UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERÍA

**PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE
INFORMACIÓN**

**Modelo Tecnológico de Reconocimiento Facial para la Identificación de
Pacientes en el Sector Salud**

TESIS

Para optar el título profesional de Ingeniero de Sistemas de Información

AUTORES

La Madrid Arroyo, Diego Alonso 0000-0002-5018-3445

Barriga Rivera, Martín Humberto 0000-0002-8165-8327

ASESOR

Canaval Sánchez, Luis Martín 0000-0001-9880-0396

Lima, diciembre 2019

DEDICATORIA

Esta tesis se la dedico a mi padre que guía mis pasos desde del cielo, a mí madre Carolina por apoyarme a lo largo de mi carrera, a mi hermana Claudia por asesorarme en todo y a mis familiares y amigos por alentarme en toda mi educación.
-Diego La Madrid

Quiero dedicar esta tesis a mis padres Juan Barriga y Mónica Rivera y a mi hermano Juan Pedro. Por su amor, apoyo, trabajo y sacrificio en todos estos años, gracias a ustedes he logrado llegar hasta aquí y convertirme en lo que soy. He sido el orgullo y privilegio de ser su hijo y hermano, son la mejor familia.
-Martín Barriga

Resumen Ejecutivo

El fraude médico y los ciberataques en el sector sanitario son fenómenos en aumento. La suplantación de identidad es una modalidad de fraude que tiene como propósito asumir la identidad de otra persona en una institución médica para obtener bienes y servicios médicos a las aseguradoras presentando reclamaciones falsas obteniendo un beneficio económico. Por lo tanto, afecta a la población asegurada ya que involucra un monto invertido, tiempo y servicio brindado. Sólo es necesario presentar documentos de identidad para ser atendido, la cual puede ser una medida de verificación y validación de alto riesgo para el paciente si se trata de algún fraude, debido a que cuando una persona usa la identidad médica de la víctima para obtener servicios médicos o medicamentos con receta, esa información se incorpora a la historia clínica electrónica de la víctima y puede complicar su atención médica en el futuro. Identificar al paciente de forma segura e inequívoca es de vital importancia para el paciente, impidiendo que nadie pueda suplantar su identidad.

El presente proyecto detalla el desarrollo de un modelo tecnológico que tiene como objetivo la identificación de pacientes mediante un servicio cognitivo de reconocimiento facial en Cloud computing para cubrir la necesidad que tienen los sectores de salud de prevenir la suplantación de identidad. Además, en caso de emergencias, se alerta a los parientes del paciente identificado el estado de salud en el que se encuentra mediante un mensaje de texto. Se espera que el modelo les permita a los pacientes ser atendidos sin la necesidad de contar con un documento de identidad en caso se encuentren en estado de emergencia y prevenir fraudes como las suplantaciones de identidad. Finalmente, se definirá un plan de continuidad que contenga mecanismos de respaldo en tiempo real para la disponibilidad y confiabilidad. Asimismo, se contará con recursos a nivel de software, los cuales serán detallados en base a características, especificaciones y uso.

Palabras clave: Reconocimiento Facial; sector Salud; Cloud computing; Modelo Tecnológico

Abstract

Medical fraud and cyber-attacks in the health sector are increasing phenomena. Impersonation is a form of fraud whose purpose is to assume the identity of another person in a medical institution to obtain medical goods and services to insurers by presenting false claims obtaining an economic benefit. Therefore, it affects the insured population as it involves an amount invested, time and service provided. It is only necessary to present identity documents to be treated, which can be a measure of verification and validation of high risk for the patient if it is a fraud, because when a person uses the victim's medical identity to obtain services doctors or prescription drugs, that information is incorporated into the victim's electronic medical record and may complicate their medical care in the future. Identifying the patient safely and unequivocally is of vital importance to the patient, preventing anyone from supplanting their identity.

This project details the development of a technological model that aims to identify patients through a cognitive facial recognition service on cloud computing to cover the need of health sectors to prevent phishing. In addition, the closest relatives of the identified patient will be alerted to the state of health in which they are in a text message. The model is expected to allow patients to be treated without the need to have an identity document in case they are in a state of emergency and prevent fraud such as phishing. Finally, a continuity plan will be defined that contains real-time backup mechanisms for availability and reliability. Also, there will be resources at the software level, which will be detailed based on features, specifications and use.

Keywords: Facial recognition; Health sector; Cloud computing; Technological model

Tabla de Contenidos

CAPÍTULO 1: DESCRIPCIÓN DEL PROYECTO	11
1.1 Objeto de estudio.....	12
1.2 Dominio del problema.....	12
1.3 Planteamiento de la solución	13
1.4 Objetivos del proyecto	13
1.4.1 Objetivo general.....	13
1.4.2 Objetivos específicos.....	13
1.5 Indicadores de éxito	14
1.6 Planificación del alcance	14
CAPÍTULO 2: LOGROS DE LOS STUDENT OUTCOMES.....	16
2.1. Aplica conocimientos de matemáticas, ciencias, computación e ingeniería (A).....	17
2.2. Diseña y conduce experimentos en base al análisis e interpretación de datos (B)	18
2.3. Diseña sistemas, componentes o procesos para encontrar soluciones en la atención de necesidades teniendo en cuenta restricciones económicas, sociales, políticas, éticas de salud y seguridad y otras propias del entorno empresarial (C).....	19
2.4. Participa en equipos multidisciplinarios desarrollando sus tareas con profesionales de diferentes especialidades o dominio de aplicación (D)	19
2.5. Identifica, formula y resuelve problemas de ingeniería (E).....	20
2.6. Propone soluciones a problemas de ingeniería con responsabilidad profesional y ética (F) .	21
2.7. Comunica ideas o resultados de manera oral o escrita con claridad y efectividad (G)	22
2.8. Identifica el impacto de las soluciones de ingeniería en el contexto global, económico y del entorno de la sociedad (H)	22
2.9. Reconoce la necesidad de mantener sus conocimientos actualizados (I).....	23
2.10. Analiza hechos del mundo contemporáneo identificando el impacto en el desempeño	

profesional de ingeniería (J)	24
2.11. Utiliza técnicas, herramientas y metodologías necesarios para la práctica de ingeniería (K)	24
2.12. Comprende y brinda soporte para el uso, entrega y gestión de sistemas de información dentro de un entorno de sistemas de información (J CAC)	25
CAPÍTULO 3: ESTADO DEL ARTE.....	26
3.1. Método.....	27
3.2. Revisión de la literatura.....	30
3.2.1. Resumen de la tipología 1: face recognition.....	30
3.2.2. Resumen de la tipología 2: cloud computing.....	41
3.2.3. Resumen de la tipología 3: aplicaciones móviles	52
3.2.4. Resumen de la tipología 4: modelos tecnológicos.....	61
3.3. Conclusiones.....	69
3.3.1. Conclusiones para la tipología 1: artículos de face recognition	69
3.3.2. Conclusiones para la tipología 2: artículos de cloud computing	70
3.3.3. Conclusiones para la tipología 3: artículos de aplicaciones móviles	70
3.3.4. Conclusiones para la tipología 4: artículos de modelos tecnológicos.....	70
3.3.5. Conclusiones generales.....	71
CAPÍTULO 4: MARCO TEÓRICO	72
4.1. Machine learning y deep learning	73
4.2. Reconocimiento facial.....	74
CAPÍTULO 5: DESARROLLO DEL PROYECTO.....	78
5.1. Metodología aplicada	79
5.2. Viabilidad de reconocimiento facial para el sector salud	79
5.2.1. Definición del sector salud	79
5.2.2. Descripción de las funcionalidades de reconocimiento facial	80

5.2.3. Casos de éxito de sectores que implementación reconocimiento facial	81
5.3. Análisis comparativo de las soluciones de reconocimiento facial	82
5.4. Modelos de referencia para la implementación de una solución para la identificación de pacientes en el sector salud	90
5.4.1. Modelo de verificación de identidad del paciente basada en fusión de señal fisiológica..	90
5.4.2. Sistema basado en rfid y agentes múltiples para mejorar la eficiencia en la identificación y el control de los pacientes.....	92
5.5. Modelo tecnológico de reconocimiento facial para la identificación de pacientes en el sector salud	93
5.5.1. Descripción del modelo	93
5.5.2. Fases	96
CAPÍTULO 6: RESULTADOS DEL PROYECTO	102
6.1. Validación del modelo	103
6.1.1. Comparación con la literatura.....	103
6.1.2. Juicio de expertos	104
6.2. Caso de uso.....	105
6.2.1. Presentación de empresa.....	105
6.2.2. Implementación	106
6.2.3. Resultados.....	108
6.2.4. Beneficio.....	109
6.2.5. Plan de Continuidad	109
CAPÍTULO 7: GESTIÓN DEL PROYECTO	116
7.1 Producto final	117
7.2 Registro de interesados.....	118
7.3 Matriz de trazabilidad de requerimientos	121
7.4 Matriz de asignación de responsabilidades.....	123

7.5 Plan de gestión de calidad.....	128
7.5.1 Roles y responsabilidades.....	128
7.5.2 Procedimientos	128
7.6 Plan de gestión de riesgos.....	129
Conclusiones	134
Recomendaciones.....	134
Bibliografía	135
Glosario	137

Lista de Ilustraciones

Ilustración 1: Clasificación General de técnicas de reconocimiento Facial	31
Ilustración 2: Detalles de la arquitectura FRServer.....	35
Ilustración 3: Estructura del proyecto OpenFaces.....	37
Ilustración 4: Transformación en puntos azules y redimensiona a 96 x 96 pixeles	38
Ilustración 5: Flujo de entrenamiento de red de extremo a extremo de OpenFace	38
Ilustración 6: La arquitectura propuesta del reconocimiento de la cara.....	40
Ilustración 7: Windows Azure Live Smooth Streaming.	44
Ilustración 8: Arquitectura de extracción de reconocimiento de facial y voz	47
Ilustración 9: Arquitectura del modelo propuesto	50
Ilustración 10: Estructura de testeo de seguridad dividida en 3 fases.	54
Ilustración 11: Arquitectura del método del testeo	55
Ilustración 12: Socio demográfico de los encuestados.....	60
Ilustración 13: Análisis de regresión.....	61
Ilustración 14: The ECG and ABP based Authentication Approach	62
Ilustración 15: Estructuras anatómicas del oído utilizadas en el desarrollo de algoritmos	66
Ilustración 16: Secuencia de y codificación de los puntos biométricos	81
Ilustración 17: Proceso del servicio Visual Recognition.....	83
Ilustración 18: diagrama de verificación de usuario	85
Ilustración 19: cuadro Forrester	86
Ilustración 20: Cuadrante mágico de Gartner.....	87
Ilustración 21: Comparación de Servicios de Machine Learning según Altexsoft.....	88
Ilustración 22: Modelo de verificación de identidad del paciente basada en fusión de señal fisiológica	91

Ilustración 23: Sistema basado en RFID y agentes múltiples para la identificación y control de pacientes	93
Ilustración 24: Modelo tecnológico de reconocimiento facial para la identificación de pacientes en el sector salud.....	96
Ilustración 25: Flujo de identificación de pacientes por aplicativo desarrollado	100
Ilustración 26: Logo de la clínica Uroginec	105
Ilustración 27: Servicio de reconocimiento facial en Azure	106
Ilustración 28: Decodificación de la aplicación	107
Ilustración 29: Inicio de sesión de la aplicación.....	107
Ilustración 30: Cuadro de retorno de Inversión.....	109
Ilustración 31: Acuerdos entre cliente y proveedor.....	110
Ilustración 32: Formula para la disponibilidad operativa en transacciones	111
Ilustración 33: Mejora Continua del Servicio	112
Ilustración 34: Servicio Cloud DRaaS	114

Índice de Tablas

Tabla 1: Problema y Causas	13
Tabla 2: Indicadores de Éxito.....	14
Tabla 3: Papers definidos por Tema	28
Tabla 4: Encuesta de satisfacción del usuario	48
Tabla 5: Casos de éxitos que implementaron reconocimiento facial	81
Tabla 6: Benchmarking de reconocimiento Facial	89
Tabla 7: Situación actual de la clínica	96
Tabla 8: Evaluación del entorno de la clínica.....	97
Tabla 10: Distintos sistemas para la identificación de pacientes.....	103
Tabla 11: Evaluación de criterios	104
Tabla 12: Resultados de las métricas de los sistemas según su literatura	108
Tabla 13: Resultados del modelo tecnológico de reconocimiento facial	108
Tabla 14: Porcentajes de Tiempo	111
Tabla 15: Certificaciones e ISO en Azure	114
Tabla 16: Registro de Interesados	118
Tabla 17: Matriz de Trazabilidad de Requerimientos	121
Tabla 18: Matriz de asignación de Responsabilidades	123
Tabla 19: Gestión de Riesgos	130
Tabla 20: Estrategias de Respuesta	132

CAPÍTULO 1: DESCRIPCIÓN DEL PROYECTO

En este capítulo se presenta la necesidad de diseñar un modelo tecnológico a la nube de reconocimiento facial para identificar a los pacientes en el sector salud. Además, se plantean los objetivos generales y específicos del proyecto, así como, los indicadores de éxito y los riesgos del mismo durante su desarrollo. Por último, se presenta el alcance del proyecto.

1.1 OBJETO DE ESTUDIO

Existe un alto riesgo en el proceso de identificación de pacientes en el sector salud. Puesto que, por ley, la persona que desea ser atendido tiene la obligación de presentar un documento de identidad (DNI). En el sector salud, existen situaciones de las cuales las personas no cuentan con un documento de identidad por motivos de pérdida, robo, entre otros. Además, un documento no puede garantizar con exactitud la identificación de un paciente debido a los distintos casos y métodos de suplantación de identidad que se vienen dando hoy en día. Por lo tanto, se generan reclamos de atención debido a la ausencia de una solución tecnológica y un proceso optimizado de reconocimiento de pacientes.

