con la Ley de Protección de Datos Personales, se busca cuidar a las personas titulares de los datos, para que ellas puedan decidir a quién entregar su información personal porque confían en los proveedores de servicios digitales. (Dirección de Comunicación Social, 2022)

Dentro del marco legal se hace referencia a que la información sobre el procesamiento de datos personales de los ecuatorianos se consideran de carácter reservado desde la creación del ECU911, por lo que el sistema únicamente registrará y reconocerá a las personas que bajo su propio permiso acepten registrar sus datos; la videovigilancia y el reconocimiento facial se consideran justificados únicamente para reducir la criminalidad, entonces el sistema sólo se encarga de registrar la presencia de las personas sin resaltar ninguna alarma; Las personas que administran la información del sistema no tendrán acceso a la información codificada del rostro ni su algoritmo ya que la constitución del Ecuador prohíbe el tratamiento de datos sensibles, por lo que ellos no conocerán que persona ingresó ya que el sistema se encarga únicamente de registrar asistencia.

CAPITULO III – MARCO METODOLÓGICO

3.1. Descripción del área de estudio / Descripción del grupo de estudio.

La investigación se realizará en la ciudad de Tulcán en la Organización ADRA, que trabaja en ayuda humanitaria con personas de escasos recursos económicos, por lo que se requiere el control automático de asistencia de los usuarios aplicando cámaras de video con un sistema de reconocimiento facial 3D usando Inteligencia Artificial.

3.2. Enfoque y tipo de investigación.

El enfoque de investigación que se utilizará para el desarrollo del presente proyecto es la aplicada ya que se desarrollará un modelo informático para el reconocimiento facial mediante inteligencia artificial.

3.3. Procedimiento de la investigación.

3.3.1. Investigación Bibliográfica.

Se utilizará para acceder a la información sobre el funcionamiento del sistema, por lo que hay que recabar información en libros, revistas, páginas de Internet y hacer un estudio particular de cada tema para complementarlos y obtener un conocimiento general.

3.3.2. Investigación Aplicada.

Se utilizará para la realización del sistema y su codificación conforme a las necesidades de la fundación, los estándares de construcción de software y la instalación de hardware

3.3.3. Modelo Mixto.

3.3.3.1. Modelo Cuantitativo.

Se lo utilizará para realizar la tabulación de la información obtenida en las entrevistas y encuestas aplicadas a los trabajadores y usuarios de la fundación ADRA de la ciudad de Tulcán.

3.3.3.2. Modelo Cualitativo.

Se lo utilizará para realizar el análisis de los resultados obtenidos luego de la tabulación de la información y así tener una idea clara de las necesidades de la fundación.

3.4. Consideraciones Bioéticas.

Art. 3. Definición. Son las directrices y reglas que orientan el comportamiento de os docentes, investigadores, estudiantes, autoridades y personal administrativo, en las interrelaciones que ocurren en el proceso de aprendizaje y de investigación.

Art. 4. Principios Éticos. Los principios éticos descritos en el Código Orgánico de la UTN son:

1. Compromiso Social, 2. Igualdad y Democracia, 3. Criticidad, 4. Pluralismo, 5. Integridad, 6. Búsqueda de conocimiento, 7. Culturalidad, 8. Humanismo, 9. Ecologismo, 10. Equidad, 11. Imparcialidad y autonomía.

Art. 5. Valores. Los valores descritos en el Código Orgánico de la UTN, son:

1. Honestidad, 2. Respeto, 3. Justicia, 4. Laboriosidad, 5. Creatividad, 6. Perseverancia, 7. Paz, 8. Tolerancia, 9. Libertad, 10. Lealtad, 11. Solidaridad, 12. Legalidad, 13. Beneficio Social, 14. Integridad, 15. Transparencia, 16. Responsabilidad. (UTN, 2013).

3.5. Unidades de Estudio.

3.5.1. Población.

La población o universo tomado en cuenta en esta investigación es de 21 personas quienes forman parte del personal Administrativo, de atención y control de la Organización ADRA de la ciudad de Tulcán.

El autor dice que es el conjunto de elementos que tenga características definitorias que se denomina población o universo, la población es la totalidad del fenómeno a estudiar, las unidades de población que presentan características comunes y es lo que se va a estudiar y dará origen a los datos de la investigación. (Díaz, 2018).

3.5.2. Muestra.

La población presenta sus respectivos cargos y obligaciones en la Organización ADRA de Tulcán, por lo que se realizará una muestra apegada a la cientificidad investigativa con la formula estadística.

Dónde:

$$n = \frac{Z^2 * P * Q * N}{e^2(N-1) + Z^2 * P * Q}$$

Z: coeficiente de confianza, se trabaja con el 95% para lo cual de Z=1,96.

P: población (%) que tiene características de interés para el estudio.

Q: población (%) que no tiene características de interés para el estudio.

Q = 1 - P

Máxima variabilidad estadística P=Q=50%.

E: error para trabajo (<=5%).

N: población.

$$n = \frac{Z^2 * P * Q * N}{e^2 * (N-1) + Z^2 * P * Q}$$

$$n = \frac{1{,}96^2 * 0{,}5 * 0{,}5 * 21}{0{,}05^2 * (21-1) + 1{,}96^2 * 0{,}5 * 0{,}5}$$

$$n = \frac{20.1684}{1.0104}$$

$$n = 20$$

La población es de 21 personas, y aplicando la fórmula con un error del 5% el resultado es de 20 personas.

3.5.3. Técnicas e instrumentos de recolección de datos.

Para la recopilación de datos se utilizará la encuesta o test.

3.5.4. Técnica de Análisis de Datos.

La validación de confiabilidad de la presente investigación se la realizó mediante el juicio de expertos en el tema, de esta forma se demuestra si las herramientas empleadas son confiables, las pruebas de Wilcoxon se encargan de verificar el promedio de dos muestras y comprobar sus diferencias por tanto, la prueba Wilcoxon es otra elección (Quispe, 2019), se debe decir que la investigación está basada de forma cuantitativa, se debe aplicar las pruebas para brindar validez a la hipótesis, finalmente se debe proponer las recomendaciones que se demuestran mediante tablas, gráficas y cuadros. (Rendón, 2016).

3.5.5. Operacionalización de Variables.

El autor (Ñaupas, 2014), establece a los elementos de la hipótesis como variables y se clasifican en dependiente e independiente, el autor (Arias & Covinos, 2021), dice que la variable independiente administra datos para cambiar la variable dependiente, la variable dependiente es la causa que se ocasiona al interponerse la variable independiente. En la investigación se precisa que las variables son correlacionales; es necesaria la operacionalización para medir y verificar la variación entre ellas; el autor (Ríos, 2017), dice operar variables consiente en identificarlas de forma comprensible y admite definir contenidos conceptuales e indicadores, el autor (Hernández, 2014) establece que la operacionalización de variables son actividades para medir la información que debe ejecutar el investigador, el autor (Miyashiro, 2017) dice que se debe reconocer el problema para agilizar los procesos, también lo sustenta (Imai, 1989) y dice que la metodología permite mejorar proporcionalmente para obtener mejoras que permitan a la empresa realizar sus inversiones.

3.6. Análisis de los resultados.

La encuesta presenta como objetivo verificar el estado actual de la Organización ADRA en cuestión de seguridad y control y permitir el desarrollo e implementación de un sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios; el análisis e interpretación de resultados están presentes en el Anexo 1.

CAPITULO IV – DISEÑO E IMPLEMENTACIÓN

4.1. Análisis.

En el presente capítulo se realizará el proceso de diseño del sistema de seguridad informático de reconocimiento facial 3D para evitar la suplantación de identidad en la Organización ADRA el cual se inicia mediante un análisis de los procesos que realiza actualmente la empresa para el registro de las personas, posteriormente se debe crear la base de datos estructurada la cual debe estar acorde con los requerimientos de la empresa y finalmente se debe crear el sistema de reconocimiento facial el cual permite registrar a las personas beneficiarias y permite la emisión de alarmas en caso de detectar anomalías para finalmente imprimir los reportes para verificar finalmente los resultados del funcionamiento del sistema.

4.1.1. Análisis de la situación actual de la empresa.

La organización ADRA de la ciudad de Tulcán tiene como objetivo mejorar el estado de vida de las personas migrantes dentro de la ciudad de Tulcán; es decir, se encarga directamente de la movilidad de las persona que pasan por la ciudad para permitirles una estancia más cómoda y adecuada; para lo cual ubica en ciertos sectores de la ciudad carpas o pide prestado casas comunales para brindar ayudas a las personas en estado vulnerable de tal forma que se registra a las personas que asistirán en una hoja de Excel y posteriormente el día en el que se brindan las ayudas se hace que las personas se registren en hojas normales para posteriormente comparar con los datos de las personas previamente registradas.

El problema principal de la organización ADRA radica en que al no tener un control general de las personas que entran y salen de los lugares de ayuda, varias personas que no pertenecen al grupo vulnerable ingresan y reciben las ayudas, incluso ciertas personas se benefician dos o tres veces, por lo que personas que se registraron previamente no alcanzan a recibir nada provocando malestar y generando ciertos problemas entre las personas.

4.1.2. Caracterización de la propuesta.

La suplantación de identidad es una forma de engaño que se ha venido realizando desde el tiempo pasado con el fin de duplicar a ciertas personas o cometer cierto tipo de delito;

en el Ecuador se han realizado varias de estas estafas ya que antiguamente la falta de dispositivos informáticos hacía muy complicado la verificación real de las personas por lo que se podía suplantar fácilmente una identidad; pero posteriormente con el desarrollo de la tecnología y el avance en la informática, hace muy fácil la detección de una persona ya sea por su huella dactilar, iris del ojo o el reconocimiento facial.

En Tulcán y con el problema migratorio varias instituciones y fundaciones se han dedicado a atender las necesidades de las personas extranjeras que ingresan al país y que son de bajos recursos económicos, por lo que en la entrega de productos o alimentos, las personas tratan de suplantar la identidad de otras personas para recibir doble o triple ingreso de suministros; por eso, al entregar ayudas para las personas vulnerables, algunas familias salen muy favorecidas y otras quedan sin víveres para su manutención, es necesario combatir este problema social aplicando la tecnología de reconocimiento facial.

4.1.3. Requerimientos.

Se detalla las características identificadas que servirán de base para desarrollar el sistema de seguridad informático de reconocimiento facial 3D para evitar la suplantación de identidad en la Organización ADRA; estas características descritas en detalle para asegurar que el proyecto cumpla con los objetivos planteados, luego se hace una revisión detallada de las necesidades identificadas, las especificaciones se toman como referencia de acuerdo con la norma ISO/IEC/IEEE 29148, sus nomenclatura son:

- StRS: Especificación de requerimientos de las partes interesadas (Stakeholders).
- SyRP: Especificación de requerimientos de la plataforma.
- SyRA: Especificación de requerimientos de arquitectura.

4.1.3.1. Parte interesada o Stakeholders.

Las partes interesadas son individuos u organizaciones que tienen interés en la creación de un sistema, este interés puede ser de naturaleza económica, social, ambiental o incluso política; las partes interesadas pueden verse afectadas por el sistema o pueden tener la capacidad de influir en su funcionamiento (ISO/IEC/IEEE 15288, 2023); a continuación, en la tabla 2 se detallan las partes interesadas.

Tabla 2.

Definición de las partes interesadas.

Nro.	Stakeholders	Descripción
StRS1	ADRA	Gerente
StRS2	ADRA	Técnico TICS
StRS3	Fabián Cuzme	Tutor trabajo de grado
StRS4	Jefferson Cárdenas	Autor trabajo de grado

Nota. Esta tabla muestra a las personas involucradas en el desarrollo del sistema.

4.1.3.2. Requerimientos de la Plataforma.

En esta sección se describe los requisitos del sistema, se basan en las necesidades y expectativas de las partes interesadas identificadas en la entrevista realizada en la organización; a continuación, en la tabla 3 se detallan los requerimientos.

Tabla 3.

Requerimientos del sistema.

Nro.	Requerimientos	Prioridad		
		Alta	Media	Baja
SyRP1	El sistema debe tener conexión a Internet.			X
SyRP2	El sistema debe tener acceso a la base de datos.	X		
SyRP3	El diseño de la plataforma debe ser claro, conciso y fácil de entender.	X		
SyRP4	La interfaz debe proporcionar todas las funciones necesarias para el reconocimiento facial.			
SyRP5	La plataforma debe ser eficiente en términos de recursos y tiempo.	X		
		X		

Nota. Esta tabla muestra los requisitos para el buen funcionamiento del sistema.

4.1.3.3. Requerimientos de Arquitectura.

En esta parte del documento, se expondrán los requisitos en términos de infraestructura necesaria para cumplir con los objetivos del proyecto; a continuación, se describen de manera general los componentes clave que conforman la Plataforma de Gestión de Servicios Técnicos para el acceso de usuarios finales a la red en la organización ADRA.

Se debe tener en cuenta los elementos para el desarrollo como son:

Cámara de video vigilancia: La cámara debe ser de alta resolución 4K para que permita apreciar todos los rasgos físicos de cada persona y posteriormente permita comparar los rostros registrados en la base de datos con la información del video captado por la cámara en tiempo real.

Lenguaje de Programación: Los lenguajes de programación desempeñan un papel crucial en el desarrollo y la integración de las API (Interfaces de Programación de Aplicaciones), siendo fundamentales para establecer comunicaciones eficientes entre distintos sistemas.

Base de Datos: Es indispensable disponer de una base de datos robusta y confiable, que servirá como el repositorio centralizado para registrar y almacenar información de los rostros de las personas, en la tabla 4 se detallan los requerimientos de Arquitectura.

Tabla 4.

Criterios de diseño arquitectónico.

Nro.	Requerimientos	Prioridad		
		Alta	**Media**	**Baja**
SyRA1	La plataforma debe desarrollarse utilizando un lenguaje de programación con rendimiento alto.	X		
SyRA2	El lenguaje de programación debe ser escalable.	X		
SyRA3	El lenguaje de programación de la plataforma debe tener disponibilidad de Bibliotecas y Frameworks.	X		

SyRA4	El framework debe tener un rendimiento alto para aplicaciones grandes.	X
SyRA5	El lenguaje de programación elegido requiere que el IDE una interfaz compleja de navegar. El lenguaje de programación prefiere un IDE de código abierto, que ofrezca flexibilidad, personalización.	X
SyRA6	El IDE del lenguaje de programación requiere de una comunidad de soporte fuerte.	X
SyRA7	La base de datos debe poseer una escalabilidad adecuada, permitiendo así manejar el crecimiento esperado de la aplicación de manera eficaz y sin requerir recursos excesivos.	X
SyRA8	La base de datos debe ofrecer un nivel de seguridad aceptable, equilibrando protección de datos y facilidad de gestión.	X

Nota. Esta tabla muestra los criterios del diseño arquitectónico del sistema.

4.1.3.4. Elección del lenguaje de programación para la Plataforma.

Tabla 5.

Elección del lenguaje de programación.

Lenguaje de programación	Visual Basic	Phyton
SyRA1	X	X
SyRA2	X	X
SyRA3	X	-

Nota. El lenguaje de programación seleccionado es Visual Basic ya que cumple con todos los requerimientos que el sistema exige.

