

Universidad Autónoma del Caribe

Facultad de Ingeniería

Programa de Ingeniería Electrónica y Telecomunicaciones



**Implementación de un sistema de seguridad con detección facial para la empresa**

**Publimoda del Caribe.**

Liván José Borrero Castro

Brainer Gómez Deluque

Colombia, Barranquilla

2021

Implementación de un sistema de seguridad con detección facial para la empresa Publimoda del  
Caribe.

Liván José Borrero Castro

Brainer Gómez Deluque

Trabajo de grado presentado para optar el título de Ingeniero Electrónico y en  
Telecomunicaciones

Director

Ing. Evert De Los Ríos Trujillo

Co-Director

Ing. Saling Pallares Escorcía

Universidad Autónoma del Caribe

Facultad de Ingeniería

Programa de Ingeniería Electrónica y Telecomunicaciones

Colombia, Barranquilla

2021

## Resumen

Este trabajo de grado presentó la implementación de un sistema de seguridad por reconocimiento facial que permitirá llevar un registro detallado del ingreso diario de personas a la empresa, teniendo en cuenta aspectos como la inseguridad ya que esta problemática afecta día a día a gran parte de la población, lo que hace necesario desarrollar alternativas de seguridad que permita alcanzar un estado de confort que brinde un bienestar a clientes y trabajadores de la empresa.

La seguridad en cualquier sitio es de vital importancia, por ello se buscan alternativas viables en las que prevalezca la solución frente a cualquier tipo de inseguridad que se pueda presentar. En el desarrollo de este proyecto se plantea la manera de combinar seguridad y accesibilidad de manera controlada a las instalaciones de una empresa, es por esto que se implementó un sistema de seguridad con detección facial, el cual captura, reconoce y registra todo tipo de movimiento que suceda al alrededor del espacio donde se encuentra la cámara de alta resolución y, a su vez, permite controlar el acceso para que ingresen funcionarios de la empresa o personas registradas en la base de datos, todo lo anteriormente mencionado es posible gracias a un algoritmo de visión artificial que posee el software del XVR a utilizar. Una investigación aplicada busca estrategias para generación de conocimientos y así lograr un objetivo, por lo cual esta fue la que se utilizó en la metodología del presente proyecto, dando como resultado un sistema eficaz en comparación de rostros con buena fiabilidad sin dejar atrás la seguridad que este sistema le otorga en general a la empresa.

### **Abstract**

This degree project presented the implementation of a facial recognition security system that will allow a detailed record of the daily entry of people to the company, taking into account aspects such as insecurity since this problem affects a large part of the company day by day. population, which makes it necessary to develop security alternatives that allow reaching a state of comfort that provides well-being to customers and company workers.

Security in any place is of vital importance, for this reason viable alternatives are sought in which the solution prevails against any type of insecurity that may arise. In the development of this project, the way to combine security and accessibility in a controlled way to the facilities of a company is proposed, which is why a security system with facial detection was implemented, which captures, recognizes and records all types of movement that happens around the space where the high-resolution camera is located and, in turn, allows controlling access for company officials or people registered in the database, all of the aforementioned is possible thanks to an algorithm vision machine that has the XVR software to use. An applied research seeks strategies to generate knowledge and thus achieve an objective, for which this was the one used in the methodology of this project, resulting in an effective system in comparison of faces with good reliability without leaving behind the security that this system generally grants the company.

Nota de Aceptación

---

---

---

---

Presidente del Jurado

---

Jurado

---

Jurado

Barranquilla, 25 de junio de 2021

### **Dedicatoria**

A Dios, por darnos la oportunidad de vivir esta maravillosa etapa y por estar con nosotros en cada paso que damos, por fortalecer nuestros corazones e iluminarnos, y por haber puesto en el camino a aquellas personas que han sido parte de nuestro proceso durante todo el periodo de estudio.

A nuestros padres, por ser pilar fundamental en todo lo que somos, en toda nuestra educación, por su incondicional amor y apoyo. Todo este trabajo ha sido posible gracias a ellos.

## **Agradecimientos**

El desarrollo de este proyecto no puedo catalogarlo como algo fácil, lo que puedo es afirmar que durante todo este tiempo pude disfrutar de cada momento, de cada investigación y procesos que se realizaron en éste. Lo disfruté mucho y sobre todo el trabajar con mi compañero de proyecto.

Agradezco a Dios por haberme acompañado y guiado a lo largo de mi carrera universitaria, por ser mi fortaleza en los momentos de debilidad y por brindarme una vida llena de aprendizajes y experiencias. Gracias por estar presente no sólo en esta etapa tan importante en mi vida, sino todo momento ofreciéndome y buscando lo mejor para mí.

A mis padres, por ser un pilar fundamental en todo lo que soy, por sus consejos y su motivación constante. Ambos han servido como inspiración para seguir adelante, consolidar mis metas y forjar un destino del que estaré orgulloso. Mis logros siempre serán de ellos.

A mi hermana, por estar presente en los grandes y pequeños momentos de mi vida.

A mis demás familiares, quienes de una u otra forma contribuyeron en hacer realidad esta meta y en ningún momento dudaron de mis capacidades.

Al Ing. Saling Pallares porque con su esmero, dedicación y orientación colaboró significativamente en este proyecto.

A todos mis compañeros por haber hecho de mi etapa universitaria u trayecto de vivencias que nunca olvidaré.

A mis demás profesores por impulsar y contribuir al desarrollo de mi formación profesional.

**Brainer Gómez Deluque**

Agradezco a Dios primeramente porque sin su ayuda y sin su guía no hubiese sido posible esta culminación con éxito, por darme fortaleza para continuar y nunca desistir en este proceso.

A mis padres por su motivación para que pudiese ser lo que hoy soy. Les dedico todo mi esfuerzo en reconocimiento del sacrificio que han hecho a lo largo de mi formación académica. Resalto su apoyo en los momentos de duda, desesperación y felicidad.

A mis hermanos por ser mi motivación para salir adelante y mi ejemplo a seguir.

A mi familia ya que cada uno aportó un granito en mi formación.

Al Ing. Saling Pallares porque con su esmero, dedicación y orientación colaboró significativamente en este proyecto.

A mis profesores por contribuir en mi formación como profesional.

A mis compañeros de estudio por acompañarme durante esta etapa de mi vida.

**Liván José Borrero Castro**



## Contenido

Resumen.....	3
Abstract.....	4
Introducción .....	15
Capítulo 1 Descripción del Proyecto .....	17
Planteamiento del Problema .....	17
Formulación del Problema.....	18
Impacto Esperado.....	19
Usuarios Directos e Indirectos .....	19
Objetivos.....	19
Objetivo General.....	19
Objetivos Específicos.....	19
Metodología .....	20
Etapas .....	20
Recopilación de la información .....	20
Selección de la tecnología adecuada.....	21
Implementación, instalación y configuración del sistema de detección facial .....	22
Materiales y Equipos Utilizados .....	25
Capítulo 2 Marco Teórico y Estado del Arte .....	28
Inteligencia artificial .....	28

	10
Cámara digital.....	29
Tipos de cámaras.....	30
Cámara infrarroja.....	30
Cámara de interiores.....	30
Cámaras antirrobo.....	30
Cámaras IP.....	30
Cámaras con movimiento y zoom.....	30
Cámaras ocultas.....	30
Instalación de cámara para reconocimiento facial.....	30
Procesamiento de imágenes.....	31
Control de acceso.....	33
Tipos de control de acceso.....	34
Sistemas de control de acceso autónomos.....	34
Sistemas de control de acceso en red.....	35
Métodos de verificación para el control de acceso.....	36
Verificación de dígitos.....	36
RFiD.....	36
Biometría.....	37
Talanqueras o torniquetes.....	37
Reconocimiento ocular.....	38

	11
Reconocimiento por huella dactilar .....	39
Reconocimiento facial .....	39
Fases de un reconocimiento facial .....	41
Detección del rostro .....	41
Plantilla .....	42
Bootstrap.....	42
AdaBoost.....	42
Extracción de características.....	43
Reconocimiento .....	44
XVR .....	44
Capítulo 3 Análisis de Resultados y Propuesta Ingenieril .....	49
Capítulo 4 Conclusiones .....	61
Capítulo 5 Recomendaciones.....	63
Bibliografía .....	64
Anexos .....	68

**Lista de Figuras**

<b>Figura 1.</b> .....	23
<b>Figura 2.</b> .....	23
<b>Figura 3.</b> .....	24
<b>Figura 4.</b> .....	24
<b>Figura 5.</b> .....	25
<b>Figura 6.</b> .....	25
<b>Figura 7.</b> .....	25
<b>Figura 8.</b> .....	26
<b>Figura 9.</b> .....	26
<b>Figura 10.</b> .....	27
<b>Figura 11.</b> .....	31
<b>Figura 12.</b> .....	31
<b>Figura 13.</b> .....	35
<b>Figura 14.</b> .....	36
<b>Figura 15.</b> .....	37
<b>Figura 16.</b> .....	38
<b>Figura 17.</b> .....	39
<b>Figura 18.</b> .....	40
<b>Figura 19.</b> .....	41
<b>Figura 20.</b> .....	45
<b>Figura 21.</b> .....	50
<b>Figura 22.</b> .....	50

<b>Figura 23.</b> .....	51
<b>Figura 24.</b> .....	52
<b>Figura 25.</b> .....	53
<b>Figura 26.</b> .....	54
<b>Figura 27.</b> .....	54
<b>Figura 28.</b> .....	55
<b>Figura 29.</b> .....	56
<b>Figura 30.</b> .....	57
<b>Figura 31.</b> .....	57
<b>Figura 32.</b> .....	58
<b>Figura 33.</b> .....	59
<b>Figura 34.</b> .....	60
<b>Figura 35.</b> .....	60

## Lista de Anexos

Anexo 1. Manual de usuario XVR DH-XVR5116H-4KL-I2.....	68
Anexo 2. Guía de inicio rápido 1 (XVR).....	68
Anexo 3. Guía de inicio rápido 2 (XVR).....	68
Anexo 4. Datasheet XVR.....	68
Anexo 5. Datasheet camara DH-HAC-HDW1801EM/EM-A.....	68
Anexo 6. Manual de usuario ARB1606.....	68
Anexo 7. Datasheet ARB1606.....	68

## Introducción

El reconocimiento facial se ha desarrollado con rapidez. Desde que Alphonse Bertillon en 1883 sentara las bases del sistema de reconocimiento facial, pues usaban como base un sin número de medidas antropométricas como: la distancia de los ojos, la simetría o los diferentes rasgos faciales de un individuo. Se puede decir que el reconocimiento facial es una herramienta muy importante en el medio en tanto que permite identificar a través de ciertas características a un individuo. Los avances parten desde el estudio de la biometría, y esta sumada a la tecnología, da como resultado la toma de medidas y el análisis de datos biológicos como el ADN, la huella de la mano, el iris y la voz (labores biométricas). Así nacen los sistemas de reconocimiento facial, que toma sus decisiones de identificación con la ayuda de las características personales (fotografías y videos) de cada persona y plasmándolo en una imagen digital los mismos que pueden ser reconocidas o verificadas de forma automatizada mediante un ordenador.