Se procede el desarrollo del proyecto que tiene como base la necesidad de brindar al sector salud un sistema de reconocimiento facial para la identificación de pacientes, y de ser el caso, los que están en estado de emergencia se les comunique a los familiares el estado actual del paciente bajo un mensaje de texto.

Finalmente, se define un plan de continuidad que contenga mecanismos de respaldo en tiempo real para la disponibilidad y confiabilidad ante la integración de entidades del estado. Se contará con recursos a nivel de software, los cuales serán detallados en base a características, especificaciones y uso.

1.2 DOMINIO DEL PROBLEMA

El dominio del problema considerado para el presente proyecto se detalla en el siguiente cuadro:

Tabla 1: Problema y Causas

Problema	Causas
Identificar al paciente sin documento de identidad o no perteneciente y notificar la atención médica al pariente ante una emergencia en el sector salud.	<ul style="list-style-type: none">• Ausencia de un medio tecnológico para identificar al paciente sin documento de identidad.• Ausencia de validación del documento perteneciente al paciente.• Notificar de manera inmediata la atención de un paciente a un pariente ante una emergencia.

Fuente: Elaboración Propia

1.3 PLANTEAMIENTO DE LA SOLUCIÓN

La finalidad del proyecto es diseñar un modelo tecnológico de reconocimiento facial para identificar los pacientes en el sector salud. Lo que permite identificar y reconocer la información de manera inmediata de los pacientes. Para el modelo se usará el servicio cognitivo de reconocimiento facial para detectar una persona y realizar un análisis biométrico para la identificación de esta bajo una data Set con una alta disponibilidad. Además, se siguen las buenas prácticas de desarrollo en cloud, lineamientos de seguridad y se cubren aspectos legales que implica la ley de protección de datos.

1.4 OBJETIVOS DEL PROYECTO

1.4.1 OBJETIVO GENERAL

OG: Implementar un modelo tecnológico para identificar y notificar la atención de los pacientes en el sector salud.

1.4.2 OBJETIVOS ESPECÍFICOS

OE1: Analizar servicios cognitivos de reconocimiento facial y procesos de atención en el sector salud.

OE2: Diseñar un modelo tecnológico para identificar y notificar la atención de los pacientes en el sector salud.

OE3: Validar el funcionamiento del modelo tecnológico para identificar y notificar la atención de los pacientes en el sector salud.

OE4: Elaborar un plan de continuidad acorde al modelo tecnológico validado para una alta disponibilidad y usabilidad.

1.5 INDICADORES DE ÉXITO

Tabla 2: Indicadores de Éxito

Código del Indicador	Indicadores de Éxito	Objetivos Específicos
IE1	Conformidad del cliente y el experto sobre el análisis realizado y los documentos requeridos.	OE1
IE2	Conformidad del cliente sobre el diseño del modelo tecnológico	OE2
IE3	Conformidad del cliente y el experto sobre el funcionamiento del modelo tecnológico desarrollado.	OE3
IE4	Conformidad del cliente sobre el plan de continuidad propuesto.	OE4

Fuente: Elaboración Propia

1.6 PLANIFICACIÓN DEL ALCANCE

El alcance del proyecto incluye el diseño de un modelo tecnológico para identificar a los pacientes en el sector salud ante una aplicación móvil que le permita la difusión de la información y ubicación de una persona en estado crítico mediante los siguientes puntos:

- Investigación del proceso de atención al paciente, canales de comunicación y acceso a información disponible de las personas atendidas.
- Investigar sobre open Source accesibles y medibles al desarrollo del modelo.
- Llevar un análisis comparativo en el servicio de reconocimiento facial que existe dentro de los Open Source.
- Investigar sobre el dataset que se requiere para la validación de reconocimiento facial.
- Realizar un informe con el análisis y diseño del modelo.
- Realizar un informe con las políticas, parámetros, evaluaciones y competencias del proyecto.
- Validación del modelo mediante un testeo por parte de un escenario.
- Validación del modelo por parte de expertos.

CAPÍTULO 2: LOGROS DE LOS STUDENT OUTCOMES

Este capítulo describe el cumplimiento de manera exitosa de los Students Outcomes en el proyecto. Estos son criterios basados en buenas prácticas de estándares de calidad en programa educativos como ciencias, ingeniería, computación y tecnología. Adicionalmente, se muestra la evidencia del cumplimiento de las competencias generales que debe tener un profesional.

2.1. APLICA CONOCIMIENTOS DE MATEMÁTICAS, CIENCIAS, COMPUTACIÓN E INGENIERÍA (A)

El Student outcome A explica la capacidad de aplicar conocimientos de matemáticas, ciencias, computación e ingeniería durante los años universitarios. Para el proyecto, este student outcome se encuentra en el diseño del modelo y el método desarrollado.

Se recolectó información de las investigaciones realizadas de reconocimiento facial bajo la tecnología machine learning. Debido a ello, se evaluó los puntos de medición de la tecnología. Se realizó fórmulas matemáticas para determinar porcentaje de exactitud, falsos positivos y verdaderos negativos de los datos incorporados.

Para los cálculos de gestión de tiempo en el plan de trabajo dentro en la fase de planificación en el sprint 1 se ejecuta los conceptos de PMBOK para calcular los esfuerzos en realizar las actividades y entregables del proyecto. Utilizando ciencias exactas, se logró determinar la cantidad recursos en las actividades para cumplir con el tiempo determinado dentro del plan de trabajo. Para el análisis, se realizó un estudio de benchmarking de los distintos servicios cognitivos. Por último, se aplica conocimiento de ciencias y computación para diseñar la tecnología de información que esta implementado el caso de uso.

Bajo las evidencias o entregables se registraron los documentos desarrollados:

- Current IT Enviroment
- Benchmarking
- Estudio de viabilidad

2.2. DISEÑA Y CONDUCE EXPERIMENTOS EN BASE AL ANÁLISIS E INTERPRETACIÓN DE DATOS (B)

El student outcome B explica el desarrollo del análisis e interpretación de datos para la toma de decisiones en base a los resultados obtenidos. Al realizar el benchmarking de los servicios cognitivos se describieron varios criterios de las características del servicio de RF, funcionalidad, fiabilidad, portabilidad, eficiencia, mantenibilidad y portabilidad para seleccionar el adecuado. El servicio seleccionado por el benchmarking fue validado mediante la literatura y que cuenta con los análisis obtenidos, los resultados en base a sus objetivos, planes a futuro y planes de mejora.

Se realizó la validación del modelo tecnológico en el caso de uso. Para ello se instaló la aplicación adaptado a la tecnología aplicada en la clínica Uroginec. El personal de la clínica ejecuta la aplicación dentro del proceso propuesto. Los resultados ante la ejecución del proyecto se almacenan dentro de la base de datos de la clínica autorizado por el administrador. Bajo ello se realiza el análisis de los resultados para medir la exactitud, los posibles problemas en cuanto al ambiente para la captura de la foto y medir la satisfacción del cliente. Además, el modelo fue validado por juicio de expertos.

Esto se puede evidenciar en el siguiente capítulo:

- Capítulo 5: Desarrollo del proyecto
- Modelo Tecnológico

2.3. DISEÑA SISTEMAS, COMPONENTES O PROCESOS PARA ENCONTRAR SOLUCIONES EN LA ATENCIÓN DE NECESIDADES TENIENDO EN CUENTA RESTRICCIONES ECONÓMICAS, SOCIALES, POLÍTICAS, ÉTICAS DE SALUD Y SEGURIDAD Y OTRAS PROPIAS DEL ENTORNO EMPRESARIAL (C)

El student outcome C explica el diseño de sistemas, componentes o procesos para encontrar soluciones a partir del escenario de la clínica. Se ejecuta el análisis realizado en la literatura para el diseño del modelo tecnológico de reconocimiento facial para la identificación de pacientes. Con ello, se verifica los componentes del modelo, que permite detectar el rostro y luego identificar al paciente bajo en Cloud. Esto permite reconocer de manera eficaz y confiable a los pacientes. Además, para ver el análisis completo dentro del proceso evaluado se realizó un diseño de ASIS y TOBE para definir la detección del paciente dentro del proceso correspondiente.

Esto se puede evidenciar en los siguientes documentos:

- Business Process
- Modelo Tecnológico.
- Costos y presupuestos.

2.4. PARTICIPA EN EQUIPOS MULTIDISCIPLINARIOS DESARROLLANDO SUS TAREAS CON PROFESIONALES DE DIFERENTES ESPECIALIDADES O DOMINIO DE APLICACIÓN (D)

El student outcome D se desarrolla en base al trabajo en equipo. Para finalizar el proyecto se respetaron los tiempos del cronograma. Se plantearon reuniones con el profesor gerente de manera presencial en las horas de clase. La comunicación con el cliente fue de manera presencial una vez a la semana. La comunicación con el coautor fue por Skype y presencial una vez a la semana. Asimismo, estas reuniones se especifican en los documentos de gestión según el PMBOK. Para realizar la validación del modelo propuesto, se recurrió con el gerente de plataforma Windows en Cloud de la empresa Falabella. El señor Roberto Zubiaur, tuvo el rol de Juicio Experto dentro de la validación, y ayudó con el proyecto al definir los

indicadores que se usaron para presentar los resultados finales. Las reuniones fueron por medio del correo electrónico y presencial. Adicionalmente, se tuvo comunicaciones por correo electrónico para la validación del modelo dentro de la empresa virtual IT Service. En la validación del caso de uso, se comunicó con el administrador de la clínica por correo y presencial.

Esto se ha evidenciado en los siguientes entregables:

- Cronograma del proyecto
- Plan de Comunicaciones
- Actas de reunión
- Certificado QS

2.5. IDENTIFICA, FORMULA Y RESUELVE PROBLEMAS DE INGENIERÍA (E)

El student outcome E analiza las situaciones para proponer soluciones en problemas de ingeniería. Se hace referencia al problema central de suplantación de identidad en los pacientes. Por ello, se realiza la solución en base al modelo tecnológico propuesto.

Por medio de investigaciones y estudios en la literatura, se realizan buenas prácticas, marcos de trabajo y pruebas de validaciones. De esta manera, se identificó las mejores opciones para el desarrollo del proyecto. Luego del análisis, se diseña el modelo tecnológico con la finalidad de resolver el problema.

Esto se ha evidenciado en los siguientes entregables:

- Benchmarking
- Project Charter
- Capítulo 5 de la memoria

2.6. PROPONE SOLUCIONES A PROBLEMAS DE INGENIERÍA CON RESPONSABILIDAD PROFESIONAL Y ÉTICA (F)

El student outcome F propone realizar confidencialidad y responsabilidad de cumplir tiempos de compromisos acordado. Se realizó un esfuerzo en respetar los tiempos y cumplir con las actividades planificadas del cronograma. Además, se realizó la gestión continua que se adquirió al proyecto y al modelo. Para cumplir con la gestión se utilizó la metodología de PMBOK y pautar las entregas a tiempo. Se recolectó distintas fuentes para la elaboración del modelo respetando el contenido referenciado en todo el proyecto tanto para las citas directas como en los documentos desarrollados en las actividades del proyecto. Además, dicho procedimiento se aplicó para la elaboración del artículo académico que formar parte del proyecto tecnológico.

La validación es una etapa crítica para determinar la validez de la solución propuesta del proyecto debía ser realizada con sumo cuidado respetando los criterios implícitos de validar una solución en sistema de información con responsabilidad profesional y ética. Para cumplir estos criterios se optó por aplicar el en la clínica Urogiec, el cual considera nociones sobre ética y profesionalismo durante las reuniones con personal para realizar la el aplicativo y recopilar la información necesaria para el modelo tecnológico.

Esto se ha evidenciado en los siguientes entregables:

- Project Charter
- Cronograma del proyecto
- Plan de gestión del cronograma del proyecto
- Diccionario EDT
- Actas de reunión

2.7. COMUNICA IDEAS O RESULTADOS DE MANERA ORAL O ESCRITA CON CLARIDAD Y EFECTIVIDAD (G)

El student outcome G se logra dar como referencia a las comunicaciones realizadas durante el proyecto. Se realizó diversas reuniones con el profesor gerente y el cliente. Durante las reuniones se ha plasmado ideas y conceptos bajo una serie de entregables. Para entender los acuerdos dentro de los distintos roles, se utilizó una comunicación oral y escrito de manera efectiva. Se pactan los acuerdos y entregables que está registrado en el acta de reunión.

Además, para el equipo de proyecto es de suma importancia contar con constancias o certificados de revisión de todos sus entregables (tanto para QA como Q) por el experto en la materia correspondiente, con el cual se asegurará la calidad de los mencionados.

Esto se ha evidenciado en los siguientes entregables:

- Constancia de revisión de toda la documentación por QS y QA
- actas de reuniones con las partes interesadas
- Constancia de revisión y aprobación de Paper
- Acta de aprobación de la validación por el juicio de experto.

2.8. IDENTIFICA EL IMPACTO DE LAS SOLUCIONES DE INGENIERÍA EN EL CONTEXTO GLOBAL, ECONÓMICO Y DEL ENTORNO DE LA SOCIEDAD (H)

El student outcome H hace referencia a la propuesta de valor que brinda la clínica y las diferencias de otro producto innovador que está en el mercado. Inicialmente, se evaluó el Project Charter para conocer los problemas y los impactos posibles. Se realizó un análisis para determinar una solución para las suplantaciones de identidad en los pacientes en el sector salud. También, se propondrá un plan de continuidad para fomentar la investigación sobre aspectos o propuestas de proyectos con un impacto similar ya sea en la misma área de estudio que el proyecto mencionado en la memoria u otras enfocadas al desarrollo del

contexto económico actual del país. El paper del proyecto detalla el impacto de la solución debido al estudio realizado y la literatura investigada que evidencie resultados sobre el problema propuesto.

