

**PROPUESTA PARA LA ACTUALIZACIÓN DEL SISTEMA DE ACCESO
BIOMÉTRICO PARA LAS INSTALACIONES DE ORANGE BUSINESS
SERVICES**

AILEEN STEPHANIE ROJAS CAPERA

**UNIVERSIDAD SANTO TOMÁS DE AQUINO
FACULTAD DE INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C**

2020

**PROPUESTA PARA LA ACTUALIZACIÓN DEL SISTEMA DE ACCESO
BIOMÉTRICO PARA LAS INSTALACIONES DE ORANGE BUSINESS
SERVICES**

AILEEN STEPHANIE ROJAS CAPERA

**Trabajo opción de grado Pasantías en la Empresa ORANGE BUSINESS
SERVICES con el propósito de obtener el título de Ingeniera de
Telecomunicaciones**

**Director: Victor Manuel Castro
Ingeniero Electrónico**

**UNIVERSIDAD SANTO TOMÁS DE AQUINO
FACULTAD DE INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C
2020**

RECTOR GENERAL

Padre Juan Ubaldo López Salamanca, O.P.

VICERRECTOR ADMINISTRATIVO Y FINANCIERO GENERAL

Padre Luis Francisco Sastoque Poveda, O.P.

VICERRECTOR ACADÉMICO GENERAL

P. Mauricio Antonio Cortés Gallego O.P

SECRETARIA GENERAL

Ingrid Lorena Campos Vargas

SECRETARIA DE DIVISIÓN

E. C. Luz Patricia Rocha Caicedo

DECANO FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES

Ingeniero Germán Macías Muñoz

Nota de Aceptación.

Firma Ingeniero. Víctor Manuel Castro
Tutor Asignado

Firma del Jurado

Firma del Jurado

Fecha

CONTENIDO

	Pág.
INDICE DE TABLAS.....	7
INDICE DE FIGURAS.....	8
INTRODUCCIÓN.....	10
CAPÍTULO I.....	11
1.1 PLANTEAMIENTO DEL PROBLEMA.....	11
1.2 JUSTIFICACIÓN.....	12
1.3 OBJETIVOS.....	13
1.3.1 Objetivo General	13
1.3.2 Objetivos Específicos.....	13
CAPÍTULO II.....	14
2.1.0 ESTADO DEL ARTE	14
2.1.1 Validación de pagos con el uso del reconocimiento facial.	14
2.1.2 Implementación de un sistema de reconocimiento facial en el aeropuerto Menorca en España	14
2.1.3 Uso de un sistema biométrico para el ingreso y salida de vehículos en los centros comerciales en Sudáfrica	15
2.1.4 Control de acceso biométrico para transmisiones de medios digitales en redes para el hogar.....	15
CAPITULO III.....	16
3.1.0 MARCO TEÓRICO	16
3.1 ¿Qué es Biometría?.....	16
3.2 Definición de un sistema Biométrico	16
3.2.1 Funcionamiento de un control de acceso Biométrico	16
3.3 Tipos de Sistemas Biométricos.....	17
3.3.1 Lectores de Huellas Dactilares	18
3.3.2 Control Biométrico por verificación de voz.....	20

3.3.3 Reconocimiento por patrones	20
3.3.4 Reconocimiento por retina	21
3.3.5 Reconocimiento por Iris.....	22
3.3.6 Reconocimiento Facial	23
3.3.7 Deep learning de Hikvision.....	28
CAPITULO IV.....	30
4.1.0 DESARROLLO DEL PROYECTO.....	30
4.1.1 Requerimientos para el control de acceso.....	30
4.1.2 Esquema actual.....	31
4.1.3 Planos de las instalaciones con su sistema Biométrico actual	31
4.1.4 Cualificación de los beneficios y costos asociados con cada una de las propuestas de solución	33
4.1.4.1 SOLUCIÓN POR PARTE DE IOT TECH	34
4.1.4.2 SOLUCIÓN POR PARTE DE PROWARE HS S.A	41
4.1.4.3 SOLUCIÓN POR PARTE DE SYSCOM.....	46
4.1.4.4 CUADROS COMPARATIVOS DE LAS SOLUCIONES BIOMÉTRICAS.....	51
4.1.4.5 PROPUESTA FINAL DEL SISTEMA BIOMÉTRICO.....	55
4.1.4.5.2 Beneficios al implementar un sistema de control de acceso facial	58
CAPITULO V.....	59
CONCLUSIONES.....	59
BIBLIOGRAFÍA	61
WEBGRAFÍA	62

INDICE DE TABLAS

Pág.

Tabla 1. Modelos de reconocimiento de patrones . Fuente: Statistical Pattern Recognition	28
Tabla 2. Características generales de los equipos propuestos en la solución de IOT Tech.	37
Tabla 3. Propuesta por parte de IOT Tech usando tecnología Hikvision.....	39
Tabla 4. Características generales de los equipos propuestos en la solución de Proware HS S.A.....	44
Tabla 5. Costos de la propuesta por parte de PROWARE.....	45
Tabla 6. Características generales de los equipos propuestos en la solución de SYSCOM.	49
Tabla 7. Propuesta por parte de SYSCOM usando tecnología ZKTeco	50
Tabla 8. Cuadro Técnico comparativo de las diferentes soluciones.	51
Tabla 9. Cuadro comparativo de los costos finales de cada solución.	54

INDICE DE FIGURAS

Pág.

Figura 1. Fases de un sistema biométrico. Fuente: Autor	17
Figura 2. Imagen de una huella dactilar. Fuente: Tipos de Sistemas Biométricos.	18
Figura 3. Modelado de la captura de un fragmento de voz de una persona	20
Figura 4. Lectura del Iris. Fuente: Reconocimiento del Iris.	23
Figura 5. Fotograma Facial. Fuente: Reconocimiento Facial.	24
Figura 6. Proceso del reconocimiento facial. Fuente: Autor.	24
Figura 7. Ejemplo del Funcionamiento de Deep learning. Fuente: Quanta Magazine.	29
Figura 8. Sistema Actual. Fuente: Autor	31
Figura 9. Ubicación actual de los lectores de huella dactilar en la Oficina XX.	32
Figura 10. Ubicación actual de los lectores de huella dactilar en la Oficina YY.	33
Figura 11. Matriz DOFA sobre la empresa IOT Tech. Fuente: Autor	34
Figura 12. Matriz DOFA Cruzado sobre IOT Tech. Fuente: Autor.	35
Figura 13. Topología de Conexión de control de acceso usando Hikvision. Fuente: Autor.	40
Figura 14. Matriz DOFA sobre la empresa PROWARE HS SA. Fuente: Autor.	42
Figura 15. Matriz DOFA Cruzado sobre PROWARE. Fuente: Autor.	43
Figura 16. Topología de conexión de control de acceso del sistema de control de acceso de PROWARE. Fuente: PROWARE.	46
Figura 17. Matriz DOFA sobre la empresa SYSCOM. Fuente: Autor	47
Figura 18. Matriz DOFA Cruzado sobre SYSCOM. Fuente: Autor.	48
Figura 19. Topología de conexión de control de acceso ZKTeco. Fuente: ZKTeco.	50
Figura 20. Conexión de sensor de puerta, botón de salida y alarma . Fuente: ZKTeco.	51
Figura 21. Sistema de control de acceso Propuesto + CCTV. Fuente: Autor	56
Figura 22. Topología de conexión propuesta. Fuente: Autor	58

GLOSARIO

TECNOLOGÍA BIOMÉTRICA: Son dispositivos electrónicos especializados en el análisis, identificación y/o autenticación de una persona basado en sus rasgos o características humanas únicas.

1: N: Identificación uno a muchos. Es un método de validación biométrica que compara la plantilla capturada de una huella digital, venas dactilares o rostro, mediante el uso de un dispositivo de asistencia o control de acceso sin la necesidad de un identificador previo.

NVR: Un NVR es una grabadora de vídeo de red.

LECTOR ESCLAVO: Es un lector externo que depende de una terminal o dispositivo maestro. El lector esclavo envía los datos vía Wiegand o RS485 al dispositivo maestro conectado a él, para procesar la información y validar el acceso.

ANTI-PASSBACK: Es una función de control de acceso que restringe la entrada de un usuario a una misma área por segunda ocasión sin haber registrado una salida previamente y viceversa. Está diseñada con el fin de evitar que los usuarios de un sistema de control de acceso compartan una tarjeta de acceso o una persona ajena al sistema tenga acceso a las instalaciones mediante la suplantación de identidad.

ESCALABILIDAD: Capacidad de un sistema para crecer en cantidad de dispositivos o terminales ya sean de asistencia o control de acceso.

ESCLUSA: Es una función de control de acceso, el cual permite la apertura de una puerta simultáneamente en un grupo de 2 o más puertas. Este tipo de funciones se realizan gracias a un Software de administración.

EVENTOS: Los eventos son registros de información o de datos relacionados a un acceso, verificación de un usuario, este tipo de información es almacenada en el dispositivo.

CERRADURA MAGNÉTICA: Está compuesta por dos imanes que permite conocer el estado de una puerta, ya sea abierta o cerrada, estas pueden ser monitoreadas o controladas por un panel de acceso.

TCP/IP: Protocolo para la transmisión de datos en una red local LAN o WAN.

INTRODUCCIÓN

En el mundo la Biometría es utilizada para diferentes fines, actualmente este tipo de tecnología está siendo empleada para el control de acceso en los establecimientos. Los sistemas biométricos que se emplean para un sistema de seguridad se dividen en tres tipos, el primero es la Biometría estática, la cual abarca características físicas de las personas, como: el iris, la retina, facciones de la cara y manos. El segundo es la Biometría dinámica, estudia el comportamiento de algunas características como la voz, la firma y la dinámica de escritura de una persona. Por último, se encuentra la combinación de los dos primeros, este se le denomina “Biometría multimodal” ¹.

Estos sistemas pueden ser aplicados de acuerdo a las necesidades del cliente, sin embargo, el que es más utilizado en la actualidad es la Biometría estática, en específico la herramienta más común es el detector de huellas dactilares, por ser único y presentar un menor rango de error.

Este trabajo tiene la intención de analizar y determinar cuál es la mejor opción para el control de acceso en la empresa ORANGE BUSINESS SERVICES, al tener en cuenta principalmente los aspectos técnicos y económicos. Por lo tanto, este documento está dividido en tres partes: en la primera, se definirá el estado del arte, en donde se contemplarán algunos proyectos referentes a sistemas biométricos para el control de acceso en el ámbito empresarial; en la segunda se describen temas relacionados a la biometría, los tipos y sus derivados. Y, por último, se desarrollará un análisis de diferentes soluciones para el control de acceso de detección facial.

¹ SISTEMAS BIOMÉTRICOS. Borja, C. T. (2010). Obtenido de Trabajos de Sistemas Informáticos: <https://docplayer.es/4089383-Sistemas-biometricos-cesar-tolosa-borja-alvaro-giz-bueno.html>

CAPÍTULO I

1.1 PLANTEAMIENTO DEL PROBLEMA

En las instalaciones de ORANGE BUSINESS SERVICES, se encuentran instalados lectores de huella dactilar, que permiten y regulan el ingreso del personal de la empresa, por ende, su funcionalidad es de suma importancia para su seguridad.

Un problema con el que cuenta actualmente sus oficinas, es que los lectores de huella dactilar son obsoletos. Y como empresa de Telecomunicaciones enfocada en la vanguardia de la tecnología, busca hacer un cambio de la infraestructura tecnológica actual, y además al tener en cuenta la actual situación que se vive a nivel mundial por la actual crisis sanitaria, se busca la prevención y control de la propagación de COVID-19, evitando la mayor parte posible el contacto y manipulación de zonas comunes. Al ver estos problemas y velando por la seguridad dentro de las instalaciones, algunos directivos de la empresa optaron por la implementación de un sistema de reconocimiento facial, como una nueva modificación para su control de acceso.

Para el desarrollo de este proyecto dentro de la empresa, se debe tener en cuenta un proceso de planeación de los gastos económicos y recursos que serán proyectados para la futura implementación del mismo. Al considerar esta problemática, surge el interrogante de ¿Cuál de los sistemas que ofrece el mercado sería una buena opción para actualizar el sistema que hoy en día se tiene en la empresa ORANGE BUSINESS SERVICES?

1.2 JUSTIFICACIÓN

El análisis que se realizará a lo largo de este documento tiene como fin actualizar de manera eficaz, funcional y con menores afectaciones el sistema de control de acceso a las oficinas y data center de la empresa ORANGE BUSINESS SERVICES e integrarlo con el actual sistema de video vigilancia CCTV, para lograr este objetivo se propone y sugiere la implementación de un sistema de acceso de detección facial integrado al actual sistema de video vigilancia, esta solución no solo otorgará un status de alto nivel de infraestructura, sino que de igual manera proporcionará un gran nivel de seguridad para los funcionarios, visitantes, e información crítica de los clientes, entre otros.

La tecnología ha llegado a nuestras vidas, puesto que, formará parte del futuro. La seguridad de la información es una prioridad en todas las empresas, no podemos continuar atados a tecnologías obsoletas. Al proponer un nuevo sistema de control de acceso no solo estarían dando un paso enorme en la evolución, si no que la empresa estaría llegando al nivel de seguridad de los más grandes y poderosos edificios del mundo que usan tecnología de detección facial en sus sistemas de seguridad.

Algunos sitios en los que se ha implementado este tipo de herramienta biométrica han sido plataformas como Google Photos, Facebook, donde el sistema busca similitudes de las características faciales de diferentes personas que tienen agregado un individuo a su lista de amigos, surgiendo opciones como el etiquetado de personas en común. En el caso de la seguridad y video vigilancia, se pueden ver este tipo de implementaciones en los aeropuertos con el fin de buscar o seguir el rastro de una persona en caso de que esté presente actitudes sospechosas, otro uso de este tipo de herramientas, se ha encontrado en los escáneres de seguridad de los aeropuertos, donde se usa el reconocimiento facial en los pasaportes electrónicos de los viajeros, facilitando los datos personales de estos a los agentes aduaneros para que el proceso de migración sea más fácil y lograr detectar que viajeros porten pasaportes falsos. ²

² 4 CASOS DE APLICACIÓN DEL RECONOCIMIENTO FACIAL. - Neuromarketing. La. Melgar, J. (12 de 12 de 2017). Obtenido de Neuromarketing. La Información del sector para Latinoamérica: <https://neuromarketing.la/2017/12/aplicacion-del-reconocimiento-facial/>

1.3 OBJETIVOS

1.3.1 Objetivo General

Realizar una propuesta para actualizar el sistema de acceso biométrico para la empresa ORANGE BUSINESS SERVICES.

1.3.2 Objetivos Específicos

- Definir los requerimientos para el sistema de control de acceso de la empresa.
- Conocer las diferentes tecnologías para un sistema de control de acceso biométrico.
- Realizar un análisis comparativo de los diferentes proveedores y sus soluciones.
- Diseñar una propuesta más adecuada basada en los requerimientos de las soluciones dadas por los proveedores.

CAPÍTULO II

2.1.0 ESTADO DEL ARTE

Alrededor de todo el mundo, así como en Colombia se han realizado diferentes proyectos donde se utiliza la Biometría en un sistema de control de acceso, para distintas actividades o servicios. En este capítulo se investigaron algunos casos donde fue empleado un sistema biométrico de detección facial.

2.1.1 Validación de pagos con el uso del reconocimiento facial.

En Colombia fue lanzado el primer sistema que permite hacer pagos por medio del reconocimiento facial, gracias a la alianza entre Redeban y Carulla.

El principal objetivo es facilitar el pago de los productos en las cajas, convirtiéndose en un sistema de pago auto asistido. Para el proceso de estos pagos, “el cliente debe colocar el rostro para que sea escaneado en la aplicación del almacén, vinculando a su tarjeta de crédito o débito, posteriormente debe dirigirse a uno de los puntos de pago y por último debe ingresar su número de cédula con el fin de verificar la autenticidad de la información”³. Esta modalidad se encuentra disponible en el establecimiento de Smartmarket de la tienda Carulla, ubicado en la carrera 11 con 91.

2.1.2 Implementación de un sistema de reconocimiento facial en el aeropuerto Menorca en España

En el 2019 el aeropuerto de Menorca se convirtió en uno de los primeros aeropuertos en Europa en aplicar el sistema de reconocimiento facial en tres puntos: “Control, Facturación, Acceso de Seguridad y en la Puerta de Embarque”⁴.