Principalmente el sistema de seguridad con detección facial se implementa para añadirle un nivel de seguridad adicional a la empresa, como sabemos los sistemas de videovigilancias por circuito cerrado sólo capturan y almacenan imágenes de lo que pasa a diario en donde está ubicada la cámara, más no permite tener una gestión para identificar plenamente los rostros que pasen por la zona de captura de la cámara, motivo por el cual nos incentivamos a implementarlo con reconocimiento facial, para así poder registrar y gestionar una acción dependiendo de lo que se desee, por ejemplo, emitir un sonido a través de un zumbador que indicará que la cámara capturó un rostro registrado en la base de datos, o accionar un actuador, el cual permita desbloquear la puerta para así permitir el paso de la persona que acaba de ser detectada en caso de que esta persona no se encuentre registrada.

Como sabemos los DVR convencionales son dispositivos de grabación de video en formato digital (Digital Video Recorder, por sus siglas en ingles) que son los encargados de digitalizar imágenes y en algunas ocasiones audios, que nos proporciona una cámara de seguridad. Pero para este sistema se optó por un XVR que es un DVR Penta-hibrido que soporta 5 tecnologías distintas, HDCVI, AHD, TVI, CVBS, IP, en este caso se usó la tecnología HDCVI porque ofrece resoluciones en el rango de la alta definición.



## Capítulo 1

### Descripción del Proyecto

#### Planteamiento del Problema

En Colombia el desarrollo tecnológico va en aumento dado que las empresas avanzan para automatizar cada aspecto de ellas, desde la fabricación de algún objeto, el uso eficiente de energía, hasta la seguridad de la misma empresa. El control de ingreso a las instalaciones de las empresas para empleados y visitantes resulta ser crucial en aspectos como la seguridad, puesto que es necesario verificar la identidad de cada persona para garantizar que ningún intruso ingrese a las instalaciones de esta, de tal forma que se puedan evitar riesgos de seguridad; adicionalmente es importante para llevar registro y control de los horarios de ingreso y salida de empleados y visitantes. Esto hace que varios sectores se apropien de esta tecnología y quieran invertir en este aspecto de modernización ya que los beneficios son bastantes buenos para la industria y las grandes necesidades que esta cubre. Por esta razón se ve mucho más frecuente la necesidad de desarrollar tecnologías de automatización en un ámbito de propiedad privada siendo esto necesario para generar confort y seguridad, sin embargo, éste no es muy común ya que las personas no tienen conocimiento de los beneficios que se pueden obtener.

“Que Colombia sea el país más conflictivo de Latinoamérica se debe a la inseguridad ciudadana. Así lo afirman las conclusiones del Índice de Paz elaborado por el Institute for Economics and Peace, que analiza 162 Estados y encuentra que Colombia obtiene el puesto 150, lo que le deja más atrás que México (138), Venezuela (129), Perú (119), Brasil (91) o Chile (30).

Son cuatro escalones de descenso para Colombia con respecto al anterior ranking, y en el resultado pesó especialmente el sector sociedad y seguridad, que obtiene una puntuación de 3,4 sobre 5.” (Cynthia de Benito, Editorial La República S.A.S, 2014).

En la actualidad las empresas utilizan mecanismos tales como tarjetas de acceso, biometría dactilar o vigilancia física con personal; no obstante estos mecanismos presentan algunas falencias tales como la fácil suplantación a través de identidad con documentos falsos o extraviados, para el caso de vigilancia física con personal, o el ingreso de personas que por alguna u otra razón tengan en su poder tarjetas de acceso para los casos en los que este sea el mecanismo de verificación de identidad. Si esta situación se mantiene permanecerán latentes los riesgos derivados de mecanismos de verificación de identidad tradicionales, y un problema común de las empresas es no tener un registro detallado y un control del personal que está ingresando día a día a sus instalaciones y esto puede afectar en el caso de ser víctima de algún acto delincuenciales porque no sería posible identificar a plenitud el culpable, por ello, se planteó implementar un sistema por reconocimiento facial con tecnología de la más alta definición para obtener una imagen mucho más real capaz de capturar hasta el más mínimo detalle facilitando y garantizando la identificación de la persona dado que la inseguridad es uno de los problemas más recurrentes en la ciudad, y también porque hoy en día es el sistema más apropiado de biometría debido a que a diferencia de la huella dactilar no es necesario tener contacto con el dispositivo, teniendo en cuenta que la huella dactilar no cumple con estándares de bioseguridad con respecto a la emergencia sanitaria que atraviesa el mundo.

### **Formulación del Problema**

¿Cómo implementar un sistema de seguridad con detección facial en la empresa Publimoda del Caribe?

## **Impacto Esperado**

La empresa Publimoda del Caribe solicita un sistema de seguridad con detección facial debido a que actualmente no cuenta con un sistema de seguridad que le permita llevar un registro y control detallado de las personas que ingresan al establecimiento.

Por tal motivo, es necesaria la implementación de un sistema de seguridad con detección facial que permite gestionar y supervisar el ingreso de personas a la empresa. Dicha implementación es realizada por los autores del proyecto haciendo uso de un XVR de la marca Dahua DH-XVR5116H-4KL-I2 que cuenta con un software de reconocimiento facial por medio de un algoritmo de visión artificial.

## **Usuarios Directos e Indirectos**

Empleados y clientes de la empresa.

## **Objetivos**

### **Objetivo General**

- Implementar un sistema de seguridad mediante identificación por reconocimiento facial, para la gestión de acceso de la empresa Publimoda del Caribe.

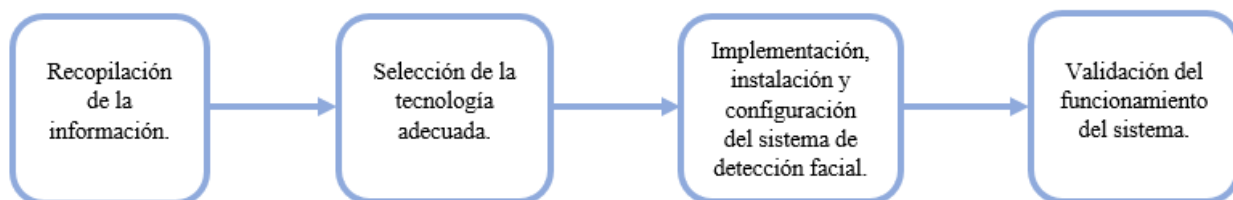
### **Objetivos Específicos**

- Seleccionar la tecnología y equipos que permitan gestionar y supervisar el acceso a la empresa.
- Instalar el sistema seleccionado acorde a la tecnología establecida.

- Configurar los parámetros que permitan llevar a cabo las condiciones necesarias para el control de acceso.
- Realizar pruebas de funcionalidad para la validación del sistema implementado.

## Metodología

El tipo de metodología más adecuada a desarrollar es una investigación aplicada, ya que esta se enfoca en encontrar estrategias para lograr un objetivo concreto como conseguir elementos que puedan ser de utilidad. La investigación aplicada busca la generación de conocimiento con aplicación directa a los problemas de la sociedad o el sector productivo. Esta se basa fundamentalmente en los hallazgos tecnológicos de la investigación básica, ocupándose del proceso de enlace entre la teoría y el producto.



**Fuente:** Autores

## Etapas

### Recopilación de la información

Se recopila información sobre técnicas de reconocimiento facial. Para esto se realiza una investigación avanzada en internet con respecto a tecnologías existentes y sus aplicaciones.

Además, se hizo un estudio de los mecanismos del acceso en la empresa donde se tuvo en cuenta:

- Mecanismos.
- Fiabilidad.

- Confort.
- Costos.

### **Selección de la tecnología adecuada**

Se realizó un análisis de las características de cada tecnología utilizada para el reconocimiento facial y el almacenamiento de la imagen capturada.

Se hizo un estudio previo del dispositivo ideal para la implementación que deseamos realizar de reconocimiento facial. Para esto se realizaron comparaciones de los dispositivos disponibles en el mercado los cuales en primera parte deben contar con un software que permita desarrollar las funciones de seguridad que se buscan en el proyecto y una cámara que brinde la mayor precisión para el respectivo análisis de imagen en el sistema por lo que debe ser una con la más alta resolución posible.

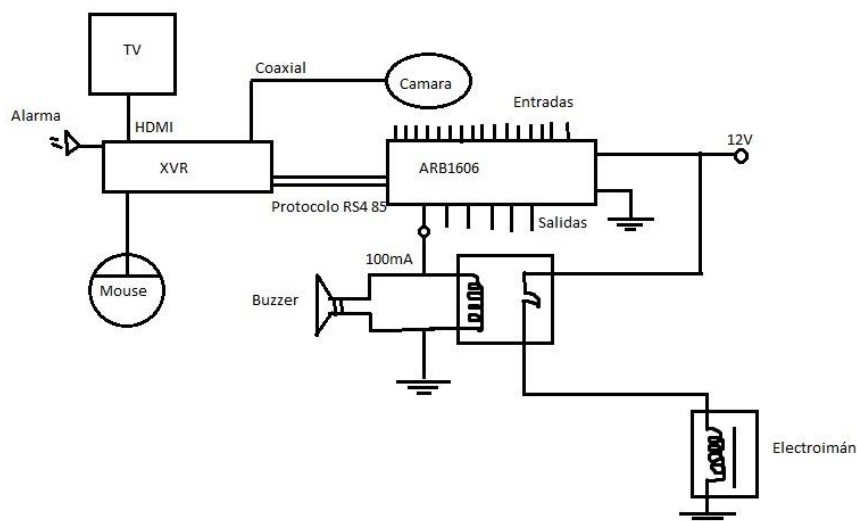
Para escoger la tecnología utilizada se tuvo en cuenta varios aspectos con respecto a las tecnologías ya existentes e implementadas, la principal es que esta tecnología del XVR permite controlar el acceso, a diferencia de otras encontradas en la industria que simplemente hacen una comparación facial del rostro de la persona detectada y muestra en pantalla sus datos, esta tecnología además de hacer eso, es capaz de restringir el ingreso de una persona desconocida, es decir, que no se encuentra en su base de datos, y también de permitir el ingreso a una persona que ya se encuentre registrada, teniendo para ambos casos un sistema de alarma que varía en su sonido de acuerdo a si el ingreso es permitido o denegado. Por otro lado, el XVR es una tecnología DVR pero mejorada, teniendo la capacidad de capturar y almacenar video en tiempo real y a su vez reconociendo permanentemente el rostro de la persona sin omitir ningún detalle, siendo esto posible gracias al algoritmo de visión artificial que este posee capaz de identificar

todos esos detalles y también que por ser penta-híbrido (posee 5 tecnologías) es que resulta posible utilizar en el proyecto la tecnología HDCVI en la que se puede agregar una cámara de la más alta resolución que existe actualmente (4k) que realiza comparaciones mucho más precisas que el de una cámara de cualquier otra resolución, evitando así que el sistema presente falsos positivos, logrando una efectividad del 95%.