Esto se ha evidenciado en los siguientes entregables:

- Business Principles, Goals and Drivers
- Current IT Environment
- Benchmarking
- Estudio de Viabilidad
-

2.9. RECONOCE LA NECESIDAD DE MANTENER SUS CONOCIMIENTOS ACTUALIZADOS (I)

El student outcome I hace referencia a la necesidad de las actualizaciones de los entregables. En este modelo tecnológico, se detalla distintas versiones para realizar actualizaciones de una manera competitiva en el mercado. Para ello se realizan estudios de tecnología y utilizando fuentes confiables y literaturas de investigación considerando un periodo de 3 años como máximo.

Se ha contado funcionalidades de reconocimiento facial en informes de Forrester y Gartner y los últimos años para tener actualizaciones sobre las tendencias en herramientas de servicios cognitivos. Por último, se da entregables del plan de continuidad que trazará constantes actualizaciones y versiones de las herramientas que forman parte del modelo.

Esto se ha evidenciado en los siguientes entregables:

- Paper del proyecto
- Benchmarking
- Plan de continuidad
- Modelo Tecnológico de reconocimiento facial para la identificación de pacientes

- Capítulo 3 y 4 de la memoria

2.10. ANALIZA HECHOS DEL MUNDO CONTEMPORÁNEO IDENTIFICANDO EL IMPACTO EN EL DESEMPEÑO PROFESIONAL DE INGENIERÍA (J)

El student outcome J hace referencia a los hechos y situaciones actuales que impactan al mundo contemporáneo. Se han realizado diversas investigaciones que hace referencia a como la actualidad y los hechos de importancia impactan a la problemática que resuelve el proyecto. Como resultado se obtuvo información de la literatura investigada sistemas de adopción de identificación de pacientes en el sector salud. Aunque, se evidencian ausencias de modelos estándar para la implementación de tecnología cognitivas de identificación de pacientes. Es por ello, que se propone el modelo tecnológico de reconocimiento facial que fue testeado en una clínica.

Esto se ha evidenciado en los siguientes entregables:

- Papers

2.11. UTILIZA TÉCNICAS, HERRAMIENTAS Y METODOLOGÍAS NECESARIOS PARA LA PRÁCTICA DE INGENIERÍA (K)

El student outcome K hace referencia a la gestión que se le adquirió al proyecto. Por ello se utilizó la metodología PMBOK para un mejor manejo continuo del proyecto. Además, utilizamos los entregables de la metodología CCRA-V4 para proyectos que son dedicados al desarrollo de proyecto en servicios Cloud. Se adaptó los entregable a la metodología de PMBOK para evitar conflictos y medidos en el tiempo de entrega dentro del cronograma. También, se utilizaron técnicas para la evaluación del uso de herramientas en el proyecto. Para esto, se utilizó el Benchmarking para elegir las herramientas ideales. Por último, se respetó el plan de trabajo propuesto por el comité para la ejecución de metodologías hábiles. Todas las metodologías y herramientas utilizadas fueron debidamente aprobadas por el Profesor Cliente y esto se evidencia en las actas de reunión.

Esto se ha evidenciado en los siguientes entregables:

- Documentos de PMBOK
- Entregables CRRA-V4
- Plan de trabajo

2.12. COMPRENDE Y BRINDA SOPORTE PARA EL USO, ENTREGA Y GESTIÓN DE SISTEMAS DE INFORMACIÓN DENTRO DE UN ENTORNO DE SISTEMAS DE INFORMACIÓN (J CAC)

El student outcome J CAC hace referencia a las acciones de soporte que garantice la continuidad del proyecto. Para ello se realizó un manual de instalación para brindar las facilidades de la instalación y funcionalidades del software al caso de uso. Se elaboró un plan de soporte que brindan los errores frecuentes que se requiera solucionar de manera entendible y sencilla. Finalmente se elaboró un plan de continuidad para dar mejoras y soluciones que a las situaciones que no dejan ejecutar el software.

Esto se ha evidenciado en los siguientes entregables:

- Plan de continuidad
- Plan de soporte
- Manual de Instalación

CAPÍTULO 3: ESTADO DEL ARTE

En este capítulo se presenta los trabajos científicos realizados previamente referente a la identificación de pacientes, tantos como sistemas, frameworks o marcos de trabajo

3.1. MÉTODO

Ante los reportes encontrados sobre las suplantaciones de identidad en el sector salud que genera costos innecesarios se vio la necesidad de automatizar y optimizar la identificación de los pacientes.

El banco de artículos científicos donde se realizó la búsqueda de los papers fue en IEEE (Institute of Electrical and Electronics Engineers), Sciencedirect y Web of Science. Las palabras clave que se utilizaron para dicha búsqueda fue Cloud Computing Saas, Face Recognition, Machine Learning, Mobile application y m-health. El periodo de los artículos científicos buscados fue entre los años 2015 y 2017, es decir, con un límite de 4 años de antigüedad.

Los congresos donde se encuentran nuestros artículos científicos y están registrados en Scimago Journal & Country Rank son los siguientes:

- Journal of ComputerScience&Technology
- ProcediaComputerScience
- Procedia Social and BehavioralSciences
- IEEE Transactionson Industrial Informatics
- Computers and MathematicswithApplications
- International Journal of Computer Applications Technology and Research
- Industrial Marketing Management
- Springer-Verlag
- IEEE Wireless Communications and Networking Conference 2016
- PoznanUniversity of Technology
- Computers and Communications

En la siguiente tabla se detallarán los temas, títulos, nombres de autores, antigüedad del estudio de los artículos científicos:

Tabla 3: Papers definidos por Tema

TEMA	#	TITULO	AUTOR (AÑO)
Face Recognition	1	Evaluation of Face Recognition Methods in Unconstrained Environments (Evaluación de los métodos de reconocimiento facial en ambientes sin restricciones)	Agrawal, Amrit Kumar and Singh, Yogendra Narain (2015)
	2	The case of face recognition on mobile devices (El caso del reconocimiento facial en dispositivos móviles)	Hassan, Galal and Elgazzar, Khalid (2016)
	3	OpenFace A general purpose face recognition (OpenFace Un reconocimiento facial de uso general)	Brandon Amos, Bartosz Ludwiczuk, Mahadev Satyanarayanan (2016)
	4	Face recognition using total loss function on face database with ID photos (Reconocimiento facial usando la función de pérdida total en la base de datos de caras con fotos de identificación)	Cui, Dongshun and Zhang, Guanghao and Hu, Kai and Han, Wei and Huang, Guang-Bin (2017)
Cloud Computing	5	Reporting an experience on design and implementation of e-Health systems on Azure cloud (Informar sobre una experiencia en diseño e implementación de sistemas de salud electrónica en la nube Azure)	Lu, Shilin and Ranjan, Rajiv and Strazdins, Peter. (2015)
	6	Cloud-Assisted Speech and Face Recognition Framework for Health Monitoring (Marco de reconocimiento de voz y voz asistido por la nube para el control de la salud)	Hossain, M Shamim and Muhammad, Ghulam (2015)
	7	A New Framework for Cloud Storage Confidentiality to Ensure Information Security (Un nuevo marco para la confidencialidad del almacenamiento en la nube para garantizar la seguridad de la información)	Singh, Deepak and Verma, Harsh K (2016)

Aplicaciones Móviles	8	Security Testing for Android mHealth Apps (Pruebas de seguridad para aplicaciones mHealth de Android)	Konstantin Knorr & David Aspinall (2015)
	9	Mining android apps to recommend permissions (Minería de aplicaciones de Android para recomendar permisos)	Karim, Md Yasser and Kagdi, Huzefa and Di Penta, Massimiliano (2016)
	10	Consumer Attitude: Does It Influencing the Intention to Use mHealth? (Actitud del consumidor: ¿Influye en la intención de usar mHealth?)	Hussein, Zuhail and Oon, Siti Waringin and Fikry, Amily (2017)
Modelos Tecnológicos	11	Fusion of Electrocardiogram and Arterial Blood Pressure Signals for Authentication in Wearable Medical Systems (Fusión de Electrocardiograma y Señales de la Presión Arterial para Autenticación en Sistemas Médicos Usables)	Cai, H., & Venkatasubramanian, K. K. (2016)
	12	Radio Frequency Identification (RFID) in Health Care: Privacy and Security Concerns Limiting Adoption (Identificación por radiofrecuencia (RFID) en la atención médica: preocupaciones de privacidad y seguridad que limitan la adopción)	Rosenbaum, B. P. (2015)
	13	Ear biometrics for patient identification in global health: a cross-sectional study to test the feasibility of a simplified algorithm (Biometría auricular para la identificación del paciente en salud global: un estudio transversal para evaluar la viabilidad de un algoritmo simplificado)	Ragan, E. J., Johnson, C., Milton, J. N., & Gill, C. J. (2016)
	14	Use of identification wristbands among patients receiving inpatient treatment in a teaching hospital (Uso de pulseras de identificación entre pacientes que	Hoffmeister, L. V., & Moura, G. M. S. S. D. (2015)

		reciben tratamiento hospitalario en un hospital docente)	
--	--	--	--

Fuente: Elaboración Propia

3.2. REVISIÓN DE LA LITERATURA

A continuación, se realizará un resumen de cada uno de los papers mencionados anteriormente considerando la motivación del autor (es), la descripción de su aporte(s) y el proceso que empleó para resolver el problema.

3.2.1. RESUMEN DE LA TIPOLOGÍA 1: FACE RECOGNITION

3.1.1.1. Evaluation of face recognition methods in unconstrained environments (Evaluación de los métodos de reconocimiento facial en ambientes sin restricciones)

Motivación del autor:

La motivación de los autores se centra la automatización de reconocimiento facial. Puede ser visto como un problema de reconocimiento de patrones. Cuanto más alta sea la dimensión del espacio, más se necesita el cálculo que necesitamos para encontrar una coincidencia verdadera. Un sistema de reconocimiento facial (FRS) generalmente está diseñado para medir la similitud entre las imágenes faciales de la sonda y la galería. Una FRS automatizada generalmente implica la localización de puntos faciales como ojos, nariz, boca y contorno facial normalizando la geometría facial y la apariencia como la iluminación y las propiedades de la escala de grises. Eligiendo una representación facial adecuada, selección de combinaciones de características distinguidas y desarrollo de técnicas de correspondencia exacta y escalable.

El mayor desafío para identificar a las personas por su geometría facial es la falta de análisis estadísticos disponibles para medir la individualidad. Las FRS automatizadas generan probabilidades de coincidencia sobre una base subjetiva según el método elegido sin tener el marco estadístico real de la individualidad de las caras. El proceso de coincidencia en una FRS genera el puntaje de similitud de una imagen de sonda para cada imagen en la galería y toma la decisión sobre la coincidencia más cercana en contra de un humano que examina las coincidencias más altas.

Descripción del Aporte del autor:

El autor describió los métodos de reconocimiento facial:

Métodos de reconocimiento facial:

Se han desarrollado varios métodos de reconocimiento facial. Podemos clasificar estos métodos en dos grupos que incluyen métodos basados en la apariencia y métodos basados en modelos. Los métodos anteriores utilizan características de textura holística que se aplican a regiones de toda la cara o específicas en una imagen de la cara, mientras que los últimos métodos emplean la forma y la textura de la cara.

Ilustración 1: Clasificación General de técnicas de reconocimiento Facial

1. Reconocimiento facial basado en Métodos:

Los métodos más populares de reconocimiento facial basado en la apariencia son: análisis de componentes principales (PCA), análisis de componentes independientes (ICA) y análisis discriminante lineal (LDA). La PCA, se encuentra en un conjunto de los vectores de proyección más representativos tales que las muestras proyectadas retienen más información sobre muestras originales. El ICA, capta ambos segundos y más altos estadísticas de orden y proyecta los datos de entrada en los vectores de la base que son estadísticamente independientes como sea posible. El LDA utiliza la información de clase y encuentra un

conjunto de vectores que maximizan la dispersión entre clase y reducir al mínimo el de dispersión dentro de la clase. Los métodos PCA y LDA han demostrado su éxito en la detección de rostros, el reconocimiento y el seguimiento. Las representaciones en estos métodos de subespacio se basan en estadísticas de segundo orden del conjunto de imágenes que no abordan las dependencias estadísticas de orden superior, como las relaciones entre tres o más píxeles. Se utiliza un nuevo método para realizar una forma no lineal de análisis de componentes principales como PCA.

2. Método de Reconocimiento facial basado en modelos:

El esquema de reconocimiento facial basado en modelos tiene como objetivo construir un modelo del rostro humano, que sea capaz de capturar las variaciones faciales. El conocimiento previo del rostro humano se utiliza mucho para diseñar el modelo. Un sistema más reciente basado en características, basado en el emparejamiento de gráficos de grupos elásticos.

3 métodos de reconocimiento de rostros sin restricciones:

El método propuesto identificó las partes ocluidas t en el nivel de píxel y aplicando el reconocimiento facial solo en las partes no ocluidas. El resultado experimental muestra que el método propuesto es superior a KLD-LGBPHS, S-LNME, OA-LBP y RSC. Se propuso cinco enfoques para determinar si el sujeto de la muestra de prueba está inscrito en la galería de la cara. El resultado experimental ha demostrado un buen rendimiento en el reconocimiento contra varias posibles complicaciones. Una representación basada en componentes en el reconocimiento facial automatizado ha sido demostrada por Bonnen. El resultado experimental muestra que el método es robusto para cambiar en pose facial y precisión de reconocimiento de la cara se mejora en escenarios forenses.