Con la colaboración de Everis Aeroespacial, Dormakaba y Defensa y Seguridad, implementaron tecnologías para la validación de los datos biométricos del pasajero, como son sus rasgos faciales y pasaporte con el objetivo de agilizar el proceso de

³ ¿CÓMO HACER PAGOS CON RECONOCIMIENTO FACIAL EN COLOMBIA? Negocios, E. y. (07 de febrero de 2020) Dinero, págs. <https://www.dinero.com/tecnologia/articulo/como-hacer-pagos-con-reconocimiento-facial-en-colombia/281547>.

⁴ EL RECONOCIMIENTO FACIAL, PIONERO EN UN AEROPUERTO ESPAÑOL: ASÍ FUNCIONA EN MENORCA. Brands, E. (25 de Julio de 2019). El Confidencial, pág. 1. Obtenido de El Confidencial: https://www.elconfidencial.com/tecnologia/2019-07-25/biometria-reconocimiento-facial-aeropuertos-aena-bra_2133875/

embarque sin necesidad de mostrar el billete aéreo o su documento. Lo más importante de esta implementación es la protección de los datos personales, el uso de esta información están bajo el acuerdo RGPD (Reglamento General de Protección de Datos) este reglamento fue establecido en la Unión Europea 2016/680 ⁵.

Por tal motivo toda información que es usada durante la estancia del viajero dentro del aeropuerto es eliminada después de su embarque. Convirtiéndose en el “Aeropuerto 4.0 de Aena (Aeropuertos Españoles y Navegación Aérea)”⁶ siendo este uno de los aeropuertos con la mejor prestación de servicios aeroportuarios.

2.1.3 Uso de un sistema biométrico para el ingreso y salida de vehículos en los centros comerciales en Sudáfrica

Para realizar el pago del uso del establecimiento de parqueo en los centros comerciales en Sudáfrica, se utiliza la huella dactilar, con el fin de agilizar el pago sin la necesidad de que el cliente tenga que mostrar una factura. Esta iniciativa ha sido buena ya que evita el consumo de papel, cuando el dedo del cliente es escaneado por el sistema, éste le informa al personal que se encuentra en la salida del establecimiento que esté ya realizó su pago⁷.

2.1.4 Control de acceso biométrico para transmisiones de medios digitales en redes para el hogar

En este documento se puede observar una variedad de aplicaciones que podrían tener un control de acceso biométrico para la retransmisión de contenido de IPTV para el hogar. Donde los usuarios que quieran hacer uso del servicio deberán ser agregados por un usuario maestro, este proceso se hace mediante módulos de reconocimiento facial o por medio de autenticación de huellas digitales. Para el acceso al contenido se requiere de las huellas mediante un PDA (Asistente Digital Personal) que principalmente podría ser un celular o cualquier dispositivo de bolsillo que tenga conexión a Internet.

⁵ XATAKA. Arantxa, H. (07 de marzo de 2018). Obtenido de Xataka: <https://www.xataka.com/legislacion-y-derechos/gdpr-rgpd-que-es-y-como-va-a-cambiar-internet-la-nueva-ley-de-proteccion-de-datos>

⁶ AENA. Aena. (2019). Obtenido de AENA: <http://www.aena.es/es/corporativa/perfil-compania.html>

⁷ USING A BIOMETRIC SYSTEM TO CONTROL ACCESS AND EXIT OF VEHICLES AT SHOPPING MALL IN SOUTH AFRICA. R.T.Hans. (29 de agosto de 2014). Obtenido de IEEE: <http://ieeexplore.ieee.org.bdigital.udistrital.edu.co:8080/document/7006236/?part=1>

CAPITULO III

3.1.0 MARCO TEÓRICO

A continuación, se explicará algunos términos y conceptos que serán necesarios para que el lector entienda un poco más de qué se trata un sistema de Biometría y algunos tipos de subsistemas que existen dentro de esta área.

3.1 ¿Qué es Biometría?

La palabra Biometría proviene del griego bios y metrón, donde bios significa vida y metrón que significa medida. Es por ello que se hace referencia a todos los “Equipos biométricos que miden e identifica las características de una persona”⁸.

3.2 Definición de un sistema Biométrico

Un sistema biométrico es un método automático de identificación con el fin de identificar a un usuario en tiempo real. Su principal ventaja es realizar el reconocimiento de una persona por medio de sus rasgos o un patrón único que lo diferencia de los demás.

Para la realización de un sistema biométrico, es necesario distinguir el tipo de registro biométrico. En la Biometría, se distinguen dos tipos, la Biometría Estática y la Biometría Dinámica. Donde la Biometría Estática hace referencia a las características físicas, es decir se enfoca a los aspectos fisiológicos o morfológicos de una persona, como la huella dactilar, las características del iris, patrones en la retina, entre otras. Mientras que la Biometría Dinámica, se enfoca en las características conductuales de una persona, por ejemplo: dinámica de la firma, pulsaciones en el teclado, entre otras.⁹

3.2.1 Funcionamiento de un control de acceso Biométrico

Un dispositivo biométrico consta de tres partes principales para el análisis de la información, por una parte, tenemos un mecanismo que capta y lee los datos de una imagen analógica o digital, en donde se guardan estos datos obtenidos en una base de información. Por otra parte, se encuentra un mecanismo que realiza la

⁸ KASPERSKY. KASPERSKY. (02 de marzo de 2020). Obtenido de <https://latam.kaspersky.com/resource-center/definitions/biometrics>

⁹ BYOSIS. Byosis. (2019). Obtenido de <https://www.biosys.es/sistemas-biometricos/>

comprensión, almacenamiento y comparación de los datos obtenidos. Y por último se encuentra la interfaz que se usa para la obtención de los datos dependiendo de sus aplicaciones.

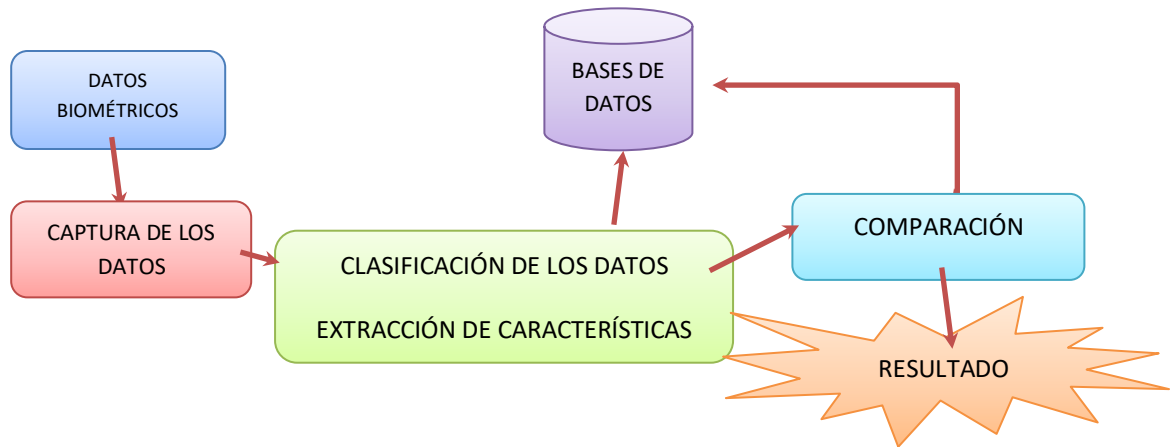


Figura 1. Fases de un sistema biométrico. Fuente: Autor

3.3 Tipos de Sistemas Biométricos

Las características principales de un sistema Biométrico es que tienen un desempeño rápido y exacto con respecto a la identificación de un individuo. A la hora de determinar su desempeño es necesario tener en cuenta ciertos factores como los recursos tecnológicos que se invirtieron en su fabricación, costos y cantidad de dispositivos que serán necesarios de acuerdo a la cantidad de usuarios y efectos ambientales. Otra característica de los sistemas Biométricos, es su fiabilidad.

Para que un sistema biométrico sea 100% seguro este debe de reconocer las características de una persona viva. Ya que pueden existir mecanismos sencillos que pueden llegar a burlar la seguridad de este tipo de sistemas, como explica un estudio de la Universidad de Clarkson, en donde se comprobó que es posible engañar a los dispositivos como los lectores de huellas digitales. Ya que es posible recrear una huella digital en un molde de plástico, plastilina o hasta en gelatina. Por ende, en ciertas situaciones depende de la ética de la persona.¹⁰

Por lo que en la actualidad varias empresas han buscado la manera de mitigar estos problemas, al hacer uso de las diferentes combinaciones de los sistemas biométricos o modificando sus sistemas para que estos detecten con mayor

¹⁰ DCHAIN. Flory, N. (2018). Obtenido de <http://dchain.com/caracteristicas-de-un-sistema-biometrico/>

profundidad las características de la persona. Como, por ejemplo, la “Biometría Multi-Modal”¹¹. La cual realiza las siguientes combinaciones:

- Iris + Huella Dactilar + Rostro
- Iris + Huella Dactilar + Venas
- Huella Dactilar + Firma

A continuación, se describirán los cuatro tipos de sistemas Biométricos más conocidos y utilizados por las empresas en la actualidad.

3.3.1 Lectores de Huellas Dactilares

Lo primero que se debe saber es que ninguna persona posee las mismas huellas dactilares que otra. Porque cada huella dactilar está conformada por un conjunto de pequeños arcos, ángulos, remolinos, entre otros aspectos referentes a su forma, como se puede observar en la siguiente Figura.



*Figura 2. Imagen de una huella dactilar*¹². Fuente: Tipos de Sistemas Biométricos.

Una huella dactilar tiene aproximadamente 30 minucias. La Oficina Federal de Investigaciones (FBI) de EE. UU. ha demostrado que “no existen dos personas que puedan tener más de ocho minucias en común”¹³. Por otro lado, cabe resaltar que los Lectores de Huellas Dactilares son los sistemas biométricos más usados en la actualidad. Ya que estos sistemas son muy útiles para restringir accesos hasta controlar el uso de dispositivos o el ingreso a las instalaciones de una empresa.

Algunos inconvenientes que presentan este tipo de sistemas, que no siempre puede ser utilizado en las personas, a lo que se hace referencia en este caso es que, dependiendo del tipo de trabajo, se pueden encontrar casos en los que los trabajadores tienen la huella dactilar desgastada o posiblemente no tienen una. En la mayoría de estos casos sucede debido a que el trabajador ha estado sometido a duras condiciones y a medida que pasa el tiempo sus huellas van desapareciendo,

¹¹ MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE DE ESPAÑA. Misfud, E. (27 de abril de 2012). Obtenido de <http://recursostic.educacion.es/observatorio/web/ca/cajon-de-sastre/38-cajon-de-sastre/1045-sistemas-fisicos-y-biometricos-de-seguridad>

¹² "Tipos de sistemas biométricos - Sistemas Biométricos", Sites.google.com, 2020. [Online]. Obtenido de: <https://sites.google.com/site/sistemasbiometricosvaldivia/home/huella-dactilar>. [Acceso: 06- abril- 2020].

¹³ BIOMETRICS. GEMALTO. (26 de febrero de 2020). Obtenido de Authentication & Identification (definition, trends, use cases, lwas and latest news): <https://www.gemalto.com/govt/inspired/biometrics>

por ejemplo, el uso o manejo de químicos, productos congelados, trabajos en la industria del metal, entre otros.

Históricamente hablando el reconocimiento de huellas dactilares comenzó en los años 60, el primer sistema de identificación de personas por huellas dactilares fue creado por Juan Vucetich, este procedimiento se creó y se patentó en Argentina, para este procedimiento se hizo uso de 101 casos de diferentes huellas donde se clasificaron en 4 grupos de acuerdo a sus formas. En arcos, presillas internas, presillas externas y verticilos. El primer caso en el que se hizo uso de este procedimiento fue en 1892 en un caso de asesinato donde identificaron que el culpable era la madre de los hijos y no el esposo, esclareciendo el crimen. Por ende, este sistema fue de suma importancia para la identificación de criminales ya que así podían mantener un control de seguridad.

A continuación, se explicará la clasificación de los tipos de huellas dactilares.

3.3.1.1 Tipos de Huellas Dactilares

En nuestras puntas de los dedos podemos encontrar diferentes dactilogramas, un dactilograma son las formas de las crestas que dan forma única a nuestra huella dactilar. Existen tres tipos:

- Dactilograma Natural: Se encuentra en la yema del dedo y forma las crestas de forma natural.
- Dactilograma Artificial: Son las copias de un dactilograma natural, estas se obtienen por medio del uso de una tinta.
- Dactilograma Latente: Estas huellas se encuentran en objetos y no son visibles a simple vista, a menos que se aplique un reactivo.

Ya para los años 80 se hace uso de dispositivos electrónicos como computadores y dispositivos de captura en aplicaciones. Con la evolución de las comunicaciones y el intercambio de la información, el uso y recopilación de la información de una huella dactilar se ha convertido en un asunto complejo, es por tal motivo que se crearon diferentes métodos para la adquisición de huellas, haciendo los sistemas de seguridad más rigurosos y exigentes.

Para la identificación exitosa de una huella dactilar, se siguen tres pasos principales. El primer paso consiste en la adquisición de las huellas, el segundo paso es la extracción de las características de las crestas que componen la huella y por último está la comparación de los patrones de las huellas recopiladas anteriormente con la muestra que se toma diariamente del sujeto.

3.3.2 Control Biométrico por verificación de voz

Este tipo de sistema utiliza el tono de voz de cada persona. Algunos inconvenientes que presenta este tipo de sistemas, es que, al momento de verificar la identidad del individuo, se pueden presentar interferencias al momento de verificar la voz, debido a ciertas condiciones en el ambiente como lo son los ruidos exteriores, alguna enfermedad que pueda afectar el tono de la voz o hasta el envejecimiento de la persona.

Este tipo de tecnología tiene tres formas de reconocer la voz:

- Dependencia: El usuario repite siempre el mismo texto.
- Texto aleatorio: El sistema genera un texto aleatorio en el que el usuario tendrá que repetir.
- Independencia del texto: El usuario puede decir cualquier frase.

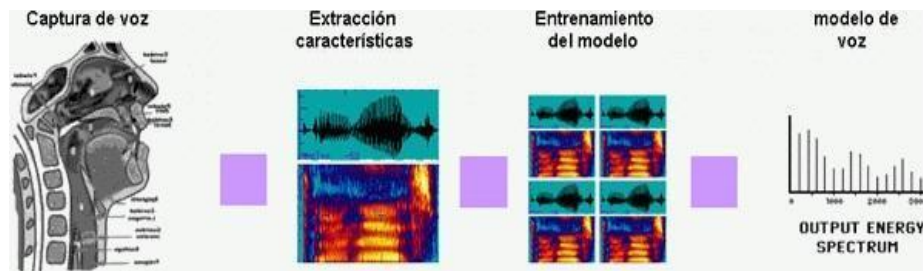


Figura 3. Modelado de la captura de un fragmento de voz de una persona ¹⁴.

Fuente: Proyecto Fin de carrera (Modelado, Diseño e Implementación de una plataforma Biométrica).

3.3.3 Reconocimiento por patrones

El reconocimiento de patrones es una de las ramas importantes en la Inteligencia Artificial, ya que permite clasificar la información en categorías o en patrones. Gracias al uso de diferentes sistemas informáticos para la adquisición de señales o imágenes de las cuales se pueden obtener características de los objetos para la identificación de los mismos. Es por tal motivo que a partir de esto se derivan algunos conceptos que se deben tener en cuenta.

- Patrón: Un patrón es un conjunto de características de una imagen.

¹⁴ D. Osuna Escorihuela, "Modalidad de voz", E-archivo.uc3m.es, 2011. [Online]. Obtenido de: https://e-archivo.uc3m.es/bitstream/handle/10016/13197/PFC_Daniel_Osuna_Escorihuela.pdf;jsessionid=E77EB55F8894CB6A231E9E46BF5D8B11?sequence=1. [Acceso: 08- abril- 2020].

- Clase de patrones: Conjunto de patrones que son similares.
- Extracción de características: La cual busca extraer información importante que determinará su clasificación.

El objetivo de la Biometría por patrones es asignar el patrón a la clase que pertenece. Para su clasificación se dividen en diferentes enfoques. Por un lado, podemos encontrar el reconocimiento lógico combinatorio de patrones, donde se busca modelar los problemas lo más cercano a la realidad sin la necesidad de fundamentos. El enfoque estadístico analiza la muestra y a partir de esto realiza el reconocimiento mediante el uso de medidas numéricas y de probabilidad. Por último, el enfoque sintáctico busca las relaciones que tienen los patrones y se hace un estudio en base a teorías del lenguaje formal.