De los sistemas analizados anteriormente en la tabla 5 y por el uso de varios sistemas externos se seleccionó Visual Basic que es perfectamente compatible con todos los sistemas que se utilizarán para el funcionamiento del sistema y trabaja perfectamente bajo el sistema operativo Windows 11 Home Edition.

4.1.3.5. Elección del Framework.

En la tabla 6 se realiza el análisis y selección del Framework con el que trabajará la plataforma.

Tabla 6.

Elección del Framework.

Framework	.NET Framework	Django
SyRA4	X	-

Nota. El Framework seleccionado es .NET Framework ya que es compatible con Visual Basic que es el lenguaje de programación seleccionado.

4.1.3.6. Elección del entorno de desarrollo.

En la tabla 7 se realiza el análisis y selección del entorno de desarrollo del sistema.

Tabla 7.

Elección del IDE para Visual Basic.

Framework	Visual Studio Code
SyRA5	X
SyRA6	X

Nota. El IDE seleccionado es Visual Studio Code ya que es compatible con Visual Basic.

4.1.3.7. Elección de la Base de Datos.

Para la elección de la base de datos se ha tomado en cuenta las diferentes características de las bases de datos SQL Server y MySQL, las cuales se detallan en la tabla 8 que está continuación.

Tabla 8.

Elección de la base de datos.

Bade de Datos	SQL Server	MySql
SyRA7	X	X
SyRA8	X	-

Nota. La Base de Datos seleccionada es SQL Server ya que es segura, estable y perfectamente compatible con Visual Studio.

Los dos sistemas de base de datos son similares y presentas excelentes características, por el uso del sistema operativo Windows 11 y por una mayor facilidad de uso se seleccionó SQL Server.

4.1.3.8. Elección del Sistema Operativo.

Para el desarrollo del sistema informático de reconocimiento facial se debe seleccionar un Sistema Operativo compatible con todos componentes analizados anteriormente; a continuación, en la tabla 9 se detalla la información.

Tabla 9.

Selección de sistema operativo.

Software	Características
Windows	11 Home Edition
Linux	Raspbian Raspberry Pi

Nota. Esta tabla muestra los Sistemas Operativos compatibles con el sistema.

Se seleccionó Windows 11 Home Edition ya que es una plataforma compatible con gran variedad de software de programación como es el software de reconocimiento facial en 3D, su multitarea está mejorada por lo que se puede trabajar con varios programas a la vez y no requiere de la aplicación de comandos.

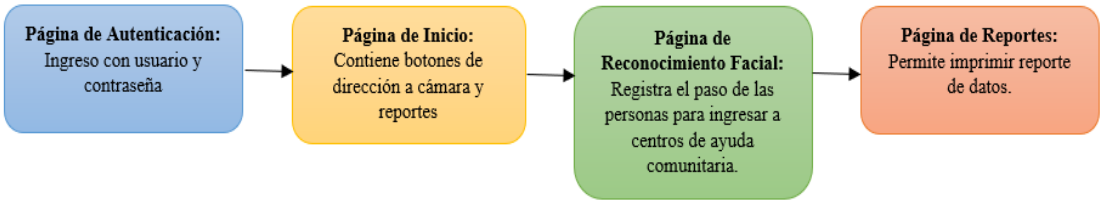
4.2. Diseño.

El sistema informático se realizó con la base de datos SQL Server 2014, que tiene 4 tablas donde se almacena la información referente al reconocimiento facial 3D aplicado al control y registro del personal y usuarios beneficiarios; tiene un frontal potente desarrollado en Visual Studio 2022 en el programa C++, permitiendo manejar fácilmente la información de la aplicación.

El sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador se diseñó considerando los componentes anteriormente definidos en la sección 3.1.3., en ese contexto en la figura 1, se puede observar la interacción del sistema con cada uno de los bloques que lo componen**; e**n el diagrama de bloques del sistema el primer bloque es el de ingreso mediante contraseña, el segundo bloque es la página principal, el tercer bloque es el de reconocimiento facial y el cuarto bloque son los reportes de información.

Figura 1.

Diagrama de bloques de los elementos visuales del sistema.



Nota. Diagrama de bloques que permite la interacción de todos los módulos del sistema.

4.2.1. Caracterización.

Para diseñar un sistema de seguridad informático de reconocimiento facial 3D con técnicas de inteligencia artificial que prevenga la suplantación de identidad en la Organización ADRA Ecuador, se realizó un estudio general sobre la problemática en el sector de ayudas económicas. El objetivo es automatizar la vigilancia de personal y beneficiarios mediante cámaras de alta definición capaces de reconocer rostros de manera masiva.

El sistema propuesto se alinea con el objetivo general de esta investigación: implementar un sistema de reconocimiento facial 3D que facilite el control y registro de personal y usuarios. Esto permitirá optimizar los procesos de administración y gestión, contribuyendo a prevenir suplantaciones. La propuesta cumple con los estándares técnicos adecuados, respaldando la idea defendida.

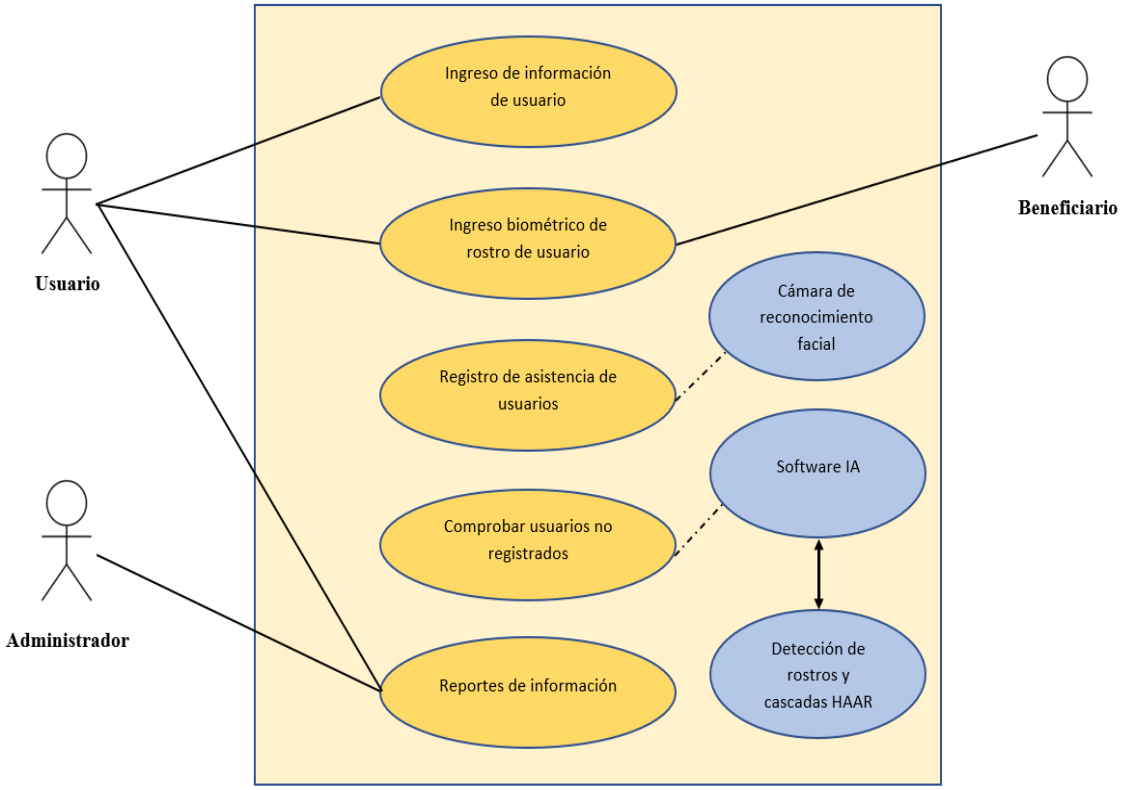
Las herramientas utilizadas en el desarrollo del sistema de seguridad son las siguientes:

- Para desarrollar la base de datos se utilizó Microsoft SQL Server 2014; con un potente motor de base de datos, da seguridad para administrar procesos y almacenar información con agilidad buscando registros y generación de reportes.
- Como plataforma de desarrollo se utilizó Visual Studio 2022 - lenguaje Visual C++, tiene una buena compatibilidad con SQL Server 2014 y es un lenguaje de programación orientado a objetos que es compatible con herramientas de Visión Artificial y reconocimiento facial en 3D.

En la figura 2 se muestra el diagrama de casos de uso donde se muestra la interacción de los usuarios y beneficiarios con el sistema y la aplicación de la Inteligencia Artificial ANI (Artificial Narrow Intelligence).

Figura 2.

Diagrama de casos de uso.



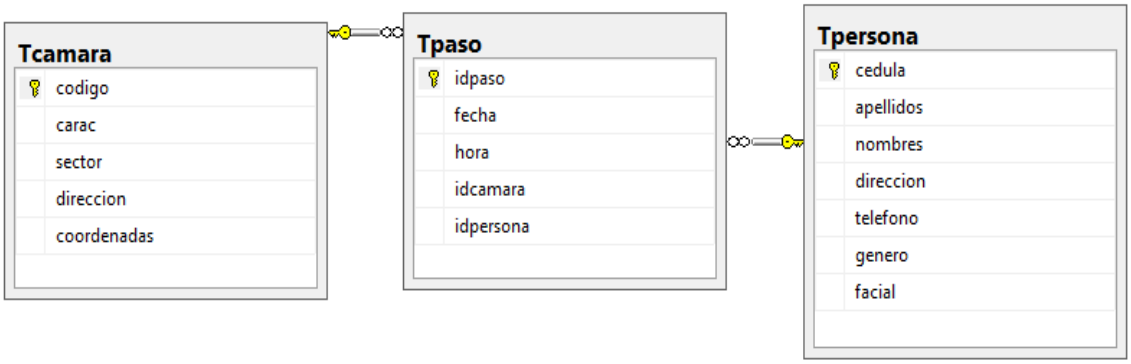
Nota. El registro de asistencia de usuarios depende directamente del código de reconocimiento facial y la suplantación de identidad o doble ingreso depende del módulo de Inteligencia Artificial.

4.2.2. Base De Datos (SQL Server).

En la realización del sistema informático con visión artificial para evitar la desaparición de personas en la ciudad de Tulcán, han sido necesarias 4 tablas; a continuación, en la figura 3 se detalla el modelo entidad relación.

Figura 3.

Diagrama Entidad Relación de la base de datos.



Nota. Diagrama entidad relación de la base de datos del sistema la cual consta de 3 tablas relacionadas.

Tabla Tcamara

Se guardan datos de las cámaras que se ubicarán en los diferentes sectores de atención a personas vulnerables en la ciudad de Tulcán, en la figura 4 se observan los detalles.

Figura 4.

Tabla de registro de cámaras de la base de datos.

Column Name	Data Type	Allow Nulls
codigo	nchar(20)	☐
carac	nchar(200)	☑
sector	nchar(100)	☑
direccion	nchar(100)	☑
coordenadas	nchar(60)	☑

Nota. Se muestran los campos de la tabla Tcamara en donde se registra la información de cada una de las cámaras que se utilizarán y el sector en donde se instalarán.

Diccionario De Datos

- **codigo** = *Almacena el código de la cámara*
  Valor = {Caracter}
  Carácter = [A-Z|a-z|0-9|’].
- **carac** = *Almacena las características de la cámara*
  Valor = {Caracter}
  Carácter = [A-Z|a-z|0-9|’]

- **sector** = *Almacena el sector de ubicación de la cámara*

  Valor = {Caracter}

  Carácter = [A-Z|a-z|’].
- **direccion** = *Almacena la dirección de la cámara*

  Valor = {Caracter}

  Carácter = [|A-Z|a-z|0-9|’].
- **coordenadas** = *Almacena las coordenadas geográficas de la cámara*

  Valor = {Caracter}

  Carácter = [|-,.|0-9|’].

Tabla Tpersona

Se guardan datos del registro de las personas beneficiarias de ayudas de la Organización ADRA, en la figura 5 se observan los detalles.

Figura 5.

Tabla de registro de personas de la base de datos.

Column Name	Data Type	Allow Nulls
cedula	nchar(15)	☐
apellidos	nchar(60)	☑
nombres	nchar(60)	☑
direccion	nchar(60)	☑
telefono	nchar(15)	☑
genero	nchar(10)	☑
facial	varbinary(MAX)	☑

Nota. Se muestran los campos de la tabla Tpersona en donde se registra la información de cada persona que asistirá a las campañas de ayuda comunitaria.

Diccionario de datos

- **cedula** = *Almacena el número de cédula de las personas*

  Valor = {Caracter}

  Carácter = [0-9].
- **apellidos** = *Almacena el apellido de las personas*

  Valor = {Caracter}

  Carácter = [A-Z|a-z]

- **nombres** = *Almacena el nombre de las personas*
  Valor = {Caracter}
  Carácter = [A-Z|a-z].
- **direccion** = *Almacena la dirección de las personas*
  Valor = {Caracter}
  Carácter = [A-Z|a-z |0-9].
- **telefono** = *Almacena el número de teléfono de las personas*
  Valor = {Caracter}
  Carácter = [0-9].
- **genero** = *Almacena el género de las personas*
  Valor = {Caracter}
  Carácter = [A-Z|a-z]
- **facial** = *Almacena la información facial de las personas*
  Valor = {Varbinary}
  Carácter = [0-1].

Tabla Tpaso

Se guardan datos acerca de las diferentes personas beneficiarias que asisten a recibir las ayudas que brinda la Organización ADRA, en la figura 6 se observan los detalles.

Figura 6.

Tabla de registro de paso de personas de la base de datos.

	Column Name	Data Type	Allow Nulls
▶🔑	idpaso	numeric(18, 0)	☐
	fecha	nchar(20)	☑
	hora	nchar(20)	☑
	idcamara	nchar(20)	☑
	idpersona	nchar(15)	☑

Nota. Se muestran los campos de la tabla Tpaso en donde se registra la información de la bitácora del paso de cada persona frente a la cámara para su registro en caso de existir más de un paso el sistema emitirá alarmas.

Diccionario de datos

- **idpaso** = *Almacena el código de paso de cada persona frente a una cámara*

Valor = {Numérico}

Carácter = [0-9].

- **fecha** = *Almacena la fecha de paso de cada persona frente a una cámara*

  Valor = {Caracter}

  Carácter = [/-|0-9]

- **hora** = *Almacena la hora de paso de cada persona frente a una cámara*

  Valor = {Caracter}

  Carácter = [:|0-9].

- **idcamara** = *Almacena el código de la cámara que capta a una persona*

  Valor = {Caracter}

  Carácter = [A-Z|a-z|0-9|].

- **idpersona** = *Almacena la cédula de la persona captada*

  Valor = {Caracter}

  Carácter = [|0-9|].

Tabla Tclave

Se guardan datos acerca de los usuarios que administran el sistema informático, en la figura 7 se observan los detalles.

Figura 7.

Tabla de registro de usuario y contraseña de la base de datos.

Nombre del campo	Tipo de datos
usuario	Texto corto
password	Texto corto
permisos	Texto corto

Nota. Se muestran los campos de la tabla Tclave en donde se registra la información del usuario, permisos y su respectiva contraseña para el ingreso al sistema.