### **Implementación, instalación y configuración del sistema de detección facial**

Se llevó a cabo la conexión física sistema, cuenta con una cámara digital de alta resolución (4K) alimentada con 12V, cableada con cable coaxial porque viaja a través de él video, audio y datos simultáneamente brindando validez y fiabilidad al momento de hacer la comparación de rostros en la base de datos, el XVR Dahua DH-XVR5116H-4KL-I2 que se encarga de capturar, registrar y validar los rostros detectados por la cámara haciendo uso de la base de datos al momento de identificar un rostro y a su vez conectado con un electroimán que se encarga de activar la puerta para permitir el ingreso, un módulo ARB1606 de 16 entradas y 6 salidas digitales de 12 voltios que se encargará de energizar un relé normalmente cerrado y el relé des energizará el electroimán porque el hecho de que esté normalmente cerrado indica que el electroimán permanentemente está energizado, su consumo es de 3 amperios a 12 voltios, también se conecta un pulsador que permita activar la puerta para la salida.

**Figura 1.**  
*Diseño de conexión del sistema*



Utilizando el mismo módulo ARB1606 permite configurar una alarma en la interfaz de entrada y salida cuando se establece la comunicación entre el XVR y el módulo.

Se realizó la configuración de los dispositivos anteriormente mencionados.

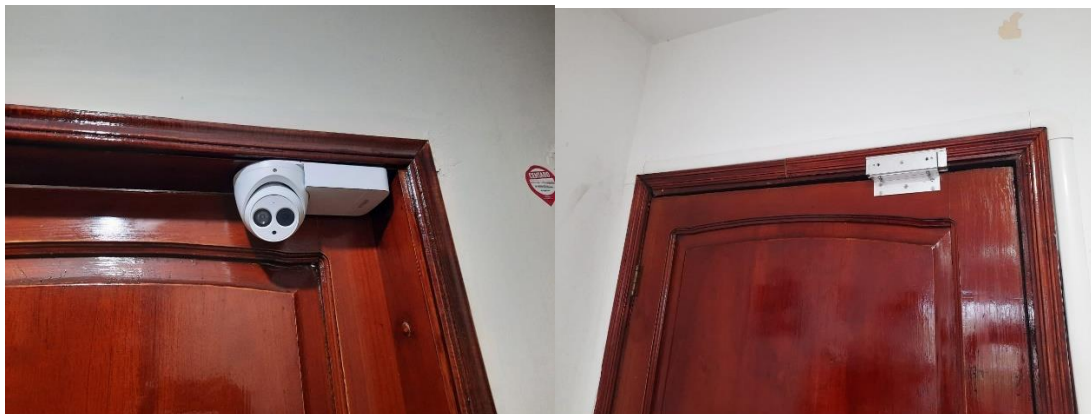
Se hizo pruebas de eficiencia y funcionalidad del sistema de reconocimiento facial y la alarma configurada.

**Figura 2.**  
*Conexión física del sistema*



**Figura 3.**

*Conexión cámara digital y electroimán*

**Figura 4.**

*Pulsador de salida*





## Materiales y Equipos Utilizados

### Figura 5.

*XVR Penta híbrido 16 canales, referencia DH-XVR5116H-4KL-I2 marca Dahua.*



*Nota:* Fuente: Datasheet XVR

### Figura 6.

*Cámara digital AHC-HDW1801EMN-A-0360B*



*Nota:* Fuente: Datasheet camara DH-HAC-HDW1801EM/EM-A

### Figura 7.

*Electroimán LM1802 imán de 350 libras a 12voltios.*



*Nota:* Fuente: Adaptado de GVS Colombia

<https://www.gvscolombia.com/producto/LM1802>

**Figura 8.**

*Disco duro especial para XVR capacidad 1TB.*



*Nota:* Fuente: <https://www.powercomputer.net.co/es/discos-duros-internos/1750-disco-duro-1-tb-western-digital-purple-especial-para-dvr.html>

**Figura 9.**

*Módulo de entradas y salidas digitales. ARB1606.*



*Nota:* Fuente: DHI-ARB1606\_Datasheet\_20180413

**Figura 10.**

*Relé térmico*



*Nota:* Fuente: Adaptado de Electrocrea <https://electrocrea.com/products/relevador-12v-10a-de-1-polo-2-tiros>

## Capítulo 2

### Marco Teórico y Estado del Arte

Debido a que el proyecto de grado se centra en la implementación de un sistema de seguridad con detección facial, resulta indispensable definir algunos conceptos que son necesarios para el desarrollo del proyecto.

#### **Inteligencia artificial**

Para IBERDROLA, la Inteligencia Artificial (IA) es la combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano. Una tecnología que todavía nos resulta lejana y misteriosa, pero que desde hace unos años está presente en nuestro día a día a todas horas.

Es probablemente la disciplina técnico-científica con más potencial de los últimos años, la que plantea una revolución sin parangón en nuestro mundo. Andrew Ng, uno de las personalidades más conocidas en este ámbito, la llama "la electricidad del siglo XXI". Y sin embargo es difícil dar una definición concisa y clara de qué es la inteligencia artificial.

Para Alan Turing la inteligencia artificial lo da como un ejemplo, en 1950 publicó un artículo llamado Computing machinery and intelligence, donde argumento en esta época que desde que una máquina de computación pueda actuar como un ser humano se le puede denominar un objeto inteligente. Este planteó un test donde se encierra a una persona en una habitación y a una máquina en otra donde no la puede ver el ser humano, si la persona no reconoce si es una máquina o un ser humano, en caso de ser una máquina se puede considerar inteligente, teniendo por referencia este test o prueba, el objeto que realice esta prueba y la apruebe, tiene las siguientes capacidades o características.

- Aprendizaje.

- Representación de conocimiento.
- Razonamiento.
- Reconocimiento del lenguaje natural.

(García, 2012)

### **Cámara digital**

Una cámara digital es una cámara de fotos que apela a un sensor electrónico para digitalizar las imágenes y guardarlas en una memoria. Esto diferencia a estas cámaras de las cámaras fotográficas analógicas.

Las primeras cámaras de fotos recurrían a un proceso fisicoquímico para registrar las imágenes. Las mismas eran grabadas en un rollo o carrete que luego debía someterse a una acción conocida como revelado, que permitía plasmar las fotos en un papel.

Las cámaras digitales, en cambio, guardan las fotos como datos digitales en una memoria. El usuario tiene la posibilidad de almacenar las imágenes en la misma cámara o de guardarlas en diferentes equipos digitales: una computadora (ordenador), una memoria USB, etc. De todas formas, es posible imprimir las fotos para tenerlas en papel.

Por lo general las cámaras digitales permiten registrar no solo fotos, sino también videos y sonidos. La calidad de los documentos generados suele medirse de acuerdo a la cantidad de píxeles, aunque hay otros factores que deben tenerse en cuenta (como la sensibilidad y el tamaño del sensor). (Pérez, Merino, 2016).

## **Tipos de cámaras**

**Cámara infrarroja:** Esta es perfecta para lugares oscuros y aplica para la vigilancia las 24 horas al día, de forma automática enciende el infrarrojo en el momento que hay menos luminosidad.

**Cámara de interiores:** Se trata de las cámaras caseras, estas no necesitan de grandes características en cuanto a la luminosidad (nocturnas, infrarrojas, etc.), ya que permanecen en lugares iluminados.

**Cámaras antirrobo:** Este tipo de cámara por lo general está ubicado en zonas urbanas, por lo que debe tener una carcasa resistente a golpes, lluvia, calor, entre otros.

**Cámaras IP:** Estas se conectan directamente a internet para enviar o subir la información a la nube, así mismo se puede observar la imagen que esté transmitiendo mediante un dispositivo configurado con la cámara y conectado a internet.

**Cámaras con movimiento y zoom:** Se utilizan para circuitos cerrados de Tv (CCTV), donde existe una persona monitoreando la cámara y esta les realiza movimiento o zoom.

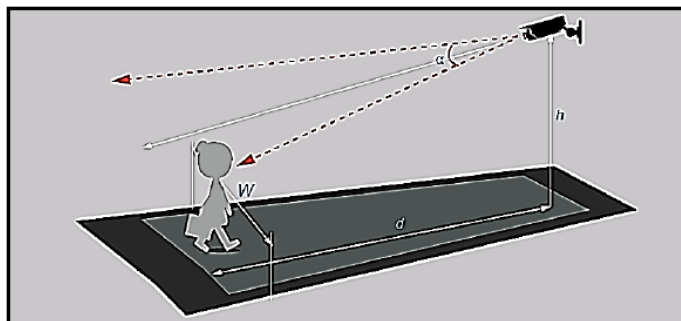
**Cámaras ocultas:** También llamadas cámaras espías, por lo general se instalan dentro de algún objeto, como; detectores de humo, sensores de movimiento, espejos, tornillos, enchufes, entre otros, de esta forma no se ven y pasan por desapercibidas.

**Instalación de cámara para reconocimiento facial:** Al momento de instalar la cámara es muy importante tener en cuenta el ángulo de inclinación que debe tener esta, para poder visualizar desde una mejor perspectiva del rostro el cual se quiere reconocer, y por otro lado evita los objetos obstructores que puede haber dentro del recinto o del pasillo.

La figura 10, ilustra la correcta posición de una cámara de seguridad teniendo en cuenta la altura y el ángulo de instalación, y esto es para que el lente logre enfocar de una manera correcta la cara de las personas. (Comunidad Huawei Enterprise, 2019).

**Figura 11.**

*Ángulos, distancias y alturas de la posición de la cámara*



*Nota:* Fuente: Comunidad Huawei Enterprise [www.huawei.com](http://www.huawei.com)

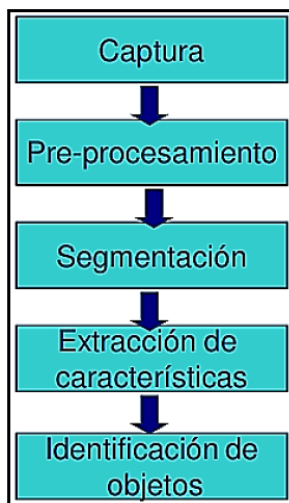
**Procesamiento de imágenes**

El procesamiento de imágenes tiene como objetivo mejorar el aspecto de las imágenes y hacer más evidentes en ellas ciertos detalles que se desean hacer notar. La imagen puede haber sido generada de muchas maneras, por ejemplo, fotográficamente, o electrónicamente, por medio de monitores de televisión. El procesamiento de las imágenes se puede en general hacer por medio de métodos ópticos, o bien por medio de métodos digitales, en una computadora.

Las imágenes tienen etapas de procesamiento las cuales se clasifican como se muestra en la figura 11, donde en primera instancia se hace la captura después pasa por un procesamiento para luego identificar los objetos captados.

**Figura 12.**

*Diagrama de bloques de las etapas del procesamiento de imágenes*



*Nota:* Fuente: Procesamiento digital de imágenes

La primera etapa llamada **captura**, es donde la cámara capta el objeto, donde depende de distintas variables como lo es la distancia del objeto o persona, la resolución de la cámara (Mpx) y las propiedades que se aplican a la cámara para esta captura de imagen.

**El pre-procesamiento**, visualiza y procesa todo el entorno de la imagen que no es de interés como lo son las interferencias de otras personas, objetos, entre otros que no son de interés para el procesamiento de la imagen.

**La segmentación**, se encarga de fraccionar, reconocer y extraer las características, objetos o interferencias que tiene la imagen en el momento que se realiza la captura.