3.1.1.2. the case of face recognition on mobile devices (el caso del reconocimiento facial en dispositivos móviles)

Motivación del autor:

La motivación que realiza los autores es que se realizaron pocos esfuerzos de investigación se han abordado en el reconocimiento facial en dispositivos móviles con sus limitaciones y con un estudio de caso de la aplicación del reconocimiento facial en computación en mobile-cloud. Concluyen que el tema es factible y prometedor, pero requiere una investigación más amplia. Se propuso un sistema de reconocimiento facial que utiliza el sensor Kinect de Microsoft y un servidor Cloud alojado en Microsoft Azure. Su objetivo de investigación giraba resolviendo uno de los principales desafíos en el reconocimiento facial, prevenir el reconocimiento de caras falsas en los fondos, que la cara humana real. Ninguna de las investigaciones anteriores propuso un reconocimiento facial que funciona en dispositivos móviles debido a los altos cálculos necesarios para tal proceso y las limitaciones de los recursos móviles.

Descripción del Aporte del autor:

Esta investigación presenta una implementación de la LBPH (Histograma de patrón binario local) de reconocimiento facial en la nube utilizando la biblioteca OpenCV. El usuario toma una fotografía en el dispositivo móvil con una interfaz ligera que realiza un preprocesamiento en la imagen antes de enviarla al servidor de la nube. El servidor de nube realiza varias tareas incluyendo la extracción de características faciales, combinando las características con la base de datos de caras y enviando respuesta al dispositivo móvil del usuario. Se describirá los pasos que desarrollan los componentes.

1. Aplicación para reconocimiento de rostros: La interfaz de usuario es una aplicación móvil nativa que es responsable de una foto, realizar la detección de rostros y enviarla al servidor

de Cloud para el reconocimiento. La biblioteca Open-Source se utiliza para realizar procesamiento de imágenes. La aplicación puede realizar el entrenamiento facial y reconocimiento facial, ambos siguen el mismo procedimiento, excepto que el procedimiento de entrenamiento sólo sube la imagen con propósitos de entrenamiento.

2. Servidor de Reconocimiento de Rostro: El FRServer es el componente central de este sistema y es responsable de realizar todas las funciones de reconocimiento facial incluyendo el algoritmo de reconocimiento facial LBPH (Histograma de patrón binario local). El servidor realiza varias funciones en etapas: inicializar el servidor, recibe una solicitud de reconocimiento, ejecuta el algoritmo LBPH y envía una respuesta. La actualización del entrenamiento del clasificador LBPH se realiza y es guardado en un archivo durante la etapa de inicialización. El servidor lee el archivo clasificador LBPH y comprueba si hay imágenes no procesadas en la base de datos. Si alguna imagen no está procesada, el archivo clasificador es actualizado con la nueva imagen. El algoritmo LBPH carga la imagen en el reconocedor, que devuelve el valor de distancia de similitud entre la imagen y la coincidencia más cercana. Si la distancia está dentro de un umbral predeterminado de una persona específica (es decir, categoría o grupo), la persona es identificada correctamente y la etiqueta de categoría se envía al cliente. De lo contrario, se informa al cliente que esta persona no se encuentra en la base de datos. Al final, el LBPH se actualiza con la nueva imagen.

3. Base de Datos de Reconocimiento Facial: El componente de base de datos se implementa utilizando MySQL y crea una tabla que contiene todos los detalles de las caras con los nombres correspondientes, IDs, ubicación del archivo de imagen y un indicador que indica si la cara se ha agregado al clasificador entrenado. Para mantener la coherencia, el servidor actualiza el clasificador durante la inicialización con todas las imágenes cuyo atributo "entrenado" es falso (0). Este atributo indica si una imagen se ha utilizado para la formación o no. Cuantas más imágenes se agreguen al sistema, más preciso será el clasificador de reconocimiento facial. El clasificador también se actualiza al final de cada proceso de reconocimiento con la nueva imagen y etiqueta.

Ilustración 2: Detalles de la arquitectura FRServer.

Proceso para resolver el problema:

Para probar el rendimiento de extremo a extremo de la arquitectura propuesta, se ejecutó un conjunto de experimentos para explorar diferentes aspectos. En primer lugar, se probó el sistema sin descarga de computación). Luego, se implementó el servidor FRS en diferentes instancias de Amazon EC2 con diferentes capacidades para estudiar el impacto de los ciclos informáticos. También se investigó el impacto del tamaño del conjunto de datos de formación de clasificadores. Todas las pruebas se realizan 10 veces y se informa el promedio. Para cada uno de los casos de prueba, el entrenamiento del clasificador se realiza fuera de línea, por lo que el overhead de la formación se ignora.

3.1.1.3. openface a general purpose face recognition (openface un reconocimiento facial de uso general)

Motivación del autor:

OpenFace es de código abierto bajo la licencia de Apache 2.0. Es formado por una red en los Datasets más grandes disponibles para una investigación, con una orden de magnitud más pequeño que DeepFace y dos órdenes de magnitud más pequeño que FaceNet. Se muestran resultados competitivos de precisión y rendimiento en el punto de referencia de

verificación de LFW a pesar de que nuestro conjunto de datos de capacitación es más pequeño. Se presenta un punto de referencia de clasificación de LFW y se muestran los resultados de rendimiento competitivo en él. Se tiene la intención de mantener OpenFace como una biblioteca que se mantiene actualizada con las últimas arquitecturas de redes neuronales profundas y tecnologías para reconocimiento de rostros a comparación de los trabajos ya realizados. Estos estudios y las direcciones de investigación son complementarios a este estudio. El autor no estudia los impactos de la ejecución de técnicas en diferentes. OpenFace es muy adecuado para escenarios móviles en comparación con otras técnicas.

Descripción del Aporte del autor:

Se Usa el detector de cara pre-entrenado para una mayor precisión que el detector de OpenCV. Compilamos el código C nativo con gcc y el código CUDA con NVIDIA basado en LLVM nvcc.

La parte de detección de rostros devuelve una lista de cuadros delimitadores alrededor de las caras en una imagen que puede estar en diferentes condiciones de postura y de iluminación. Un problema potencial con el uso de los cuadros delimitadores directamente como una entrada en la red neuronal es que las caras podrían mirar en diferentes direcciones o bajo diferentes condiciones de iluminación. FaceNet puede manejar esto con un gran conjunto de datos de entrenamiento, pero una heurística para nuestro conjunto de datos más pequeño es reducir el tamaño del espacio de entrada al normalizar las caras para que los ojos, la nariz y la boca aparezcan en ubicaciones similares en cada imagen. La normalización de las caras es un tema de investigación activo en la visión por computadora. Muchas técnicas modernas como DeepFacefrontalizan la cara a un modelo 3D para que la imagen parezca como si la cara mirara directamente hacia la cámara. OpenFace usa una simple transformación afín 2D para hacer que los ojos y la nariz aparezcan en ubicaciones similares para la entrada de la red neuronal.

Ilustración 3: Estructura del proyecto OpenFaces

Proceso para resolver el problema:

Se construye en un escenario móvil el reconocimiento de rostro en tiempo real de un usuario. Se hace un sistema de alta precisión con el bajo entrenamiento y tiempo de predicción. En la Figura 3 ilustra cómo la transformación afín normaliza las caras. Los 68 puntos de referencia se detectan con el detector de puntos faciales. Dada una cara de entrada, nuestra transformación afín hace que las esquinas de los ojos y la nariz se acerquen a los lugares medios. La transformación afín también cambia el tamaño y recorta la imagen a los bordes de los puntos de referencia para que la imagen de entrada a la red neuronal sea de 96 x 96 píxeles.

Ilustración 4: Transformación en puntos azules y redimensiona a 96 x 96 pixeles

Ilustración 5: Flujo de entrenamiento de red de extremo a extremo de OpenFace

3.1.1.4. Face recognition using total loss function on face database with id photos (reconocimiento facial usando la función de pérdida total en la base de datos de caras con fotos de identificación)

Motivación del autor:

Los autores describen que se construyó una base de datos de caras llamada WDRef, que incluye alrededor de 3000 sujetos y más de 1000 temas asociados con más de 40 imágenes. Sin embargo, solo proporcionaron características de bajo nivel de estas imágenes y el enlace

oficial a estas características ya no está disponible. Cross-AgeCelebrityDataset (CACD) está diseñado para el reconocimiento mutuo de rostros y se lanzó un nuevo juicio mediante la recopilación de más de 160 imágenes faciales de 2k celebridades con edades comprendidas entre 16 y 62. Sin embargo, no solo la edad sino también muchos otros factores que afectan el rendimiento de un sistema de reconocimiento facial en las aplicaciones reales. Entonces, CACD no es una base de datos lo suficientemente general.

Descripción del Aporte del autor:

Los autores realizan una base de datos de reconocimiento facial en el cual tienen ID de identidad. Estas fotos no identificadas deben ser lo suficientemente diverso como para simular el escenario del mundo real. Con la ayuda de los motores de búsqueda se obtuvo las fotografías de identificación de 100 celebridades chinas. Se crean carpetas y nombres de las celebridades y fotos de identificación que se almacenan en las carpetas correspondientes. De acuerdo con las normas elaboradas por International Civil Aviation Organization (OACI) sobre el tamaño de la foto de pasaporte, debe ser de 70x80.

Primero se aplica un preprocesamiento de datos para cada imagen en la base de datos que consiste en fotos de identificación y sin identificación. Este módulo incluye eliminación de ruido de imagen, detección de rostros, segmentación de rostros y ecualización de histogramas (para disminuir el efecto de iluminación no uniforme). No se implementa la detección de puntos faciales porque algunos puntos de referencia no son visibles cuando el ángulo de la pose de la cabeza es grande. Obtenemos una cara limpia después del preprocesamiento de datos y luego extraemos las características de la imagen de la cara. Simultáneamente, damos salida a las características de cada imagen de rostro y las almacenamos en una base de datos de rasgos faciales con sus índices correspondientes.

En la etapa de prueba, se aplica el preprocesamiento de datos para la imagen de prueba y obtenemos las regiones de la cara (si existe al menos una cara). el método de detección de rostros propuesto usando multitarea en cascada redes convoluciones.

Se creó la base de datos de la cara (FDID) con las fotografías de identificación de las celebridades de internet y como muchas de sus fotos se identifican como sea posible. Se selecciona al azar 36 celebridades (18 hombres y 18 mujeres) y muestra sus fotos de identificación. La razón por la que prestar más atención al carnet de identidad es que por lo general proporciona más información de una persona entre todas sus imágenes de la cara.

Ilustración 6: La arquitectura propuesta del reconocimiento de la cara.

Proceso para resolver el problema:

Se realiza el modelo propuesto con un conjunto de datos la estructura de red similar de DeepFace. Se reemplaza la función de pérdida de softmax con nuestra función de pérdida total propuesta y se prueba con nuestra base de datos y algunos videos de la vida real. Las fotos ID y no de 80 de las celebridades recopiladas se seleccionan aleatoriamente para la capacitación y se comprueban diez fotos de celebridades, y se logran el mejor modelo de características (principalmente ajuste de los parámetros de las redes) y el algoritmo de cálculo de disimilitud. Las restantes 10 fotos de identificación de las celebridades no se usan

para realizar pruebas, y la precisión de las pruebas es del 79.64%, que es aproximadamente un cinco por ciento más alta que la precisión de DeepFace en FDID.

3.2.2. RESUMEN DE LA TIPOLOGÍA 2: CLOUD COMPUTING

3.2.2.1. Reporting an experience on design and implementation of e-Health systems on azure cloud (informar sobre una experiencia en diseño e implementación de sistemas de salud electrónica en la nube Azure)

Motivación del autor:

Según los autores menciona que en el cuidado de la salud (imágenes médicas), el crecimiento de tamaño exponencial de los estudios de diagnóstico ha requerido un aumento continuo de la potencia de cálculo. La difusión de la tele radiología requiere una eficacia cada vez mayor en la transmisión de datos incluso en áreas con ancho de banda de red limitado. La evolución de las tecnologías de diagnóstico por imágenes ha creado una necesidad tener mayor de recursos. Con tales aumentos en el tamaño de las imágenes, los archivos de almacenamiento obsoletos y la capacidad de espacio pueden obstaculizar la eficacia general de la atención médica. El médico necesita archivar estas imágenes durante mucho tiempo para protegerse contra demandas por negligencia profesional. Además, a medida que el paciente se mueve de un lugar a otro, múltiples imágenes de los mismos órganos se llevan a cabo una y otra vez debido a la falta de soluciones técnicas disponibles para el intercambio de imágenes entre las organizaciones de salud.

Descripción del Aporte del autor:

El autor describe el desarrollo de dos aplicaciones y los desplegó sobre la plataforma en la nube de Windows Azure mencionando las ventajas de la nube. La primera aplicación se denomina Sistema de gestión de la práctica médica basado en Cloud, y el segundo llamado Sistema de práctica de telemedicina basado en la nube.

Sistema de gestión de la práctica médica basado en Cloud

La aplicación se integra con los sistemas típicos de administración de salud, que se pueden usar para hospitales, clínicas y otras organizaciones médicas. La mayoría de los procesos y datos comerciales relevantes para la salud se gestionan de manera eficiente, incluidos EHR, recetas electrónicas, archivos de salud personales, datos de rayos X, etc.

En esta aplicación, desarrollamos los componentes de software usando C # en la plataforma Visual Studio 2012. Adoptamos el modelo de programación MVC y la herramienta SQL Server 2008. Además, la base de datos es MS SQL y se implementa en el sistema de base de datos SQL Azure de la plataforma Windows Azure. Los usuarios pueden ejecutar los scripts de SQL Server, que se desarrollan en la máquina local. La base de datos se replicará en una instancia de SQL Azure.