Diccionario de datos

- **usuario** = *Almacena el nombre de usuario*

  Valor = {Caracter}

  Carácter = [A-Z|a-z|0-9].

- **password** =*Almacena la clave de usuario*

  Valor = {Caracter}

  Carácter = [A-Z|a-z|0-9]

- **permisos** = *Almacena los permisos de usuario*
  Valor = {Caracter}
  Carácter = [0-9|].

4.2.3. Formularios.

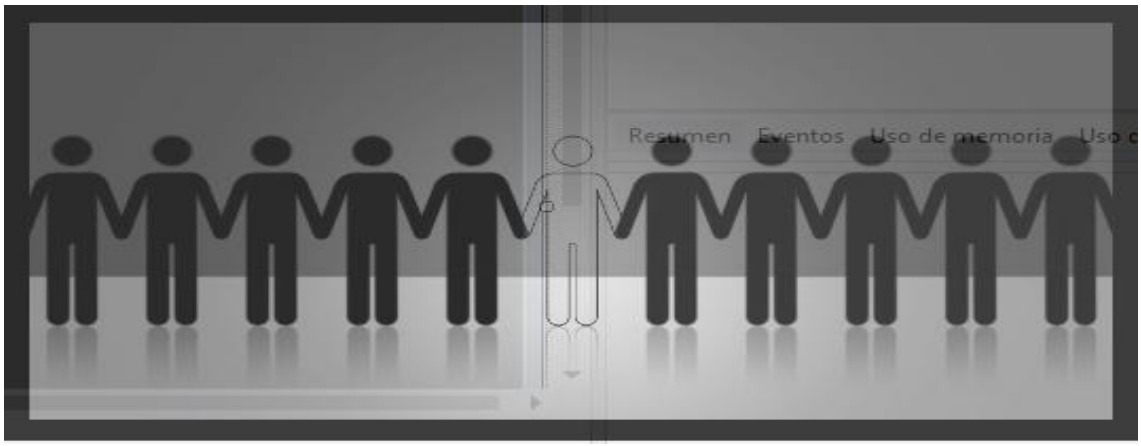
En total son ocho formularios, se detallan algunos de ellos a continuación:

Formulario de Bienvenida

Pantalla de bienvenida al sistema la cual se mantiene activa durante 3 segundos, en la figura 8 se observan los detalles.

Figura 8.

Formulario inicial del Sistema.



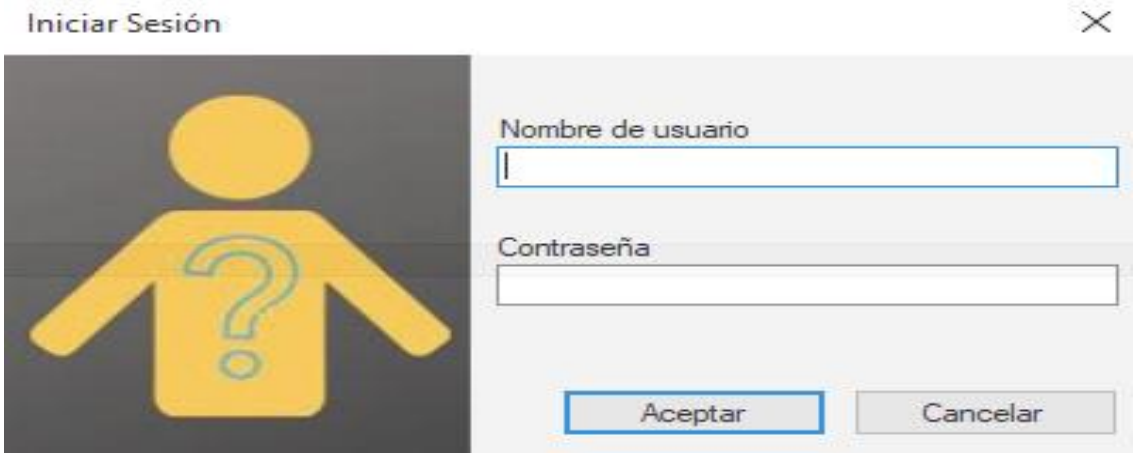
Nota. Se muestra el formulario de bienvenida al Sistema, este formulario permanece activo durante 3 segundos y luego da paso al formulario de usuario y contraseña.

Formulario de inicio de sesión.

Se debe ingresar nombre de usuario y contraseña para poder acceder al sistema, en la figura 9 se observan los detalles.

Figura 9.

Formulario de inicio de sesión.



Nota. Se muestra el formulario de inicio de sesión, este formulario permite ingresar el nombre de usuario y la contraseña de cada persona que administra el sistema.

Formulario Menú principal.

El formulario principal tiene un menú que llama y permite enlazar a todos los formularios del sistema, consta de: registrar, que desplaza a registro de cámaras y personas; Administrar que despliega a reconocimiento de personas; seguridad desplaza el formulario de usuarios y respaldo de la información que se guardará en el disco duro del equipo; y, por último, salir, en la figura 10 se observan los detalles.

Figura 10.

Formulario Menú Principal.

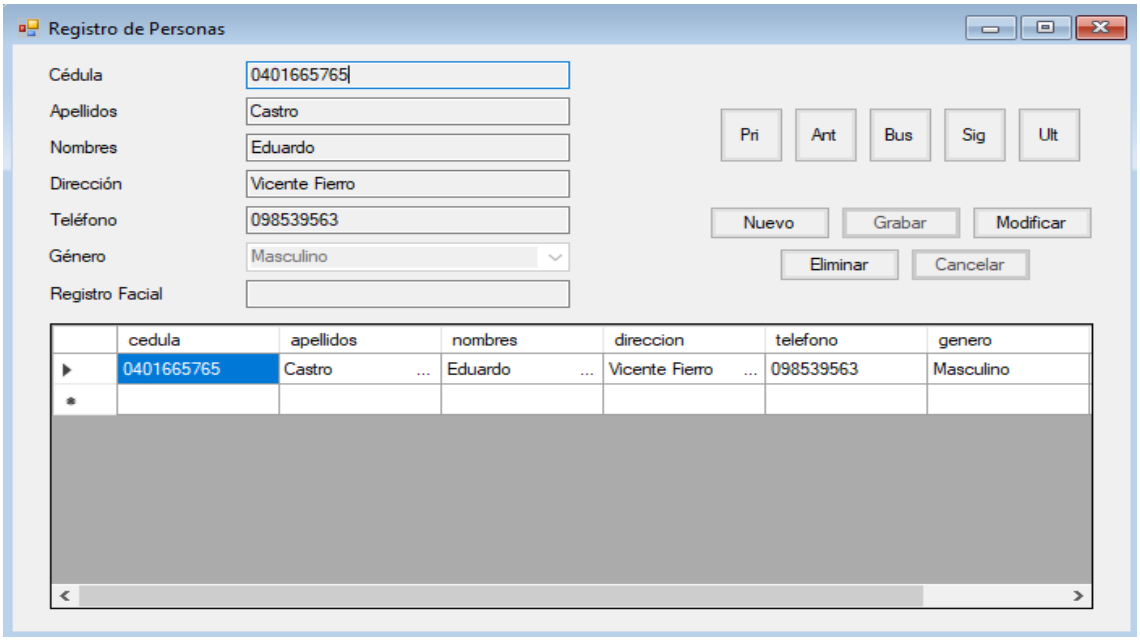
Nota. Se muestra el formulario menú principal, este formulario permite al usuario el acceso a todos los formularios del sistema.

Formulario Personas.

Permite el registro del personal beneficiario de la Organización ADRA y su respectivo código facial, mediante el cual las cámaras reconocerán a cada asistente al lugar de atención; el código facial es único para cada persona ya que reconoce los diferentes rasgos del rostro y los codifica para así obtener un algoritmo diferente, en la figura 11 se observan los detalles.

Figura 11.

Formulario Personas.



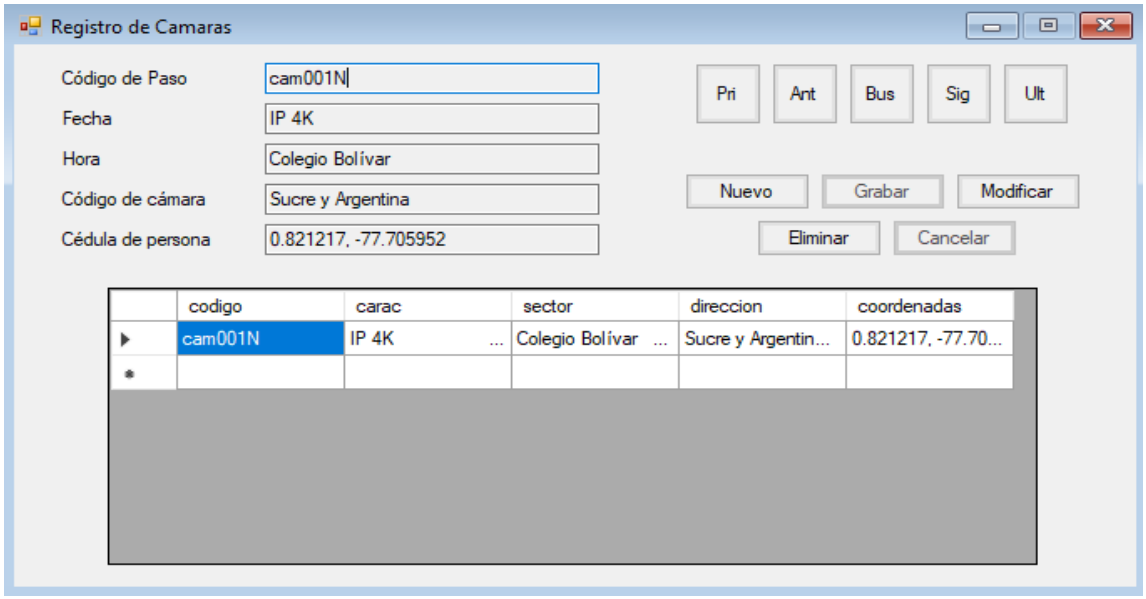
Nota. Se muestra el formulario personas, este formulario permite el ingreso de información de todas las personas beneficiarias de las ayudas comunitarias que realiza la Organización ADRA de la ciudad de Tulcán.

Formulario Cámaras.

Permite registrar los datos de las cámaras que se ubicarán en los diferentes sectores de atención de Tulcán, tiene los campos código, características, sector, dirección y coordenadas; además presenta los deferentes botones que manipulan la información, en la figura 12 se observan los detalles.

Figura 12.

Formulario Cámaras.



Nota. Se muestra el formulario cámaras, este formulario permite el ingreso de información de las cámaras y sus ubicaciones en las diferentes partes dónde se realizan las reuniones.

Formulario de administración de registro de personas.

Permite el registro de beneficiarios que ingresen a los lugares que son centros de atención a vulnerables, cada cámara debe estar conectada al sistema para guardar la información del reconocimiento de los asistentes en la base de datos y verificar en tiempo real que no existe suplantación de identidad, así se puede obtener un registro general de las personas que asistieron a cada evento y de las que quisieron realizar reemplazo, en la figura 13 se observan los detalles.

Figura 13.

Formulario paso y registro de personas.

Nota. Se muestra el formulario de registro de paso de personas, este formulario se encarga del reconocimiento facial y registro de la bitácora del paso de las personas ante la cámara.

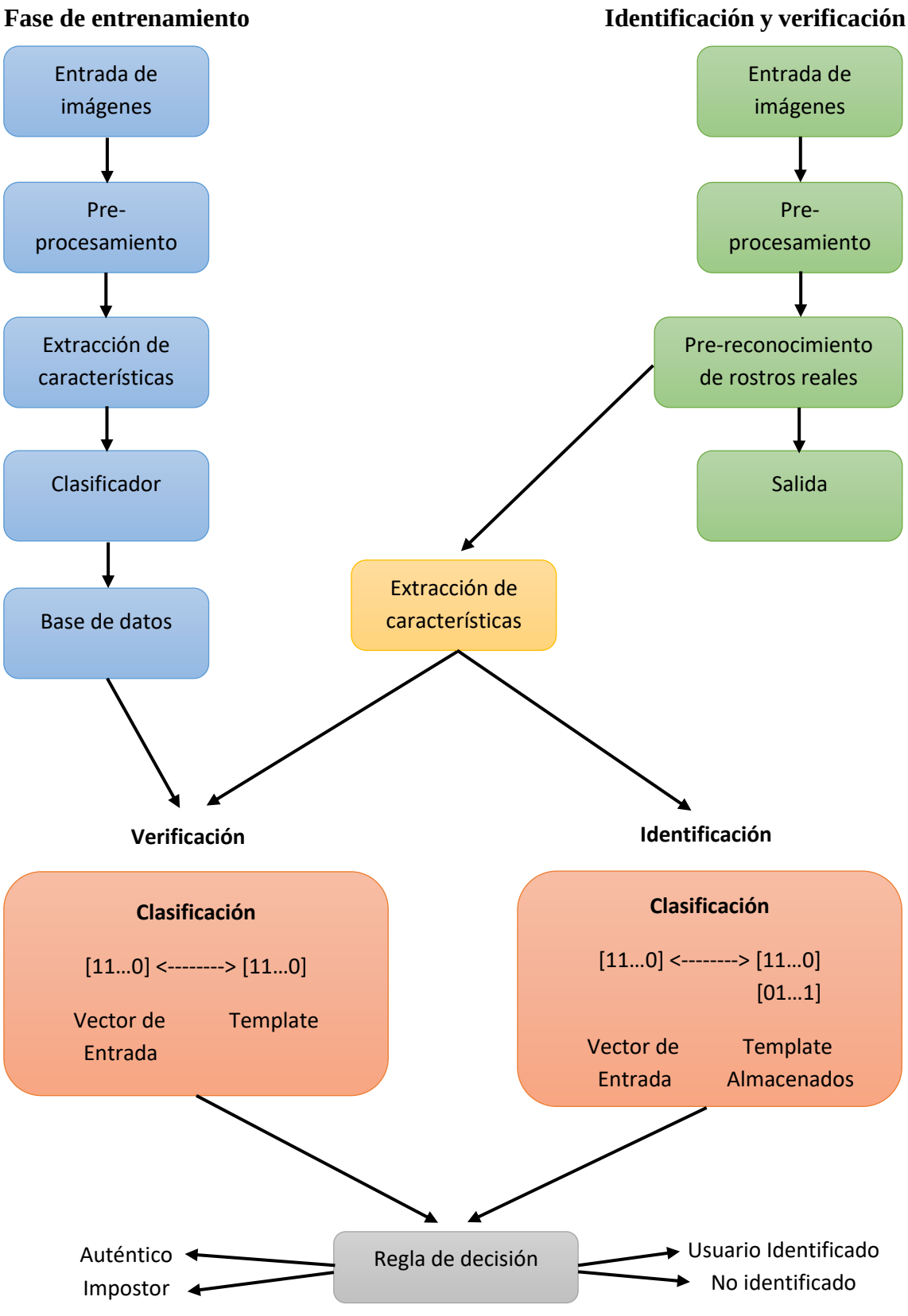
4.3. Módulo de Inteligencia Artificial.