En la **extracción de características** como lo indica, es seleccionar las características que se desean para el procesamiento de la imagen, ya sea para un software o un algoritmo.

Al momento de identificar el objeto(s) o la persona de la que se quiere extraer las características, se debe analizar mediante un algoritmo que tenga características de decisión para que tome el camino correcto para seleccionar el objeto o la persona a procesar, para luego reconocerla, este algoritmo debe estar previamente definido. (Wainschenker, 2011).



## Control de acceso

El control de acceso es un término muy usado en cuanto se refiere a la seguridad de un lugar o establecimiento, este es un componente muy importante ya que permite monitorear y controlar electrónicamente el tráfico de personas a través de objetos como puertas, ascensores, talanqueras, entradas principales etc.

Un control de acceso es un sistema automatizado que permite de forma eficaz, aprobar o negar el paso de personas o grupo de personas a zonas restringidas en función de ciertos parámetros de seguridad establecidos por una empresa, comercio, institución o cualquier otro ente. En base a esto se desarrolló una serie de soluciones basándose en la tecnología disponible en el mercado utilizando estándares y arquitecturas abiertas lo cual posiciona como referencia dentro del sector de seguridad el control de acceso.

Algunas de las características más esenciales del control de acceso son:

- Restringir el paso a sitios por horarios, puertas y usuarios.
- Controlar flujo de personas por las instalaciones de una Compañía.
- Trazabilidad (Generación de Reportes).
- Registro de tiempos y asistencia.
- Control automático de entradas y salidas de vehículos o personas.
- Control de personas dentro de una edificación.
- Permite un control exacto del personal sin necesidad de presencia de supervisores para el registro de los ingresos y salida de los empleados.
- Protección de activos, reemplazo de llaves.
- Reemplazo de guardas y personal de seguridad.

(Sisca CCTV, 2015)

## **Tipos de control de acceso**

Dado que los controles de acceso son sistemas automatizados que permite de forma eficaz, controlar el paso de personas a zonas restringidas en función de ciertos parámetros de seguridad establecidos por una empresa, establecimiento, comercio, institución o cualquier otro ente. Los controles de acceso también hacen posible llevar un registro automatizado de los movimientos de un individuo o varios dentro de un espacio determinado.<sup>21</sup>

Hay varias formas de clasificar los controles de acceso: sea por las dimensiones del espacio en el que se van a colocar o por la fuente de información que utilice el lector.

Con base a la primera opción, los controles se pueden dividir en:

1. **Sistemas complejos:** implican operaciones en red, destinados a grandes plantas industriales. Generalmente, requieren la apertura de varios controles de acceso o puertas.
2. **Sistemas para establecimientos comerciales de mediana envergadura** donde se suele necesita un control de acceso no tan robusto con la apertura de 2 a 4 puertas.
3. **Sistemas pequeños** destinados a locales de poco metraje o viviendas donde se requiera un control de acceso muy poco frecuente con la apertura de 1 o máximo 2 puertas.

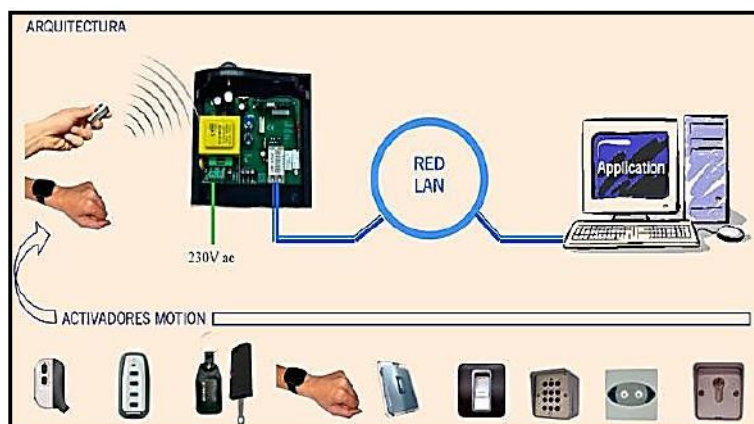
**Sistemas de control de acceso autónomos:** Estos sistemas permiten controlar una o más puertas sin estar conectados a un ordenador o sistema central, quiere decir que este tipo de control de acceso no guarda registro de entradas o salidas.

Los controles de acceso autónomos más sencillos funcionan simplemente como una llave electrónica, es decir, solo identifican a la persona y le permiten ingresar o salir de las instalaciones.

**Figura 13.***Sistemas de control de acceso autónomo*

*Nota:* Fuente: Adaptado de Vionix <https://vionix.cl/sistemas-de-control-de-acceso/>

**Sistemas de control de acceso en red:** Estos sistemas son más complejos y cuentan con más funcionalidades que los anteriores, ya que se integran a través de un ordenador con un software que permite llevar el registro de todas las personas que entran o salen del centro, se puede extraer todo tipo de datos como la hora, fecha, también se ha utilizado en identificación, entre otros que se evidencian en la figura 13. Estos sistemas de control de acceso son totalmente personalizables para cada cliente, pudiéndose realizar combinaciones complejas que ofrecen funcionalidades adaptadas a cada necesidad. (TD sistemas control y gestión, 2019)

**Figura 14.***Sistemas de control de acceso a la red*

*Nota:* Fuente: <https://images.app.goo.gl/DSqrfV2udXHTgvVG9>

### **Métodos de verificación para el control de acceso**

Para el control de acceso se utilizan un gran número de métodos para verificar que el usuario no es un impostor además de dar acceso al propietario de cualquier cosa que resguarde el control de seguridad, en el mercado existen grandes variedades de control de acceso desde los más complejos como lo son el reconocimiento por biometría hasta una talanquera o control por verificación de dígitos.

**Verificación de dígitos:** Es un método tanto físico como digital, y se usa para el control de acceso a una cerradura, compuerta, caja fuerte etc. Estos métodos por verificación de dígitos son por lo regular dispositivos con teclado los cuales se ingresa un cierto número de caracteres los cuales verifican la entrada con una clave proporcionada por el usuario principal para a continuación dar acceso a una cerradura.

**RFID:** Es un método automático de identificación el cual se basa en el almacenamiento y captura a distancia de datos usando dispositivos etiquetas o tags. Una etiqueta RFID es un dispositivo pequeño como se muestra en la figura 12, que puede ser adherida o incorporada a un producto, o a una persona como una pegatina, con el propósito de identificarlo a distancia usando ondas de radio.

Los sistemas RfID se componen básicamente de tres elementos:

**Tag RfID:** Compuesto por una antena, un transductor de radio y un chip. Los hay de diferentes tipos, principalmente se clasifican en pasivas, activas y sema-activas.

**Lector RfID:** Compuesto de antenas, un transceptor y un decodificador. El lector envía periódicamente señales para ver si hay algún tag en sus inmediaciones. Cuando capta una señal de un tag, extrae dicha información y se la pasa al sistema de procesamiento de datos.

**Sistema de procesamiento de datos:** Es una aplicación que gestiona y procesa los datos recibidos del lector RfID.

**Biometría:** Con la incorporación de estos conceptos a la tecnología se ha logrado prestar servicios de seguridad y fiabilidad para el ingreso de personal a instalaciones que así lo requieren. Un ejemplo de ello es el uso de lectores de huella dactilar en los controles de acceso.

### Figura 15.

*Método de control de acceso por biometría*



*Nota:* Fuente: <https://images.app.goo.gl/5w7XwHyoN7ccTqSd7>

**Talanqueras o torniquetes:** Es un método de control de acceso el cual permite la entrada y salida de usuarios por medio de barras perpendiculares al armazón y que tiene una separación entre barra y barra el espacio necesario para que pase una persona lo cual lo hace ideal para el control de acceso a personas identificando una por una, en la figura 15 se muestra el torniquete, este método es

muy eficiente ya que se puede acoplar en un sinnúmero de métodos como RFID, verificación de huella dactilar o verificación de dígitos etc. (Serratosa, 2017)

**Figura 16.**

*Método de control de acceso por torniquete*

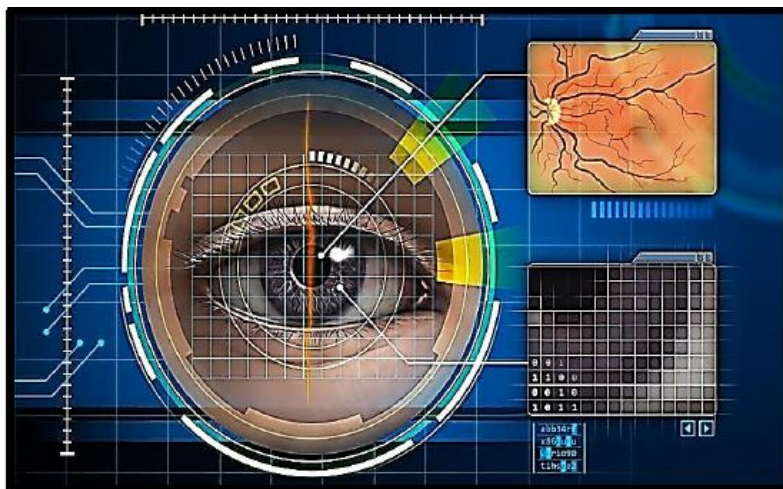


*Nota:* Fuente: <https://images.app.goo.gl/HaYvgwB6uGNSYuyj7>

**Reconocimiento ocular:** Reconocimiento de iris/retina, es uno de los sistemas de identificación más usados ya que los patrones oculares cuentan con una probabilidad de coincidencia muy cercana a cero dados a que anteriormente se almacena una imagen en una base de datos para la comparación de los patrones oculares por lo tanto es un sistema demasiado eficiente dado que los ojos son el único órgano humano que a pesar de los años nunca envejece o cambia su aspecto físico. A pesar de esto posee algunas desventajas ya que al realizar la lectura con un láser es incómodo para el usuario y además si este usa lentes se verá afectado su patrón y no podrá realizarse la identificación, a continuación, en la figura 16 se evidencian algunas características del ojo humano.

**Figura 17.**

*Método de control de acceso por reconocimiento ocular*



*Nota:* Fuente: <https://images.app.goo.gl/YhejgYcn3EEc6MVt6>

**Reconocimiento por huella dactilar:** La huella dactilar ha sido uno de los parámetros físicos para la caracterización de una persona, dada su buena eficacia para determinar la identidad de alguien ya que se ha comprobado que no existen huellas similares ni siquiera entre gemelos o entre dedos de la misma persona. El uso de estos patrones fue uno de los primeros en establecerse como modelo de autenticación biométrica. Cuando un usuario desea autenticarse ante el sistema sitúa su dedo en un área determinada. En este proyecto se toma una imagen que posteriormente se normaliza mediante un sistema de finos espejos para corregir ángulos, y es de esta imagen normalizada de la que el sistema extrae las minucias (ciertos arcos, bucles o remolinos de la huella) que va a comparar contra las que tiene en su base de datos, en la figura 16, se evidencia una huella dactilar. (Vargas, Balsero, 2016).