A continuación, se explicará los tipos de patrones que están presentes en un objeto.

3.3.3.1 Tipos de patrones

- **Patrones Vectoriales:** Reconocen diferentes objetos por medio de la recopilación de sus características, comparándolos con diferentes grupos que tienen diferentes descripciones.
- **Patrones Estructurados:** La recopilación de las muestras son codificados mediante las relaciones de los componentes del objeto, este tipo de patrones son usados generalmente en las huellas dactilares, porque cada una es única.

En este tipo de sistema, existen dos formas de reconocimiento ocular, uno de ellos es el reconocimiento por retina y el otro es el reconocimiento por Iris.

3.3.4 Reconocimiento por retina

El reconocimiento por retina mide el patrón de los vasos sanguíneos en el fondo del ojo, para la detección de estos patrones es necesario proyectar una luz infrarroja a través de la pupila. “El descubrimiento de este tipo de patrones se remonta a principios del siglo XX”¹⁵. Este hecho se dio a mediados del año 1935 cuando los oftalmólogos Carleton Simon e Isadore Golstein, se dieron cuenta en una de sus investigaciones que era imposible tener a dos personas que presentaran el mismo patrón capilar de sus retinas.

¹⁵ BIOMETRICS. GEMALTO. (26 de febrero de 2020). Obtenido de Authentication & Identification (definition, trends, use cases,lwas and latest news): <https://www.gemalto.com/govt/inspired/biometrics>

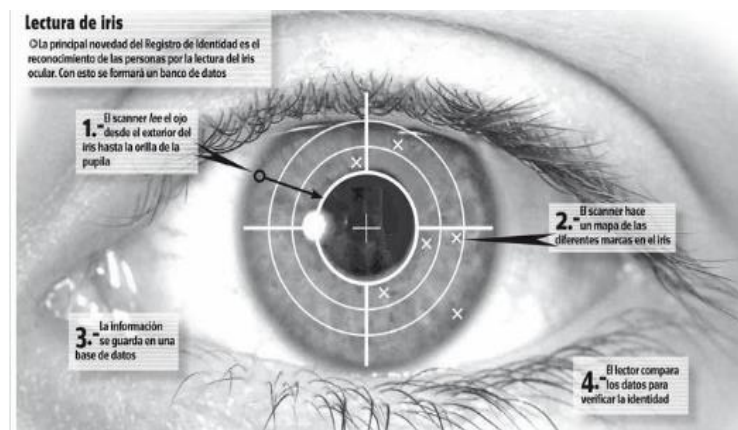
Para finales del año 1970 fue patentado el primer escáner de retina, a partir de ese momento inició su comercialización en el campo de la medicina, así como para el ámbito de la biometría. Para entender un poco mejor cómo funciona este tipo de sistema biométrico, se explicará brevemente su funcionalidad.

3.3.4.1 Funcionamiento del Sistema Biométrico por Retina

Es un tipo de tecnología biométrica invasiva la cual captura y analiza los patrones vasculares que se encuentran ubicados alrededor del nervio óptico. El escáner ilumina con luz infrarroja la región de la retina, almacenando información sobre el contraste de los patrones vasculares que se reflejan. Algunos problemas que se pueden presentar en el escaneo de retina, pueden suceder por problemas ópticos de las personas.

3.3.5 Reconocimiento por Iris

El reconocimiento por iris es más estable que usar otras características del ojo como son el caso de la retina o la córnea. Algunas ventajas al hacer uso de la retina son el antifraude, independientemente del estado de la persona el reconocimiento es posible sin importar las variaciones de la iluminación. Además de que es una técnica exacta, para la recolección de los datos se emplean unas cámaras infrarrojas especiales con el fin de obtener una imagen correcta del iris. “Esta técnica no es invasiva ya que debido a que la córnea está lubricada, éste posee un alto índice de reflexión por lo que el escáner no afecta directamente el ojo”¹⁶.



¹⁶ ¿EL RECONOCIMIENTO DE IRIS ES UNA TÉCNICA INVASIVA? Serban. (31 de Julio de 2018). Obtenido de ¿EL RECONOCIMIENTO DE IRIS ES UNA TÉCNICA INVASIVA?: <https://www.serban.es/reconocimiento-de-iris-tecnica-no-invasiva/>

Figura 4. Lectura del Iris¹⁷. Fuente: Reconocimiento del Iris.

Una vez que la imagen del iris ha sido capturada se realiza un procesamiento de la imagen obtenida con el fin de aislar el iris con el resto de la imagen, una vez que está procesada la imagen se realiza la extracción de las características biométricas y por último se realiza la comparación 1: N con los datos almacenados anteriormente del individuo para así confirmar qué es la persona correcta.

3.3.6 Reconocimiento Facial

En los últimos años el reconocimiento facial ha tomado fuerza en el área de la investigación como es en el análisis de imágenes, extracción de características de archivos digitales, entre otros. Este tipo de procedimiento emula la identificación de una persona siguiendo un patrón específico que se encuentra en nuestro cerebro. Según un estudio que se realizó por una revista científica, demostraron que la neuroimagen muestra pequeñas regiones que se encuentran en el lóbulo temporal del cerebro, las cuales se encargan del reconocimiento de las caras. Nombrando a estas regiones como “Áreas Faciales”¹⁸ estas regiones se encargan principalmente de reconocer ciertas características únicas de una persona como su color de piel, tamaño de los ojos, nariz, contorno, todo este proceso se realiza de manera semiconsciente, en otras palabras, podemos decir que cada persona realiza toda esta captura de datos sin que se cuenta.

Y es a partir de este estudio que se ha definido el sistema de reconocimiento facial como un ordenador que identifica automáticamente los rasgos faciales de una persona y la convierte en una imagen digital. Este procedimiento se realiza mediante un análisis de las características faciales, obtenidas por una imagen o por un fotograma (video), como se puede observar en la Figura 5, para así poder realizar la comparación de los datos obtenidos con la base de datos.

¹⁷ R. iris, "Reconocimiento de iris", Innovagalingenieriasseguridad1.blogspot.com, 2020. [Online]. Obtenido de: <http://innovagalingenieriasseguridad1.blogspot.com/2011/11/reconocimiento-de-iris.html>. [Acceso: 10-abril- 2020].

¹⁸ INVESTIGACIÓN CIENTÍFICA. Sheikh, K. (1 de agosto de 2017). Obtenido de Quedarse con la cara: <https://www.investigacionyciencia.es/revistas/investigacion-yciencia/el-multiverso-cuntico-711/quedarse-con-la-cara-15476>



Figura 5. Fotograma Facial¹⁹. Fuente: Reconocimiento Facial

Para que el proceso de reconocimiento facial sea exitoso se deben tener en cuenta las siguientes fases. La primera es la detección del rostro del individuo, la segunda es la extracción de las características faciales y por último la clasificación y reconocimiento facial.

En la Figura 6, se muestra todo el procedimiento que se lleva a cabo para el reconocimiento facial de una persona.

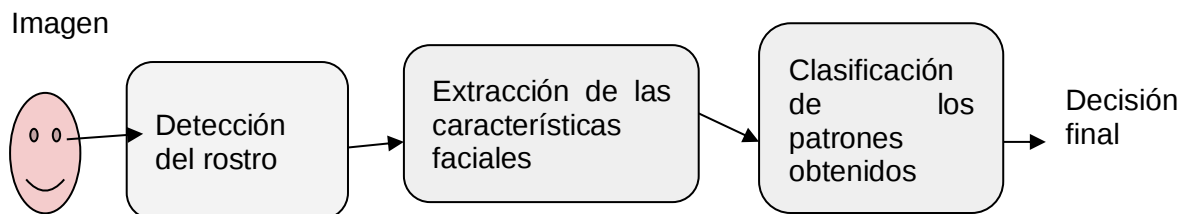


Figura 6. Proceso del reconocimiento facial. Fuente: Autor.

3.3.6.1 Fases de un reconocimiento facial

En esta parte se hablará de algunos conceptos teóricos sobre el funcionamiento de un sistema de control de acceso a partir de la detección facial, extracción de las características y la clasificación de los patrones extraídos.

Las fases o etapas del reconocimiento facial son 5 principalmente:

- Detección del rostro
- Acondicionamiento

¹⁹RECONOCIMIENTO FACIAL, R. Facial, Sites.google.com, 2020. [Online]. Obtenido de: <https://sites.google.com/site/recofacialzs/>. [Acceso: 20- abril- 2020].

- Normalización
- Extracción de las características
- Reconocimiento

3.3.6.1.1 Detección del rostro

Principalmente en la detección se busca localizar la región facial ignorando el fondo de la imagen. Para ello se utilizan plantillas que ayudan a la detección de la cara y eliminan los patrones que no son rostros, denominadas “**bootstrap**” o EigenFace.

Bootstrap es una técnica de identificación que se basa en patrones, estos patrones son los rostros de las personas, donde los falsos positivos de una imagen se agregan como “patrones de no-rostro”²⁰ cuando aparecen nuevos falsos positivos se seguirán agregando como patrones, de tal manera que esta técnica sirve como un clasificador de patrones. Por otro lado, EigenFace es una herramienta matemática PCA, la cual “comprime las imágenes obtenidas del PCA formando espacios de fracciones”²¹, cada espacio es una matriz que contiene una serie de vectores que contienen la variación de valores grises de cada pixel obtenido de la imagen, formando así una imagen normalizada. En la parte de clasificación se busca que la imagen facial sea más parecida a la muestra que se obtuvo.

3.3.6.1.2 Acondicionamiento

En la parte del acondicionamiento se localiza las componentes y escalas a la que se encuentra el rostro, este proceso se realiza mediante transformaciones geométricas²².

3.3.6.1.3 Normalización

La “Normalización Espacial”²³ busca alinear los centros del rostro, como los ojos, determinando el número de píxeles entre la distancia que hay entre ellos, además también se realiza la extracción de las características de solo la región facial,

²⁰ SISTEMA DE RECONOCIMIENTO FACIAL. Scarel, G. M. (2010). Universidad Nacional del Litoral, Facultad de Ingeniería y Ciencias Hídricas, 16.

²¹ EXE. EXE. (29 de junio de 2017). Obtenido de La ciencia tras un sistema de reconocimiento facial: <http://www.exe.cl/idi/la-ciencia-tras-un-sistema-de-reconocimiento-facial/>

²² RECONOCIMIENTO FACIAL CON BASE EN IMÁGENES. José Augusto Cadena, R. H. (15 de mayo de 2017). Obtenido de Universidad Técnica de Cotopaxi: <https://dialnet.unirioja.es/servlet/articulo?codigo=6145639>

²³ HERRAMIENTA DE RECONOCIMIENTO FACIAL. CASO PRÁCTICO: ACCESO A SISTEMA DE PRÉSTAMO DE LIBROS. ESCOM, 8-40. Aparicio Duran Carmen, C. S. (17 de mayo de 2017). Obtenido de <https://repository.ucatolica.edu.co/bitstream/10983/24032/1/Final%20Trabajo%20de%20grado.pdf>

omitiendo otros factores como el cabello. Después de obtenidos los datos de la imagen se convierte esta información en vectores, mediante la concatenación de las filas de la imagen.

3.3.6.1.4 Extracción de características

La extracción de las características consiste en la obtención de los rasgos característicos de cada rostro para que después puedan ser clasificados en diferentes enfoques.

- Enfoque Holístico, se basa en que la imagen del rostro es un todo.
- Enfoque de las características locales, a este tipo de enfoque se da importancia a las diferentes partes de la cara.
- Enfoque Híbrido, este enfoque abarca todas las características locales tanto globales para hacer el reconocimiento.

A continuación, se explicará algunos métodos para la extracción de las características.

3.3.6.1.4.1 Active Shape Model (ASM) - Modelo de forma Activa

Este tipo de modelo se concentra en los rasgos complejos y claves de la cara, como la nariz, ojos, boca, cejas y labios. Es un modelo estadístico que se construye a partir de un conjunto de imágenes que contienen puntos de referencia. Los ASM se clasifican en: “Snakes, Deformable Templates y Point Distribution Model”²⁴.

- Snakes, son usados para determinar los límites de la cabeza de la persona.
- Deformable Templates, es una mejoría de Snakes al incorporar información del ojo.
- Point Distribution Model (PDM), este modelo muestra las formas faciales como son los vectores. Da forma a los puntos obtenidos de la imagen facial y se construye una PDM.

²⁴ FACE DETECTION APPROACHES: A SURVEY. INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY, Modi, M. F. (2014). Pág. 1107-11108.

3.3.6.1.4.2 Análisis de bajo nivel

Este análisis se basa en la obtención de “características visuales de bajo nivel, como el color de la piel, movimiento, escala de grises”²⁵

- Color de piel, esta característica es fácil de detectar durante el procedimiento de extracción de la imagen.
- Movimiento, en casos donde se hace uso de secuencias de video como un sistema de vigilancia, se podrá ver las siluetas como partes de la cara y el cuerpo de las personas.
- Escala de grises, cuando se hace uso la escala de grises es muy conveniente ya que algunos rasgos como cejas, labios y pupilas son más oscuros que otras regiones de la cara.

3.3.6.1.5 Reconocimiento

En la parte del reconocimiento se realiza la clasificación de las características extraídas del rostro de la persona. Donde se determina un patrón de entrada el cual será identificado como un miembro de una clase ya predeterminada. Por lo tanto, para el reconocimiento de la persona se debe determinar el sujeto, basados en las aproximadas encontradas en el patrón del rostro del sujeto se puede determinar su clasificación, para el diseño de los clasificadores se pueden distinguir tres aproximaciones, estas están basadas en la similitud, aproximación probabilística y optimización de un criterio de error.

Las aproximaciones basadas en la similitud son simples ya que los patrones parecidos son asignados a una misma clase, esto se realiza mediante una plantilla. Un ejemplo es la técnica de Eigenfaces, la cual busca el vecino más cercano mediante la distancia de Euclides, por lo tanto, cada resultado es la media de los patrones de entrenamiento.

La aproximación probabilística consiste en la toma de decisiones estadísticas para poder establecer los bordes de las diferentes clases, por lo que cada patrón es una densidad de probabilidad. Por último, la aproximación por criterio de error, consiste en la minimización de los errores de la respuesta obtenida y la salida del clasificador.

A continuación, se podrá observar la Tabla 1, donde se muestran los modelos de reconocimiento que plantea un enfoque, representación de los píxeles y algunas de sus características.

²⁵ FACE DETECTION APPROACHES: A SURVEY. INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY, Modi, M. F. (2014). Pág. 1107-11108.

Tabla 1. Modelos de reconocimiento de patrones ²⁶. Fuente: Statistical Pattern Recognition

Enfoque	Representación	Función de reconocimiento	Criterio típico
Comparación de plantillas	Muestras, píxeles, curvas	Correlación, medida de distancia	Error de clasificación
Estadístico	Características	Función discriminante	Error de clasificación
Sintáctico o estructural	Primitivas	Reglas, gramática	Error de aceptación
Redes neuronales	Muestras, píxeles, características	Función de red	Error cuadrático medio

3.3.7 Deep learning de Hikvision

A continuación, se explicará de forma sencilla y concreta en qué consiste la solución de Acceso a instalaciones que ofrece Hikvision a sus clientes.

El Deep learning es una extensión de la tecnología SDT (Tecnología de datos de Vigilancia), donde las tecnologías aprenden profundamente volviéndose más poderosas. Es por tal motivo que este tipo de tecnologías fortalecerá la seguridad en todos sus ámbitos. Usa “una red neuronal artificial y estos se componen en diferentes niveles jerárquicos”²⁷. El nivel inicial (Capa de entrada) consiste en que la red aprende algo nuevo y luego envía esta información al siguiente nivel. En el siguiente nivel (Capa oculta) se toma la información que se suministró del anterior nivel, la combina y compone una nueva información un poco más compleja. En el último nivel (Capa de Salida) se toma la decisión de la información y muestra los datos de salida.

Para tener una mejor idea de cómo funciona Deep learning, se puede observar en la Figura 7.

²⁶ Vista de Reconocimiento óptico de números escritos a mano usando funciones de base radial y sistema memética diferencial | Revista vínculos", Revistas.udistrital.edu.co, 2020. [Online]. Obtenido de: <https://revistas.udistrital.edu.co/index.php/vinculos/article/view/8016/9801>. [Acceso: 20- mayo- 2020].