Sistema de práctica de telemedicina basado en la nube

Está integrado con funciones múltiples, como la cita e, la consultoría electrónica, la telemedicina y la prescripción electrónica. Con base en la plataforma en la nube de Azure, los pacientes pueden ver a los médicos por control remoto a través de Internet y consultar cualquier problema de salud. El médico puede verificar los registros de salud, los gráficos de rayos X, etc. para el paciente e incluso verificar los datos fisiológicos en vivo del paciente en tiempo real con alguna red de sensores corporales. La aplicación de telemedicina es un sistema híbrido. Combina diversas técnicas de comunicación y hardware. En este experimento, adoptamos la cámara web como el dispositivo frontal del usuario y Microsoft. En la plataforma en la nube de Azure, el servidor de medios de transmisión en vivo se implementa para el procesamiento de video / audio. Windows Azure ofrece el servicio escalable de transmisión de video a través del servicio de medios de rol web que se ejecuta en la máquina virtual.

En el proceso de transmisión ascendente, se utilizará para recopilar los datos de la cámara en el cliente (ya sea un paciente o un médico) y codificar la transmisión de video en al formato de Silverlight; Mientras tanto, la transmisión se trasladará a una función web de Windows Azure, que es una máquina virtual. En el proceso de transmisión descendente, un rol web de Windows Azure carga la transmisión de video por saldo y lo publica en el punto de extracción. Este proceso lo ejecuta el servidor de medios en la función de Windows Azure. Este punto de publicación permite que el reproductor de video extraiga la transmisión de video desde el servidor de medios. En el extremo del cliente, el reproductor Silverlight debe instalarse con un navegador web, ya sea Internet Explorer o Firefox. La secuencia de video con formato Silverlight será decodificada y mostrada por el navegador web.

En el sistema de telemedicina, un paciente puede registrarse y luego iniciar sesión para buscar al médico apropiado en el control remoto para él y luego programar una cita con el médico remoto en la fecha y hora disponibles. Luego, en la fecha y hora establecidas, el paciente iniciará sesión en el sistema para reunirse con el médico designado. El paciente puede ver al médico en la interfaz del sistema por video y audio y luego hablar con el médico con su declaración. Además, el paciente puede presentar sus otros datos fisiológicos al médico, como su informe de análisis de sangre reciente, la imagen de rayos X y el cuadro de EGG u otros datos multimedia o descripciones de texto. Al final de la consulta, el médico puede dar la conclusión y la solución o prescripción. La receta será presentada al paciente en su sistema.

Ilustración 7: Windows Azure Live Smooth Streaming.

Proceso para resolver el problema:

Para resolver el problema se implementó la arquitectura de las aplicaciones con las herramientas y la base de datos. Se simuló un escenario con un gran número de usuarios en un hospital. Para esta simulación se testeó con la herramienta JMeter. Para medir la capacidad de ampliación del servicio de streaming se utilizó una máquina virtual en la cual tenía los servicios de SmoothStreaming con la intención de realzar la consulta médica entre el paciente y el médico. Además, se usó la herramienta SmoothStream Performance Testing Tool en la cual genera carga de usuarios para medir el rendimiento. También se cuantificó el Tiempo Promedio de Respuesta de la Solicitud HTTP (ARTHR) de los siguientes componentes relacionados con el Sistema de Gestión de Práctica Médica basado en la nube.

3.2.2.2. Cloud-assisted speech and face recognition framework for health monitoring (marco de reconocimiento de voz y voz asistido por la nube para el control de la salud)

Motivación del autor:

Ante las investigaciones que dio los autores, se realizó un análisis de reconocimiento por voz. Por lo que al implementar reconocimiento facial dentro del framework es de una gran utilidad. Pues, servirá como gran soporte para el monitoreo del paciente y evaluación de su salud. Esto se le suma la creciente demanda de computación en tiempo real y análisis de datos de pacientes ancianos para una atención de calidad. Cloud computing junto con la proliferación de los dispositivos de mano alivia la carga de la tarea de cómputo en físico en el lado del cliente en el lado del servidor de nube y hacer que los dispositivos de mano funcionan como interfaces de usuario con el extremo de nube de soporte correspondiente. Esto mejora de la transformación digital en el sector salud.

Descripción del Aporte del autor:

El autor propone un Framework basado en la nube para la vigilancia del cuidado de la salud de los ancianos, donde una imagen facial y la voz se utiliza para monitorizar a un paciente remotamente y evaluar su salud. El monitoreo puede ser utilizado en cualquier dispositivo dispositivos móvil. Las imágenes de habla y de voz capturadas del paciente se transmiten al servidor de la nube. En el servidor, las características del habla y del rostro se extraen, y se clasifican independientemente usando una máquina. Los resultados clasificados de las dos modalidades se fusionan para dar la decisión final. La decisión se envía a un centro de atención, donde toma la acción apropiada para atender al paciente. La voz y la imagen del rostro se eligen las modalidades de entrada, debido a su naturaleza no invasiva. En el servidor de nube, las características del habla se extraen en dos direcciones, una a lo largo del tiempo y la otra a lo largo de la frecuencia de un patrón espectro-temporal. Para los rasgos faciales, se extraen descriptores de textura homogénea y descriptores de textura de borde para definir la expresión facial en las regiones homo genéticas y no homogéneas de la cara, respectivamente.

Se clasifica el estado de los pacientes en tres estados como no grave, dolor y tenso. Cuando una persona mayor necesita ayuda, utiliza su dispositivo de mano, por ejemplo, teléfono móvil para entregar el mensaje. El dispositivo captura su discurso, así como su imagen de la cara, y envía al servidor situado en la nube. Los datos también se pueden capturar a través de cámaras de vídeo instaladas a lo largo del área de movimiento de los pacientes. En el servidor, dos modalidades (voz y rostro) se procesan por separado en 'detección de voz' y 'reconocimiento facial'. Las puntuaciones de estos dos componentes se fusionan para entregar la decisión final del estado de la persona. Con base en la decisión, los servicios de emergencia, médicos regulares o cuidadores pueden ser contactados.

La imagen del rostro es capturada por el teléfono móvil y se detecta el área facial. El rostro detectado se transmite posteriormente al servidor de nube (Reconocimiento de rostro) y se procesa para el reconocimiento del estado del paciente. Dos tipos de descriptores de vídeo MPEG-7 que son utilizados para imágenes fijas, pues se utilizan para extraer características de la imagen del rostro. Los descriptores de textura homogénea (HTD) y los descriptores de histograma de borde (EHD) son utilizados para el reconocimiento de rostros u otras aplicaciones de procesamiento de imágenes antes. HTD da una caracterización cuantitativa de la región de textura homogénea para la medida de similitud, mientras que EHD lo proporciona para la región de la textura no homogénea. El autor explicará en cálculos para calcular el HTD y el EHD en el cual, se explicará algo breve.

EHD captura las distribuciones de los bordes en una imagen y se divide en sub-imágenes 4×4. Luego, se calcula un histograma con cinco bins correspondientes a cinco categorías a cada cuadro. Finalmente, los histogramas de todas las sub-imágenes se conectan para tener los contenedores. Cada sub-imagen se divide en una cantidad de bloques de imágenes. Los bloques de imágenes están enfocados con los cinco filtros y si la salida máxima de estos filtros supera un cierto umbral, se considera como un bloque de borde que se corresponde con el histograma de la sub-imagen; de lo contrario, el bloque de imagen no contribuye al

histograma de sub-imagen. Una vez realizado el procesamiento facial, se funciona con el procesamiento de voz para realizar los resultados que necesita el doctor.

Ilustración 8: Arquitectura de extracción de reconocimiento de facial y voz

Proceso para resolver el problema:

Los autores ejecutaron la arquitectura propuesta en tres configuraciones diferentes de servidor en la nube y un servidor local. En la implementación, la aplicación se integra en un conjunto de componentes de servicio. Se utilizaron las herramientas Amazon Web Services (AWS), SQL Server y Visual Studio 2010, dispositivos portátiles de los pacientes integrados con cámaras de video o las cámaras de video montadas en la pared se usaron para recopilar y enviar datos relacionados con la cara y el habla. Se realizaron datos de capacitación con 105 sujetos ancianos, de los cuales 80 eran hombres y 25 mujeres. Se registraron los datos utilizando la interfaz web. La entrada fue un discurso independiente del texto, como "por favor ayuda", "necesito ayuda", etc. y la imagen del rostro. Durante el habla del paciente, la aplicación móvil detectó la cara y envió el marco y el habla a la nube. Los médicos etiquetaron los datos como no severos, dolorosos o tensos, previo consenso.

Se realizó una encuesta sobre los pacientes y los cuidadores para medir la satisfacción de utilizar el marco. Se hicieron cuatro preguntas y los encuestados valoraron su satisfacción en una escala de Likert. Esta escala tiene cinco niveles con sus puntajes correspondientes.

Los cinco niveles y puntajes son muy desagradables (1), en desacuerdo (2), neutrales (3), de acuerdo (4), muy de acuerdo (5). El puntaje promedio por pregunta de 50 respondedores se da en la Tabla 1.

Tabla 4: Encuesta de satisfacción del usuario

Asunto	Calificación promedio del usuario	
	Pacientes	Cuidadores
Estoy satisfecho con el reconocimiento	4.3	4.5
Estoy satisfecho con el tiempo de retroalimentación	4.1	4.2
Estoy satisfecho con los sensores	4.2	4.0
El reconocimiento estatal es importante para el cuidado de la salud	4.4	4.1

3.2.2.3. A new framework for cloud storage confidentiality to ensure information security (un nuevo marco para la confidencialidad del almacenamiento en la nube para garantizar la seguridad de la información)

Motivación del autor:

En el modelo propuesto en los últimos años, se ha encontrado un déficit en el mecanismo de seguridad. Se evidencia que existe insuficiencia de en defensa sobre algunos ataques. Por lo que existe otras maneras en que el usuario o servidor pueda verificar la integridad de datos. Se utilizaron dos servidores para de almacenamiento y de cifrado. El servidor de almacenamiento se utiliza sólo para el almacenamiento de datos y la responsabilidad principal servidor de cifrado es la autenticación y la integridad de verificación. En este mecanismo existente que garantizar la confidencialidad e integridad de los datos a través de la nube. Utiliza tres algoritmos diferentes para verificar los datos almacenados en almacenamiento en la nube. Todo esto se lleva a cabo para contribuir a nube entorno informático con el fin de evitar la pérdida de datos, la modificación de datos, y el acceso no autorizado de datos de usuario.

Descripción del Aporte del autor:

Se propone un marco de seguridad y la integridad de una manera eficiente. Se utilizó diferentes servidores y cada servidor en una red de la nube realiza misma operación. Los datos de usuario que se almacena en la nube se pueden comprobar en términos de privacidad, autenticación e integridad, por todos y cada servidor en la red. Los servidores en red de la nube están conectados el uno al otro en la forma de un anillo. Cada servidor es actúa como un servidor de almacenamiento y de autenticación. Estos servidores están realizando operaciones de la siguiente manera:

El primer usuario necesita ser autenticado por el servidor y el servidor es autenticado por el usuario, lo que se hace mediante el protocolo de acuerdo de clave de estación a estación. Luego, para la integridad del servidor de datos se calculará SHA-1. Y finalmente el servidor cifra los datos usando AES para mantener la confidencialidad de los datos.

Aquí estamos utilizando el protocolo de acuerdo de clave de estación a estación como un mecanismo de intercambio de claves. Este protocolo es una versión extendida del algoritmo de intercambio DiffieHellman Key, pero el algoritmo DiffieHellman es vulnerable al ataque Man-in-Middle. En el protocolo de acuerdo de clave de estación a estación, usamos certificados y la clave que se genera para verificar la autenticidad del usuario. Evita el ataque “man in the middle” para mantener la autenticidad del usuario y del servidor.

Ilustración 9: Arquitectura del modelo propuesto

Cuando el servidor de autenticación realiza la operación y envía los datos resultantes al siguiente servidor de almacenamiento, el servidor de almacenamiento actúa como un servidor de autenticación para el siguiente servidor en el anillo y así sucesivamente. El modelo del sistema propuesto de trabajo es de la siguiente manera:

Funcionamiento del sistema de seguridad:

1. Registrarse con el proveedor de servicios en la nube.
2. El usuario selecciona el archivo de datos para Cargar / Descargar.

Caso 1: para cargar datos

1. El usuario encripta los datos con su clave privada y los envía al servidor de autenticación.
2. El servidor de autenticación descifra el archivo con sus claves.

3. Calcula el algoritmo SHA-1 para el archivo original e inserta el resultado llamado resumen con el archivo original.
4. Finalmente, el servidor de autenticación encripta el archivo, es decir, el resumen de los datos con su clave utilizando AES y envía los datos cifrados al usuario.
5. Ahora el usuario tiene acceso al servidor de almacenamiento y carga el archivo cifrado al almacenamiento en la nube

Caso 2: para descargar datos

1. El usuario descarga el archivo de datos enviando la solicitud al servidor haciendo clic en el botón de descarga.
2. El usuario reenvía el archivo descargado al servidor de autenticación. Y el servidor de autenticación descifra el archivo usando su clave.
3. Calcula el SHA-1 en la parte de datos del archivo y lo compara con el resumen de resumen con el archivo de datos.
4. Si la coincidencia fue encontrada correcta, el archivo se verifica y el archivo se envía de vuelta al usuario; de lo contrario, se envía un mensaje de error al usuario informándole que el archivo de datos está dañado o alterado.