**Reconocimiento facial:** El reconocimiento facial es una tecnología que últimamente está siendo abarcada por varias áreas de la investigación como el análisis de imagen, extracción de características de archivos digitales etc. Esto es debido a que este proceso tecnológico puede emular la capacidad del ser humano de reconocer personas siguiendo un patrón específico ubicado en

nuestro cerebro, según la revista científica investigación y ciencia “los estudios de neuroimagen han revelado que varias regiones del tamaño de un guisante radicadas en el lóbulo temporal (la zona del cerebro situada bajo la sien) están especializadas en el reconocimiento de las caras.

Los neurocientíficos las llaman áreas faciales, estas zonas toman ciertas características faciales de la persona a reconocer como el color de la piel, tamaño de ojos, nariz y características únicas de cada persona y todo esto es un actividad semiconsciente dado que en algunas ocasiones el cerebro hace este reconocimiento sin que la persona se percate, teniendo esto en cuenta esta tecnología quiere replicar esta función siguiendo una serie de pasos como detección facial, análisis de características, comparación con base de datos.

Por otra parte, se puede definir el sistema de reconocimiento facial como una aplicación dirigida por ordenador que identifica automáticamente a una persona en una imagen digital. Esto es posible mediante un análisis de las características faciales del sujeto extraídas de la imagen o de un fotograma clave de una fuente de video, como se logra observar en la figura 17 y estas son comparadas con una base de datos.

### **Figura 18.**

*Método de control de acceso por reconocimiento facial*



*Nota:* Fuente: Adaptado de Actionsdata <https://www.actionsdata.com/blog/como-funciona-el-reconocimiento-facial>



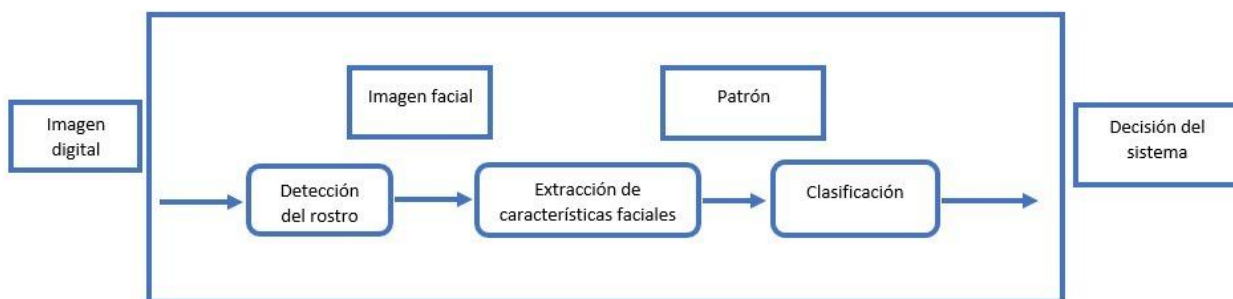
El reconocimiento facial es posible gracias a tres fases:

1. Detección del rostro.
2. Extracción de características.
3. Reconocimiento

En la figura 18 se muestra el proceso de reconocimiento facial, la cual sigue una línea donde la imagen pasa por varias fases para ser identificada.

### Figura 19.

#### *Proceso del reconocimiento facial*



### Fases de un reconocimiento facial

**Detección del rostro:** La detección de un rostro se especifica como las áreas de una imagen digital donde se aprecia el rostro de una persona, esto implica que las áreas que no contienen rostro serán descartadas, o más bien, ignorar el fondo de tal manera que se haga una silueta del rostro identificado. Para la detección de rostro existen varios métodos que resuelven este problema como el uso de plantillas.

Como solo hay que detectar caras (sin identificar sujetos específicamente) se crean patrones para zonas que representan una cara y zonas que no; generalmente la solución para encontrar patrones que no son rostros, es por medio de la modalidad denominada “bootstrap”, o el método más conocido como EigenFace.

**Plantilla:** Esta es una técnica general empleada para detectar objetos de una escena, donde es representado por formas. Para la detección de una cara este debe tomar una característica del rostro como un ojo o una nariz y se utiliza una plantilla parametrizada que representa por medio de una función de energía los cual interpreta como valles y picos, luego esta plantilla interactúa con la imagen alterando algunos parámetros Una vez ubicada la plantilla se ajustan sus parámetros para minimizar la función de energía.

**Bootstrap:** Esta técnica se basa en patrones que son rostros y se puede ver como clasificador, todos los falsos positivos se agregan como patrones de no-rostro y en una siguiente etapa, si aparecen nuevos falsos positivos, estos se siguen agregando como patrones. 29

**AdaBoost:** Es un meta-algoritmo de aprendizaje automático basado en la idea de que contar con un grupo de expertos para tomar decisiones es mejor que tener uno solo. Al grupo de expertos se le conoce como ensamble y éste representa un clasificador fuerte, es decir, un clasificador con una precisión muy buena. Por su parte, a los expertos que conforman el ensamble se les denomina clasificadores débiles, es decir, clasificadores con una precisión menor. También es denominado un algoritmo adaptativo de machine learning cuyo nombre es una abreviatura de adaptative boosting.

Como segundo paso se habla del pre-procesado, esta depende de la información que se obtuvo en la detección. Esta etapa realiza una serie de transformaciones geométricas sobre la imagen dejándola preparada para la correcta extracción de característica y se utilizan cuatro fases para normalizar y alinear la imagen.

**1. Rotación:** Una de las utilidades de calcular las coordenadas de los ojos, radica en poder determinar el ángulo de giro de una cara en una imagen y compensarlo. Al tener caras sin giro, el proceso de reconocimiento dará mejores resultados.

**2. Escalado:** Para conseguir que todos los rostros de las imágenes tengan las mismas proporciones, se utiliza la distancia entre los centros de los ojos para conseguir un radio por el cual la imagen debe ser aumentada o reducida. Esto es necesario puesto que muchas técnicas de reconocimiento requieren que todos los datos de entrada tengan el mismo tamaño (en nuestro caso la matriz de píxeles).

**3. Recorte:** Una vez la imagen ha sido rotada y escalada, se procede al recorte de la misma para obtener sólo la región de interés. Se les da a todas las imágenes las mismas dimensiones con el fin de que todas ellas tengan el mismo tamaño para que sea posible la comparación entre ellas.

**4. Ecuación del histograma:** Las imágenes pueden presentar variabilidad en la luminosidad y en el contraste lo que produce que imágenes similares sean muy diferentes respecto al valor de intensidad de sus píxeles. Mediante la ecualización de su histograma, se pretende que las imágenes que tienen la mayor parte de sus valores de intensidad concentrados en una zona reducida del histograma, pasen a extenderse por todo el rango de valores del histograma. Esto resulta en imágenes con mayor contraste y con menor variabilidad lumínica entre ellas.

**Extracción de características:** La extracción de características se refiere a la obtención de propiedades o parámetros particulares de cada rostro para luego poder ser clasificados, esto puede tomar tres enfoques diferentes.

- **Enfoque holístico**, basándose en la imagen del rostro como un todo.
- **Enfoque mediante características locales**, dando mayor importancia a las diferentes partes del rostro (geometría facial).

- **Enfoque híbrido**, basado en la idea de que el sistema de percepción humana combina características locales y globales para el reconocimiento.

Por otro lado, se pueden ver distintos métodos de extracción de características, parecidos a los enfoques anteriormente enumerados.

**Reconocimiento:** Esta etapa final está compuesta por dos ítems, los cuales hacen el trabajo de identificación de los patrones enviados por la etapa anterior y la verificación de estos patrones para una comparación de los patrones obtenidos con unos anteriormente establecidos por el sistema.

Este reconocimiento consiste en la clasificación de las características extraídas del rostro detectado, esta clasificación puede ser realizada de manera controlada, lo cual consiste en que un patrón de entrada es identificado como miembro de una clase ya predefinida. Sin embargo, hay una manera que no es controlada y esta es donde el patrón es asignado a una clase que no está predefinida o en otras palabras a una clase desconocida.

Para el reconocimiento, en cada clase hay un sujeto, por lo tanto, al clasificar las características extraídas de la cara del sujeto se está indicando a que sujeto pertenecen esos patrones, para el diseño de clasificadores se pueden distinguir tres aproximaciones basadas en:

1. Concepto de similitud.
2. Aproximación probabilística.
3. Optimización de un criterio de error.

(Scarel, 2010)

**XVR:** El XVR de Dahua es un nuevo grabador de video HD basado en la estructura abierta líder en la industria para ser compatible con múltiples tecnologías. Es la solución perfecta para actualizar sistemas de videovigilancia existentes.

El XVR es compatible con los 4 principales tipos de cámaras análogas del mercado, no sólo las cámaras tradicionales CVBS (análogas), sino también HDCVI, AHD y TVI, así como también cámaras IP. Además, XVR reconoce los formatos de señal de la cámara automáticamente, incluyendo las cámaras Dahua y las cámaras de terceros. Una verdadera función plug & play hace la operación más amigable y fácil. Todas estas características hacen de XVR una verdadera grabadora de video Penta-híbrida. (Tecnoseguro, 2016)

**Figura 20.**

*XVR Dahua*



*Nota:* Fuente: Adaptado de Tecnoseguro

<https://www.tecnoseguro.com/noticias/cctv/dahua-presenta-grabadora-video-xvr>

## Estado del arte

En el año 2004, Ana Romero realiza un proyecto de investigación titulado “Reconocimiento Facial Automático mediante Técnicas de Visión Tridimensional”, y esta se centra en la búsqueda de nuevos planteamientos que mejoren la robustez de los Sistemas de Reconocimiento Facial Automático ante variaciones de las distintas imágenes faciales de cada individuo. Se ha profundizado en metodologías que liberen en gran medida a estos sistemas, de su dependencia respecto de las condiciones de adquisición de las imágenes (iluminación, maquillaje, sombras, transformaciones geométricas, expresiones faciales, etc.), así como en la búsqueda de información 3D extraíble de imágenes de las caras humanas, que aporte un mayor poder de discriminación entre individuos, y desde entonces con el pasar de los años y el avance de la tecnología se han desarrollado varios proyectos en base al reconocimiento facial, como el de Darío Villalón, en el año 2012, que en su investigación “Diseño e implementación de una plataforma de software para reconocimiento facial en video”, plantea el diseño, implementación y validación de una plataforma de software para el reconocimiento facial en un archivo de video, utilizando métodos ya establecidos y validados en el campo de la biometría, como lo son el algoritmo Haar para detección de rostros y el algoritmo PCA Eigenface para el reconocimiento facial. De forma semejante al proyecto de investigación de Ana Romero, en el año 2014 Miguel Vázquez en su investigación “Sistema de Reconocimiento Facial Mediante Técnicas de Visión Tridimensional”, describe el desarrollo de un sistema de reconocimiento facial a partir del análisis de rostros digitalizados en tres dimensiones, el cual es una aplicación biométrica que se apoya de diferentes áreas del conocimiento tales como: el reconocimiento de patrones, la óptica, la visión artificial, geometría diferencial y la estadística, también se ha implementado el reconocimiento facial para fines sociales como es el caso de Rafael Pedroza en el año 2019, que

en su proyecto “Diseño e implementación de un sistema de biometría facial para la búsqueda e identificación de personas desaparecidas en Colombia”, plantea una solución que busca contribuir con la solución del problema de personas desaparecidas en Colombia, mejorando los actuales procesos de búsqueda y localización de personas desaparecidas. Por tal motivo se estableció como objetivo de Desarrollar un sistema basado en biometría facial para la búsqueda y localización de personas desaparecidas en Colombia, implementando servicios en la nube de la plataforma Amazon Web Services, tecnologías web y tecnologías de escritorio que brindan solución a la problemática planteada, y de forma similar bajo el mismo fin lo hizo Ervin Cáceres en el año 2018 llevando a cabo su proyecto “Aplicación móvil de reconocimiento facial en personas con antecedentes de abuso sexual en la provincia de Andahuaylas, Apurímac”, propone una aplicación móvil de reconocimiento facial en personas buscadas por la justicia en especial por el delito de abuso sexual, se centra en este pequeño grupo para medir la eficacia de la aplicación. Este será una aplicación de reconocimiento facial destinado a la identificación y reconocimiento de personas en tiempo real, llevado a cabo en la dirección zonal de Andahuaylas, para ser aplicado a la localización de individuos que se encuentran en una lista denominada “personas requisitorados por la justicia”, con el objetivo principal de incrementar los índices de seguridad colectiva brindando un sistema robusto que pueda ser utilizado en diversos lugares concurridos como: terminales, Carreteras transoceánicas, avenidas concurridas de personas, etc.