²⁷ INDRA. Moreno, C. G. (s.f.). Obtenido de Blog NEO: <https://www.indracompany.com/es/blogneo/deep-learning-sirve>

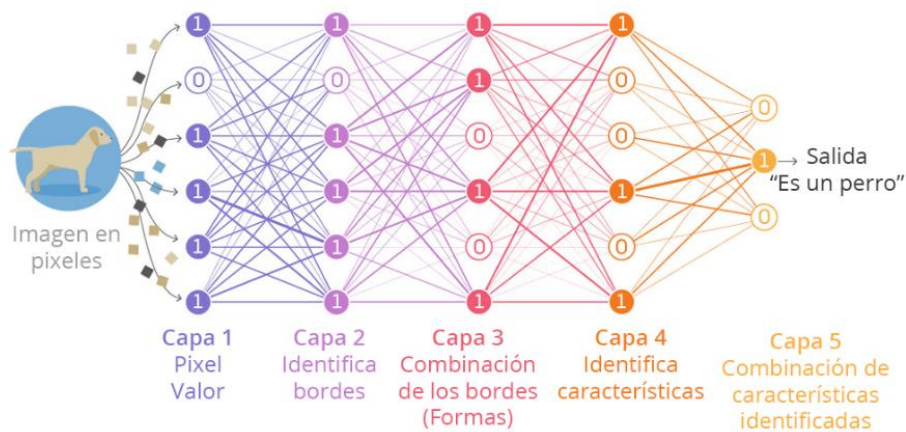


Figura 7. Ejemplo del Funcionamiento de Deep learning²⁸. Fuente: Quanta Magazine.

La idea de hacer uso de este tipo de herramienta es poder desmembrar la imagen tomada por el sistema de cámaras DeepInView y enviar los trozos de la imagen a las diferentes neuronas que componen el segundo nivel. Una vez llegan estos trozos al segundo nivel, se procesan cada uno de los píxeles y delimita los bordes. En el tercer nivel se combinan los bordes y se diseña nuevas formas. En el cuarto nivel se identifica las características de la imagen, en el siguiente nivel se hace la combinación de las características identificadas y envía una conclusión de la imagen. Por último, en la salida mostrará si es o no la persona registrada anteriormente en el sistema de seguridad y vigilancia.

Algunas ventajas que se tiene al hacer uso de este tipo de esta tecnología son:

- Es un algoritmo inteligente tradicional que solo opera en un solo nivel de la superficie. Actualmente los sistemas actuales sufren de baja exactitud, mala adecuación ambiental y tienen menos tipos de reconocimiento.
- Es un modelo algorítmico profundo, donde una señal original pasa por diferentes capas de procesamiento, haciendo una compresión parcial de la imagen y al realizar la abstracción de las características se puede percibir un solo objeto.
- Aprendizaje de funciones, donde una computadora extrae las características por sí solo. Por ende, entre mayor sea el número de características más preciso será el reconocimiento y su clasificación.

²⁸ Quanta Magazine - Illuminating Science | Quanta Magazine, Quanta Magazine, 2020. [Online]. Obtenido de: <https://www.quantamagazine.org/>. [Acceso: 21- mayo- 2020].

3.3.7.1 Características del Deep learning

Algunas de las características del Deep learning son:

- Escala de Datos, debido a la cantidad de datos que se manejan en el entrenamiento de la calidad, los diferentes modelos de reconocimiento de patrones de objetos serán más precisos para el caso de la video vigilancia.
- Poder computacional, debido al desarrollo de GPUs (Unidades de procesamiento gráfico), los superordenadores y el uso de plataformas en la nube, han permitido que el aprendizaje referente a nuevos sistemas artificiales sea más profundo.
- Arquitectura de red, gracias a la optimización constante en los algoritmos de aprendizaje profundo, permite que el reconocimiento del objeto sea más rápido.

CAPITULO IV

4.1.0 DESARROLLO DEL PROYECTO

En este capítulo se explicará a detalle los requerimientos necesarios para el control de acceso, esquema del actual sistema de control de acceso y planos de donde se encuentran ubicados los lectores biométricos de ORANGE BUSINESS SERVICES. Por otro lado, también se hará un análisis de los diferentes proveedores revisando las características técnicas y sus costos.

4.1.1 Requerimientos para el control de acceso

Se desea implementar un sistema de control de acceso por medio de:

- Detección facial
- Compatible con el actual sistema de CCTV.
- La creación de eventos.
- Facilidad de manejo.
- Reducción de costos de infraestructura, haciendo uso de cableado actual.

4.1.2 Esquema actual

A continuación, se definirá el esquema actual del sistema de control de acceso de la empresa.

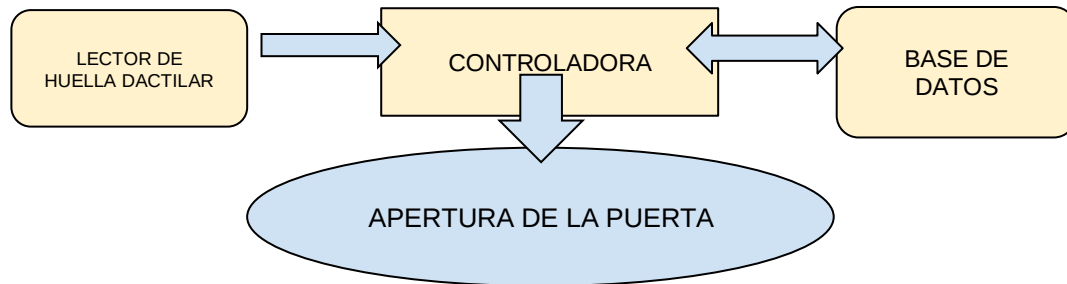


Figura 8. Sistema Actual. Fuente: Autor

4.1.3 Planos de las instalaciones con su sistema Biométrico actual

A continuación, se puede observar en la Figura 9 y en la Figura 10, dónde se visualizan la ubicación actual de los lectores de huella dactilar para el control de acceso del personal de la empresa ORANGE BUSINESS SERVICES.

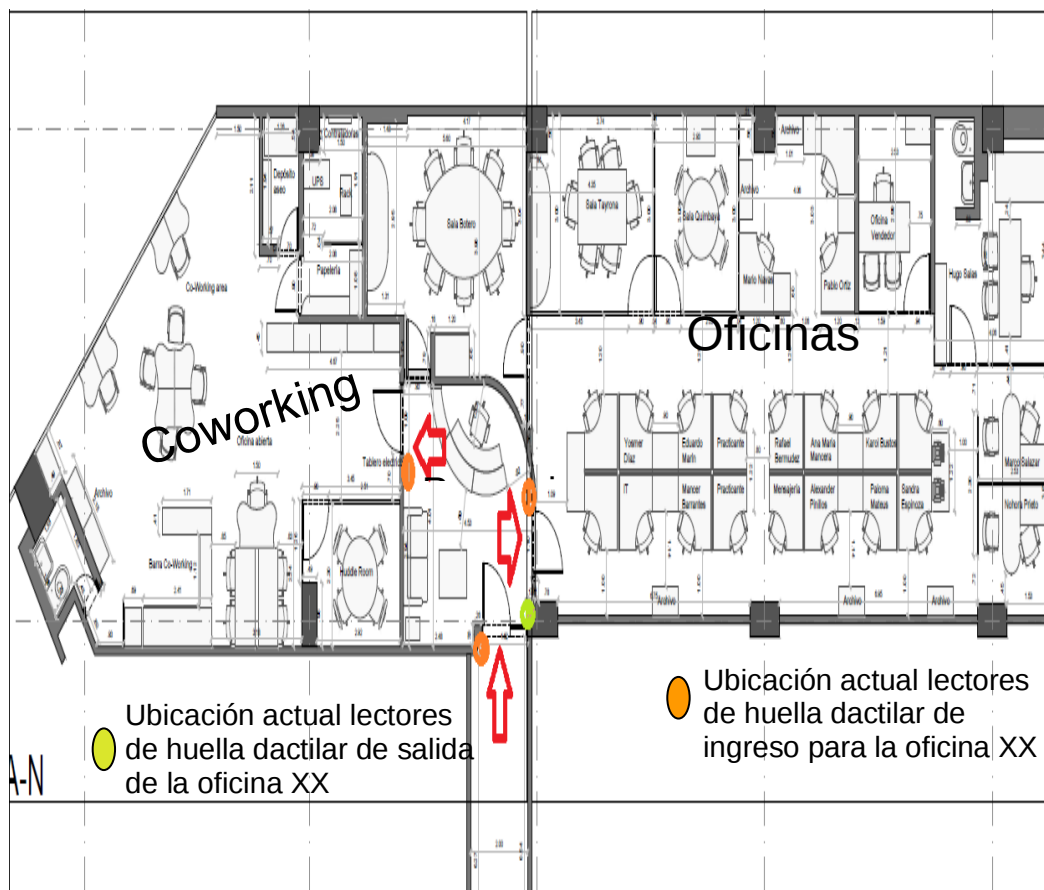
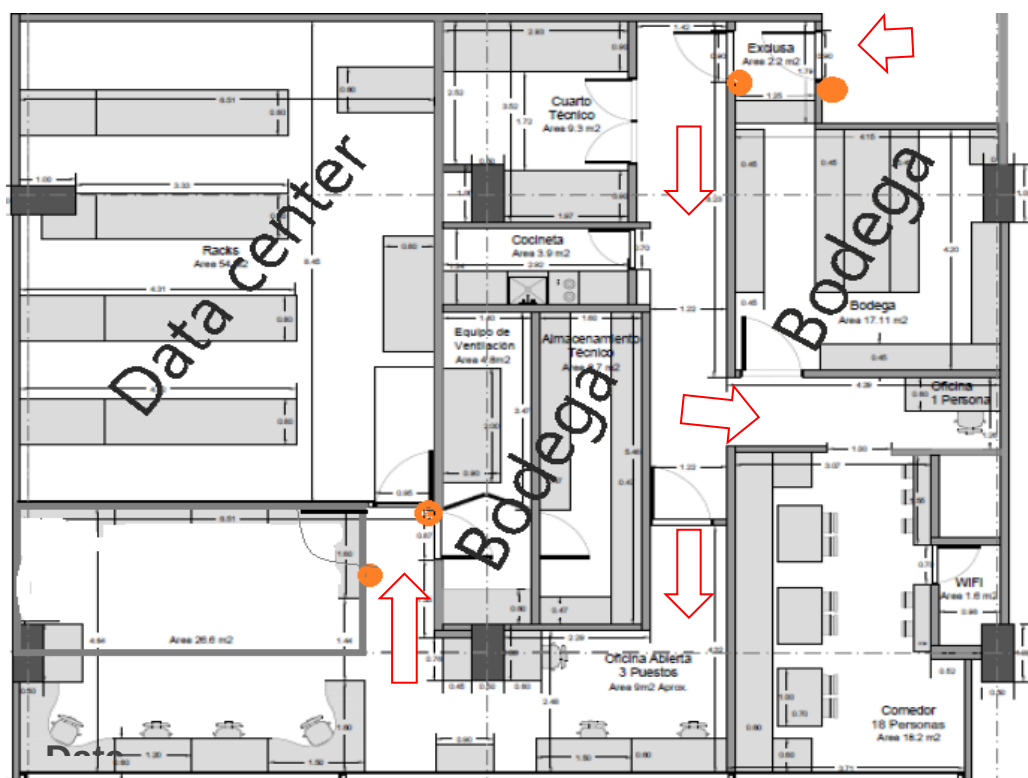


Figura 9. Ubicación actual de los lectores de huella dactilar en la Oficina XX.

Fuente: Propiedad Orange Business Services



Ubicación lectores de huella dactilar
de ingreso de la Oficina YY

Figura 10. Ubicación actual de los lectores de huella dactilar en la Oficina YY.

Fuente: Propiedad Orange Business Services

4.1.4 Cualificación de los beneficios y costos asociados con cada una de las propuestas de solución

A continuación, se explicará en que consiste cada una de las empresas que presentaron su propuesta de solución, algunos casos de éxito que ha tenido la empresa o casos en donde se ha empleado ese tipo de tecnología, por otro lado, se realiza el DOFA de cada una, para analizar cómo se encuentra actualmente la empresa, demostrando cuáles son sus fortalezas, debilidades, oportunidades y amenazas. También se especificará las características técnicas, costos y topología de conexión de cada una de las propuestas de solución.

4.1.4.1 SOLUCIÓN POR PARTE DE IOT TECH

IOT Tech es una empresa en Colombia que da soluciones tecnológicas de IOT según las necesidades del cliente. Estudian las necesidades de sus clientes, en el entorno operativo y tecnológico, para así poder implementar soluciones a la medida. Entre sus soluciones tecnológicas hacen uso de tecnología de Hikvision, adaptando tanto el hardware como el software para desarrollar soluciones innovadoras tanto para áreas de la videovigilancia, mercado vertical ofreciendo bienes y servicios específicos a sus clientes finales. Hikvision hace parte de “La Junta de Pequeñas y Medianas Empresas desde mediados de 2010”²⁹ en China.

Por tal motivo IOT Tech les apuesta a tecnologías de buena calidad y que satisfagan las necesidades de sus clientes, ya sea en áreas de la salud, finanzas, seguridad pública, energía y edificios inteligentes.

4.1.4.1.1 DOFA

IOT TECH DOFA

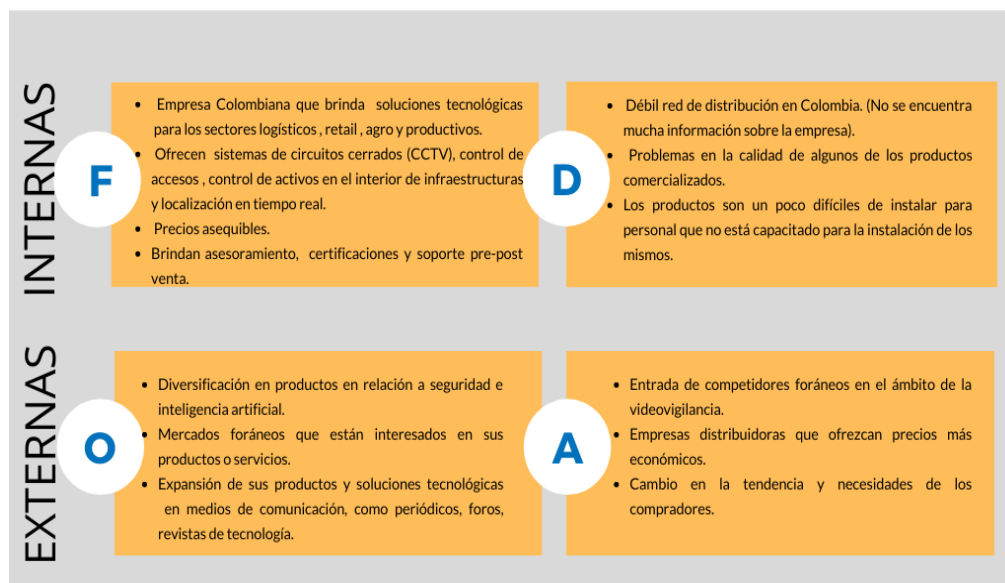


Figura 11. Matriz DOFA sobre la empresa IOT Tech. Fuente: Autor

²⁹ Hikvision. Hikvision. (2020). Obtenido de About Hikvision: <https://www.hikvision.com/es-la/Corporate/About-Hikvision>

A continuación, se realizará un análisis cruzado de las estrategias planteadas en el cuadro anterior, para determinar sus puntos fuertes referidos a los productos que ofrecen.

4.1.4.1.2 Análisis cruzado de las estrategias



Figura 12. Matriz DOFA Cruzado sobre IOT Tech. Fuente: Autor

4.1.4.1.3 Casos de éxito

Algunos casos de uso donde se hace uso de este tipo de tecnología son en el reconocimiento facial, filtro de falsa alarma, conteo de personas, datos estructurados, búsqueda de un cuerpo. En esta sección se explicará un poco de los

casos de éxito que se han obtenido al implementar la tecnología de Hikvision en Colombia³⁰.

- Cámaras Térmicas para la medición de la temperatura corporal en Palmira, al ser una de las ciudades más peligrosas en el país, la administración local ha realizado la implementación de un sistema de seguridad en la ciudad, además de realizar la implementación de una cámara térmica que permite la identificación de personas que puedan presentar fiebre alta dentro de un mercado de la ciudad de Palmira, por ser una de las regiones afectadas por la actual crisis sanitaria.
- Implementación de 3 cámaras térmicas en el Aeropuerto de El Dorado, este sistema permite la identificación de las posibles personas que pueden tener síntomas de fiebre dentro del aeropuerto, lo que permite la facilitación de posibles casos de COVID-19 que ingresen al país o están por salir del país.
- Soluciones de seguridad para la Universidad Nacional de Colombia, este sistema permite un mejor control de las personas que ingresan dentro de las instalaciones de la universidad y realizar el debido seguimiento del individuo dentro de las mismas.