Se utilizó diferentes algoritmos, como AES para el cifrado y descifrado; y el SHA-1 para la verificación de datos y el protocolo de acuerdo entre claves de estación a estación para proteger la autenticidad del usuario. Además, AES se implementa muchas veces para cargar y descargar datos, aunque si el hacker obtiene acceso a servidores en la nube, no sirve de nada, ya que AES utiliza una clave privada en su implementación. Por lo tanto, se considera que el sistema propuesto es uno de los sistemas seguros para proteger los datos en el almacenamiento en la nube.

3.2.3. RESUMEN DE LA TIPOLOGÍA 3: APLICACIONES MÓVILES

3.2.3.1. Security testing for android m-health apps (pruebas de seguridad para aplicaciones m-Health de Android)

Motivación del autor:

A diferencia de otros autores, el trabajo se centra, como primero, en aplicaciones para fines específicos, en lugar de seleccionar al azar de la amplia categoría de aplicaciones de m-Health; y sólo en aplicaciones de Android. Esto nos da una población más homogénea que puede ser estrechamente probado y comparado, en particular, se nos permitió el registro de validación de entrada para la presión arterial c especificidad y rangos de lectura de glucosa. Nuestras pruebas van más allá que el trabajo anterior: mientras que otros han aplicado métodos de pruebas dinámicas, que, además aplicamos estática analizar las técnicas y examinar los aspectos de seguridad web que es novedoso para aplicaciones de salud móvil. la comprobación de la seguridad y la creación de un paciente virtual junto con su identidad electrónica en el contexto de pruebas de seguridad es nueva.

Descripción del Aporte del autor:

Los autores describen los tipos de amenazas que hay:

- Aprendizaje no autorizado de los datos
- Manipulación de los datos
- Visualización de datos no validos

Se muestra una arquitectura en el cual se ve las vulnerabilidades que puede tener para la medición de un sistema de control para la diabetes e hipertensión. Los ataques son clasificados de esta manera:

A1. Eavesdropper: permite ver cualquier tráfico de red no protegido.

A2. Atacante activo en la red: permite eliminar, desviar, modificar los datos en tránsito y las cuentas de usuario de la fuerza bruta.

A3. Hombre en el medio: es capaz de aprovechar los protocolos SSL implementados

incorrectamente al desviar el túnel SSL a su propio servidor y así permite leer los datos.

A4. Propietarios de tiendas de aplicaciones: las tiendas de aplicaciones mantienen registros de descarga de aplicaciones, además pueden publicar clasificaciones de usuarios que revelan de manera explícita qué aplicaciones usarán los usuarios.

A5. Desarrolladores de aplicaciones: pueden insertar rastreadores en sus aplicaciones para observar el comportamiento del usuario, cometer errores que filtran información o incluso incluir códigos maliciosos.

A6. Desarrollador de malware: puede haber malware por separado en el teléfono que se dirige a aplicaciones y transferencias médicas de datos a través de Internet.

A7. Los terceros, como el servidor de anuncios y análisis, el servidor web, los sitios de redes sociales y el almacenamiento externo, suelen proporcionar políticas de privacidad que establecen cómo se manejan los datos de los usuarios. Sin embargo, estas políticas pueden faltar, ser intrusivas o incorrectas.

A8. Atacante con acceso físico al teléfono inteligente: suponemos que puede extraer la tarjeta SD y acceder a datos no protegidos; también podría eludir los mecanismos de seguridad como los PIN y el cifrado.

A9. El usuario de la aplicación o el propietario del teléfono inteligente, que puede liberar datos de manera consciente o involuntaria.

Luego se describe un método de prueba para la seguridad de la información dividiendo en 4 partes: análisis estático, análisis dinámico, seguridad en el servidor y política de inspección.

TABLE I. STRUCTURE OF SECURITY TESTING

	What is tested?	How is it tested?	Sample vulnerability
Security	Static code analysis off and on phone (A)	Tools e.g. MalloDroid, Addons Detector	Faulty SSL implementation → MITM attacks
	Dynamic analysis (B)	Manual with tool support e.g. tcpdump, adb	Outdated third party libraries used
	Web security (C)	Manual	Password or medical data in cleartext Unencrypted medical data in backup Empty/simple password
Privacy	Analysis of privacy policies (D)	Manual. Checking policy for 1. base info, 2. completeness based on OECD, 3. invasiveness	Policy missing or outdated (1.) Description of user rights missing (2.) Medical data shared with 3rd parties (3.)
Safety	Input validation of sel. medical data (B)	Manual. Checking input fields in GUI	Lethal values accepted Junk input accepted → SQLi, XSS, XSRF

Ilustración 10: Estructura de testeo de seguridad dividida en 3 fases.

Análisis Estático:

Se basa en la información contenida en los archivos del APK en el cual está el manifiesto y el código compilado. Las pruebas se realizaron en una estación de trabajo y el dispositivo. Como el primer paso extraemos los permisos de las aplicaciones, la cual indican qué acciones (como Internet, Bluetooth, el acceso a los contactos de la libreta de direcciones) están permitidas. Los permisos deciden sobre la aplicabilidad de ciertas pruebas. Se utiliza la herramienta AndroGuard.

Análisis Dinámico:

Es principalmente manual, pues el proceso es difícil de automatizar. Se investigó si se aceptan entradas anormales e ilegales, y cómo los datos exportados se almacenan o transmiten.

Conexión con el servidor:

Para aplicaciones que interactúan con un servidor web para realizar una copia de seguridad o sincronizar datos, se analizan las siguientes cuestiones de seguridad relacionadas con la seguridad en la web. Como un paso preparatorio, se necesita una cuenta de usuario en el sitio web correspondiente al paciente.

Inspección de las políticas de privacidad:

Almacenamiento de los datos médicos en un servidor externo más subraya preocupaciones

de privacidad (y permite A7 atacante). Para comprobar si hay debilidades este sentido, proponemos la inspección de las políticas de privacidad.

Ilustración 11: Arquitectura del método del testeo

Proceso para resolver el problema:

Se realiza el ensayo descrito con las fases establecidas y un ambiente adecuado para la elaboración del ensayo. Se seleccionó distintas aplicaciones de mhealth para la diabetes e hipertensión. Se creó un usuario de prueba con 70 cm de altura, 99 kg de peso, presión alta de 200 mmHg / 120 mmHg, una frecuencia cardíaca fisiológicamente improbable (333 bpm), y un nivel de glucosa en sangre de 111 mmol / L. El móvil fue un Nexus 7 de Android 4.4.2 y se operó una MV con un Sistema Operativo Linux 12.04, para la conexión y ejecución con distintas herramientas.

3.2.3.2. Mining Android apps to recommend permissions (minería de aplicaciones de Android para recomendar permisos)

Motivación del autor:

El enfoque basado en el descubrimiento de reglas de asociaciones puede señalar los casos de relaciones poco frecuentes, y por lo tanto posiblemente sospechosos, permisos API. A pesar de que la API requiere permisos están muy-bien documentadas, su nivel de comprensión todavía causa malos usos. Por lo tanto, los enfoques tales como nuestra propuesta ApMiner podría proporcionar recomendaciones rápidas a los desarrolladores, incluso antes de obtener respuestas sobre StackOver flujo. El enfoque de los autores se puede utilizar para detectar comportamientos sospechosos y para ayudar a los desarrolladores en la selección de los permisos apropiados. En segundo lugar, mientras que los enfoques de otro autor tienen inconsistencias de relieve entre la descripción y las API, nuestro enfoque pone de relieve las posibles incoherencias entre las API y permisos. A lo mejor de nuestro conocimiento, las herramientas más relacionadas con ApMiner son Polizón, PScout, y Androguard para identifica el API a las asignaciones de permisos realizando un análisis estático de la aplicación y luego confiando en un permiso de Android.

Descripción del Aporte del autor:

ApMiner se basa en la premisa de que, si las API y las misiones frecuentemente ocurren en aplicaciones de Android existentes desplegados en un mercado, entonces pueden ser recomendados para los desarrolladores de una nueva aplicación. Se utiliza la técnica de minería de conjunto de elementos frecuentes para generar reglas de asociación para codificar el uso de la API-permiso. Como tal, se consideran como una práctica común. Primero se explica cómo la minería conjunta de elementos frecuentes se puede utilizar para identificar las reglas de permisos API.

A. Identificar Normas de permiso de API mediante la minería de elementos de archivo frecuentes

La minoría de elementos frecuentes es una técnica de minería de datos ampliamente utilizada para el análisis de afinidad para descubrir relaciones de concurrencia entre entidades en

transacciones. El conjunto de transacciones corresponde al conjunto de aplicaciones existentes alimentadas para entrenamiento. Las entidades corresponden a las API y los permisos utilizados en las aplicaciones en “T”. Es decir, una transacción es un conjunto de API y permisos utilizados en una aplicación. Por lo tanto, nuestros conjuntos de elementos frecuentes son los conjuntos de API y

permisos encontrados para concurrir en T.

B. Extracción y asignación de permisos y API

El requisito previo para aplicar la minería de elementos frecuentes es la formación de transacciones “T”, que están compuestas por entidades. Estas transacciones forman nuestro conjunto de entrenamiento. En nuestro contexto, cada transacción corresponde a una aplicación existente y las entidades hacen referencia a sus API y a los permisos requeridos. Los permisos se especifican en el archivo `AndroidManifest.xml`, que se encuentra en el nivel raíz de la aplicación. Las APIs se encuentran en los archivos de código fuente de Java, a través del uso de la declaración de importación. La extracción de las API y el archivo es sencilla para las aplicaciones de código abierto. Es importante tener en cuenta que en Android la relación entre un permiso específico y una API particular es necesariamente el caso de que el uso de un permiso siempre requiera el uso de un conjunto específico de API y viceversa.

El enfoque de calidad es el rendimiento de la predicción de ApMiner en términos de precisión, recuperación y puntuación F cuando se consideran los tres niveles de granularidad diferentes de las minas de reglas de asociación, es decir, del BaseMiner, FilteredMiner y FilteredMiner. mapeos de permisos y clases de API. Analiza el sistema operativo Android y rastrean desde API hasta llamadas de permiso con análisis estático. La perspectiva es de un desarrollador de aplicaciones que necesita ayuda con las API y los permisos para usar. Las unidades de análisis de nuestro estudio son 600 aplicaciones de código abierto para Android de F-Droid.

C. Formando Transacciones o Conjunto de Entrenamiento

El primer nivel de mapeo, denominado BaseMiner, consideramos todo el conjunto de permisos relacionados con todo el conjunto de API se usa para una aplicación. Todas las clases API y las entidades de autorización en una aplicación se ensamblan juntas en una sola transacción. La formación de transacciones en este nivel no requiere ninguna trazabilidad entre las clases API y los permisos. Extraemos todos los permisos del archivo de manifiesto de una aplicación y los colocamos en la transacción de la aplicación. Luego, usamos srcML para analizar el código fuente de la aplicación. Esto nos permite identificar los usos de la API de Android. Además, tenemos una lista pre-procesada de todos los nombres de clase API utilizados en la pila de software de Android y las bibliotecas estándar de Java. Solo guardamos los nombres que coinciden con los de la lista de nombres de Android pre-procesados en la transacción de la aplicación.

D. Recomendaciones con las Reglas de la Asociación

Una vez que se forman las transacciones, se realiza una minería de patrones frecuente, que da como resultado conjunto de elementos frecuentes “E” de APIs y permisos. A partir de estos conjuntos de elementos, formamos reglas de asociación. Para cualquier conjunto dado de API para las cuales un desarrollador necesita ayuda con recomendaciones de permisos, usamos las reglas de asociación para recomendar los permisos requeridos. Seleccionamos reglas de asociación en las que ocurre como el antecedente y otro conjunto de permisos “P” de forma el consecuente. Varias reglas son posibles para la misma entidad. Cuando se encuentran múltiples reglas para una entidad dada, primero se clasifican por sus valores de confianza y luego por sus valores de soporte; ambos en orden descendente (más alto el valor, más fuerte es la regla). Permitimos que un punto de corte especificado por el usuario seleccione las reglas n superiores.

Proceso para resolver el problema:

Para apoyar a los desarrolladores en la elección de permisos y para identificar los casos de permisos excesivos, proponemos un enfoque, llamado ApMiner, recomendar permisos dados un conjunto de API de Android. ApMiner combina el análisis-que estática construye

rastros candidatos entre APIs y permisos a diferentes niveles de granularidad-con el descubrimiento de reglas de asociación, de los usos de permisos mineras en otras aplicaciones, que ya están publicados en los mercados de buena reputación. Se realiza una evaluación, realizada en 600 de código abierto aplicaciones tomadas de la F-Droid.

3.2.3.3. Consumer attitude: does it influencing the intention to use mhealth? (actitud del consumidor: ¿influye en la intención de usar mhealth?)

Motivación del autor:

En general, la aceptación de la tecnología mHealth fue bastante impresionante, sin embargo, hubo una cohorte de encuestados que se resistieron al uso de dicha tecnología e indicaron una actitud negativa. Estos encuestados, en su mayoría, no tenían un teléfono móvil o un teléfono inteligente y, básicamente, se sentirán incómodos con la tecnología.

Descripción del Aporte del autor:

Bajo la revisión de distintas soluciones se formula un método de estudio para comprobar la relación que tiene los usuarios con las aplicaciones móviles. La intención de este método será la calificados para determinar la actitud y el comportamiento para utilizar las aplicaciones de salud móviles. Bajo esto se determinará una encuesta para encontrar resultados analíticos y comprobar los resultados.