El sistema cuenta con un módulo de Inteligencia Artificial el cual se encarga del reconocimiento de rasgos faciales de cada rostro para luego general un código único y posteriormente grabarlo en la base de datos; al tener en la base de datos generados todos los códigos de rostro de las personas en estado vulnerable, posteriormente en las diferentes brigadas de apoyo social el sistema puede reconocer a cada persona y se encarga de procesar la información para ayudar a verificar posibles personas no registradas, posible suplantación de identidad y doble presentación a recibir la ayuda comunitaria.

En la figura 14 se puede observar el gráfico en dónde se muestra el proceso de análisis de imágenes que contienen rostros y la utilización del respectivo clasificador encargado de comparar y buscar en la base de datos los diferentes rasgos que presenta cada persona para verificar si la persona está registrada en el sistema.

Figura 14.

Implementación del módulo de Inteligencia Artificial.



Nota. En el módulo de Inteligencia Artificial y su relación con el sistema se puede observar cómo al obtener la imagen se generan las características y rasgos del rostro y mediante un clasificador se genera un código el cual es procesado y enviado a la base de datos.

4.4. Implementación.

Para la implementación del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios se ha realizado lo siguiente.

4.4.1. Definición de variables.

Con la implementación del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios se han presentado las siguientes variables a analizar en la tabla 10.

Tabla 10.

Variables del sistema.

VARIABLE	DEFINICIÓN	ACTUADORES
Sistema de seguridad informático	Conjunto de programas que se encargan de ejecutar una acción mediante el desarrollo de procesos.	Computador, usuarios e Internet
Suplantación de identidad	Acción de hacerse pasar por otra persona durante un evento.	ECU, Policía
Reconocimiento facial 3D	Permite identificar personas mediante un código facial 3D generado por un algoritmo.	Técnicos

Nota. Esta tabla muestra las diferentes variables que presenta el sistema.

4.4.2. Proceso Manual.

Actualmente, en Tulcán no existe un control automático de personas que suplantan a terceros, el control que se presenta ahora es la verificación por firma o huella dactilar, lo que permite un control oportuno, pero el problema es que tarda en pasar a las personas

una a una y en las multitudes es imposible su control; por lo que estos métodos se usan en lugares controlados como en las diferentes empresas para pasar lista o en otras ocasiones como el control de asistencia con firma de cada persona.

4.4.3. Requerimientos.

Los requerimientos técnicos necesarios para la instalación del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios se detallan en la tabla 11.

Tabla 11.

Detalles de hardware para el funcionamiento del sistema.

DETALLE	Mínimo	Recomendado
Procesador	Intel Core I3 2.5GHz	Intel Core I5 o Superior
Memoria RAM	4Gb	8Gb o superior
Disco Duro	320Gb	500Gb o superior
Adaptador de Video	2Gb 2Mpxls	4Gb acelerador gráfico o superior 2Mpxls
Cámaras	2K	4K o superior

Nota. Esta tabla muestra el hardware requerido para el funcionamiento del Sistema.

4.4.4. Instalación Del Sistema.

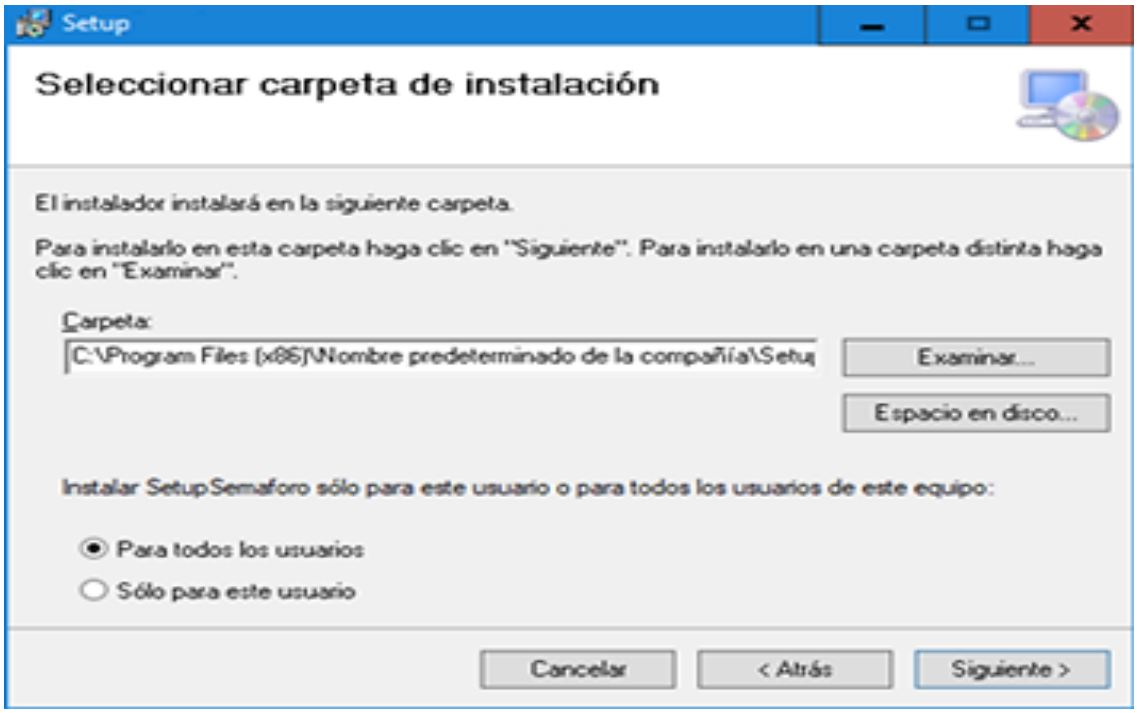
El sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios, se compone de varios archivos que están comprimidos en un solo programa instalador; el cual al ser ejecutado permite almacenar los archivos en las carpetas correspondientes del disco duro, previo a la instalación del sistema se debe instalar .NET Framework 5 que es la plataforma en la cual funciona el sistema.

Los pasos para instalar el sistema se detallan a continuación:

Abrir la carpeta de instalación del sistema y dar clic en el icono SetupSystem; a continuación, aparece la pantalla de bienvenida en dónde se debe dar clic en el botón Siguiente; posteriormente, aparece la pantalla de destino del sistema; es decir, en dónde se van a grabar los archivos necesarios para su funcionamiento. La dirección predeterminada es “Archivos de programa\SetupSystem\”; pero si se desea se puede cambiar esta dirección, dar clic en el botón “Examinar”. Una vez seleccionado el destino clicará en el botón Siguiente.

Figura 15.

Imagen de instalación del Sistema.

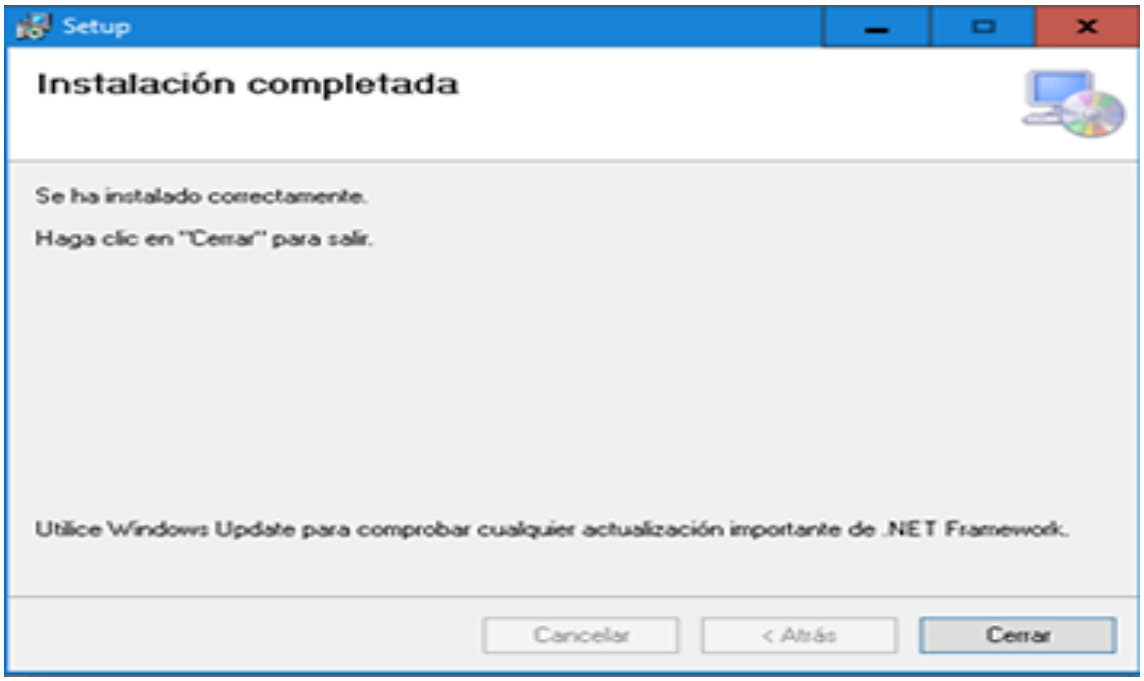


Nota. Se muestra la pantalla de instalación del sistema en dónde se muestra la carpeta para copiar los archivos y si el Sistema funcionará con un usuario único o con todos los usuarios.

Luego aparece la ventana de confirmación de datos de instalación, clic en Siguiente; la pantalla siguiente muestra el proceso de copia de archivos del sistema; en esta pantalla no se debe actuar hasta que la barra azul llegue al 100%; al final, una vez terminada la copia, aparece la pantalla de finalización, y en el botón Cerrar. Finalizada la instalación, el programa ya está listo para su funcionamiento.

Figura 16.

Imagen de instalación del sistema.



Nota. Se muestra la pantalla de finalización de la instalación del sistema.

A continuación, se detalla el código principal del sistema.

4.4.5. Código fuente.

En el Anexo 2 se encuentra el código completo de la aplicación desarrollada; por cuestiones de seguridad se omiten algunas partes de código.

Código Leer Rostro

```
‘Inicia la captura de video
   Public Sub Iniciar(ByVal timer As Timer, ByVal padre As Form)

        'Configura la ventana de captura
        CapHwnd = capCreateCaptureWindowA("WebCam", 0, 0, 0, Ancho, Alto,
padre.Handle.ToInt32(), 0)
        Application.DoEvents()
```

Código Principal

```
‘Proceso de reconocimiento de texto en imágenes en tiempo real
Private Sub Timer2_Tick(sender As Object, e As EventArgs) Handles Timer2.Tick
```

```
        Dim BMP As Bitmap = New Bitmap(PictureBox1.Image)
        Dim LECTOR As New Tesseract("tessdata", "eng",
Tesseract.OcrEngineMode.OEM_TESSERACT_ONLY)
        LECTOR.Recognize(New Image(Of Bgr, Byte)(BMP))
        TextBox1.Text = LECTOR.GetText
    End Sub
```

4.4.6. Seguridades.

El sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios, almacenará información muy importante ya que cada día se grabarán nuevos registros referentes a la asistencia de personas vulnerables a los centros de apoyo dentro de la ciudad de Tulcán.

Presenta un módulo que permite realizar un respaldo de la base de datos; ya que, si es eliminada por algún motivo, al iniciar el sistema se verifica el estado de los archivos de la base de datos y si los archivos no existen, ésta se restaura automáticamente.

También posee datos de usuarios, como son administrador y súper administrador, el administrador solo puede acceder a ciertas funciones del sistema y el súper administrador puede acceder a todas las funciones del sistema y también puede crear y modificar usuarios.

CAPÍTULO V – VERIFICACIÓN Y VALIDACIÓN.

5.1. Pruebas y mantenimiento del sistema.

Las pruebas de caja blanca también conocidas como pruebas estructurales o pruebas basadas en la lógica interna de un programa, se centran en evaluar el código fuente interno de una aplicación y consisten en verificar el funcionamiento de los algoritmos del sistema mediante el análisis del valor que adopta cada variable en la memoria RAM, para esto se realizó ejecuciones en modo paso a paso se verificó que cada algoritmo evalúe la información y regrese valores exactos de la codificación de cada rostro.

La prueba de caja negra es un test funcional o prueba comportamental, es un tipo de prueba de software directa, cuya finalidad es analizar la compatibilidad entre las interfaces de cada uno de los componentes del software; en donde se evaluó el funcionamiento del sistema mediante la ejecución e ingresando información valiosa y errónea para verificar los errores que se puedan presentar; en esta fase se permitió a varias personas administrar el sistema y que ingresen la información que deseen.

5.1.1. Pruebas de caja blanca.

Son pruebas de código funcional del sistema, mediante la realización de las pruebas de seguimiento de valores de las variables del código utilizado en el sistema, se evidenció que el sistema funcionó de manera perfecta y la administración de variables en la memoria RAM es óptima; por lo tanto, se consume el mínimo de recursos; en la tabla 12 se puede observar los valores obtenidos.

Tabla 12.

Datos de la memoria RAM del sistema.

Cámara	Existen rostros	Está registrado en la base de datos	Resultado de lectura
Leer imagen	Si	Si	Guardar paso de persona
Leer imagen	Si	No	Alarma
Leer imagen	No	No	No guarda registro

Nota. Esta tabla muestra los datos almacenados en la memoria RAM.

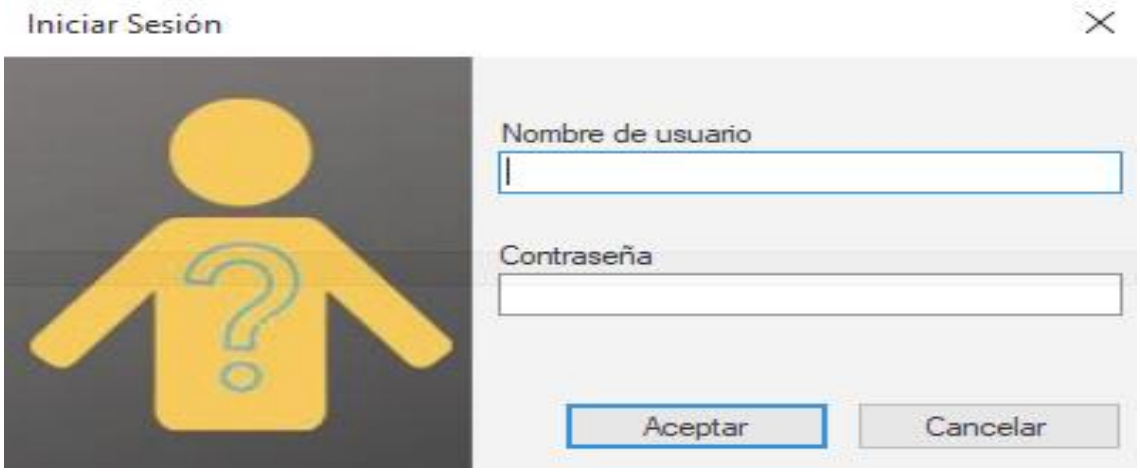
Se aplicaron varias pruebas de flujo de datos en las variables de memoria RAM, para verificar posibles errores en el código al procesar la información de la base de datos del sistema; en la tabla 12 se evidencia que la información obtenida de los procesos encargados de leer los rostros de cada imagen y su procesamiento verifican si una persona está o no registrada en el sistema para así guardar su registro de paso.