Lo anterior nos demuestra como el reconocimiento facial con el pasar de los años ha sido implementado en diversas áreas, una de ellas también esas áreas es la de la salud, como lo hicieron Diego Lamadrid y Martín Barriga en el año 2019, en su proyecto “Modelo Tecnológico de Reconocimiento Facial para la Identificación de Pacientes en el Sector Salud”, plantea el

desarrollo de un modelo tecnológico que tiene como objetivo la identificación de pacientes mediante un servicio cognitivo de reconocimiento facial en Cloud computing para cubrir la necesidad que tienen los sectores de salud de prevenir la suplantación de identidad.



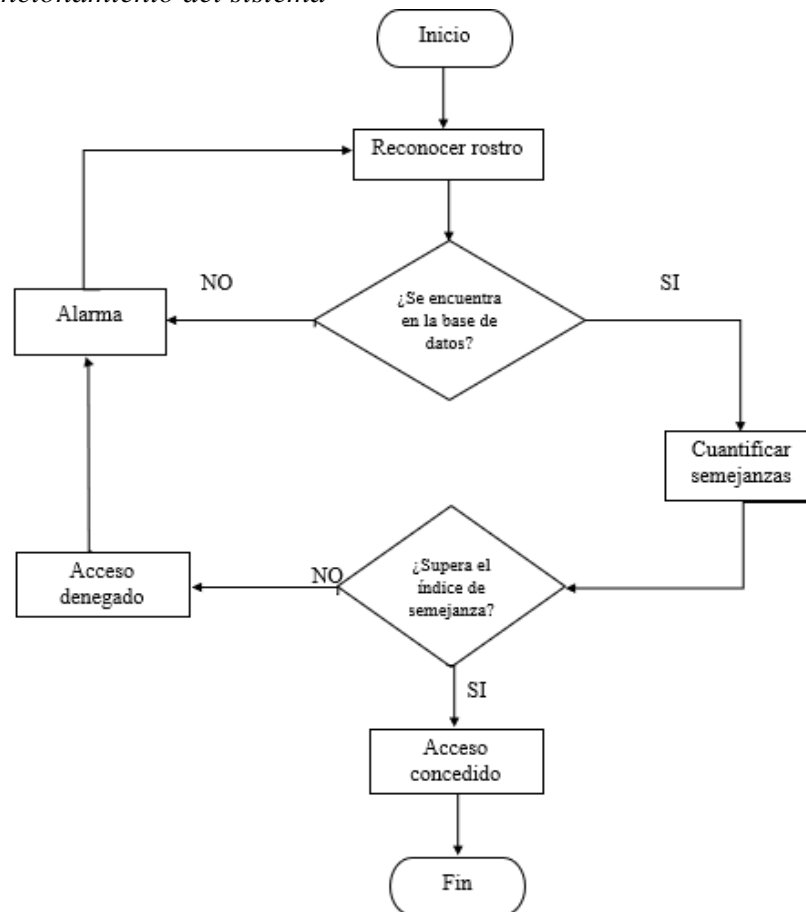
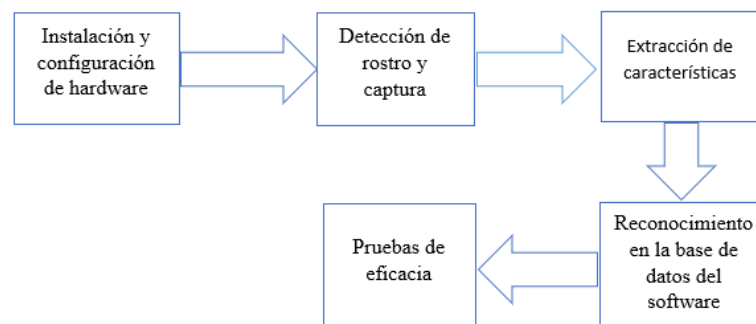
## Capítulo 3

### Análisis de Resultados y Propuesta Ingenieril

Según lo planteado en la metodología este proyecto se basa en un desarrollo en cascada, el cual es un modelo lineal donde se plantea una serie de procesos secuenciales para llegar a un objetivo final. Este objetivo final como bien se sabe, es la implementación de un sistema de reconocimiento facial para el control de acceso a una empresa, el cual tiene unas especificaciones y requerimientos. En este capítulo se tomaron todas las consideraciones de los capítulos anteriormente descritos para la implementación de dicho sistema.

Para el desarrollo de este sistema fueron necesarias varias herramientas las cuales ayudaron en gran proporción a realizarlo. Estas herramientas de hardware tienen que ajustarse a las condiciones establecidas, además, de tener en cuentas las condiciones típicas de acceso a la empresa.

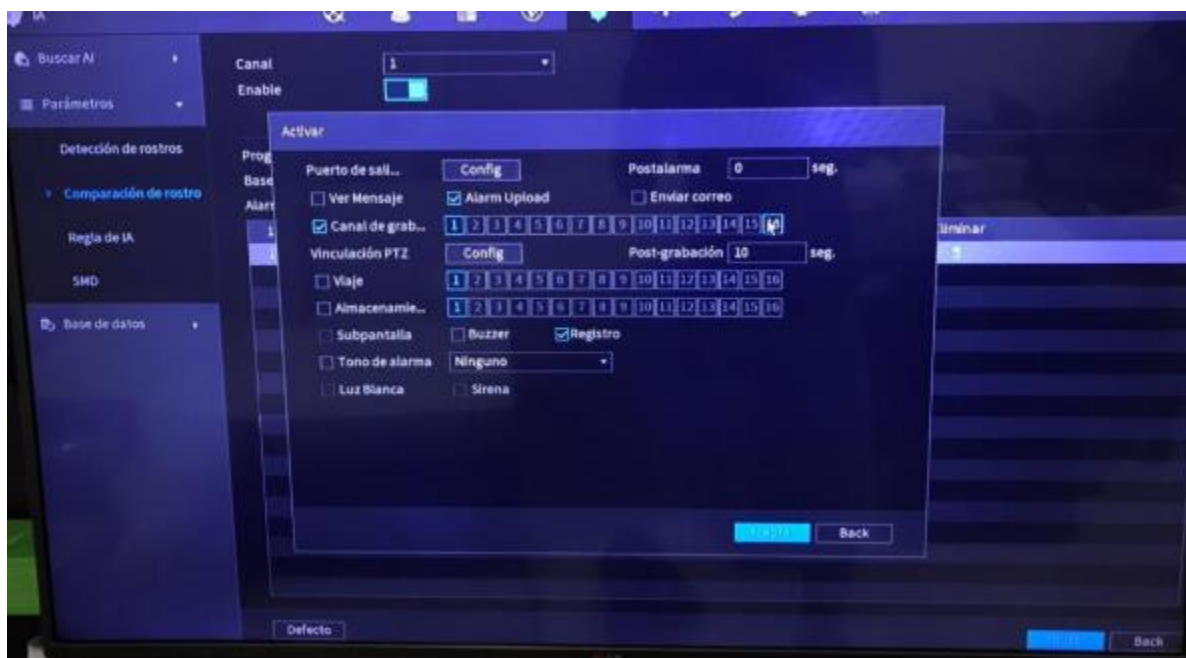
Una de estas herramientas de hardware, el cual se mencionó anteriormente y se aclaró lo indispensable del uso de dispositivos que cumplan con los requerimientos mínimos, para esto se tuvieron en cuenta los dispositivos mencionados en el capítulo anterior los cuales cumplen con las características necesarias para el éxito del proyecto.

**Figura 21.***Diagrama funcionamiento del sistema***Figura 22.***Proceso de implementación del proyecto*

Antes de iniciar con el registro de datos, se configura previamente lo que se hará el software cuando detecte un rostro, en este caso, el canal habilitado donde se encuentra la cámara de alta definición es el canal 1 del XVR, y con este se activará una alarma siempre que el sistema detecte un rostro esté o no registrado en la base de datos, quiere decir que cualquier persona que pase por el lugar y sea detectada por la cámara, habilitará la alarma de registro.

### Figura 23.

#### Configuración XVR



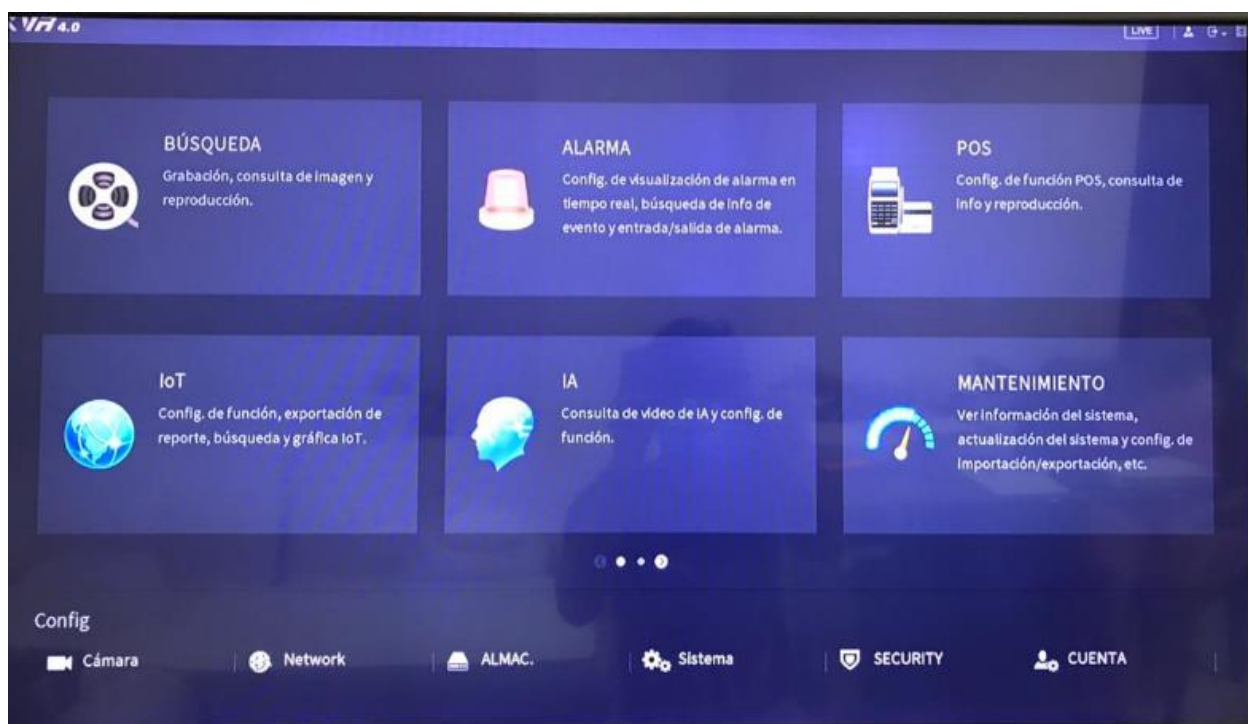
Se configura las horas y días en que se quiere que este activo el sistema, por determinación de la empresa, se decidió que estará activo las 24 horas del día, 7 días a la semana, sin embargo, cabe resaltar que se puede configurar a gusto dependiendo las necesidades que el usuario requiera.