La propuesta presentada oficialmente por IOT Tech frente a los requerimientos solicitada por la empresa consiste en:

- Controladores de acceso – DS-K2604
- Lectores faciales DS-K1T606MF -3 puerta principal – oficinas XX.
- Lectores faciales DS-K1T3331 -5 puertas - oficinas XX & YY.
- Licenciamientos lectores, cada lector tendrá este licenciamiento para la integración con el software de gestión.
- Software de gestión HikCentral.
- Hikcentral, este software permite gestionar dos puertas.

4.1.4.1.4 Características Técnicas de los equipos

En la Tabla 2 se describen las características generales de los equipos propuestos por la empresa IOT Tech para dar solución a la problemática de la empresa.

³⁰HIKVISION DIGITAL TECHNOLOGY. Tecno seguro-noticias, 2020.Obtenido de: <https://www.tecnoseguro.com/empresas/fabricantes/hikvision>

Tabla 2. Características generales de los equipos propuestos en la solución de IOT Tech.

Ítem	Modelo	Descripción	Características
1	DS-K2604	Four-door Access Controller, Storage with 100,000	Controlador de acceso • Control de acceso por horarios y puertas. • Verificación Multi-usuario. • Funciones de primera tarjeta y contraseña. • IP68, IK04, Alta Capacidad • Capacidad: 100.000 tarjetas, 300.000 eventos. • Comunicación: TCP/IP. • 4 entradas Wiegand Multi-Formato. • 8 RS-485 • 4 entradas para sensor de estado de puerta. • 4 entradas para botón de petición de salida (REX). • Incluye fuente de 12VCD / 8A con cargador de batería. Este tipo de controlador también puede trabajar sin tener conexión a la red y cuenta con un interruptor a prueba de manipulaciones.
2	DS-K1T606MF	DeepinGo series Face Recognition Terminal	Terminal de reconocimiento facial • Distancia de reconocimiento facial: 0.3 m a 1 m. • Capacidad: 3.200 rostros, 5.000 tarjetas. • El tiempo de duración para el reconocimiento facial es de 1 segundo. • Cámara de 2 MP, lente angular. • Fuente de alimentación: 12 V CC / 2ª. • Pantalla táctil LCD de 5 pulgadas con una resolución de 480 x 800.
3	DS-K1T331	Face Recognition Terminal	Terminal de reconocimiento facial • Distancia de reconocimiento facial: 0.3 m a 1.5 m. • Capacidad: 300 rostros, 1.500 tarjetas (al conectar un lector de tarjetas externo a través de RS485).

			• El tiempo de duración para el reconocimiento facial es de 1 segundo. • Cámara de 2 MP. • Fuente de alimentación: 12 V DC. • Pantalla táctil LCD de 4.7" × 4.3" × 0.9". • Interfaces: 1 USB, 1 para cerradura eléctrica, 1 para contacto de puerta (door contact), 1 para botón de salida y 1 para RS-485.
4	HikCentral-ACS-Base/2Door	Doors manageable	Puertas Manejables HickCentral-ACS-Base-2Door es un paquete básico de control de acceso el cual incluye los requisitos previos para la ampliación de puertas. Al hacer uso de HikCentral, permite el intercambio de información, cooperación multiservicio, la adición de dispositivos para la gestión, reproducción de archivos de video, entre otras funciones.
5	HikCentral-Attendance-Base	Shift management and attendance report.	Licencia HikCentral El paquete de software HikCentral es una licencia para hasta 64 cámaras. Entre sus funciones permite la gestión avanzada de usuarios, permite integrar video, control de acceso e intrusión. Es una plataforma de gestión centralizada, con una arquitectura cliente-servidor.
6	TL-SG108E	Switch Easy Smart 8 puertos Gigabit	El switch Easy Smart no gestionable es adecuado para redes de pequeñas empresas. Su diseño plug and play permite su despliegue sin necesidad de un técnico, las características de este equipo permiten la gestión inteligente de QoS, VLAN, IGMP Snooping, entre otras.

Fuente: Autor

4.1.4.1.5 Costos

Tabla 3. Propuesta por parte de IOT Tech usando tecnología Hikvision

Ítem	Referencia	Descripción	Cantidad	Precio Unitario	Precio	Precio Total en COP
1	DS-K2604	Four-door Access Controller, Storage with 100,000	1	\$ 542 USD	\$ 542 USD	\$4.336.000
2	DS-K1T606MF	DeepinGo series Face Recognition Terminal	3	\$ 1007 USD	\$ 3.021 USD	\$12.084.000
3	DS-K1T331	Face Recognition Terminal(secundarios)	5	\$456 USD	\$2.280 USD	\$9.120.000
4	HikCentral-ACS-Base/2Door	Doors manageable	4	\$ 178 USD	\$ 712 USD	\$2.848.000
5	HiKCentral-Attendance-Base	Shift management and attendance report.	1	\$ 1035 USD	\$ 1035 USD	\$4.140.000
6	TL-SG108E	Switch 8 Puertos Gigabit No administrable	1	\$63.7 USD	\$63.7 USD	\$254.800
7	Instalación	Cableado, Instalación y puesta en funcionamiento	GL	\$6.670.890	\$6.670.890	
Total					\$ 39.453.690	

Fuente: IOT Tech

4.1.4.1.6 Topología de conexión de control de acceso

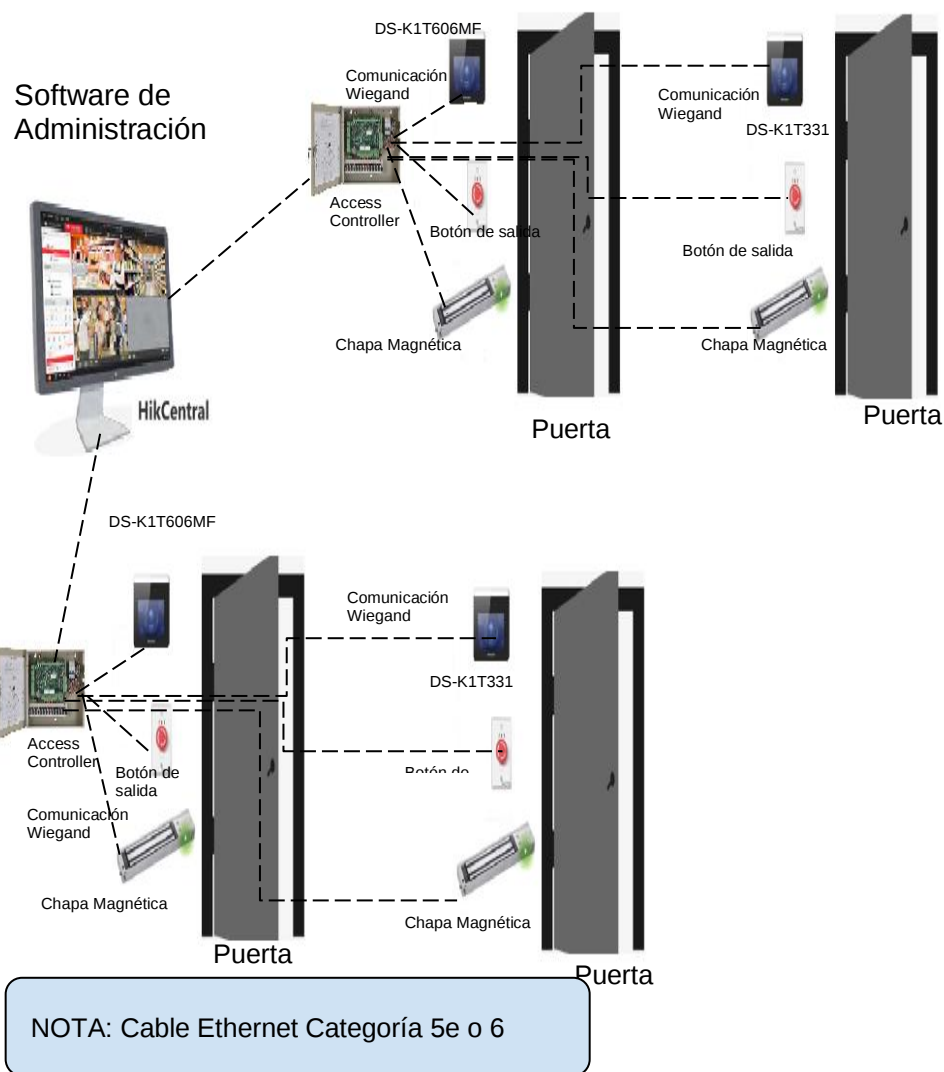


Figura 13. Topología de Conexión de control de acceso usando Hikvision. Fuente: Autor.

Una controladora de Hikvision permite la conexión múltiple de hasta 4 puertas, por lo que es necesario emplear 2 controladoras en el diseño. La conexión entre las controladoras con los lectores faciales, botón de salida y la chapa magnética se realiza mediante conexión Wiegand. Estas controladoras se administran mediante el software de Administración, además permite la integración con el sistema de videovigilancia actual. Siendo un sistema seguro para múltiples puertas usando varios controladores.

4.1.4.2 SOLUCIÓN POR PARTE DE PROWARE HS S.A

PROWARE es una empresa colombiana que fue fundada en el año 1995³¹ (S.A, 2020), con el fin de brindar soluciones y servicios en las áreas de la Informática y las Telecomunicaciones. Es una empresa que provee al mercado nacional toda una gama de equipos tecnológicos, contando con el respaldo directo de los fabricantes, distribuidores y mayoristas. Garantizando su alto desempeño y confiabilidad hacia sus clientes.

Por otro lado, también realiza la comercialización de forma directa o por medio de aliados asociados que permiten el crecimiento de clientes. Algunos de sus productos son Falcon, Aguila y Kantor. Además, tiene presencia directa en 10 ciudades del país.

En sus soluciones siempre buscan mostrar la calidad de ellos, además de comprometer y beneficiar a sus colaboradores mediante una capacitación especializada, con el fin de que sus clientes se encuentren capacitados de cómo es el funcionamiento de los sistemas de acceso que ellos proveen. Por último, siempre busca satisfacer las necesidades de los clientes, generando rentabilidad para sus socios y aliados

³¹ PROWARE. S. A, P. H. (15 de 05 de 2020). Obtenido de Nosotros: <https://www.proware.com.co/nosotros/>

4.1.4.2.1 DOFA

PROWARE H.S S.A DOFA

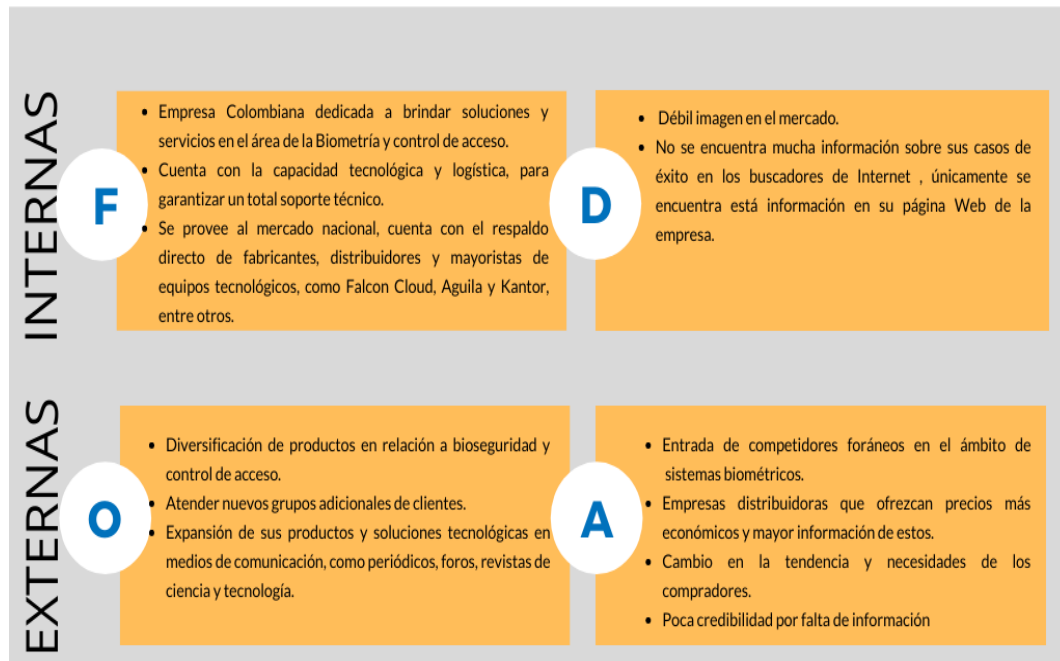


Figura 14. Matriz DOFA sobre la empresa PROWARE HS SA. Fuente: Autor

4.1.4.2.2 Análisis cruzado de las estrategias

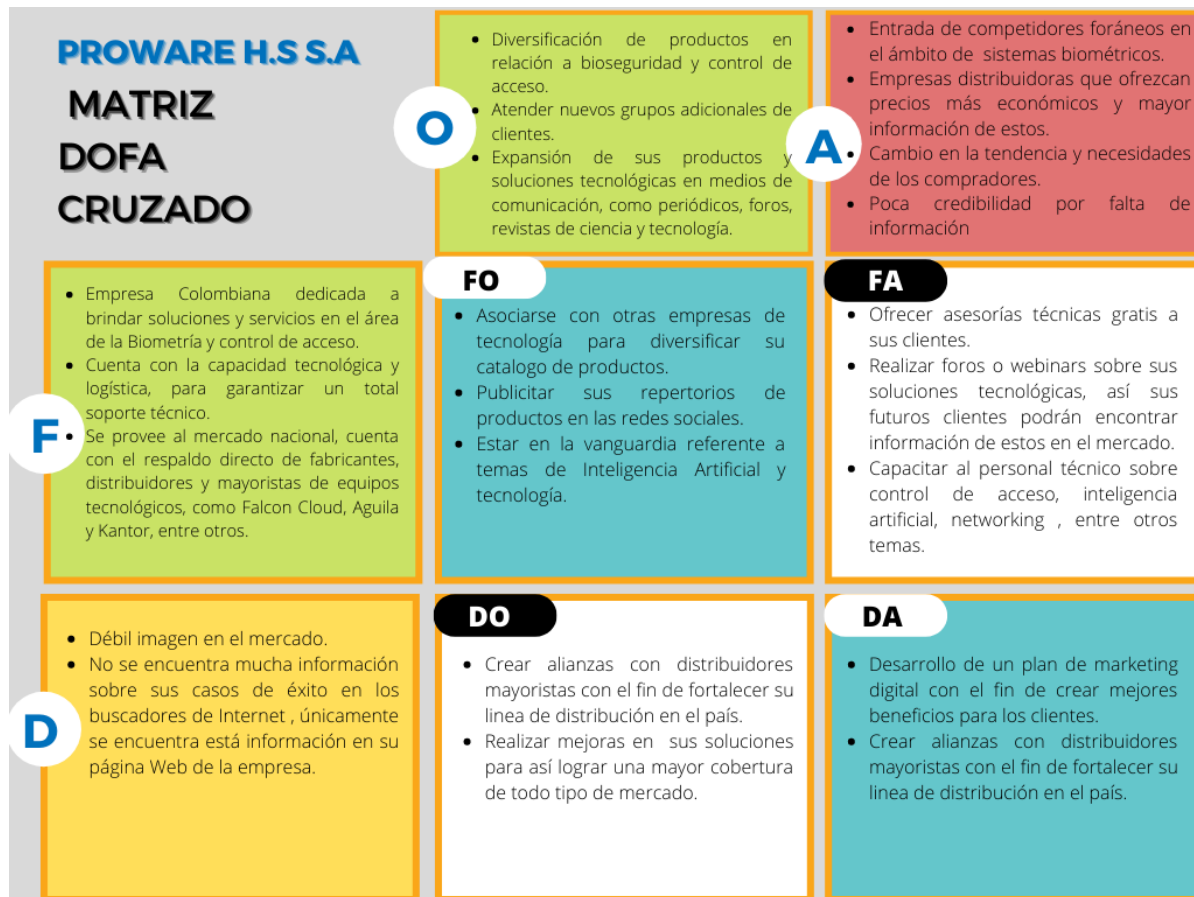


Figura 15. Matriz DOFA Cruzado sobre PROWARE. Fuente: Autor

4.1.4.2.3 Casos de éxito

Algunos de sus casos de éxito han sido para empresas cómo “Quala, MCDonald 's, entre otras”³² .Donde se destaca su sistema Falcon Cloud el cual permite la gestión y la administración de la asistencia de los trabajadores en una compañía. Entre sus soluciones resaltan:

³² PROWARE. S. A, P. H. (15 de 05 de 2020). Obtenido de Aliados: <https://www.proware.com.co/nuestros-aliados/>

- Un sistema de marcación, el cual suministraba la información detallada del tiempo empleado de un trabajador en la línea de producción de la empresa Quala, con el fin de dar cumplimiento del horario de los más de 5.000 colaboradores que se encuentran en estos puntos de marcación.
- Un control de asistencia de los empleados, para las 77 tiendas que tiene Adidas en Colombia, con el fin de dar a conocer a la empresa el tiempo trabajado, horas extras realizadas, incapacidades o días ausentes de los trabajadores, así como días compensatorios y vacaciones.