5.1.2. Pruebas de caja negra.

Las pruebas de caja negra fueron aplicadas directamente al funcionamiento del sistema y la manipulación de los formularios, tomando en cuenta que existen varios usuarios y cada uno tiene sus respectivos permisos; esto brinda seguridad de ingreso al sistema ya que cada usuario debe ingresar sus credenciales para su registro.

Figura 17.

Imagen del sistema en ejecución.



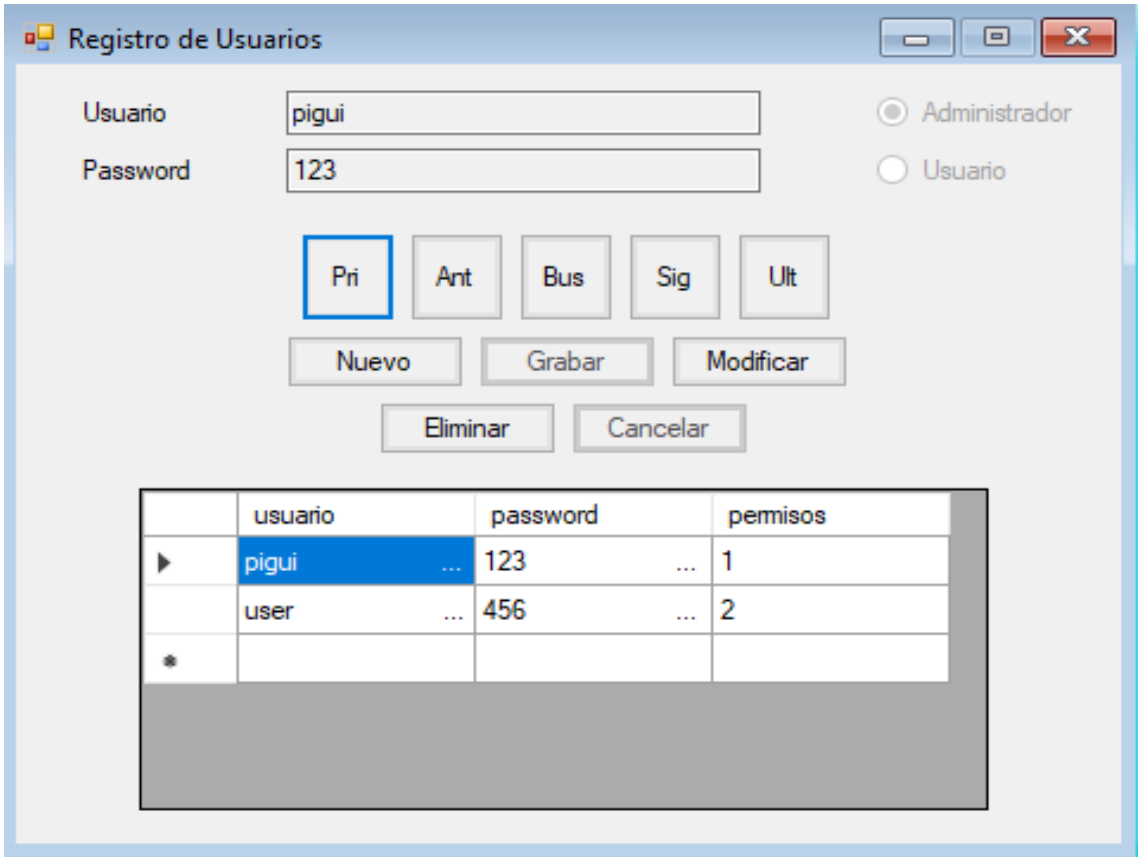
Nota. Se muestra la ejecución del sistema en el formulario de ingreso de usuario y contraseña para poder acceder al sistema, en caso de información mal ingresada el sistema no permite el acceso.

En la figura 17 se ingresaron datos erróneos de nombre de usuario y contraseña y hacer clic en aceptar el sistema emitió una alerta que dice que los datos son incorrectos y permite el ingreso al formulario principal únicamente cuando los datos ingresados son los correctos.

- ✓ El resultado de la prueba es Pass.

Figura 18.

Imagen del sistema en ejecución.



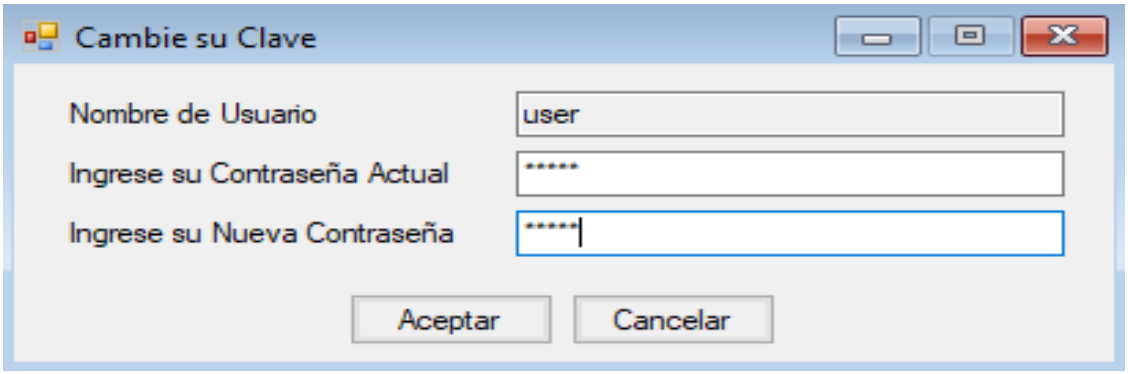
Nota. Se muestra la ejecución del sistema en el formulario de registro de usuarios en dónde se ingresa información de cada persona que administrará el sistema, los campos que presenta son usuario, password y permisos, también se puede seleccionar si la persona será administrador o usuario.

En la figura 18 se observa el formulario de registro de usuarios al cual solo pueden acceder los súper administradores del sistema; permite crear nuevos usuarios y brindar permisos de acceso a ciertas funciones del sistema, para la prueba se ingresó un nuevo usuario y se reinició el sistema para observar que el usuario registrado si es funcional.

- ✓ El resultado de la prueba es Pass.

Figura 19.

Imagen del sistema en ejecución.



Nota. Se muestra la ejecución del sistema en el formulario de cambio de clave en dónde un usuario puede cambiar su contraseña cuando sea oportuno.

En la figura 19 se observa el formulario de cambio de clave de usuario; el formulario permite modificar la clave de un usuario para mantener la seguridad del sistema; para la realización de la prueba de hizo que un usuario cambiara su contraseña antigua por una nueva y al reiniciar el sistema se pidió al usuario que ingrese su contraseña anterior e ingrese pero el sistema emitió una alerta de datos incorrectos, posteriormente se pidió al usuario que ingrese su contraseña actual y el sistema permitió el ingreso al formulario principal.

- ✓ El resultado de la prueba es Pass.

Figura 20.

Imagen del sistema en ejecución.

Nota. Se muestra la ejecución del sistema en el formulario principal como administrador en dónde se puede acceder a todos los formularios del sistema.

En la figura 20 se observa el Menú Principal con las funciones de administrador el cual muestra todo el menú disponible ya que un administrador puede acceder a todas las funciones del sistema, en la presente prueba se pidió al usuario que ingrese a las opciones del menú principal y verifique si todo funciona de forma correcta.

- ✓ El resultado de la prueba es Pass.

Figura 21.

Imagen del sistema en ejecución.

Nota. Se muestra la ejecución del sistema en el formulario principal como usuario en dónde se puede acceder a ciertos formularios del sistema.

La figura 21 muestra el formulario Menú Principal con las funciones de usuario que muestra ciertos menús disponibles ya que un usuario solo tiene acceso a ciertas funciones del sistema, para la realización de la prueba se pidió a un usuario que ingrese sus credenciales y acceda al menú principal y verifique si se muestra la pestaña administrar; se verificó que la pestaña no existe en el menú.

- ✓ El resultado de la prueba es Pass.

Figura 22.

Imagen del sistema en ejecución.

Nota. Se muestra la ejecución del sistema en el formulario de registro de personas mediante reconocimiento facial.

La figura 22 muestra el formulario de registro de ingreso de personas, que reconoce a cada persona y si está registrada, graba la información del registro de ingreso con las cámaras instaladas en el centro de ayuda comunitaria dentro de Tulcán, para la realización de la prueba se pidió a varias personas previamente registradas que pasen frente a la cámara para que el sistema compare sus rostros con la información de la base de datos, el sistema si reconoció los diferentes rostros.

Se realizaron varias pruebas de reconocimiento facial para verificar la calidad del comportamiento del algoritmo implicado en el sistema, de tal forma que se registraron varios rostros en la base de datos del sistema y se realizaron pruebas de paso de personas ante una cámara de video; entonces, a la luz natural el reconocimiento facial presentó un alcance del 95% de precisión ya que de 10 rostros, todos fueron captados y en ocasiones por pasar con la cabeza hacia abajo o con algún objeto un rostro no fue reconocido; con luz artificial el algoritmo obtuvo un 85% de precisión, esto ocurre por las sombras y la baja intensidad que ofrece la luz artificial sobre todo si se encuentra lejana al objetivo en detección; bajo visión nocturna la precisión es del 20% ya que el rostro se vuelve oscuro y poco reconocible para el algoritmo; por lo que es recomendable utilizar el sistema a la luz natural o con una fuente clara de luz artificial para que su funcionamiento sea óptimo y no existan posibles errores de reconocimiento facial.

- ✓ El resultado de la prueba es Pass.

5.2. Validación.

Para la validación de la propuesta se utilizó la evaluación y test aplicando finalmente una encuesta que se encuentra en el Anexo 3 al personal evaluador del sistema quienes son tres Ingenieros en Sistemas con título de cuarto nivel según la norma ISO/IEC 12119, se pidió a personas expertas en el tema de reconocimiento facial en 3D que manipulen el software y la revisión de la estructura del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios y su configuración, se realizaron pruebas de software mediante su ejecución en presencia de los expertos, obteniendo buenos resultados y confirmando su buen funcionamiento; el test de encuesta se detalla a continuación:

- **Indicador 1:** Carácter Tecnológico – Científico del Sistema.
- **Indicador 2:** Efectividad de la Estructura Metodológica del desarrollo del Sistema.
- **Indicador 3:** Novedad del sistema.
- **Indicador 4:** Viabilidad para la aplicación práctica del desarrollo de sistema.
- **Indicador 5:** Actualidad del desarrollo del sistema.

Luego se encuestó a cada experto en el tema haciéndole llenar una ficha de validación de la propuesta la que posee aspectos fundamentales del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios, obteniendo los siguientes resultados:

Validador 1.

- Nº de cédula: 0401288139
- Nombres y Apellidos: Fernanda Becerra.
- Título de mayor jerarquía: Magister
- Institución que labora: Unidad Educativa San Gabriel.
- Cargo Actual: Docente
- Años de servicio: 8 años.

- Experiencia profesional: 10 años.

Validador 2.

- Nº de cédula: 1002140729
- Nombres y Apellidos: Carrera Pozo Oscar Freed.
- Título de mayor jerarquía: Magister en Redes y Comunicaciones.
- Institución que labora: Cooperativa Pablo Muñoz Vega
- Cargo Actual: Director de Tecnologías.
- Años de servicio: 1 años.
- Experiencia profesional: 35 años

Validador 3.

- Nº de cédula: 0401592514
- Nombres y Apellidos: Andrés Cabascango.
- Título de mayor jerarquía: Ingeniería en Sistemas.
- Institución que labora: Unidad Educativa Vicente Fierro
- Cargo Actual: Telemática.
- Años de servicio: 7 años.
- Experiencia profesional: 10 años

5.2.1. Resultados de la Validación de la Propuesta.

Una vez realizadas las validaciones de los expertos en seguridad informática se obtuvieron los siguientes resultados:

En el primer indicador de la calidad se preguntó por el carácter tecnológico - científico del desarrollo del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios; obteniendo los resultados que se detallan en la tabla 13.

Tabla 13.

Análisis e interpretación de resultados

Expertos de Sistemas		
Valoración	**Número**	**Porcentaje**
Muy Satisfactorio	3	100%
Satisfactorio	0	0%
Poco satisfactorio	0	0%
No satisfactorio	0	0%
Total	3	100%

Nota. Esta tabla muestra el nivel de satisfacción tecnológico científico del Sistema.

Interpretación: Los expertos manifiestan que el carácter tecnológico - científico del desarrollo del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios es muy satisfactorio.

En el segundo indicador de la calidad se preguntó por la efectividad de la Estructura Metodológica del desarrollo del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios; obteniendo los resultados que se detallan en la tabla 14.

Tabla 14.

Análisis e interpretación de resultados.

Expertos de Sistemas		
Valoración	**Número**	**Porcentaje**
Muy Satisfactorio	0	0%
Satisfactorio	3	100%
Poco satisfactorio	0	0%
No satisfactorio	0	0%
Total	3	100%

Nota. Esta tabla muestra el nivel de satisfacción de la estructura metodológica del Sistema.

Interpretación: Los tres expertos en informática, han expresado que la efectividad de la Estructura Metodológica del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad

en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios es satisfactorio.

En el tercer indicador de la calidad se preguntó por la novedad del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios; obteniendo los resultados que se detallan en la tabla 15.

Tabla 15.

Análisis e interpretación de resultados.

Expertos de Sistemas		
Valoración	**Número**	**Porcentaje**
Muy Satisfactorio	3	100%
Satisfactorio	0	0%
Poco satisfactorio	0	0%
No satisfactorio	0	0%
Total	3	100%

Nota. Esta tabla muestra el nivel de satisfacción de la novedad del Sistema.

Interpretación: En cuanto a la novedad del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios, los expertos manifestaron ser muy satisfactorio.

En el cuarto indicador de la calidad se preguntó por la viabilidad para la aplicación práctica del desarrollo de sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios, obteniendo los resultados que se detallan en la tabla 16.

Tabla 16.

Análisis e interpretación de resultados.

Expertos de Sistemas		
Valoración	**Número**	**Porcentaje**
Muy Satisfactorio	3	100%
Satisfactorio	0	0%
Poco satisfactorio	0	0%
No satisfactorio	0	0%
Total	3	100%

Nota. Esta tabla muestra el nivel de satisfacción de la vialidad del Sistema.

Interpretación: La viabilidad para aplicar práctica el sistema de seguridad informático de reconocimiento facial 3D con técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios, es satisfactoria, según los expertos.

En el quinto indicador de la calidad se preguntó por la actualidad del desarrollo del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios; obteniendo los resultados que se detallan en la tabla 17.

Tabla 17.

Análisis e interpretación de resultados.

Expertos de Sistemas		
Valoración	**Número**	**Porcentaje**
Muy Satisfactorio	3	100%
Satisfactorio	0	0%
Poco satisfactorio	0	0%
No satisfactorio	0	0%
Total	3	100%

Nota. Esta tabla muestra el nivel de satisfacción de la actualidad del Sistema.

Interpretación: Según los tres expertos en informática, es de carácter actual e indispensable el desarrollo del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios.

5.2.2. Impacto.

El sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios tiene un impacto en varias áreas de la comunidad, entre las cuales constan las siguientes:

Impacto Social: El reconocimiento facial 3D en tiempo real de las personas acuden a los centros de ayuda social en Tulcán permite registrar su asistencia y comportamiento que presenta, por lo que, si una persona es registrada recibiendo ayuda humanitaria y luego regresa con otra identidad, la cámara emitirá una alarma ya que el rostro ya se captó anteriormente y no puede acceder 2 veces a ella; así forma una sociedad solidaria con todos.