**Figura 24.***Configuración XVR*

Para el desarrollo de este proyecto se cuenta con un software suministrado por el XVR (XVR 4.0), el cual muestra una interfaz evidenciando las funciones que este posee.

### Figura 25.

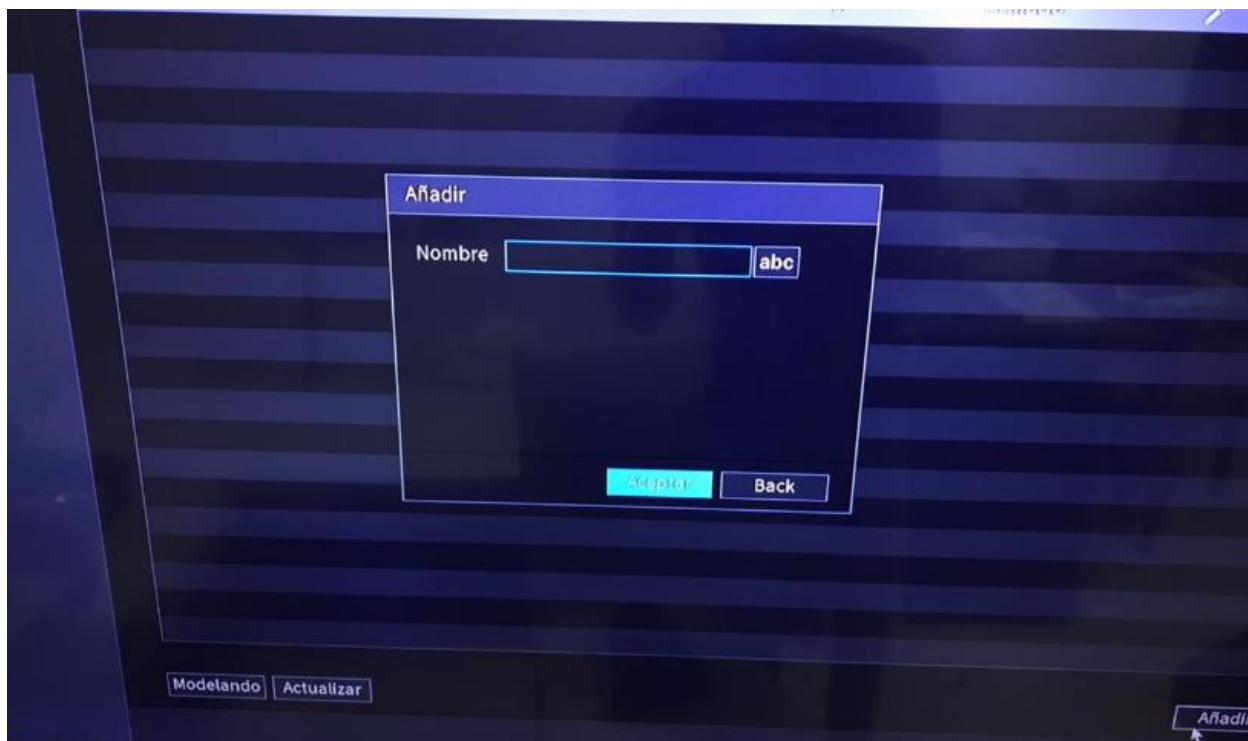
#### Interfaz



Antes de empezar con la detección de rostros, se crea una base de datos en el sistema, la cual almacena los rostros que tendrán autorización de ingresar. Se llamó “PERMITIDOS”.

**Figura 26.**

*Base de datos*



En la figura 25, se muestra el modo de en vivo regular, el cual hace seguimiento a lo que capta la cámara sin ninguna función añadida.

**Figura 27.**

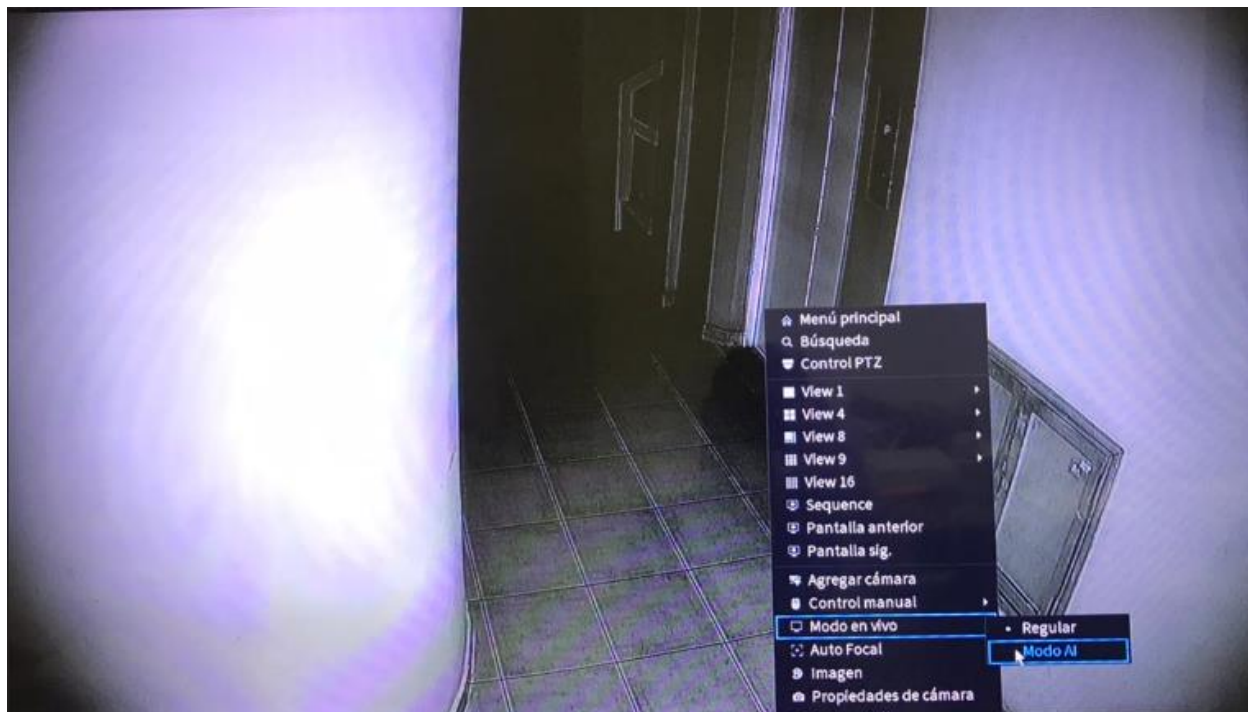
*Modo regular*



Para activar la visión artificial e iniciar la comparación de rostros para el acceso a la empresa, se cambia al modo AI, por sus siglas en inglés Artificial Intelligence (Inteligencia Artificial).

**Figura 28.**

*Cambio de modo en vivo a modo AI*



Se muestra un panel donde saldrán todos los rostros identificados por la cámara, estén o no en la base de datos.



**Figura 29.**

*Panel de rostros captados*



Se continuó con el registro del primer rostro, para esto el sistema debe detectarlo para que muestre la opción si se desea añadir en la base de datos.



**Figura 30.***Rostro detectado*

El sistema con visión artificial muestra detalles sobre el rostro detectado, como su género, su expresión, edad y si lleva lentes o no. Además de mostrar una etiqueta en rojo llamada “STRANGER” debido a que no está registrado en la base de datos.

**Figura 31.***Detalles de la persona captada*



Para el registro, se elige la opción “Agregar a b. de datos de rostros”, que se muestra en la figura 30.

### Figura 32.

*Opción “Agregar a b. de datos de rostros”*



En la interfaz de registro, se tienen varias opciones para llenar la información del rostro captado, como el nombre de la persona, género (lo detecta automáticamente), cumpleaños, región, provincia, dirección, tipo de credencial y su número. Además de elegir en cual base de

datos almacenar la información, ya que se puede crear más de una, en este caso solo se tiene la anteriormente llamada “PERMITIDOS”.

**Figura 33.**

*Interfaz de registro*

Registro

Nombre

Cumplimientos Año  Mes  F...

Provincia

Tipo de c...

Género  M...  Mujer

Región

Dirección

No. de cr...

1	<input type="checkbox"/>	Nombre	No. de registro	No. de fallos	No. de errores
1	<input type="checkbox"/>	PERMITIDOS	4	0	0

Reiniciar Buscar

Nombre : LAURA TPB  
Género : Mujer  
No. de credencial :

Modelado exitoso

Nombre : LAURA  
Género : Mujer  
No. de credencial :

Modelado exitoso

Nombre : Iivan borrero  
Género : Masculino  
No. de credencial :

Modelado exitoso

Se verifica que el software detecta correctamente el rostro antes registrado.

**Figura 34.**

*Comparación de rostros*



Se evidencia que tanto la cámara con la función de visión nocturna activa y con luz normal, da acceso a la persona, con una fiabilidad del 99%.

**Figura 35.**

*Detección del rostro registrado*





## Capítulo 4

### Conclusiones

La implementación de un sistema de reconocimiento facial se plantea como una propuesta tecnológica novedosa que reemplazaría el proceso manual con el que normalmente se lleva a cabo un control de registro o acceso. Al recopilar la información de los diferentes dispositivos que podían hacer el proceso de reconocimiento facial, durante la definición de requerimientos de los dispositivos se decidió utilizar el XVR Dahua DH-XVR5116H-4KL-I haciendo previa indagación de diferentes tecnologías y dispositivos que hay en el mercado, por las funciones innovadoras que este ofrece en comparación a los demás, porque además de monitorear permanentemente el sistema de seguridad, tiene la ventaja de contar con un algoritmo de la inteligencia artificial que al hacer la detección y comparación de rostros puede identificar absolutamente todos los detalles faciales y emocionales de la persona, verificando su eficiencia haciendo prueba con diferentes ítems, poses y condiciones de luz, y también permitiendo que se le adapten diferentes configuraciones y tecnologías que garanticen la gestión y control del acceso al establecimiento.