Los resultados del estudio en que se basa este trabajo indican que la actitud es significativa con la intención de utilizar la salud móvil. Esto demuestra que la actitud juega un papel importante en el crecimiento y desarrollo de la salud móvil. Estos hallazgos están en línea con el anterior estudio concluyó que la actitud positiva o negativa hacia la salud móvil dará lugar a su intención de aceptar o rechazar la tecnología. Por el contrario, de acuerdo con Wicklund, encontró que la actitud del consumidor no está convencida de que puede dar un teléfono inteligente de datos precisa de su estado de salud. Se cree que son todavía necesita un médico calificado para entender los datos y tomar decisiones mejor informadas. Sin

embargo, los consumidores en el estudio mencionan que el acceso a la aplicación mHealth les permitiría mejorar la gestión de su propia salud.

Proceso para resolver el problema:

Se aplica la encuesta a cuatrocientos ochenta usuarios de teléfonos inteligentes. Los encuestados fueron reclutados aleatoriamente mediante muestreo intencional en todo el estado. Se utilizó un método de encuesta como método de recopilación de datos, mientras que los cuestionarios se distribuyeron en este estudio; que proporcionó a los encuestados conjuntos de preguntas sobre las características sociodemográficas, la actitud hacia mHealth y la sección intención de uso. Los encuestados dieron su consentimiento para la conducta ética con el fin de que puedan comenzar la encuesta.

Demographic / Social Variables	Categories	Frequency N=480	(%)
Sex	Male	198	41.3
	Female	281	58.5
Age (Years)	18-20	70	14.6
	21-30	246	51.3
	31-40	91	19.0
	41-50	56	11.7
	51-60	17	3.5
Level of education	Primary	51	10.6
	Secondary	112	23.3
	Tertiary	317	66.0
Health problems	Yes	90	18.8
	No	360	75.0
	Don't know	30	6.2

Ilustración 12: Socio demográfico de los encuestados

TABLE III: REGRESSION ANALYSIS

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	β	Std. Error	Beta		
1 Constant	.862	.092		9.335	.000
ATT	.732	.024	.816	30.840	.000

Dependent Variable: Intention

Ilustración 13: Análisis de regresión

3.2.4. RESUMEN DE LA TIPOLOGÍA 4: MODELOS TECNOLÓGICOS

3.2.4.1. Fusion of electrocardiogram and arterial blood pressure signals for authentication in wearable medical systems (fusión de electrocardiograma y señales de la presión arterial para autenticación en sistemas médicos usables)

Motivación del autor:

En los últimos años, varios esfuerzos se han dirigido hacia la autenticación de usuarios en contextos portátiles utilizando señales fisiológicas como electrocardiograma (ECG), resonancia vocal, frecuencia cardíaca y EEG. La mayoría de estos esfuerzos se han centrado en crear una plantilla para un usuario basada en puntos de características en las formas de onda de la señal seguidas por enfoques estadísticos o de aprendizaje automático para autenticar al usuario. También se ha trabajado en el uso de la fusión de varias señales fisiológicas como una forma de autenticar a los usuarios. Estos se han realizado para mejorar la precisión del proceso de autenticación como cuando se combinaron ECG con señales de electroencefalograma (EEG) o para mejorar la autenticación basada en ECG particularmente en presencia de artefactos tales como movimientos. No se ha demostrado que ninguna de estas soluciones funcione tanto para usuarios normales como para usuarios con dolencias que afectan a la señal fisiológica que se utiliza para la autenticación. En los últimos años, se han realizado algunos esfuerzos para considerar la diversidad de la población de usuarios cuando se utiliza la autenticación de señal fisiológica. Sin embargo, estos enfoques producen una precisión relativamente baja y altas tasas de falsos negativos (es decir, rechaza usuarios

legítimos).

Descripción del Aporte del autor:

Se presenta un enfoque combinado de electrocardiograma (ECG) y presión arterial (ABP). El enfoque aprovecha el hecho de que la interrelación entre las señales ECG y ABP medidas sincrónicamente de diferentes usuarios tiene diferentes características. La figura 1 muestra la configuración de nuestro sistema. Funciona en dos etapas: etapa de inscripción y etapa de autenticación. En el

En la etapa de inscripción, recolectamos datos de ECG y ABP de un usuario que intentamos autenticar, extraemos características específicas de él y construimos un modelo específico para el usuario. Este modelo forma una "plantilla" que describe el comportamiento fisiológico único del usuario. Durante la etapa de autenticación, recogemos fragmentos breves de las señales ECG y ABP actuales de un usuario desconocido que intenta autenticarse, extrae las mismas características de los fragmentos y las alimenta al modelo específico del usuario, que luego etiqueta estas nuevas características. como perteneciente o no al usuario (ver figura). Describimos los dos pasos en detalles a continuación.

Ilustración 14: The ECG and ABP based Authentication Approach

Proceso para resolver el problema:

Primero se probó el modelo de autenticación para ver si puede autenticar correctamente a un usuario legítimo después de que su modelo específico para el usuario está capacitado. Para

cada modelo capacitado, tenemos exactamente un usuario legítimo. Por lo tanto, dividimos su $T_{curr} = 15$ minutos de señales de ECG y ABP medidas sincrónicamente en 300 intervalos de 3 segundos (ventanas), cada uno de los cuales produjo un punto de característica de 11 dimensiones. Estos 300 puntos de característica se ingresaron en el modelo específico del usuario, que luego los etiquetó como positivos o negativos. Idealmente, deberíamos obtener todas las etiquetas positivas para los puntos y autenticarlos a todos, ya que todos provienen del usuario legítimo.

En general, con un tiempo de entrenamiento establecido en 20 minutos y un tiempo de identificación de 3 segundos, nuestro enfoque arrojó una precisión del 97,43%, con un EER del 2,39%, con un FPR del 1,2% y un FNR del 3,94%.

3.2.4.2. Radio frequency identification (RFID) in health care: privacy and security concerns limiting adoption (Identificación por radiofrecuencia (RFID) en la atención médica: preocupaciones de privacidad y seguridad que limitan la adopción)

Motivación del autor:

La identificación por radiofrecuencia (RFID) es una tecnología que proporciona una utilidad significativa en la sociedad, incluida la cadena de suministro, envío, fabricación, vías de peaje, comercio minorista, servicios bibliotecarios, industria alimentaria y atención médica. La tecnología RFID puede mejorar la confiabilidad, el acceso, la calidad y la eficiencia de los datos de una manera rentable. Desafortunadamente, sin embargo, RFID tiene limitaciones en términos de privacidad de los datos y puede no ser una solución completamente segura en el cuidado de la salud. La implantación de RFID en el cuidado de la salud es cada vez más frecuente. Las implementaciones de cuidado de la salud de RFID incluyen la administración de ubicaciones de pacientes, empleados, equipos, medicamentos, registros, seguimiento de recursos y autenticación. Con RFID, los datos de atención médica pueden transferirse y almacenarse de manera automatizada mediante un programa informático. Como resultado, la tecnología RFID es útil en el seguimiento de los activos a medida que se mueven en una organización de atención médica (por ejemplo, equipos, empleados, mercadería, medicamentos, pacientes, etc.).

Descripción del Aporte del autor:

La RFID en la autenticación de atención médica tiene la capacidad de mejorar la conveniencia y la confiabilidad, tal vez a expensas de la privacidad y la seguridad. La autenticación de usuarios es un proceso frecuente, omnipresente y que consume mucho tiempo en la era de los recursos electrónicos en el cuidado de la salud. Es necesario un equilibrio satisfactorio entre la comodidad y la privacidad para mejorar las tasas de adopción. Se propone desarrollar un esquema de autenticación RFID para mejorar la privacidad y la seguridad. Los entornos de atención de la salud existentes carecen de sistemas de autenticación seguros y la RFID en el ámbito de la atención médica introduce inquietudes sobre la confidencialidad, la capacidad de forzarse (etiqueta o lector), la privacidad de la ubicación y la escalabilidad. Por lo tanto, se propone un protocolo cifrado para lograr tanto la privacidad de la ubicación como la escalabilidad. La solución implica una etiqueta RFID con capacidad computacional, atípica para la mayoría de las implementaciones actuales. Es probable que las consideraciones de costo sean un obstáculo importante en la adopción de protocolos de seguridad más rigurosos y, en adelante, la adopción generalizada de RFID en el dominio de autenticación.

Proceso para resolver el problema:

Se argumenta que la tecnología RFID es una tecnología de infraestructura, pero el valor proviene de datos capturados y analizados en aplicaciones subyacentes. Se describen las lecciones aprendidas de la implementación de un sistema de gestión de la atención médica habilitado con RFID. Se presentan un marco de 11 pasos para seguir al implementar la tecnología RFID en el ámbito de la atención médica.

La sugerencia es la división en las etapas de preparación, implementación y mantenimiento. Además, la configuración de seguridad y permisos es un paso crítico en el diseño para garantizar una comunicación efectiva. Y, lo que es más importante, el monitoreo continuo del sistema y la evaluación del desempeño son necesarios para garantizar un sistema que funcione correctamente. Las lecciones específicas compartidas incluyen pruebas adecuadas de interferencia peligrosa, establecer las expectativas del usuario de que la RFID a veces

puede tener baja legibilidad, formular un plan de negocios sólido, y la gestión de riesgos y la planificación de emergencia.

3.2.4.3. Ear biometrics for patient identification in global health: a cross-sectional study to test the feasibility of a simplified algorithm (biometría auricular para la identificación del paciente en salud global: un estudio transversal para evaluar la viabilidad de un algoritmo simplificado)

Motivación del autor:

La biometría es un método para reconocer a las personas a través de atributos fisiológicos únicos, es un campo en avance para la identificación de personas y promete ser aplicado en m-Health. La biometría se está convirtiendo en un medio cada vez más popular de identificación a nivel internacional. Los sistemas internacionales a gran escala para fines de inmigración, verificación de identidad, control de áreas de acceso restringido y control de información restringida ahora están activos en el Reino Unido (Reino Unido), Bélgica y otros países de la Unión Europea. También vale la pena señalar el programa de identificación biométrica Aadhaar de la India, que se estableció con el objetivo de inscribir a todos los adultos en el sistema para ayudar en la entrega de programas de bienestar social. Sin embargo, estos sistemas son ejemplos principales de la tendencia general de la aplicación biométrica para la identificación de personas; son a gran escala, complejos, multiescalares y generalmente inapropiados como análogos para nuestra configuración de interés. Desarrollamos siete criterios que un sistema biométrico elegido debería cumplir para resolver el desafío de la identificación de personas en los PIBM.

Descripción del Aporte del autor:

En primer lugar, al utilizar fotografías de orejas abiertas, evaluamos una serie de enfoques diferentes para convertir datos de imágenes en formatos numéricos algorítmicamente. El objetivo fue identificar las estructuras anatómicas cuya presencia era relativamente uniforme entre los individuos e identificar las estructuras convertibles en representaciones algorítmicas numéricas. Las estructuras anatómicas que incluimos en nuestra investigación se destacan en la Fig. 20. El desarrollo de nuestro método de medición algorítmica se derivó

en parte de la literatura sobre biometría auricular, pero también se guió empíricamente a través de ensayo y error de diferentes combinaciones de características y medidas.

En segundo lugar, realizamos un estudio de validación en dos pasos utilizando imágenes capturadas de voluntarios humanos. El objetivo fue probar primero nuestra capacidad para convertir datos de imágenes en formatos numéricos utilizando el algoritmo final del paso uno. Luego usamos esos datos numéricos para volver a conectar los sujetos a sus identidades.

Ilustración 15: Estructuras anatómicas del oído utilizadas en el desarrollo de algoritmos

Proceso para resolver el problema:

El proceso de identificar qué estructuras anatómicas incluir en el algoritmo destacó la alta variabilidad entre individuos. Por ejemplo, mientras que un individuo puede tener un antitragus pronunciado, otro puede tener una estructura convexa en su lugar. Además, un individuo puede tener un doblez distinto a la hélice, mientras que otro puede tener un oído que aparentemente no se dobla en absoluto. Incluso dentro de un conjunto relativamente pequeño de imágenes de oído de código abierto, se hizo evidente que muy pocas estructuras podían depender de una persona a otra y que el algoritmo elegido necesitaría múltiples enfoques para explicar la probable ausencia de uno o más estructuras.

Las estructuras en las que se basó el algoritmo final incluyeron hélice, antihélix, tragus, antitragus, incisura intertragica y lóbulo de la oreja (Fig. 1). Los principales puntos de interés en cada una de estas estructuras incluyen lo que denominamos el "punto de anclaje", o donde el punto crucial de la hélice se encuentra con la antihélix perpendicularmente, el punto más sobresaliente del tragus y el antitragus, la altura máxima desde la parte superior del oído a la parte inferior del lóbulo, y el borde exterior de la hélice. El "punto de anclaje" resultó fundamental en este análisis, ya que era la única característica anatómica que podía ser identificada de manera confiable en un tema del siguiente, y por lo tanto se convirtió en el punto de partida para el algoritmo. El algoritmo final se dividió en tres secciones. El primero, denominado «triángulo interior», consistía en un triángulo que comenzaba en el punto de anclaje y el primer borde corría tangencialmente a través del trago hasta que alcanzaba la base de la incursión intertragica, y el segundo cruzaba tangencialmente sobre el antitrago hasta alcanzar el antihélix y el tercer borde que conecta de nuevo al punto de anclaje.

3.2.4.4. Use of identification wristbands among patients receiving inpatient treatment in a teaching hospital (uso de pulseras de identificación entre pacientes que reciben tratamiento hospitalario en un hospital docente)

Motivación del autor:

En la vida diaria, se puede observar que los servicios de salud adoptan diferentes formas de identificar a los pacientes, por ejemplo, pulseras, carteles en la cabecera, calcomanías en la ropa e insignias de identidad. Desde el lanzamiento del PNSP, las instituciones han necesitado compatibilizar los dispositivos estipulados por el protocolo y los deseos de los pacientes. A pesar de que existen pocos estudios que aborden específicamente el tema de la identificación del paciente, es posible observar una preocupación mundial en relación con esta práctica, ya que está estrechamente relacionada con cualquier procedimiento realizado con los pacientes, como la administración de medicamentos, operaciones y transfusión de sangre o productos sanguíneos, entre otros.