Impacto Económico: Al formar una sociedad solidaria, las ayudas a personas vulnerables serán enfocadas a toda una población y no sólo a unas personas por lo que la Organización ADRA gastará menos dinero y su beneficio será para todos.

Impacto Tecnológico: El sistema administra tecnología de visión artificial que permite reconocer facialmente en 3D a personas para verificar y registrar su asistencia a los centros de apoyo comunitario a personas vulnerables en Tulcán.

Impacto Educativo: El proyecto se refiere al uso de la tecnología de reconocimiento facial en 3D, lo que ayuda a crear nuevos proyectos que usen esta tecnología, así los estudiantes universitarios podrán desarrollar conocimientos en esta área de estudio.

Impacto Ambiental: Puesto que es un proyecto tecnológico que se basa en la tecnología de reconocimiento facial en 3D, el proyecto no genera impacto ambiental alguno.

CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones.

Como resultado del desarrollo de la presente investigación se ha llegado a las siguientes conclusiones:

- La implementación de un sistema de reconocimiento facial 3D basado en inteligencia artificial ha demostrado ser altamente eficaz. A través de pruebas y validaciones, se ha logrado una tasa de aciertos superior al 95%, lo que minimiza el riesgo de suplantación de identidad. Esto se debe a que el reconocimiento 3D permite capturar características faciales únicas que son difíciles de replicar, lo que otorga un nivel de seguridad más alto frente a métodos de identificación bidimensional.

- La fusión de tecnologías de reconocimiento facial con inteligencia artificial permite al sistema adaptarse y aprender de nuevos patrones de comportamiento y datos biométricos. Esto significa que el sistema puede actualizarse y mejorar continuamente, manteniendo su eficacia frente a métodos de suplantación más sofisticados. Además, su capacidad de procesamiento en tiempo real facilita la identificación instantánea, optimizando las operaciones dentro de la Organización ADRA Ecuador.

- Para garantizar una integración efectiva del sistema, es esencial proporcionar capacitación a todos los usuarios. Esto no solo incluye cómo utilizar el sistema, sino también la comprensión de su importancia y sus implicaciones. Además, establecer protocolos claros sobre el acceso y el manejo de datos sensibles contribuirá a la confianza en el sistema y a su uso responsable. Se recomienda realizar auditorías periódicas para evaluar el desempeño del sistema y su adaptación a nuevas amenazas.

- El uso de tecnologías de reconocimiento facial plantea preocupaciones éticas relacionadas con la privacidad y la vigilancia. Es fundamental que ADRA Ecuador establezca políticas claras sobre la recolección y el uso de datos biométricos, asegurando la transparencia con los usuarios. Fomentar un diálogo abierto sobre estos temas puede ayudar a mitigar preocupaciones y construir confianza. También sería beneficioso desarrollar un marco regulatorio que garantice el uso ético de la tecnología.

- Se sugiere llevar a cabo estudios longitudinales que evalúen la efectividad del sistema en diferentes contextos y entornos organizacionales. Asimismo, investigar nuevas tecnologías emergentes en el campo del reconocimiento facial y la inteligencia artificial podría proporcionar valiosas mejoras al sistema. La colaboración con expertos en ciberseguridad y ética tecnológica también es crucial para anticipar y responder a nuevas amenazas y desafíos.

6.2. Recomendaciones.

Como recomendaciones principales luego de realizar la presente investigación se presentan las siguientes:

- Se recomienda realizar constante mantenimiento de la base de datos puesto que el tamaño del campo donde se registra el código facial puede ser muy grande y ocupar demasiado espacio, entonces la base de datos puede hacerse menos versátil; entonces, es necesario borrar registros que no se estén utilizando para que la búsqueda de información sea más rápida.

- Se recomienda realizar mantenimiento a las cámaras utilizadas para el reconocimiento facial ya que dependiendo del lugar en donde se instalen, pueden averiarse o ensuciarse; por tanto, se deben limpiar o reemplazar de forma constante.

- Se recomienda a la empresa ADRA estar pendiente y realizar constantemente las actualizaciones de Software ya que se realizarán cambios dependiendo de los actuales requerimientos con el fin de que el sistema funcione de la mejor forma.

- Se recomienda al personal encargado de la administración del software y hardware estar atento a las alarmas que genera el sistema para reconocer a personas que pretenden suplantar la identidad de terceros.

BIBLIOGRAFÍA

JIimenez M. (2018). PROYECTO DE INVESTIGACIÓN. Sistema de visión artificial para la detección de aglomeración de personas en un semáforo Loja, Ecuador.

Vizcaíno J. (2018). PROYECTO DE INVESTIGACIÓN. "Sistema informático de visión artificial para mejorar la gestión del parqueadero de la Uniandes Tulcán. Tulcán, Ecuador.

Ruano D. (2022). PROYECTO DE INVESTIGACIÓN. "Sistema informático con visión artificial para evitar el robo de vehículos en la empresa Seguros Olímpicos de la ciudad de Tulcán. Tulcan, Ecuador.

López, A. (2017). Ingeniería del software e inteligencia artificial. Madrid: Polígono industrial arroyomolinos.

Gonzalez, Lee, (2015), Robótica: Control, Detección, Visión e Inteligencia.

Russell, Norvig, (2013), Inteligencia Artificial.

Gómez, F. (2017). Fundamentos de la Visión Artificial.

OpenCV. (2016). OpenCV.

Noya, E. C. (2015). multimedia. Madrid: G.F. Printing.

García, A. P. (2017). Software. Madrid: polígono industrial arroyomolinos.

Juan, A. (2013), http://www.dipolerfid.es/

Barrietos. (2014). Introducción a SQL Server. Barcelona: Eden.

Baturone. (2015). Programación Orientada a Objetos. Puebla: Ariel.

BrowserAdvertising. (10 de Enero de 2014). EGOMEXICO. Obtenido de http://www.egomexico.com/tecnologia_rfid.htm

AMICUS. (2015). Facial Recognition. Recuperado el 10 de Mayo de 2019, de https://www.amicusint.org/articles/2015/10/13/face-recognition

Blanco, E. L. (2008). EcuRed. Obtenido de EcuRed: https://www.ecured.cu/Sistema_inform%C3%A1tico

Contaval. (2016). Qué es la visión artificial y para qué sirve. Recuperado el 24 de Abril de 2019, de https://www.contaval.es/que-es-la-vision-artificial-y-para-que-sirve/

Greenberg, E. (2019). Videovigilancia en la vía pública. Buenos Aires.

Ibermática. (2011). Sistema de seguimiento de la mirada. Recuperado el 8 de Mayo de 2019, de http://rtdibermatica.com/?p=648

Kendall, K. &. (2015). Ciclo de vida del desarrollo de sistemas. New Yersey: Rutgers.

Merchán, J. M. (2018). DISEÑO E INSTALACIÓN DE SISTEMAS DE VIDEOVIGILANCIA CCTV DIGITALES. Madrid.

OpenCV. (2019). OpenCV. Recuperado el 17 de Mayo de 2019, de https://opencv.org/

ProgramaciónExtrema. (2018). El algoritmo de Viola & Jones. Recuperado el 27 de Abril de 2019, de http://programacionextrema.es/2018/02/27/algoritmo-viola-jones-diario-programador/

RicardoGeek. (2019). Detección De Caras Con OpenCV y Python. Recuperado el 15 de Mayo de 2019, de https://ricardogeek.com/deteccion-de-caras-con-opencv-y-python/

STACKPOINTERS. (2018). Object Detection Framework. Recuperado el 4 de Mayo de 2019, de http://stackpointers.com/python/log/

Troya, C. (2016). LBP y ULBP – Local Binary Patterns y Uniform Local Binary Patterns. Obtenido de https://cesartroyasherdek.wordpress.com/2016/02/26/deteccion-de-objetos-vi/

Anexo 1.

Interpretación de Resultados

Encuesta dirigida al personal de la organización ADRA de la ciudad de Tulcán.

Pregunta 1: ¿Conoce usted del uso de la tecnología en beneficio de personas en estado vulnerable para brindar una mayor seguridad y control?

Tabla 18. Beneficio tecnológico.

Pregunta Nro. 1		
Opciones	**Cantidad**	Porcentaje (%)
Si	6	**30,00%**
No	14	**70,00%**
Total	**20**	**100%**

Fuente. Investigación de campo.

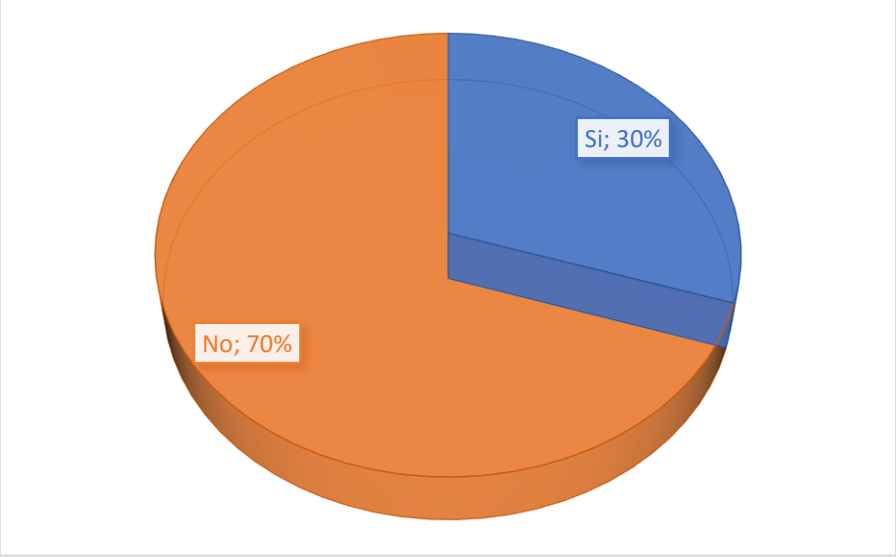


Figura 23: Pregunta 1 de la encuesta.

Fuente: Investigación de campo.

Interpretación de Datos.

El 30.00% de las personas encuestas dicen que, si conocen acerca del uso de la tecnología en beneficio de personas en estado vulnerable para brindar una mayor seguridad y control, mientras que el 70.00% de los encuestados dicen no conocer acerca del tema, por lo que se concluye que la mayoría de personas desconocen a cerca de los beneficios que la tecnología de reconocimiento facial les puede brindar.

Pregunta Nro. 2: ¿Conoce usted el código de los derechos humanos en relación al uso de cámaras de vigilancia y privacidad?

Tabla 19. Conocimiento Legal.

Pregunta Nro. 2		
Opciones	**Cantidad**	Porcentaje (%)
Si	4	**20,00%**
No	16	**80,00%**
Total	**20**	**100%**

Fuente. Investigación de campo.

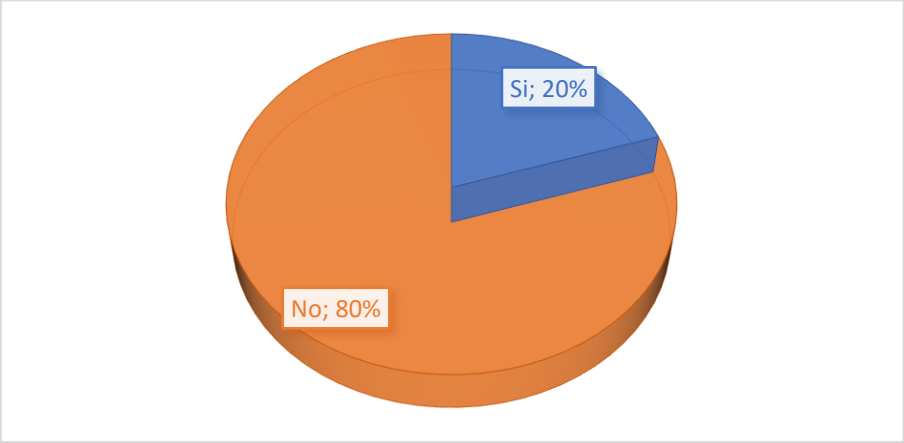


Figura 24: Pregunta 2 de la encuesta.
Fuente: Investigación de campo.

Interpretación de Datos.

El 20.00% de las personas encuestas dicen que, si conocen acerca del código de los derechos humanos en relación al uso de cámaras de vigilancia y privacidad, mientras que el 80.00% de los encuestados dicen no conocer acerca del tema, por lo que se concluye que la mayoría de personas desconocen a cerca de la existencia de las leyes de privacidad, sus causas y consecuencias.

Pregunta Nro. 3: ¿Está de acuerdo en la vigilancia mediante reconocimiento facial 3D para evitar la suplantación de identidad de las personas vulnerables a las que atiende la organización ADRA de la ciudad de Tulcán?

Tabla 20. Consideración personal.

Pregunta Nro. 3		
OPCIONES	**CANTIDAD**	PORCENTAJE (%)
SI	13	**65,00%**
NO	7	**35,00%**
TOTAL	**20**	**100%**

Fuente. Investigación de campo.

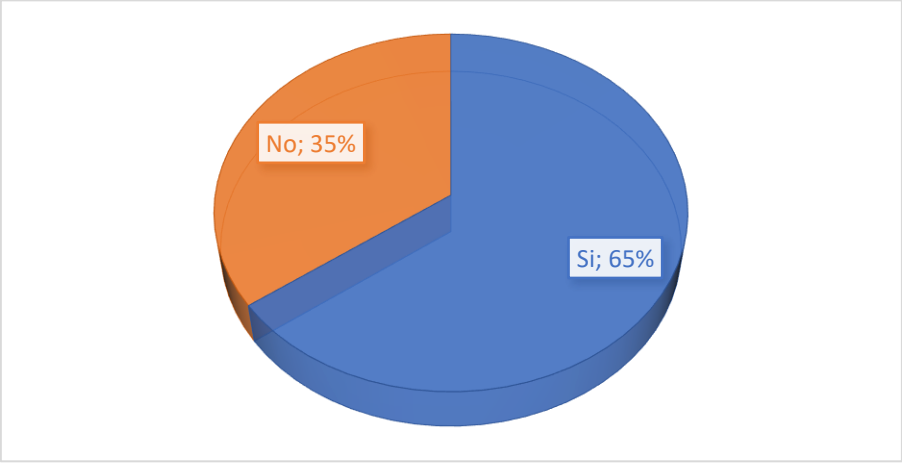


Figura 25: Pregunta 3 de la encuesta.
Fuente: Investigación de campo.

Interpretación de Datos.

El 75.00% de los encuestados dicen que, si están de acuerdo en la vigilancia mediante reconocimiento facial de las personas vulnerables a las que atiende la organización ADRA de la ciudad de Tulcán, mientras que el 25.00% de los encuestados dicen que no están de acuerdo, por lo que se concluye que la mayoría de personas consideran que es de gran beneficio la implementación de sistemas de reconocimiento facial.

Pregunta Nro. 4: ¿Actualmente de qué forma controlan el acceso a los sitios de asistencia a personas vulnerables?

Tabla 21. Conocimiento personal.