Al utilizar una cámara de alta resolución (4k) se logra en gran parte el éxito del proyecto, dado su precisión aumenta un 95% con respecto al de una cámara de 1080p lo que hace que el sistema trabaje de una forma más eficaz al momento detectar un rostro, dado que, a mejor resolución, la imagen será más clara e impedirá que el algoritmo falle. El proyecto se implementó en una empresa, pero no se descarta poderlo utilizar en otros espacios, incluyendo viviendas, ya que el software y la base de datos tienen la capacidad de almacenar diferentes rostros por lo cual no quedará limitado para lugares más pequeños en número de personas, y, además de controlar el acceso a la empresa, monitorea y graba todo lo que suceda en el rango

donde está ubicada la cámara, por lo tanto al juntar la seguridad y la inteligencia artificial da como resultado esta implementación.

Algunos aspectos a tener en cuenta en esta implementación, como el ángulo de la toma de imágenes que es donde está ubicada la cámara, también factores de luz, si hay demasiada opacidad, el algoritmo no podría detectar con la misma precisión.

## Capítulo 5

### Recomendaciones

Se evidenció en el desarrollo de este proyecto, busca la seguridad y confort en la empresa, por lo tanto, se espera que otros proyectos enfocados en lo mismo sean también implementados en el hogar o en cualquier otro tipo de establecimientos, pero agregando sistemas más automatizados y tecnológicos como por ejemplo el uso de una cerradura inteligente para la puerta, notificaciones por medio de una aplicación móvil entre otros.

De acuerdo con el desarrollo y las pruebas realizadas a esta tecnología, es posible forjar futuras aplicaciones de este proyecto al análisis de imágenes en videos para seguimiento automático de personas con actividad sospechosa en la empresa, o con expresiones faciales que correspondan con algunos estados emocionales que puedan representar un riesgo para la seguridad de las instalaciones.

Para un funcionamiento más eficiente del reconocimiento facial, se recomienda contar con un espacio que tenga la iluminación adecuada para ello.

También se recomienda instalar la cámara en un ángulo y distancia que le permita al sistema captar con precisión los detalles faciales y ser detectado automáticamente, para que funcione de manera óptima.

## Bibliografía

Vázquez López, Miguel Ángel. (2014). Sistema de Reconocimiento Facial Mediante Técnicas de Visión Tridimensional. Repositorio Institucional.

<https://cio.repositorioinstitucional.mx/jspui/bitstream/1002/436/1/15950.pdf>

Villalón De la Vega, Darío Eduardo. (2012). Diseño e implementación de una plataforma de software para reconocimiento facial en video. Repositorio Académico de la Universidad de Chile. [http://repositorio.uchile.cl/bitstream/handle/2250/112271/cf-](http://repositorio.uchile.cl/bitstream/handle/2250/112271/cf-villalon_dd.pdf?sequence=1&isAllowed=y)

[villalon\\_dd.pdf?sequence=1&isAllowed=y](http://repositorio.uchile.cl/bitstream/handle/2250/112271/cf-villalon_dd.pdf?sequence=1&isAllowed=y)

Pedroza Manga, Rafael Eduardo. (2019). Diseño e implementación de un sistema de biometría facial para la búsqueda e identificación de personas desaparecidas en Colombia. Repositorio Unicartagena.

<https://repositorio.unicartagena.edu.co/bitstream/handle/11227/8512/TESIS%20PEDROZA%20MANGA.pdf?sequence=1&isAllowed=y>

Moreno Diaz, Ana Belén. (2004). Reconocimiento Facial Automático mediante Técnicas de Visión Tridimensional. Universidad Politécnica de Madrid.

<http://oa.upm.es/625/1/10200408.pdf>

Cáceres Mariño, Ervin Lewis. (2018). Aplicación móvil de reconocimiento facial en personas con antecedentes de abuso sexual en la provincia de Andahuaylas, Apurímac. Repositorio Universidad Nacional José María Arguedas.

[https://repositorio.unajma.edu.pe/bitstream/handle/123456789/358/Ervin\\_Lewis\\_Tesis\\_Bachiller\\_2018.pdf?sequence=1](https://repositorio.unajma.edu.pe/bitstream/handle/123456789/358/Ervin_Lewis_Tesis_Bachiller_2018.pdf?sequence=1)



Garduño Santana, Martín Adrián. (2018). Reconocimiento por biometría facial para aplicaciones en ciudades inteligentes. Repositorio Universidad Autónoma del Estado de México. <http://ri.uaemex.mx/bitstream/handle/20.500.11799/68484/Reconocimiento+por+Biometria+Facial+para+Aplicaciones+en+Ciudades+Inteligentes.pdf?sequence=1>

La Madrid Arroyo, Diego Alonso. & Barriga Rivera, Martín Humberto. (2019). Modelo Tecnológico de Reconocimiento Facial para la Identificación de Pacientes en el Sector Salud. Repositorio Académico Universidad Peruana de Ciencias Aplicadas. [https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/648832/La%20Madrid\\_ad.pdf?sequence=3&isAllowed=y](https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/648832/La%20Madrid_ad.pdf?sequence=3&isAllowed=y)

Espinosa Olgún, David Eduardo. & Jorquera Guillen, Peter Ignacio. (2015). Reconocimiento Facial. Pontificia Universidad Católica de Valparaíso. [http://opac.pucv.cl/pucv\\_txt/txt-1000/UCD1453\\_01.pdf](http://opac.pucv.cl/pucv_txt/txt-1000/UCD1453_01.pdf)

Cajas Idrovo, Marco Vinicio. & Viri Ávila, Pablo Andrés. (2017). Diseño e implementación de un sistema de seguridad vehicular mediante reconocimiento facial a través de visión artificial. Universidad Politécnica Salesiana sede Cuenca. <https://dspace.ups.edu.ec/bitstream/123456789/13566/1/UPS-CT006920.pdf>

Espinoza Tituana, Waldemar Victoriano. & Ortiz Pesantes, Tatiana Maricela. (2016). Sistema de reconocimiento facial automatizado para el control de asistencia de recursos humanos. Repositorio Digital - Universidad Nacional de Loja. <https://dspace.unl.edu.ec/jspui/handle/123456789/14237>

Reconocimiento facial con base en imágenes (2017) ARTICULO Cadena Moreano, José Augusto Montaluisa Pulloquina, Raúl Humberto Flores Lagla, Galo Alfredo Chancusig Chisag, Juan Carlos Guaypatín Pico, Oscar Alejandro. Boletín Redipe Vol. 6 Núm. 5 Pág. 143-151.

¿Qué es la inteligencia artificial? (2020, 30 abril). Iberdrola.

<https://www.iberdrola.com/innovacion/que-es-inteligencia-artificial>

Pastor, J. (2018, 2 noviembre). Qué es la inteligencia artificial. Xataka.

<https://www.xataka.com/robotica-e-ia/que-inteligencia-artificial>

Pérez Porto, J., & Merino, M. (2016). Definición de cámara digital — Definicion.de. Definición.de. <https://definicion.de/camara-digital/>

Wainschenker, Rubén. 2011. “Procesamiento Digital de Imágenes Objetivos de La Materia.” Disponible en: <http://www.exa.unicen.edu.ar/catedras/pdi/FILES/TE/CP1.pdf>

VI. PROCESAMIENTO DE IMAGENES. (2010). Biblioteca Digital.

[http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen2/ciencia3/084/htm/sec\\_9.htm](http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen2/ciencia3/084/htm/sec_9.htm)

Cctv, S. (2015, 26 febrero). ¿Qué es un control de acceso? Sisca - Sistemas Integrales de seguridad. <http://sisca.co/que-es-un-control-de-acceso/>

Balsero Alvaro, Vargas Cristian; Diseño e implementación de un prototipo para el control de acceso en la sede de ingeniería de la universidad distrital francisco José de caldas mediante el uso de torniquetes controlados por carnet con tecnologia nfc y lector biométrico de huella dactilar; Universidad Distrital Francisco José de Caldas Facultad de Ingeniería, Ingeniería electrónica,

<http://repository.udistrital.edu.co/bitstream/11349/3430/1/vargasgarciacristiangerman2016.pdf>

Knvul Sheikh. 1 de agosto de 2017. Quedarse con la cara. INVESTIGACIÓN CIENTÍFICA, 711(15476), 5-6. <https://www.investigacionyciencia.es/revistas/investigacion-y-ciencia/el-multiverso-cuntico-711/quedarse-con-la-cara-15476>

Scarel, G. M. 1. (2010). Sistema de reconocimiento facial. Universidad Nacional del Litoral. [http://sinc.unl.edu.ar/sinc-publications/2010/SMS10/sinc\\_SMS10.pdf](http://sinc.unl.edu.ar/sinc-publications/2010/SMS10/sinc_SMS10.pdf)

(2020, 4 marzo). Reconocimiento facial. Interpol. <https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Reconocimiento-facial>

Cruz, G. (2016, 12 julio). Control acceso. Slide Share. [https://www.slideshare.net/german\\_cruz/8control-acceso](https://www.slideshare.net/german_cruz/8control-acceso)

Serratosa, F. (s. f.). La biometría para la identificación de las personas. Academia. Recuperado 21 de mayo de 2021, de [https://www.academia.edu/31531606/La\\_biometr%C3%ADa\\_para\\_la\\_identificaci%C3%B3n\\_de\\_las\\_personas\\_Francesc\\_Serratosa\\_PID\\_00195448](https://www.academia.edu/31531606/La_biometr%C3%ADa_para_la_identificaci%C3%B3n_de_las_personas_Francesc_Serratosa_PID_00195448)

Marketing. (2018, 26 junio). Sistema de control de acceso. TD Sistemas. <https://www.tdsistemas.com/que-es-un-sistema-de-control-de-acceso/>

Action Data. (2019, 13 septiembre). ¿Cómo funciona el reconocimiento facial? <https://www.actionsdata.com/blog/como-funciona-el-reconocimiento-facial>

Editorial La República S.A.S., & De Benito, Cynthia. (2014, 20 junio). La inseguridad ciudadana hace de Colombia el país más conflictivo de América Latina. Diario La República. <https://www.larepublica.co/globoeconomia/la-inseguridad-ciudadana-hace-de-colombia-el-pais-mas-conflictivo-de-america-latina-2136581>

## Anexos

Anexo 1. Manual de usuario XVR DH-XVR5116H-4KL-I2

[User's Manual XVR DH-XVR5116H-4KL-I2](#)

Anexo 2. Guía de inicio rápido 1 (XVR)

[Quick Start Guide V1.0.1 XVR DH-XVR5116H-4KL-I2](#)

Anexo 3. Guía de inicio rápido 2 (XVR)

[Quick Start Guide V1.0.0 XVR DH-XVR5116H-4KL-I2](#)

Anexo 4. Datasheet XVR

[DH-XVR5116H-4KL-I2](#)

Anexo 5. Datasheet camara DH-HAC-HDW1801EM/EM-A

[4K HDCVI IR Eyeball Camera](#)

Anexo 6. Manual de usuario ARB1606

[Alarm Box Use's Manual V1.0.0](#)

Anexo 7. Datasheet ARB1606

[DHI- ARB1606](#)