La propuesta presentada oficialmente por PROWARE frente a los requerimientos solicitada por la empresa consiste en:

- Lectores faciales Speed Face FC80VL [TD] -3 puerta principal – oficinas XX.
- Lectores faciales FCV80VL -5 puertas - oficinas XX & YY.
- Fuentes de poder.
- Software de gestión Falcon.

4.1.4.2.4 Características Técnicas de los equipos

En la Tabla 4 se describen las características generales de los equipos propuestos por la empresa PROWARE para dar solución a la problemática de la empresa.

Tabla 4. Características generales de los equipos propuestos en la solución de Proware HS S.A

Ítem	Modelo	Descripción
1	Speed Face FC80VL	Unidad Multi Biométrica Rostro, Huella, Tarjeta para control de horarios y asistencia. 1. Métodos de Identificación: Rostro, huella, tarjeta. 2. IP68, IK04, Alta Capacidad 3. Capacidad: 6.000 Rostros, 10.000 huellas, 10.000 tarjetas, 200.000 eventos. 4. Comunicación: TCP/IP, Wifi. 5. Interfaz control de acceso
2	Speed Face FC80VL [TD]	Unidad Multi Biométrica Rostro, Huella, Palma para control de horarios y asistencia. 1. Métodos de Identificación: Rostro, huella, tarjeta, palma. 2. Detección de rostro con Tapabocas, detección de temperatura, IP68, IK04, Alta Capacidad 3. Capacidad: 6.000 Rostros, 10.000 huellas, 3.000 Palmas, 200.000 eventos. 4. Comunicación: TCP/IP, Wifi. 5. Interfaz control de acceso
3	Fuente de Poder	Fuente de Poder

		Para controladoras de Acceso Biométricas, Entrada 110-220V AC, Salida 13,8 V / 5ª, Entrada directa para batería de respaldo.
4	Acceso para puertas	Cargo anual por puerta o canal de acceso El sistema biométrico estará unido en conjunto con el sistema de puertas de la instalación para permitir el acceso de las personas.

Fuente: Autor

En el siguiente punto se hablará sobre los costos que se tiene al implementar la propuesta de PROWARE HS S.A de acuerdo a la cantidad de dispositivos que se van a implementar, en adición también se mostrará los costos de la instalación del sistema y otros costos adicionales.

4.1.4.2.5 Costos

Tabla 5. Costos de la propuesta por parte de PROWARE.

Ítem	Referencia	Descripción	Cantidad	Precio Unitario	Precio Total COP
1	Activación de la plataforma	Activación de la unidad en la plataforma	8	\$30.000	\$ 240.000
2	FCV80VL	Unidad Multi Biométrica Rostro, Huella, Tarjeta para control de horarios y asistencia	5	\$ 3.305.000	\$16.525.000
3	FC80VLTD	Unidad Multi Biométrica Rostro, Palma, Huella para control de horarios y asistencia	3	\$7.905.000	\$23.715.000
4	Fuentes de poder	Fuente de Poder	8	\$ 165.000	\$ 1.320.000
5	Acceso para puertas	Cargo por puerta o canal de acceso	7	\$ 510.000	\$ 3.570.000
6	Consultoría	Hora de consultoría profesional para el sistema Acceso Cloud	10	\$150.000	\$1.500.000
7	Instalación	Instalación, configuración y capacitación	1	\$800.000	\$800.000
TOTAL					\$ 46.870.000

Fuente: PROWARE HS SA.

Un aspecto que se debe tomar en cuenta en referencia a su propuesta presentada es que su diseño se basa en un sistema de control de acceso básico, por lo que no requieren de alguna controladora, además un aspecto negativo es que para realizar el manejo de las puertas se es necesario pagar un recargo anual para el

funcionamiento de cada puerta, lo que implicaría costos adicionales. El recargo para las 7 puertas se encuentra por un valor de \$3.570.000 COP anuales.

4.1.4.2.6 Topología de conexión de control de acceso

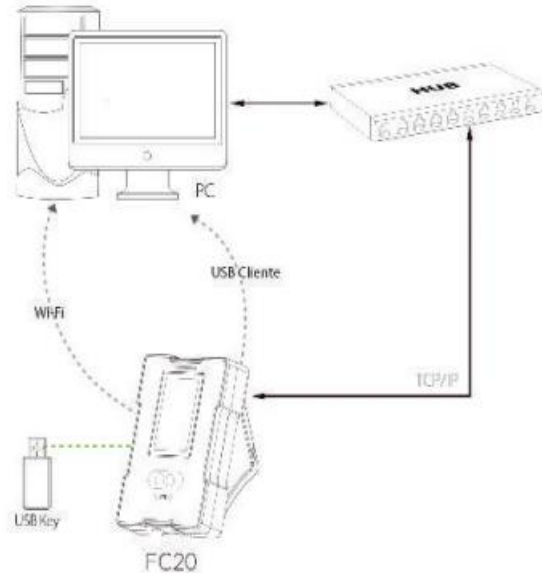


Figura 16. Topología de conexión de control de acceso del sistema de control de acceso de PROWARE³³. Fuente: PROWARE.

En la Figura 16, se puede observar que la topología de control del acceso propuesta no requiere de una controladora, siendo así un sistema de control del acceso básico donde el lector es el único dispositivo que almacena la información de los empleados de la empresa y desenergiza la chapa magnética de una de las puertas.

4.1.4.3 SOLUCIÓN POR PARTE DE SYSCOM

SYSCOM es uno de los mayores distribuidores a nivel global líder en telecomunicaciones y seguridad³⁴ con el fin de fortalecer la empresa de sus clientes asociados. Algunos de sus socios aliados son ZKTeco, conocida mundialmente por ser una empresa dedicada a la biometría, manteniendo siempre la visión de responsabilidad, integridad y excelencia, con el fin de poder aportar un cambio en el mundo con la tecnología, desarrollando así un desarrollo social seguro. Así como

³³"PROWARE HS S.A", Proware.com.co, 2020. [Online]. Obtenido de: https://www.proware.com.co/images/pdf/FC20_opt.pdf. [Acceso: 18- julio- 2020].

³⁴SYSCOM. SYSCOM (20 de 06 de 2020). Obtenido de Nosotros: https://www.syscomcolombia.com/principal/acerca_de

otras marcas que buscan hacer un aporte a la sociedad con su tecnología y soluciones.

Por tal motivo SYSCOM valora a cada uno de sus clientes y busca satisfacer sus necesidades, mejorando su productividad gracias a los productos y soluciones que ofrecen de sus diferentes asociados y así poder ayudar a los negocios de sus clientes a operar de forma eficiente y con todas las herramientas necesarias que ellos necesitan.

4.1.4.3.1 DOFA

SYSCOM DOFA

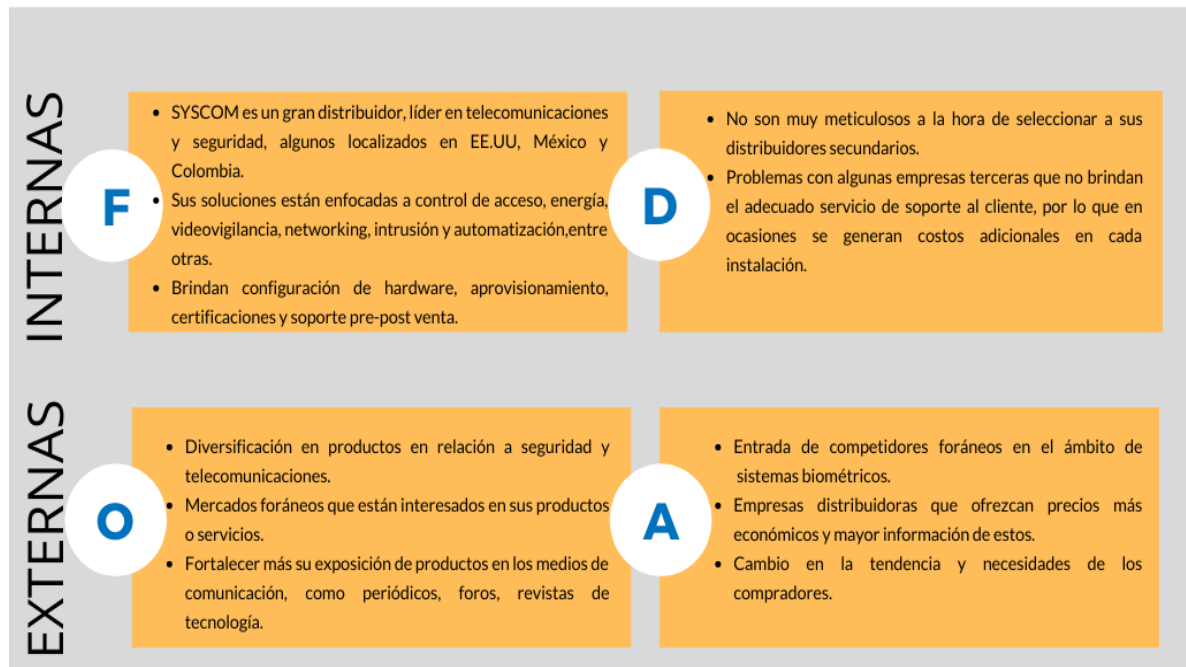


Figura 17. Matriz DOFA sobre la empresa SYSCOM. Fuente: Autor

4.1.4.3.2 Análisis cruzado de las estrategias

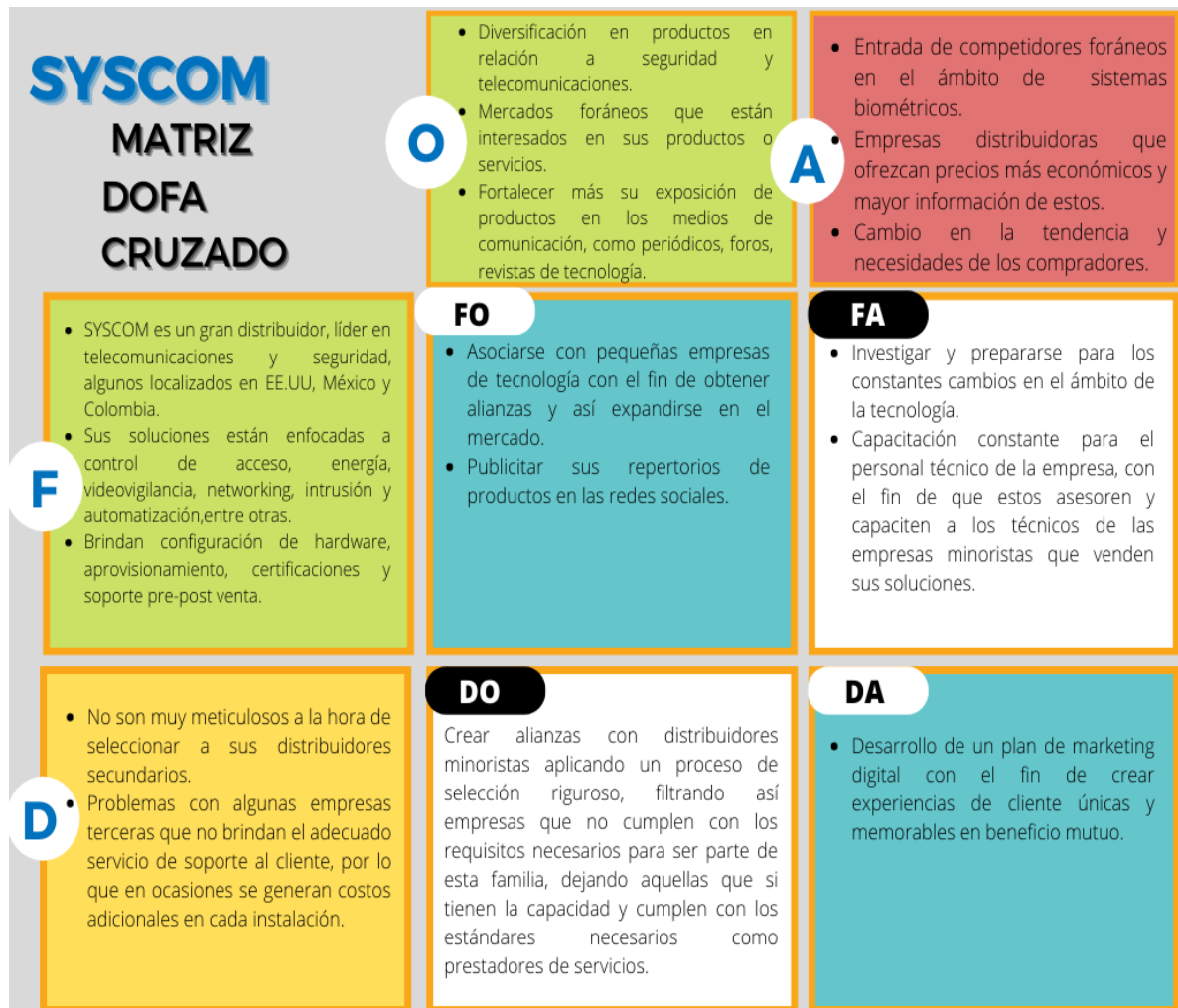


Figura 18. Matriz DOFA Cruzado sobre SYSCOM. Fuente: Autor

La propuesta presentada oficialmente por SYSCOM frente a los requerimientos solicitada por la empresa consiste en:

- Lectores faciales PROFACE -8 puertas - oficinas XX & YY.
- Licenciamientos lectores, cada lector tendrá este licenciamiento para la integración con el software de gestión.
- Software ZKBiosecurity.

4.1.4.3.3 Características Técnicas de los equipos

En la Tabla 6 se describen las características generales de los equipos propuestos por la empresa SYSCOM para dar solución a la problemática de la empresa.fg

Tabla 6. Características generales de los equipos propuestos en la solución de SYSCOM.

Ítem	Modelo	Descripción	Características
1	PROFACE	Face Recognition Terminal	Terminal de reconocimiento facial • Distancia de reconocimiento facial: 30 a 50 cm. • Capacidad: 30000 rostros, 5000 plantillas de palma. • El tiempo de duración para el reconocimiento facial es de 1 segundo. • Cámara de 2 MP, con función WDR y startlight. • Fuente de alimentación: 12 V DC. • Medición de temperatura corporal, desviación del 0.3°C. • Detección del personal en caso de que estén usando tapabocas.
2	Biosecurity	Plataforma de seguridad	ZKBioSecurity es una plataforma de seguridad que contiene múltiples módulos integrados, por ejemplo: control de acceso, gestión para visitantes, hotel, patrullaje, vídeo. Es un sistema optimizado diseñado para la identificación biométrica, además posee una interfaz del usuario moderna lo cual permite que la interacción con el usuario sea de la mejor manera posible.