Pregunta Nro. 4		
OPCIONES	**CANTIDAD**	PORCENTAJE (%)
Visual	3	**15,00%**
Registro de ingreso	15	**75,00%**
Ninguno	2	**10,00%**
TOTAL	**20**	**100%**

Fuente. Investigación de campo.

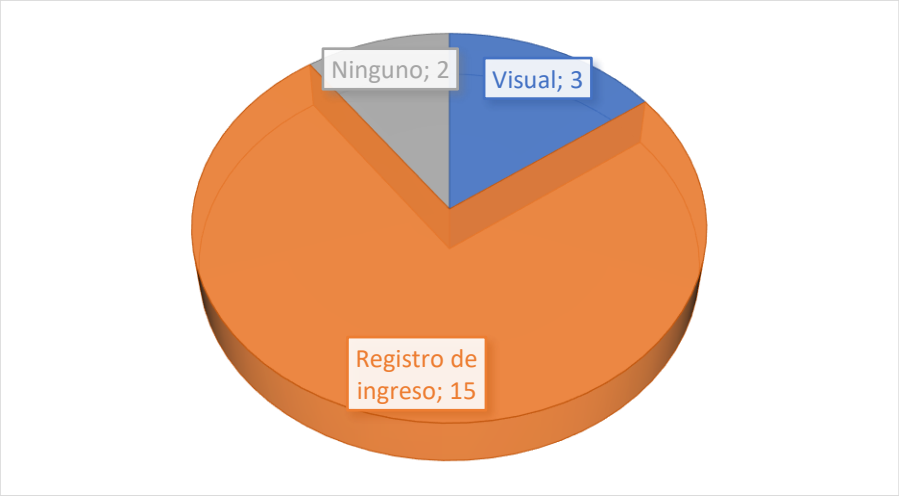


Figura 26: Pregunta 4 de la encuesta.
Fuente: Investigación de campo.

Interpretación de Datos.

El 15.00% de las personas encuestas dicen que el control de acceso a los sitios de asistencia a personas vulnerables se lo realiza de forma visual, el 75% de las personas encuestadas dicen que de realza mediante un registro y el 10% de personas encuestadas dicen que no se realiza ningún tipo de control; por lo que se concluye que la mayoría del personal lleva un control mediante registro.

Pregunta Nro. 5: ¿Alguna vez intentaron ingresar personas externas para acceder a los beneficios de la organización ADRA en su presencia?

Tabla 22. Consideración personal.

Pregunta Nro. 5		
OPCIONES	**CANTIDAD**	PORCENTAJE (%)
Si	14	**70,00%**
No	6	**30,00%**
TOTAL	**20**	**100%**

Fuente. Investigación de campo.

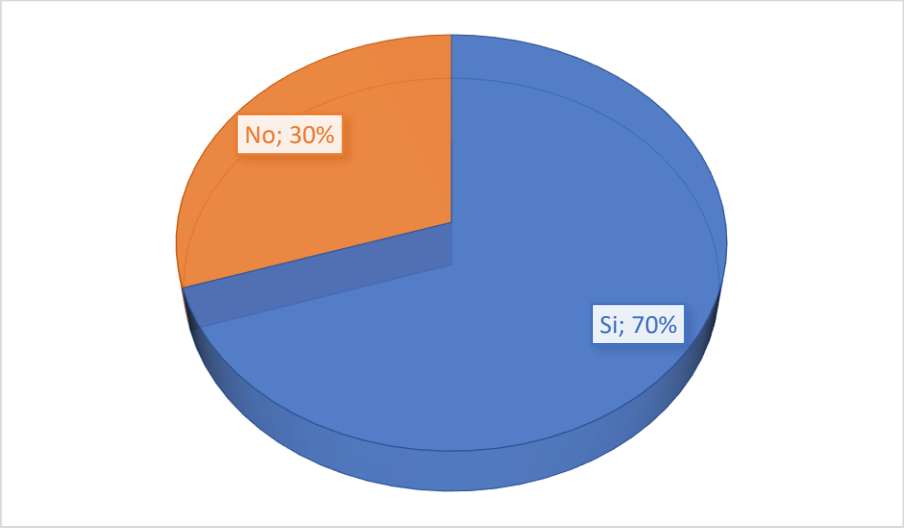


Figura 27: Pregunta 5 de la encuesta.
Fuente: Investigación de campo.

Interpretación de Datos.

El 70.0% de las personas encuestas dicen que alguna vez si intentaron ingresar personas externas para acceder a los beneficios de la organización ADRA en su presencia, mientras que el 30.00% de los encuestados dicen que no han tenido este tipo de problema, por lo que se concluye que la mayoría de personas si están de acuerdo con la implementación del sistema para tener una mayor seguridad y control de asistencia.

Pregunta Nro. 6: ¿Cree usted que, con la implementación de un sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad, la organización ADRA mejore el control de acceso a personas que no pertenecen a los grupos vulnerables en la ciudad de Tulcán?

Tabla 23. Consideración personal.

Pregunta Nro. 6		
OPCIONES	**CANTIDAD**	PORCENTAJE (%)
Si	18	**90,00%**
No	2	**10,00%**
TOTAL	**20**	**100%**

Fuente. Investigación de campo.

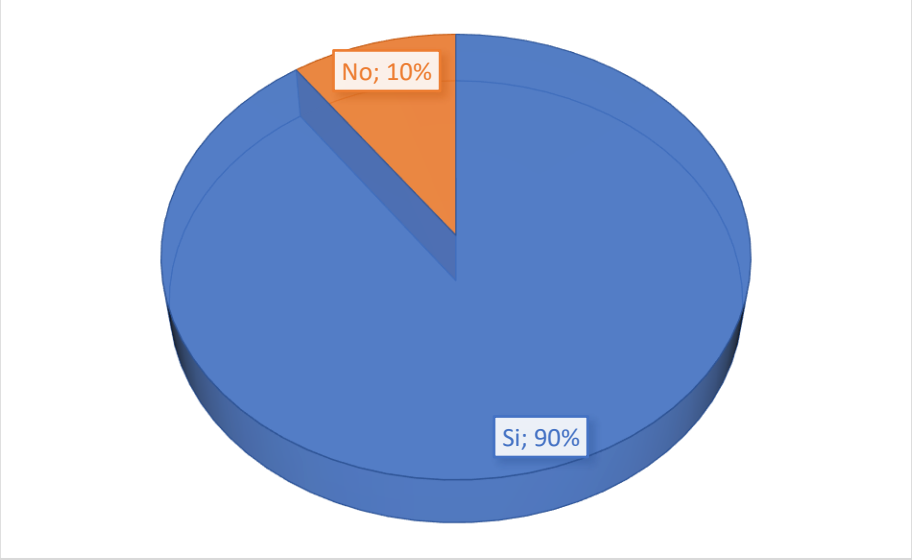


Figura 28: Pregunta 6 de la encuesta.
Fuente: Investigación de campo.

Interpretación de Datos.

El 90.0% de las personas encuestas dicen que, con la implementación de un sistema informático de reconocimiento facial, la organización ADRA mejorará el control de acceso a personas que no pertenecen a los grupos vulnerables en la ciudad de Tulcán, mientras que el 10.00% de los encuestados dicen que no mejorará el control de acceso a personas que no pertenecen a los grupos vulnerables en la ciudad de Tulcán; por lo que se concluye que la mayoría de personas si están de acuerdo con la implementación del sistema informático de reconocimiento facial.

Verificación de la idea a defender

Para la verificación se utilizó "t" de Student, como un estadígrafo de distribución libre que permite establecer la comprobación de la hipótesis, permitiendo la comparación global del grupo de frecuencias a partir de la hipótesis que se quiere verificar. Para la combinación se seleccionan de la encuesta las dos preguntas más centrales al tema de investigación considerando las dos variables. (Pregunta 1 y pregunta 6)

Formulación de la hipótesis

Se tomará en consideración 2 preguntas de la encuesta.

Pregunta 1. ¿Conoce usted del uso de la tecnología en beneficio de personas en estado vulnerable para brindar una mayor seguridad y control?

Tabla 24. Beneficio tecnológico.

Respuesta	Frecuencia	Porcentaje
Si	6	30%
No	14	70%
Total	20	100%

Elaborado por: Jefferson Cárdenas

Pregunta 6. ¿Cree usted que, con la implementación de un sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad, la organización ADRA mejore el control de acceso a personas que no pertenecen a los grupos vulnerables en la ciudad de Tulcán?

Tabla 25. Consideración personal.

Respuesta	Frecuencia	Porcentaje
Si	18	90%
No	2	10%
Total	50	100%

Elaborado por: Jefferson Cárdenas

Hipótesis alternativa (H1)

La implementación de un sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial no incide en evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios

Hipótesis Nula (H0)

La implementación de un sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial no incide en evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios.

Elección de la prueba estadística

Para la verificación de la idea a defender se seleccionó la distribución, cuya fórmula es la siguiente:

Ecuaciones:

$$\frac{\overline{X_1} - \overline{X_2}}{\sqrt{\frac{S_c^2}{n_1} + \frac{S_c^2}{n_2}}}$$ Valor estadístico de prueba

$$S_c^2 = \frac{(n1-1)S_1^2 + (n2-1)S_2^2}{n1+n2-2}$$ Varianza

$$t_{\left(1-\frac{a}{2}\right).(n1+n2-2)}$$ Valor crítico

Definición del nivel de significación y regla de decisión

Para el cálculo de los Grados de Libertad se utilizó la siguiente fórmula:

$$gl = n1 + n2 - 2$$

$$\propto = 0{,}05$$

$$n1 = 2$$

$$n2 = 3$$

$$gl = 2 + 3 - 2$$

$$gl = 3$$

Cálculo del promedio de las muestras independientes:

$$\overline{X_1} = 25$$

$$\overline{X_2} = 16{,}66667$$

Cálculo de la varianza:

$$\text{Varianza Muestral } n1 = 8$$

$$\text{Varianza Muestral } n2 = 10{,}33333$$

$$\text{Varianza} = 7{,}16667$$

Cálculo de la distribución "t" student

Cálculo del valor estadístico de prueba:

$$t = 3{,}4099717$$

Cálculo del valor crítico:

$$\text{Valor crítico} = 3{,}18244631$$

El valor crítico va de -3,18244631 hasta 3,18244631, dentro de estos valores se acepta la hipótesis nula por lo que, si el valor estadístico de prueba se encuentra dentro del intervalo, se niega la hipótesis, esto quiere decir que no es válida; pero como el valor

estadístico es de 3,4099717, entonces el valor está fuera del intervalo por lo que la hipótesis es aceptada.

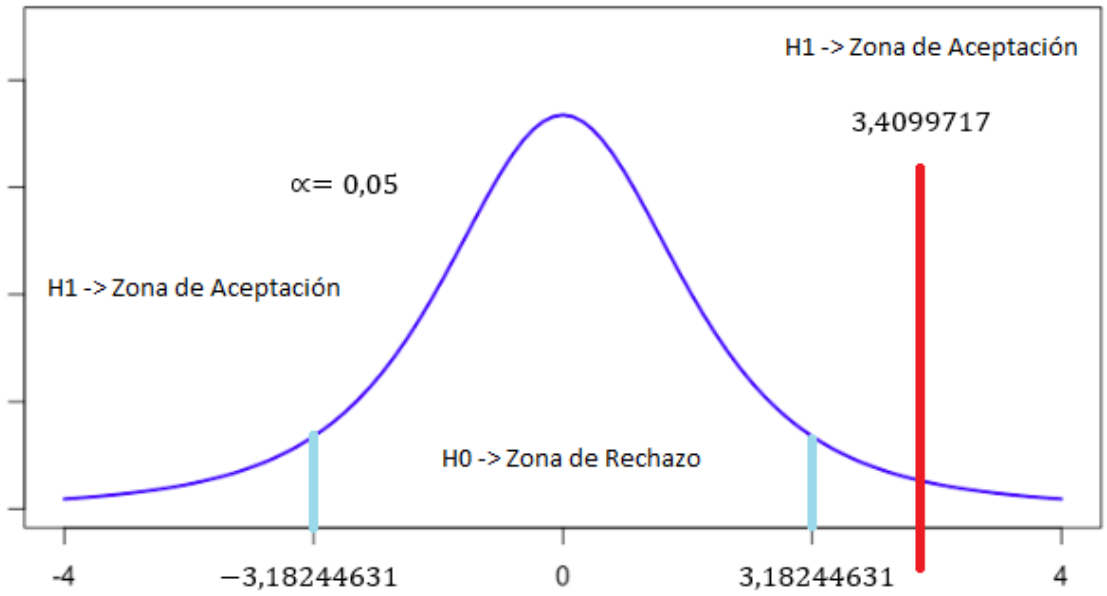


Figura 29. Distribución t-student.

Fuente: (Dagnino, 2014).

Cálculo de la probabilidad asignada al valor estadístico de prueba t:

$$p - valor = 0{,}04255157$$

El margen de error es del 5% y se expresa estadísticamente como 0,05; entonces para que la probabilidad sea aceptada, el valor de la probabilidad asignada al valor estadístico de prueba t es 0,04255157 debe ser menor al margen de error que es 0,05.

$$0{,}04255157 < 0{,}05$$

Por lo que se rechaza la hipótesis nula H0 y por lo tanto se aprueba la hipótesis alternativa H1.

Anexo 2.

Código Fuente. El código desarrollado en esta tesis es el siguiente:

Código de la Clase LeerRostro

```
'Librería para la lectura de texto en imágenes
Imports System.Runtime.InteropServices

Public Class LeerRostro
    Dim CapHwnd As Integer
'Tamaño de la ventana de la cámara
    Dim Ancho As Integer = 320
    Dim Alto As Integer = 240
'"libreria.DLL" = El nombre del API que se desea importar
' EntryPoint = indica el nombre exacto de la función del API que queremos usar
#Region "Librerias DLL"
'La función SendMessage llama al procedimiento de ventana para la ventana
especificada y no vuelve hasta que el procedimiento de ventana se ha procesado el
mensaje
    <DllImport("user32.dll", EntryPoint:="SendMessage")>
    Public Shared Function SendMessage(ByVal hWnd As Integer, ByVal Msg As
UInteger, ByVal wParam As Integer, ByVal lParam As Integer) As Integer
    End Function
    'Crea una ventana de captura
    <DllImport("avicap32.dll", EntryPoint:="capCreateCaptureWindowA")>
    Public Shared Function capCreateCaptureWindowA(ByVal Nombre As String,
ByVal dwStyle As Integer, ByVal X As Integer, ByVal Y As Integer, ByVal nWidth As
Integer, ByVal nHeight As Integer, ByVal hWnd As Integer, ByVal nID As Integer) As
Integer
    End Function

#End Region

#Region “Constantes API para lectura de imágenes”
    Const WM_USER As Integer = 1024
```

```
    Const WM_CAP_CONNECT As Integer = 1034
    Const WM_CAP_DISCONNECT As Integer = 1035
    Const WM_CAP_GET_FRAME As Integer = 1084
    Const WM_CAP_COPY As Integer = 1054
    Const WM_CAP_START As Integer = WM_USER
    Const WM_CAP_SET_PREVIEWRATE As Integer = WM_USER + 52
    Const WM_CAP_DLG_VIDEOFORMAT As Integer = WM_CAP_START + 41
    Const WM_CAP_DLG_VIDEOSOURCE As Integer = WM_CAP_START + 42
    Const WM_CAP_DLG_VIDEODISPLAY As Integer = WM_CAP_START + 43
    Const WM_CAP_GET_VIDEOFORMAT As Integer = WM_CAP_START + 44
    Const WM_CAP_SET_VIDEOFORMAT As Integer = WM_CAP_START + 45
    Const WM_CAP_DLG_VIDEOCOMPRESSION As Integer = WM_CAP_START +
46
    Const WM_CAP_SET_PREVIEW As Integer = WM_CAP_START + 50
#End Region

    'Captura frame y envía a portapapeles
    Public Sub timer_tick(ByVal picture As PictureBox)
        SendMessage(CapHwnd, WM_CAP_GET_FRAME, 0, 0)
        SendMessage(CapHwnd, WM_CAP_COPY, 0, 0)
        picture.Image = Clipboard.GetImage()
        Application.DoEvents()
    End Sub

    'Guarda el frame que está en memoria en un archivo JPG
    Public Sub Capturar(ByVal picture As PictureBox)
        Dim sfile_JPG As String = "c:\archivo.jpg"
        Dim obj_bitMap As New Bitmap(Ancho, Alto)
        Try
            picture.DrawToBitmap(obj_bitMap, New Rectangle(0, 0, Ancho, Alto))
            obj_bitMap.Save(sfile_JPG, Imaging.ImageFormat.Jpeg)
            MessageBox.Show("Imagen capturada en [" & sfile_JPG & " ]")
        Catch ex As Exception
            System.Console.WriteLine(ex)
```

```
        End Try
    End Sub
'Inicia la captura de video
    Public Sub Iniciar(ByVal timer As Timer, ByVal padre As Form)
        Try
            'Configura la ventana de captura
            CapHwnd = capCreateCaptureWindowA("WebCam", 0, 0, 0, Ancho, Alto,
padre.Handle.ToInt32(), 0)

            Application.DoEvents()

            SendMessage(CapHwnd, WM_CAP_CONNECT, 0, 0)
            SendMessage(CapHwnd, WM_CAP_SET_PREVIEWRATE, 69, 0)
            SendMessage(CapHwnd, WM_CAP_SET_PREVIEW, 0, 0)
            'se inicia el Timer
            timer.Start()
        Catch ex As Exception
            Console.WriteLine(ex)
        End Try
    End Sub

'Detiene la captura de video
    Public Sub Detener(ByVal timer As Timer)
        Try
            timer.Stop()
            Application.DoEvents()
            SendMessage(CapHwnd, WM_CAP_DISCONNECT, 0, 0)
        Catch ex As Exception
            Console.WriteLine(ex)
        End Try
    End Sub
End Class
```

Anexo 3.

ENCUESTA ANÓNIMA DIRIGIDA AL PERSONAL DE LA ORGANIZACIÓN ADRA.

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

Seguridad con reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial:

Evaluación y Concientización

Esta encuesta está diseñada para evaluar la efectividad de las medidas de seguridad de acceso implementando Reconocimiento Facial y técnicas de Inteligencia Artificial de la empresa ADRA. Nuestro objetivo es comprender la perspectiva y el nivel de conocimiento de los colaboradores de la empresa en relación con la seguridad de acceso a las instalaciones dedicadas a la prestación de ayudas comunitarias a la población vulnerable. Buscamos obtener información valiosa sobre el conocimiento de amenazas en seguridad de acceso y las medidas de seguridad implementadas en accesos donde pasa la población.

Lea detenidamente las preguntas y escoja la alternativa que usted considere conveniente.

Consentimiento informado: Acepta participar en la investigación descrita de forma libre y voluntaria. Su participación puede ser suspendida en cualquier momento, sin que esto traiga ningún tipo de consecuencias negativas para usted o la institución. Este estudio no presenta riesgos identificables para su integridad física o psicológica.

Los datos solicitados para la aplicación de este cuestionario son anónimos y serán manejados bajo absoluta confidencialidad. Estos datos estarán guardados en archivo electrónico, codificados con clave de acceso y custodiados por el Investigador responsable.

Ante cualquier duda, puede comunicarse con el responsable de esta investigación, Ing., Jefferson Cárdenas, mediante correo electrónico ejcardenasa@utn.edu.ec.

○ Si

- ○ No

Pregunta 1: ¿Conoce usted del uso de la tecnología en beneficio de personas en estado vulnerable para brindar una mayor seguridad y control?

- ○ Si
- ○ No

Pregunta 2: ¿Conoce usted el código de los derechos humanos en relación al uso de cámaras de vigilancia y privacidad?

- ○ Si
- ○ No

Pregunta 3: ¿Está de acuerdo en la vigilancia mediante reconocimiento facial 3D para evitar la suplantación de identidad de las personas vulnerables a las que atiende la organización ADRA de la ciudad de Tulcán?

- ○ Si
- ○ No

Pregunta 4: ¿Actualmente de qué forma controlan el acceso a los sitios de asistencia a personas vulnerables?

- ○ Visual
- ○ Registro de Ingreso
- ○ Ninguno

Pregunta 5: ¿Alguna vez intentaron ingresar personas externas para acceder a los beneficios de la organización ADRA en su presencia?

- ○ Si

- ○ No

Pregunta 6: ¿Cree usted que, con la implementación de un sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad, la organización ADRA mejore el control de acceso a personas que no pertenecen a los grupos vulnerables en la ciudad de Tulcán?

- ○ Si
- ○ No

Anexo 4.

ENCUESTA DIRIGIDA AL PERSONAL EVALUADOR DEL SISTEMA

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

Seguridad con reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial:

Evaluación y Concientización

Esta encuesta está diseñada para evaluar la efectividad de las medidas de seguridad de acceso implementando Reconocimiento Facial y técnicas de Inteligencia Artificial de la empresa ADRA. Nuestro objetivo es comprender la perspectiva y el nivel de conocimiento de los colaboradores de la empresa en relación con la seguridad de acceso a las instalaciones dedicadas a la prestación de ayudas comunitarias a la población vulnerable. Buscamos obtener información valiosa sobre el conocimiento de amenazas en seguridad de acceso y las medidas de seguridad implementadas en accesos donde pasa la población.

Lea detenidamente las preguntas y escoja la alternativa que usted considere conveniente.

Consentimiento informado: Acepta participar en la investigación descrita de forma libre y voluntaria. Su participación puede ser suspendida en cualquier momento, sin que esto traiga ningún tipo de consecuencias negativas para usted o la institución. Este estudio no presenta riesgos identificables para su integridad física o psicológica.

Los datos solicitados para la aplicación de este cuestionario son anónimos y serán manejados bajo absoluta confidencialidad. Estos datos estarán guardados en archivo electrónico, codificados con clave de acceso y custodiados por el Investigador responsable.

Ante cualquier duda, puede comunicarse con el responsable de esta investigación, Ing., Jefferson Cárdenas, mediante correo electrónico ejcardenasa@utn.edu.ec.

- ○ Si
- ○ No

Pregunta 1: ¿Qué opina del carácter tecnológico - científico del desarrollo del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador?

- ○ Muy satisfactorio
- ○ Satisfactorio
- ○ Poco satisfactorio
- ○ No Satisfactorio

Pregunta 2: ¿Qué opina de la efectividad de la Estructura Metodológica del desarrollo del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador?

- ○ Muy satisfactorio
- ○ Satisfactorio
- ○ Poco satisfactorio
- ○ No Satisfactorio

Pregunta 3: ¿Qué opina de la novedad del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador?

- ○ Muy satisfactorio
- ○ Satisfactorio
- ○ Poco satisfactorio
- ○ No Satisfactorio

Pregunta 4: ¿Qué opina de la viabilidad para la aplicación práctica del desarrollo del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador?

- ○ Muy satisfactorio
- ○ Satisfactorio
- ○ Poco satisfactorio
- ○ No Satisfactorio

Pregunta 5: ¿Qué opina de la calidad y actualidad del sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador?

- ○ Muy satisfactorio
- ○ Satisfactorio
- ○ Poco satisfactorio
- ○ No Satisfactorio

Anexo 5.

VALIDACIÓN DE INSTRUMENTO DE INVESTIGACIÓN

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN (CUESTIONARIO - ENCUESTA)

Proyecto:	CREACIÓN DE UN SISTEMA DE SEGURIDAD DE RECONOCIMIENTO FACIAL 3D UTILIZANDO TÉCNICAS DE INTELIGENCIA ARTIFICIAL PARA EVITAR LA SUPLANTACIÓN DE IDENTIDAD EN LA ORGANIZACIÓN ADRA ECUADOR
Autor:	Edwin Jefferson Cárdenas Argoti
Objetivo:	Implementar un sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios.

Fecha de envío para la evaluación del experto:	12 de julio de 2024
Fecha de revisión del experto:	20 de julio de 2024

En la siguiente matriz marque con una X el criterio de evaluación según corresponda en cada ítem. De ser necesario realice la observación en el apartado correspondiente.

INSTRUMENTO DE EVALUACIÓN CUALITATIVO			
ITEMS	**CRITERIOS DE EVALUACIÓN**		
	MUCHO	**POCO**	**NADA**
Instrucción breve, clara y completa.	X		
Formulación clara de cada pregunta.	X		
Comprensión de cada pregunta.	X		
Coherencia de las preguntas en relación con el objetivo.	X		
Relevancia del contenido	X		
Orden y secuencia de las preguntas	X		
Número de preguntas óptimo	X		

Observaciones:

_____
_____
_____

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

A continuación, marque con una X en el criterio de evaluación según el análisis de cada pregunta que conforma el cuestionario, las cuales se encuentran representadas en el siguiente instrumento de evaluación como ítem. De ser necesario realice la observación en el casillero correspondiente.

INSTRUMENTO DE EVALUACIÓN CUANTITATIVO				
CRITERIOS DE EVALUACIÓN				**OBSERVACIONES**
Ítem	**Dejar**	**Modificar**	**Eliminar**	
1	X			
2	X			
3	X			
4	X			
5	X			

.....

Firma del Evaluador
C.C.: 0401288139

Apellidos y nombres completos	Becerra Auz Fernanda Jackeline
Título académico	Magister en Evaluación y Auditoria de Sistemas Tecnológicos
Institución de Educación Superior	Escuela de las Fuerzas Armadas
Correo electrónico	ferjack1985@yahoo.com
Teléfono	062985175

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN (CUESTIONARIO - ENCUESTA)

Proyecto:	CREACIÓN DE UN SISTEMA DE SEGURIDAD DE RECONOCIMIENTO FACIAL 3D UTILIZANDO TÉCNICAS DE INTELIGENCIA ARTIFICIAL PARA EVITAR LA SUPLANTACIÓN DE IDENTIDAD EN LA ORGANIZACIÓN ADRA ECUADOR
Autor:	Edwin Jefferson Cárdenas Argoti
Objetivo:	Implementar un sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios.

Fecha de envío para la evaluación del experto:	12 de julio de 2024
Fecha de revisión del experto:	18 de julio de 2024

En la siguiente matriz marque con una X el criterio de evaluación según corresponda en cada ítem. De ser necesario realice la observación en el apartado correspondiente.

INSTRUMENTO DE EVALUACIÓN CUALITATIVO			
ITEMS	**CRITERIOS DE EVALUACIÓN**		
	MUCHO	**POCO**	**NADA**
Instrucción breve, clara y completa.	X		
Formulación clara de cada pregunta.	X		
Comprensión de cada pregunta.	X		
Coherencia de las preguntas en relación con el objetivo.	X		
Relevancia del contenido	X		
Orden y secuencia de las preguntas	X		
Número de preguntas óptimo	X		

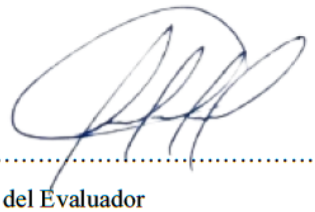
Observaciones:

_____
_____
_____

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

A continuación, marque con una X en el criterio de evaluación según el análisis de cada pregunta que conforma el cuestionario, las cuales se encuentran representadas en el siguiente instrumento de evaluación como ítem. De ser necesario realice la observación en el casillero correspondiente.

INSTRUMENTO DE EVALUACIÓN CUANTITATIVO				
CRITERIOS DE EVALUACIÓN				OBSERVACIONES
Ítem	Dejar	Modificar	Eliminar	
1	X			
2	X			
3	X			
4	X			
5	X			



.....

Firma del Evaluador
C.C.: 1002140729

Apellidos y nombres completos	Carrera Pozo Oscar Freed
Título académico	Magister en Gerencia Informática
Institución de Educación Superior	Pontificia Universidad Católica del Ecuador
Correo electrónico	oscarcarr1971@hotmail.com
Teléfono	0968975081

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN (CUESTIONARIO - ENCUESTA)

Proyecto:	CREACIÓN DE UN SISTEMA DE SEGURIDAD DE RECONOCIMIENTO FACIAL 3D UTILIZANDO TÉCNICAS DE INTELIGENCIA ARTIFICIAL PARA EVITAR LA SUPLANTACIÓN DE IDENTIDAD EN LA ORGANIZACIÓN ADRA ECUADOR
Autor:	Edwin Jefferson Cárdenas Argoti
Objetivo:	Implementar un sistema de seguridad informático de reconocimiento facial 3D utilizando técnicas de Inteligencia Artificial para evitar la suplantación de identidad en la Organización ADRA Ecuador aplicado al control y registro del personal y usuarios beneficiarios.

Fecha de envío para la evaluación del experto:	12 de julio de 2024
Fecha de revisión del experto:	20 de julio de 2024

En la siguiente matriz marque con una X el criterio de evaluación según corresponda en cada ítem. De ser necesario realice la observación en el apartado correspondiente.

INSTRUMENTO DE EVALUACIÓN CUALITATIVO			
ITEMS	**CRITERIOS DE EVALUACIÓN**		
	MUCHO	**POCO**	**NADA**
Instrucción breve, clara y completa.	X		
Formulación clara de cada pregunta.	X		
Comprensión de cada pregunta.	X		
Coherencia de las preguntas en relación con el objetivo.	X		
Relevancia del contenido	X		
Orden y secuencia de las preguntas	X		
Número de preguntas óptimo	X		

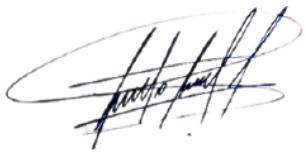
Observaciones:

_____
_____
_____

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

A continuación, marque con una X en el criterio de evaluación según el análisis de cada pregunta que conforma el cuestionario, las cuales se encuentran representadas en el siguiente instrumento de evaluación como ítem. De ser necesario realice la observación en el casillero correspondiente.

INSTRUMENTO DE EVALUACIÓN CUANTITATIVO				
CRITERIOS DE EVALUACIÓN				OBSERVACIONES
Ítem	Dejar	Modificar	Eliminar	
1	X			
2	X			
3	X			
4	X			
5	X			



.....

Firma del Evaluador
C.C.: 0401592514

Apellidos y nombres completos	Cabascango Andrés
Título académico	Ingeniero en Sistemas e Informática
Institución de Educación Superior	Universidad Regional Autónoma de los Andes
Correo electrónico	cabas.andres001@gmail.com
Teléfono	0998281689