Fuente: Autor

4.1.4.3.4 Costos

Tabla 7. Propuesta por parte de SYSCOM usando tecnología ZKTeco

Ítem	Referencia	Descripción	Cantidad	Precio Unitario	Precio Total en COP
1	PROFACE	Face Recognition Terminal	8	\$ 5.500.000	\$44.000.000
2	ZKBiosecurity	Plataforma de seguridad.	1	\$ 1.500.000	1.500.000
3	Instalación	Cableado, Instalación y puesta en funcionamiento	GL	\$5.000.000	\$5.000.000
Total					\$ 50.500.000

Fuente: Autor

4.1.4.3.5 Topología de Conexión del control de acceso

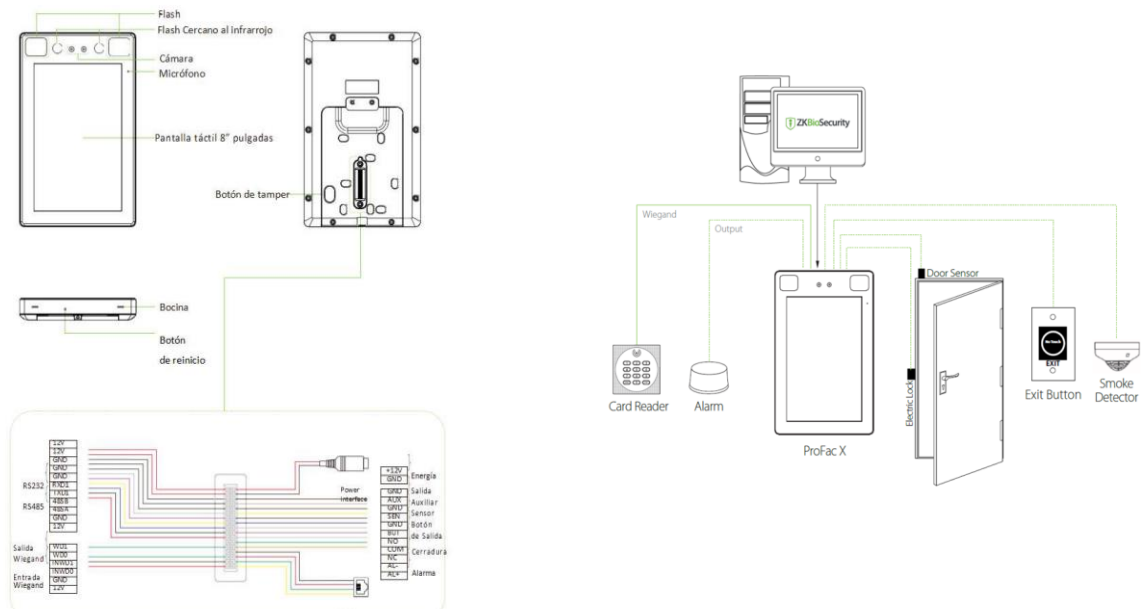


Figura 19. Topología de conexión de control de acceso ZKTeco³⁵. Fuente: ZKTeco.

³⁵ Z. LATINOAMERICA, "ZKTECO Latinoamerica", Zktecolatinoamerica.com, 2020. [Online]. Obtenido de: https://zktecolatinoamerica.com/documentos/greenlabel/control-de-acceso/ProFace_X_TD/Serie_Proface_X_TD.pdf. [Acceso: 19- julio- 2020].

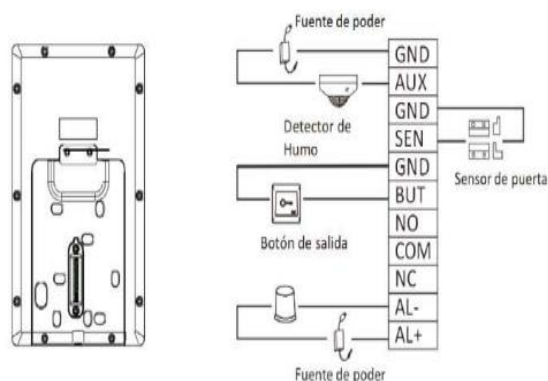


Figura 20. Conexión de sensor de puerta, botón de salida y alarma ³⁶. Fuente: ZKTeco

Como se puede observar en la Figura 19 y en la Figura 20, se puede observar la topología de conexión que ofrece SYSCOM para un sistema de control de acceso autónomo, donde un lector puede controlar una puerta. La gestión de los usuarios no se hace por un sistema centralizado, sino que en cambio se realiza mediante un administrador-identificador que en este caso es cada uno de los lectores.

4.1.4.4 CUADROS COMPARATIVOS DE LAS SOLUCIONES BIOMÉTRICAS

Tabla 8. Cuadro Técnico comparativo de las diferentes soluciones.

DESCRIPCION EMPRESA	CARACTERÍSTICAS TÉCNICAS		
	IOT TECH	PROWARE HS SA	SYSCOM
Terminal de reconocimiento facial	DeepinGo series Face Recognition Terminal (OPCION 1) - Distancia de reconocimiento facial: 0.3 m a 1 m. - Capacidad: 3.200 rostros, 5.000 tarjetas. - El tiempo de duración para el reconocimiento facial es de 1 segundo. - Cámara de 2 MP, lente angular. - Fuente de alimentación: 12 V CC / 2ª. - Pantalla táctil LCD de 5 pulgadas con	Speed Face FC80VL (OPCION 1) - Métodos de Identificación: Rostro, huella, tarjeta. - IP68, IK04, Alta Capacidad - Capacidad: 6.000 Rostros, 10.000 huellas, 10.000 tarjetas, 200.000 eventos. - Comunicación: TCP/IP, Wifi. Speed Face FC80VL [TD]	Terminal de reconocimiento facial - Distancia de reconocimiento facial: 30 a 50 cm. - Capacidad: 30000 rostros, 5000 plantillas de palma. - El tiempo de duración para el reconocimiento facial es de 1 segundo. - Cámara de 2 MP, con función WDR y startlight.

³⁶ Z. LATINOAMERICA, "ZKTECO Latinoamerica", Zktecolatinoamerica.com, 2020. [Online]. Obtenido de: https://zktecolatinoamerica.com/documentos/greenlabel/control-de-acceso/ProFace_X_TD/Serie_Proface_X_TD.pdf [Acceso: 19- julio- 2020].

	una resolución de 480 x 800. Face Recognition Terminal DS-K1T331(OPCION 2) • Distancia de reconocimiento facial: 0.3 m a 1.5 m. • Capacidad: 300 rostros, 1.500 tarjetas. • El tiempo de duración para el reconocimiento facial es de 1 segundo. • Cámara de 2 MP. • Fuente de alimentación: 12 V DC. • Pantalla táctil LCD de 4.72"x4.3"x0.9". • Interfaces: 1 USB, 1 para cerradura eléctrica, 1 para contacto de puerta, 1 para botón de salida y 1 para RS-485.	• Métodos de Identificación: Rostro, huella, tarjeta, palma. • Detección de rostro con Tapabocas, detección de temperatura, IP68, IK04, Alta Capacidad • Capacidad: 6.000 Rostros, 10.000 huellas, 3.000 Palmas, 200.000 eventos. • Comunicación: TCP/IP, Wifi. • Interfaz control de acceso	• Fuente de alimentación: 12 V DC. • Medición de temperatura corporal, desviación del 0.3°C. • Detección del personal en caso de que estén usando tapabocas.
Controladora de acceso	Four-door Access Controller DS-K2604 • Control de acceso por horarios y puertas. • Verificación Multi-usuario. • Funciones de primera tarjeta y contraseña. • IP68, IK04, Alta Capacidad • Comunicación: TCP/IP. • 4 entradas Wiegand Multi-Formato. • 8 RS-485 • 4 entradas para sensor de estado de puerta. • 4 entradas para botón de petición de salida (REX). • Incluye fuente de 12VCD / 8A con cargador de batería.	N/A	N/A

Sistema para Puertas manejables	HikCentral-ACS-Base/2Door HikCentral-ACS-Base-2Door es un paquete básico de control de acceso el cual incluye los requisitos previos para la ampliación de puertas. Al hacer uso de HikCentral, permite el intercambio de información, cooperación multiservicio, la adición de dispositivos para la gestión, reproducción de archivos de video, entre otras funciones.	Cargo anual por puerta o canal de acceso El sistema biométrico estará unido en conjunto con el sistema de puertas de la instalación para permitir el acceso de las personas.	N/A
Fuente de poder	N/A	Entrada 110-220V AC, Salida 13,8 V / 5ª, Entrada directa para batería de respaldo.	N/A
Licenciamiento y plataforma	HiKCentral-Attendance-Base El paquete de software HikCentral es una licencia para hasta 64 cámaras. Entre sus funciones permite la gestión avanzada de usuarios, permite integrar video, control de acceso e intrusión. Es una plataforma de gestión centralizada, con una arquitectura cliente-servidor.	Falcon Cloud Es una plataforma para el control de turnos, horas extras y ausentismos. Permite el fácil cálculo de las horas laboradas. Además, ayuda al Control eficiente del ingreso y salida del personal, cuenta con una interfaz para software de nómina.	ZKBioSecurity Es una plataforma de seguridad que contiene múltiples módulos integrados, por ejemplo: control de acceso, gestión para visitantes, hotel, patrullaje, video. Es un sistema optimizado diseñado para la identificación biométrica, además posee una interfaz del usuario moderna lo cual permite que la interacción con el usuario sea de la mejor manera posible.
Switch	El switch Easy Smart no gestionable de 8 puertos, es adecuado para redes de pequeñas empresas. Su diseño plug and play permite su despliegue sin necesidad de un técnico, las características de este equipo permiten la gestión inteligente de QoS, VLAN, IGMP Snooping, entre otras.	N/A	N/A

Tabla 9. Cuadro comparativo de los costos finales de cada solución.

Empresa	Ítem	Referencia	Descripción	Cantidad	Precio Unitario COP	Precio Total en COP
I O T T E C H	1	DS-K2604	Four-door Access Controller, Storage with 100,000	1	\$ 4.336.000	\$4.336.000
	2	DS-K1T606MF	DeepinGo series Face Recognition Terminal	3	\$ 4.028.000	\$12.084.000
	3	DS-K1T331	Face Recognition Terminal(secundarios)	5	\$1.824.000	\$9.120.000
	4	HikCentral-ACS-Base/2Door	Doors manageable	4	\$ 712.000	\$2.848.000
	5	HiKCentral-Attendance-Base	Shift management and attendance report.	1	\$4.140.000	\$4.140.000
	6	TL-SG108E	Switch 8 Puertos Gigabit No administrable	1	\$254.800	\$254.800
	7	Instalación	Cableado, Instalación y puesta en funcionamiento	GL	\$6.670.890	\$6.670.890
	TOTAL					\$ 39.453.690
P R O W A R E H S S A	1	Activación de la plataforma	Activación de la unidad en la plataforma	8	\$30.000	\$ 240.000
	2	FCV80VL	Unidad Multi Biométrica Rostro, Huella, Tarjeta para control de horarios y asistencia	5	\$ 3.305.000	\$16.525.000
	3	FC80VLTD	Unidad Multi Biométrica Rostro, Palma, Huella para control de horarios y asistencia	3	\$7.905.000	\$23.715.000
	4	Fuentes de poder	Fuente de Poder	8	\$ 165.000	\$ 1.320.000

	5	Acceso para puertas	Cargo por puerta o canal de acceso	7	\$ 510.000	\$ 3.570.000
	6	Consultoría	Hora de consultoría profesional para el sistema Acceso Cloud	10	\$150.000	\$1.500.000
	7	Instalación	Instalación, configuración y capacitación	1	\$800.000	\$800.000
	TOTAL					\$ 46.870.000
S Y S C O M	1	PROFACE	Face Recognition Terminal	8	\$ 5.500.000	\$44.000.000
	2	ZKBiosecurity	Plataforma de seguridad.	1	\$ 1.500.000	1.500.000
	3	Instalación	Cableado, Instalación y puesta en funcionamiento	GL	\$5.000.000	\$5.000.000
	TOTAL					\$ 50.500.000

4.1.4.5 PROPUESTA FINAL DEL SISTEMA BIOMÉTRICO

Basado en el análisis de los proveedores y la realización del cuadro comparativo sobre cada empresa y su solución, se escoge la solución presentada por IOT Tech, ya que el sistema propuesto incluye controladoras, lo que permite un mejor manejo y creación de eventos, administración de los horarios de ingreso y salida de los empleados, entre otros aspectos. Su plataforma para la gestión del sistema es eficaz y confiable con todos los protocolos de seguridad, por otro lado, sus costos de implementación son menores con respecto a las otras dos soluciones. Por lo que cumple con los requerimientos exigidos por la empresa, calidad y costos bajos.

A continuación, se muestra el diagrama futuro del sistema escalable para el control de acceso, que incluirá además la integración del sistema de video vigilancia (CCTV) actual, esta adaptación se realizará por medio de la plataforma de gestión del sistema biométrico y del NVR del sistema de video vigilancia.

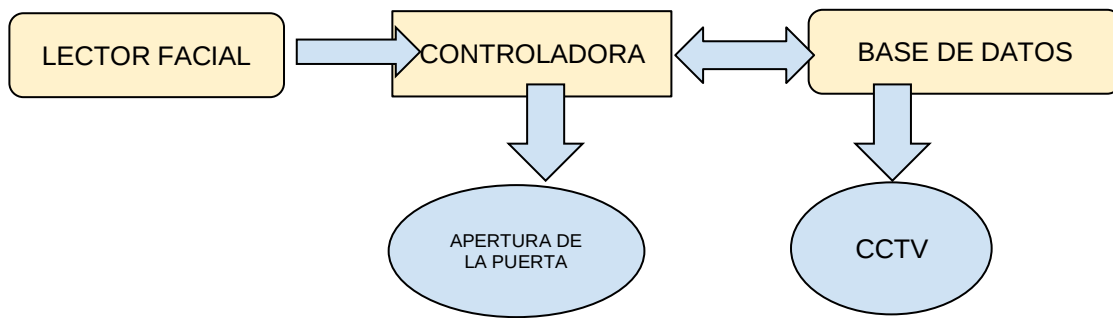


Figura 21. Sistema de control de acceso Propuesto + CCTV. Fuente: Autor

Al comparar los esquemas presentados en la Figura 8 y en la Figura 21, se puede observar algunas similitudes, por lo que esto brinda más ventajas que desventajas en el momento de realizar la implementación, algunas de ellas son:

- La instalación existente en las instalaciones se puede reutilizar tanto su infraestructura como su cableado.
- No se va a generar una obra civil mayor que afecte el entorno de los trabajadores. En este caso la única obra civil que se realizará es para el anclaje de los lectores faciales.
- Las puertas de acceso no requieren cambio.
- Es un plus realizar la integración del sistema de reconocimiento facial con el del CCTV de la empresa.

A pesar de lo explicado anteriormente, de una u otra forma surgen algunas incógnitas respecto a la implementación de un nuevo sistema de control de acceso. ¿Por qué el proyecto merece esta inversión? ¿Por qué no se elimina, ya que al parecer puede generar más problemas que beneficios? Algunos puntos buenos al desarrollar este proyecto son:

- Al realizar la implementación de un sistema de control de acceso seguro y confiable, se puede ahorrar gastos y costos fijos del personal de seguridad.
- Se tendría un mayor control del personal de la empresa, así como de sus visitantes.
- En caso de ser necesario se puede limitar el horario y días de acceso a las instalaciones para los trabajadores, mediante un control de horarios.
- Integración con el sistema de video vigilancia, con el fin de tener un sistema escalable.
- Los grandes clientes que tienen sus equipos en el data center-Hosting de la empresa, exigen que se tenga un sistema de acceso seguro y moderno. Brindando seguridad de la información.

¿Qué inconvenientes tiene el sistema biométrico actual de Huella Dactilar?

- Cómo se ha podido estudiar anteriormente, las huellas dactilares se pueden borrar con facilidad debido a un manejo previo de químicos o por problemas cutáneos.
- Para las personas de mayor edad se le dificulta el acceso biométrico debido a la pérdida de calor en el cuerpo.
- El lector biométrico está expuesto a la suciedad tanto de ambiente como de uso diario por parte de los usuarios al ingresar a las oficinas. Lo que puede provocar fallas o retrasos a la hora de ingresar. Además de que actualmente se busca habilitar un sistema de acceso con cero contactos personales.

¿Por qué se debería implementar la tecnología propuesta?

- Se pretende mostrar un avance tecnológico tanto para los trabajadores de la empresa como para el personal externo a ella (clientes). Brindándoles un espacio seguro para visitar las instalaciones.
- Al hacer uso de un sistema de reconocimiento facial se elimina el uso de la huella dactilar, el cual ha generado algunos inconvenientes en los últimos años, sumándole la actual crisis sanitaria, se requiere dar cumplimiento a la Resolución 666 de 2020 (Protocolo general de Bioseguridad), donde se es necesario habilitar sistemas de acceso con cero contactos físicos.
- No sería posible la falsificación de la identificación de un personal autorizado.
- Se puede integrar el sistema de vídeo vigilancia actual de la empresa, con el fin de brindar mayor seguridad por medio del reconocimiento facial haciendo uso del análisis de vídeo.

4.1.4.5.1 Topología de Conexión Propuesta

Con base en los análisis de proveedores anteriormente estudiados y relacionados con el marco teórico del presente documento, se realiza un estimado de conexiones de una red de control de acceso en adicción a una red de CCTV, con el fin de tener un escenario de la infraestructura de la red de ORANGE BUSINESS SERVICES y de esta forma poder buscar que el sistema cumpla con las características técnicas de dicho escenario. En la Figura 22 se plantea una topología donde se une tanto el control de acceso con el sistema de video vigilancia actual de la empresa.

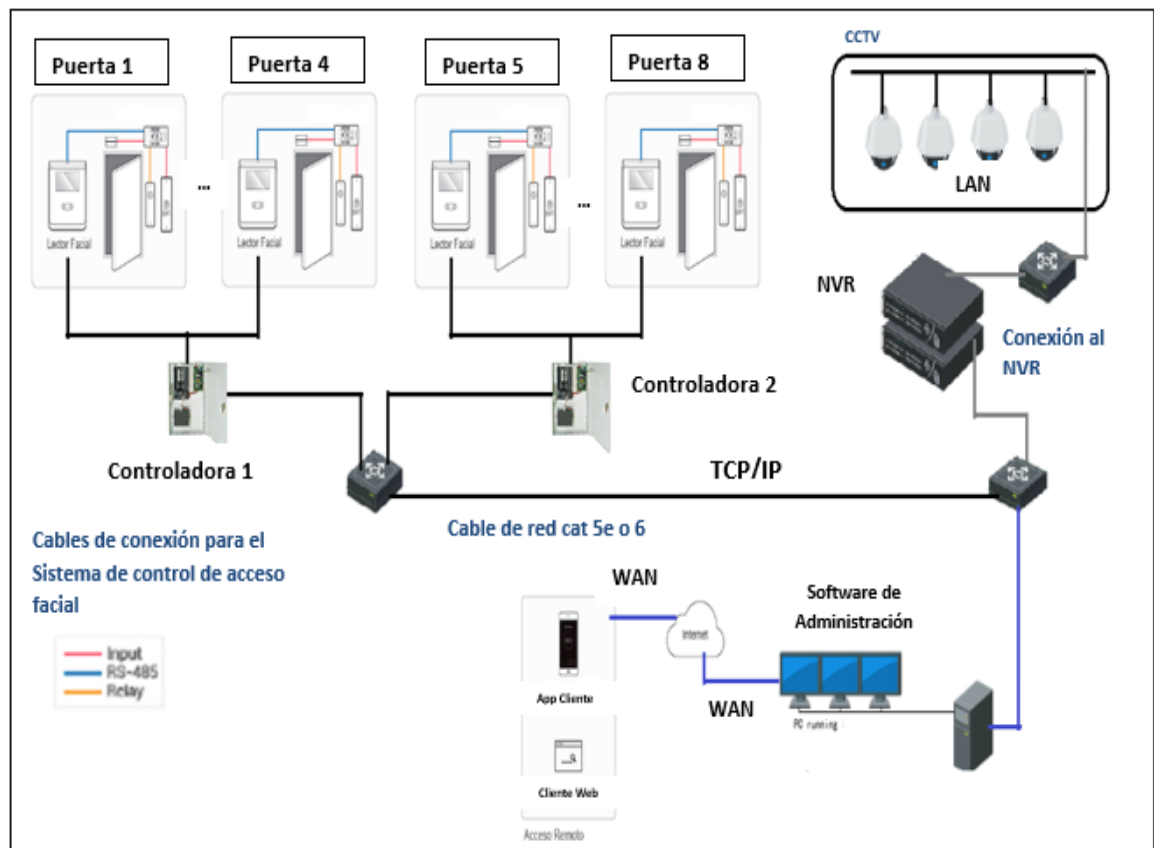


Figura 22. Topología de conexión propuesta. Fuente: Autor

Respecto al cableado estructurado y puntos eléctricos no se tendrán en cuenta por temas de confidencialidad de la empresa, pero se hará uso de la mayor parte posible del actual sistema estructurado y eléctrico con el fin de reducir costos.

4.1.4.5.2 Beneficios al implementar un sistema de control de acceso facial

A continuación, se determinará cuáles son los beneficios tanto tangibles como intangibles en los que la empresa ORANGE BUSINESS SERVICES se vería beneficiada al momento de implementar el proyecto.

4.1.4.5.2.1 Beneficios Tangibles

Algunos de los beneficios tangibles que se obtendrían al implementar esta solución, son:

- Mejoramiento del control de acceso del personal de trabajo de la empresa.
- Obtención de dispositivos de alta calidad.
- Diseño de una nueva red de control de acceso.

4.1.4.5.2.2 Beneficios Intangibles

Los beneficios intangibles son aquellos que no se miden a nivel monetario, pero si tienen un impacto en la empresa, algunos de los beneficios intangibles que se obtendrían al implementar esta solución son:

- Al no tener que hacer contacto con el lector facial, el trabajador no tendrá que manipular ningún equipo lo que evitará que este usuario esté tocando superficies, que en casos como los que se está viviendo a nivel mundial respecto a la pandemia, es de gran utilidad para el control de acceso a las oficinas, donde la higiene es primordial.
- Este método no es intrusivo, eso quiere decir que los datos obtenidos durante el escaneo son adquiridos sin que el sujeto se percate de este procedimiento.
- Es un control de acceso discreto, además de que las características físicas del rostro de una persona son más difíciles de falsificar, por lo que solamente podrán ingresar a las instalaciones las personas que se encuentran en la base de datos de la empresa, evitando así la entrada de personal no autorizado.
- El sistema de reconocimiento facial está por encima que el de huella digital que se encuentra actualmente instalado en las oficinas.

CAPITULO V

CONCLUSIONES

- La biometría es una de las mejores formas para la autenticación de usuarios, ya que hace uso de las características inherentes y únicas de un usuario, analizando y comparando las imágenes obtenidas por los lectores con el fin de determinar si es el verdadero usuario.
- Los diferentes tipos de sistemas biométricos presentados y estudiados en lo largo de este texto nos muestra en que consiste cada uno y como cada uno es una evolución del anterior, llegando incluso a crearse sistemas híbridos que combinan las mejores características de los sistemas. Pero si bien se

puede decir que este campo es muy amplio por lo que conlleva a futuras investigaciones con el fin de hacer y mejorar estos sistemas, tanto la optimización de sus equipos, así como la seguridad de la información.

- Tanto el deep learning como el machine learning son algoritmos que consisten en aprender como el cerebro humano. Por un lado, el machine learning es un algoritmo que usa arboles de decisiones mientras que deep learning hace uso de redes neuronales con el fin de tener un aprendizaje más profundo.
- Para la realización del DOFA para cada empresa fue necesario consultar sus páginas web para obtener información de la empresa, opiniones de usuarios, calidad de sus productos, entre otros factores. Además, para el tema de las propuestas se revisaron algunos casos de éxito, características técnicas de los equipos y la topología de conexión.
- La propuesta presentada por IOT Tech es un sistema de control de acceso seguro en el cual hacen uso de las controladoras, las cuales permiten la creación de eventos para gestionar las personas que han entrado a las instalaciones o tipo del evento que puede ser programado desde el sistema central, además dentro de la propuesta nos explicaron cómo se puede expandir el sistema en caso de ser necesario y la integración de este sistema con el sistema de CCTV de Orange.
- La segunda opción propuesta por PROWARE un sistema de control de acceso básico, a lo que conlleva que sus aplicaciones son de baja seguridad y susceptible a fallas ya que el lector biométrico es el que almacena la información y desenergiza la chapa magnética, lo que nos lleva a la conclusión que si un intruso retira el lector de la pared generando la vulnerabilidad del sistema o llevarse la información de los empleados que se encuentran asociados a la base de datos de esta.
- La tercera opción propuesta por SYSCOM consiste en un sistema de control de acceso autónomo, donde permite controlar una o más puertas sin la necesidad de estar conectados a un sistema central, por lo tal no guardan registro de eventos. Pero esta a su vez es una limitante ya que este tipo de sistemas no pueden limitar el acceso por horarios a los empleados o por grupos de puertas.
- Respecto al cableado estructurado del sistema, se hizo una suposición de cómo sería la conexión futura del sistema de control de acceso seleccionado, ya que este tipo de información no es brindada por ORANGE BUSINESS SERVICES por temas de confidencialidad.
- Una vez aceptada la propuesta por el Manager de ORANGE BUSINESS SERVICES en Colombia, se pasa la cotización a los directivos de Brasil para poder recibir el aval para dar inicio a la ejecución del proyecto. Además, dentro de los costos se tendrán en cuenta un presupuesto xxxx para algunas obras civiles, estas obras civiles serán únicamente para el anclaje de los lectores a las paredes, por otro lado, se busca reutilizar el cableado ya existe en las oficinas y en caso de ser necesario del cambio de algún cableado esta cuenta por parte de Orange, para la reducción de costos.

BIBLIOGRAFÍA

SISTEMAS BIOMÉTRICOS. Borja, C. T. (2010). Obtenido de Trabajos de Sistemas Informáticos: <https://docplayer.es/4089383-Sistemas-biometricos-cesar-tolosa-borja-alvaro-giz-bueno.html>

4 CASOS DE APLICACIÓN DEL RECONOCIMIENTO FACIAL. - Neuromarketing. La. Melgar, J. (12 de 12 de 2017). Obtenido de Neuromarketing. La Información del sector para Latinoamérica: <https://neuromarketing.la/2017/12/aplicacion-del-reconocimiento-facial/>

¿CÓMO HACER PAGOS CON RECONOCIMIENTO FACIAL EN COLOMBIA? Negocios, E. y. (07 de febrero de 2020) Dinero, págs. <https://www.dinero.com/tecnologia/articulo/como-hacer-pagos-con-reconocimiento-facial-en-colombia/281547>.

EL RECONOCIMIENTO FACIAL, PIONERO EN UN AEROPUERTO ESPAÑOL: ASÍ FUNCIONA EN MENORCA. Brands, E. (25 de Julio de 2019). El Confidencial, pág. 1. Obtenido de El Confidencial: https://www.elconfidencial.com/tecnologia/2019-07-25/biometria-reconocimiento-facial-aeropuertos-aena-bra_2133875/

XATAKA. Arantxa, H. (07 de marzo de 2018). Obtenido de Xataka: <https://www.xataka.com/legislacion-y-derechos/gdpr-rgpd-que-es-y-como-va-a-cambiar-internet-la-nueva-ley-de-proteccion-de-datos>

AENA. Aena. (2019). Obtenido de AENA: <http://www.aena.es/es/corporativa/perfil-compania.html>

USING A BIOMETRIC SYSTEM TO CONTROL ACCESS AND EXIT OF VEHICLES AT SHOPPING MALL IN SOUTH AFRICA. R.T.Hans. (29 de agosto de 2014). Obtenido de IEEE: <http://ieeexplore.ieee.org.bdigital.udistrital.edu.co:8080/document/7006236/?part=1>

KASPERSKY. KASPERSKY. (02 de marzo de 2020). Obtenido de <https://latam.kaspersky.com/resource-center/definitions/biometrics>

BYOSIS. Byosis. (2019). Obtenido de <https://www.biosys.es/sistemas-biometricos/>

DCHAIN. FLory, N. (2018). Obtenido de <http://dchain.com/caracteristicas-de-un-sistema-biometrico/>

MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE DE ESPAÑA. Misfud, E. (27 de abril de 2012). Obtenido de <http://recursostic.educacion.es/observatorio/web/ca/cajon-de-sastre/38-cajon-de-sastre/1045-sistemas-fisicos-y-biometricos-de-seguridad>

BIOMETRICS. GEMALTO. (26 de febrero de 2020). Obtenido de Authentication & Identification (definition, trends, use cases, lwas and latest news): <https://www.gemalto.com/govt/inspired/biometrics>

¿EL RECONOCIMIENTO DE IRIS ES UNA TÉCNICA INVASIVA? Serban. (31 de Julio de 2018). Obtenido de ¿EL RECONOCIMIENTO DE IRIS ES UNA TÉCNICA INVASIVA?: <https://www.serban.es/reconocimiento-de-iris-tecnica-no-invasiva/>

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

SISTEMA DE RECONOCIMIENTO FACIAL. Scarel, G. M. (2010). Universidad Nacional del Litoral, Facultad de Ingeniería y Ciencias Hídricas, 16.

EXE. EXE. (29 de junio de 2017). Obtenido de La ciencia tras un sistema de reconocimiento facial: <https://www.exe.cl/idi/la-ciencia-tras-un-sistema-de-reconocimiento-facial/>

RECONOCIMIENTO FACIAL CON BASE EN IMÁGENES. José Augusto Cadena, R. H. (15 de mayo de 2017). Obtenido de Universidad Técnica de Cotopaxi: <https://dialnet.unirioja.es/servlet/articulo?codigo=6145639>

HERRAMIENTA DE RECONOCIMIENTO FACIAL. CASO PRÁCTICO: ACCESO A SISTEMA DE PRÉSTAMO DE LIBROS. ESCOM, 8-40. Aparicio Duran Carmen, C. S. (17 de mayo de 2017). Obtenido de <https://repository.ucatolica.edu.co/bitstream/10983/24032/1/Final%20Trabajo%20de%20grado.pdf>

FACE DETECTION APPROACHES: A SURVEY. INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY, Modi, M. F. (2014). Pág. 1107-11108.

INDRA. Moreno, C. G. (s.f.). Obtenido de Blog NEO: <https://www.indracompany.com/es/blogneo/deep-learning-sirve>

Hikvision. Hikvision. (2020). Obtenido de About Hikvision: <https://www.hikvision.com/es-la/Corporate/About-Hikvision>

HIKVISION DIGITAL TECHNOLOGY. Tecno seguro-noticias, 2020. Obtenido de: <https://www.tecnoseguro.com/empresas/fabricantes/hikvision>

PROWARE. S. A, P. H. (15 de 05 de 2020). Obtenido de Aliados: <https://www.proware.com.co/nuestros-aliados/>

PROWARE. S. A, P. H. (15 de 05 de 2020). Obtenido de Nosotros: <https://www.proware.com.co/nosotros/>

SYSCOM. SYSCOM (20 de 06 de 2020). Obtenido de Nosotros: https://www.syscomcolombia.com/principal/acerca_de

WEBGRAFÍA

Vista de Reconocimiento óptico de números escritos a mano usando funciones de base radial y sistema memética diferencial | Revista vínculos", Revistas.udistrital.edu.co, 2020. [Online]. Obtenido de: <https://revistas.udistrital.edu.co/index.php/vinculos/article/view/8016/9801>. [Acceso: 20- mayo- 2020].

"PROWARE HS S.A", Proware.com.co, 2020. [Online]. Obtenido de: https://www.proware.com.co/images/pdf/FC20_opt.pdf. [Acceso: 18- julio- 2020].

Z. LATINOAMERICA, "ZKTECO Latinoamérica", Zktecolatinoamerica.com, 2020. [Online]. Obtenido de: https://zktecolatinoamerica.com/documentos/greenlabel/control-de-acceso/ProFace_X_TD/Serie_Proface_X_TD.pdf. [Acceso: 19- julio- 2020].

Z. LATINOAMERICA, "ZKTECO Latinoamérica", Zktecolatinoamerica.com, 2020. [Online]. Obtenido de: https://zktecolatinoamerica.com/documentos/greenlabel/control-de-acceso/ProFace_X_TD/Serie_Proface_X_TD.pdf [Acceso: 19- julio- 2020].

"Tipos de sistemas biométricos - Sistemas Biométricos", Sites.google.com, 2020. [Online]. Obtenido de: <https://sites.google.com/site/sistemasbiometricosvaldivia/home/huella-dactilar>. [Acceso: 06- abril- 2020].

D. Osuna Escorihuela, "Modalidad de voz", E-archivo.uc3m.es, 2011. [Online]. Obtenido de: https://e-archivo.uc3m.es/bitstream/handle/10016/13197/PFC_Daniel_Osuna_Escorihuela.pdf;jsessionid=E77EB55F8894CB6A231E9E46BF5D8B11?sequence=1. [Acceso: 08- abril- 2020].

R. iris, "Reconocimiento de iris", Innovagalingenieriasseguridad1.blogspot.com, 2020. [Online]. Obtenido de: <http://innovagalingenieriasseguridad1.blogspot.com/2011/11/reconocimiento-de-iris.html>. [Acceso: 10- abril- 2020].

RECONOCIMIENTO FACIAL, R. Facial, Sites.google.com, 2020. [Online]. Obtenido de: <https://sites.google.com/site/recofacialzs/>. [Acceso: 20- abril- 2020].

Quanta Magazine - Illuminating Science | Quanta Magazine, Quanta Magazine, 2020. [Online]. Obtenido de: <https://www.quantamagazine.org/>. [Acceso: 21- mayo- 2020]