Los errores en la identificación pueden originarse en el momento en que se ingresa al paciente en el sistema de asistencia. La introducción de datos con errores, en un registro

computarizado, puede comprometer todo el proceso de atención. El proceso de identificación del paciente, incluida la verificación de los datos en la pulsera en relación con los registros del paciente y con la información confirmada por él o ella, puede verse como una etapa importante en la interacción entre el paciente y el equipo de salud. Los errores causados por descuido pueden continuar ocurriendo si los pacientes no tienen muñequeras, o si la pulsera no contiene información precisa para la identificación.

Descripción del Aporte del autor:

La identificación de los pacientes, y la aplicación de la pulsera, debe ocurrir en un proceso sistematizado, esta acción se incluye como una de las medidas del cuidado proporcionado a los pacientes. Este hecho puede observarse al analizar datos recientes referentes a la unidad de tratamiento de pacientes hospitalizados de neonatología, donde el 100% de los recién nacidos tienen al menos una pulsera, y el 100% de las pulseras están de acuerdo con el SOP. La práctica de colocar muñequeras en los recién nacidos y la confirmación de los datos en las pulseras con los responsables del niño han sido absorbidos por los profesionales de esta unidad, como es el caso con las otras medidas de cuidado que se toman al admitir recién nacidos.

El proceso de implantar nuevas prácticas debe llevarse a cabo de manera colaborativa y constructiva, aliando el objetivo institucional de consolidar la atención con calidad y seguridad con los intereses y necesidades de los equipos que trabajan en la primera línea de la atención. Los cursos de educación continua, actualización, mejora y actualización con el objetivo de agregar al conocimiento adquirido en la formación curricular básica también ayudan a reducir fallas.

Validación:

La implementación de esta práctica fue verificada por las tasas de pacientes con la pulsera y por las tasas de pulseras correctas de acuerdo con el SOP de la institución. Se determinó que el uso de los dos identificadores, el nombre completo y el número de registro, está ampliamente distribuido entre los profesionales que insertan estos datos en las pulseras. También se encontraron datos que arrojaron resultados con respecto a los aspectos visuales

de la pulsera, como su integridad física, su legibilidad y su color.

Además, se identificaron las unidades de hospitalización que requieren mayor atención, debido a que presentan resultados por debajo de los encontrados en la mayoría de las áreas investigadas.

Los resultados obtenidos en las unidades de los servicios pediátricos y psiquiátricos son muy similares a las referencias disponibles en la literatura, lo que refuerza la necesidad de una revisión de las etapas de identificación con el equipo de salud, y un aumento de los pacientes y sus familias la conciencia de los miembros sobre la importancia de que estén alertas a esta práctica al participar en la construcción de la cultura de la seguridad en la institución

3.3. CONCLUSIONES

3.3.1. CONCLUSIONES PARA LA TIPOLOGÍA 1: ARTÍCULOS DE FACE RECOGNITION

Existen diversos algoritmos para el uso de reconocimiento facial en los cuales sirven para identificar rostros de manera eficaz. El sistema que obtuvo mejores resultados fue el modelo configurado por Amazon. Como tiene distintos procesos, su algoritmo LBPH (Histograma local de patrones binarios) realiza sus funciones a la par que genera eficiencia en la ejecución de reconocimiento facial de la persona. Se menciona que se reconoce a la persona en un 95% pero, mientras más imágenes de la misma persona se tenga mejor es la detección de esta. Se evidencia arquitecturas que con el apoyo de OpenFaces se detecta los rostros faciales bajo puntos biométricos y así entrenar el sistema. Por lo que se reforzaría el algoritmo utilizando 4 fotos de la misma. No se deberá exceder ese número, pues se describe que a más imágenes por persona el algoritmo tiene mayor tiempo de ejecución.

Por otro lado, se explica el almacenamiento de imágenes con una ID bajo una arquitectura obtener una base de datos de celebridades chinos. Por lo que se define como se debe almacenar imágenes a la necesidad de lo que se requiere.

3.3.2. CONCLUSIONES PARA LA TIPOLOGÍA 2: ARTÍCULOS DE CLOUD COMPUTING

En cloud computing se describe distintos sistemas que se implementaron en el sector salud. Estos sistemas ayudaron a mejorar las necesidades que tienen los médicos para realizar análisis y resultados hacia la vigilancia de la salud de los pacientes. Además, se presenta un marco de seguridad en los mecanismos de la seguridad de la información bajo la red de servidores para identificar la conexión a la misma de manera segura. La implementación de una nube en plataforma cloud (PaaS) es tan útil como los servicios y capacidades ofrecidos por la plataforma a los desarrolladores de aplicaciones en servidores físicos.

Por otro lado, los proveedores de servicios pueden utilizar las directrices y las experiencias de los estudios de caso presentados en este documento al diseñar servicios a escala de nube para plataformas. Un conjunto de servicios puede atraer a los desarrolladores de aplicaciones a la plataforma.

3.3.3. CONCLUSIONES PARA LA TIPOLOGÍA 3: ARTÍCULOS DE APLICACIONES MÓVILES

En sector de la salud las aplicaciones móviles denominadas mhealth ayuda a recibir información de la salud de los pacientes a los doctores. El desarrollo de estas aplicaciones móviles se ha puesto la investigación de protocolos de seguridad pues se describe la inseguridad que existe en estas. Además, se muestra un marco de recomendaciones de permisos y el nivel de granularidad. Para una mejor interacción con los pacientes se evidencia bajo un estudio que las tendencias de mhealth ayuda a mejorar la gestión de la atención de la salud del paciente al ver un consumo positivo por parte del operador.

3.3.4. CONCLUSIONES PARA LA TIPOLOGÍA 4: ARTÍCULOS DE MODELOS TECNOLÓGICOS.

Los sistemas o modelos tecnológicos tienen el objetivo de poder identificar de manera efectiva a los pacientes. Los resultados dan un paso positivo al uso que le dan. No obstante, los errores demostrados no corresponden a soluciones efectivas. Además, algunos sistemas tienen precios elevados para la implementación. Queda demostrado que la ausencia de un modelo tecnológico de reconocimiento facial da soporte a la investigación de la herramienta y proceder al uso de la identificación de pacientes.

3.3.5. CONCLUSIONES GENERALES

Se concluye que las herramientas y los marcos de trabajo para el desarrollo de un modelo es fundamental en la nueva tendencia de reconocimiento facial. Está claro que para el desarrollo de la base de datos la implantación de cloud PaaS y la aplicación deben estar bajo protocolos de seguridad para la información. Además, se demostró que la implementación de mhealth mejora la calidad de atención a los pacientes. El reconocimiento facial es un manejo de aprendizaje que puede beneficiar a mejorar la seguridad y evitar fraudes de identificación. La base de datos se debe realizar bajo el marco de obtención de imágenes para mejorar la calidad información. Además, solo se aceptará imágenes de VGA (640x480) o superior y en formatos JPEG y PNG. Bajo este modelo y otros propuestos se puede realizar, como plan a futuro, una gestión de información del paciente para beneficiar en la toma de decisiones a los médicos.

CAPÍTULO 4: MARCO TEÓRICO

El presente capítulo detalla los conocimientos o conceptos básicos necesarios para un mejor entendimiento del desarrollo del proyecto. Primero, se empieza con la definición de machine learning, su división y los enfoques que se aplica esta tecnología. Luego se explicará el reconocimiento facial con las soluciones que brinda.

4.1. MACHINE LEARNING Y DEEP LEARNING

Se realizó una investigación de la explicación de machine learning, permitiendo así, un concepto final del término. Para ello se tomó referencia de distintos artículos:

Machine learning según Forrester:

Según la empresa, define machine learning como a un amplio de conjunto de algoritmos que permite aprender patrones en las computadoras. Es parte de la rama de inteligencia artificial. El aprendizaje es desarrollado por distintos algoritmos.

Machine learning según Gartner:

Gartner lo define como un método de procesamiento de inteligencia artificial dentro de una computadora que permite el autoaprendizaje a partir de la experiencia. Pueden desarrollar conclusiones a partir de un conjunto de información complejo y aparentemente no relacionado. Uno de los algoritmos más utilizados son la red neuronal.

Deep learning según Ravì, D., Wong, C., Deligianni, F., Berthelot, M., Andreu-Perez, J., Lo, B., & Yang (2017):

Deep Learning es un subconjunto dentro del campo del Machine Learning, el cual predica con la idea del aprendizaje desde el ejemplo. En lugar de enseñarle a ordenador una lista enorme de reglas para solventar un problema, se presenta un modelo que pueda evaluar ejemplos y una pequeña colección de instrucciones para modificar el modelo cuando se produzcan errores. Existen distintas técnicas para implementar Deep Learning, una de las más comunes es simular un sistema de redes artificiales de neuronas dentro del software de análisis de datos. Salvando las distancias, inspiradas en el funcionamiento biológico de nuestro cerebro compuesto por la interconexión entre neuronas.¹ Se trata de proporcionar la suficiente cantidad de datos a las capas de neuronas para que puedan reconocer patrones, clasificarlos y categorizar. Una de las grandes ventajas es trabajar a partir de datos no

¹ Daniele Ravì (2017)

etiquetado y analizar sus patrones de comportamiento y ocurrencia.

machine learning según Bost, R., Popa, R. A., Tu, S., & Goldwasser, S. (2015):

La clasificación de aprendizaje de máquinas se utiliza hoy en día para numerosas tareas, como predicciones médicas o de genómica, detección de spam, reconocimiento facial y predicciones financieras. El uso de la tecnología tiene un gran punto en la construcción de los datos y la clasificación. Los algoritmos de aprendizaje creados y supervisados de dos fases para la predicción: la fase de entrenamiento durante la cual el algoritmo aprende un modelo a partir de un conjunto de datos de ejemplos etiquetados, y la fase de clasificación que ejecuta un clasificador sobre un vector de características previamente invisible, usando el modelo para generar una predicción².

Reconocimiento facial según Wang, P., Lin, W. H., Chao, K. M., & Lo, C. C. (2017)

Las redes de machine learning utilizaron redes neuronales convulsionales coronadas (CNN). Son varias capas totalmente conectadas o escasamente conectadas seguidas por una capa de clasificación final. Produce excelentes resultados en aplicaciones de imagen y voz; y acelerar el aprendizaje y reconocimiento de características biométricas.³

4.2. RECONOCIMIENTO FACIAL

Reconocimiento facial según la empresa Eset:

Alta tecnología de la identificación digital para reconocer rostros. La implementación de esta

² Cfr. Raphael Bost (2015)

³ Cfr. Ping Wang (2017)

medida nos brinda protocolos de seguridad o beneficio para el consumidor. Asigna el rostro como un identificador único. Su uso se ha empleado en aeropuertos y en áreas públicas. Ante los avances tecnológicos, el cambio del procesamiento de imágenes de 2D a 3D ayudó a mejorar la identificación. Las imágenes ahora son capaces de recopilar una gran cantidad de información adicional basada en submililitros (o microondas) para muchos aspectos faciales, desde la estructura ósea hasta las curvas alrededor de la cuenca del ojo, la nariz y la pera. Esto ayuda a reconstruir la estructura del rostro y, en última instancia, mejora la identificación y la hace más precisa. El RF es capaz de identificar las diferencias entre gemelos idénticos.

Reconocimiento facial según la CIO Perú 2014:

Es la forma en que está destinado a ser el futuro. El potencial del reconocimiento facial es sustancial, incluso si no está todavía plenamente desarrollado. Es aplicado en diferentes mercados verticales, incluyendo los sectores comerciales, de marketing, atención médica y hospitalidad. Y en muchos casos, el reconocimiento facial es una fuerza multiplicadora y un facilitador que aparece en primer lugar en los sistemas existentes.

el uso del reconocimiento facial se clasifica en dos categorías: los entornos cooperativos y los ambientes no cooperativos. En el primer caso, la persona cuyo rostro se va a escanear es consciente de ello y está abierta a un proceso en el que el reconocimiento facial está sirviendo como su credencial; la persona sabe que va a mirar directamente a una cámara, sin ningún intento de ocultar su rostro. Sin embargo, en entornos no cooperativas, las personas no son necesariamente conscientes de que su cara se está escaneando y no están haciendo ningún intento de mirar directamente a la cámara. En los ambientes no cooperativos es en donde, aun, el reconocimiento facial no es tan ampliamente implementado, dada su relativamente baja eficacia.

Con los sistemas que son 2D, tiene que tener una vista recta para tener precisión". Hay

algunas empresas, sin embargo, que están trabajando en el desarrollo del reconocimiento facial que funciona en un entorno 3D. Con el uso de cámaras geográficas que utilizan varios marcadores, éstas podrían aumentar la probabilidad de conseguir un buen escaneo, incluso cuando el sujeto no esté mirando de frente a la cámara.

Reconocimiento facial según Chaudhry, S. & Chandra, R. (2017)

El sistema de reconocimiento facial es una aplicación dirigida por ordenador que identifica automáticamente a una persona en una imagen digital. Esto es posible mediante un análisis de las características faciales del sujeto extraídas de la imagen o de un fotograma clave de una fuente de video, y comparándolas con una base de datos. El objetivo de un sistema de reconocimiento facial es, generalmente, el siguiente: dada una imagen de una cara "desconocida", o imagen de test, encontrar una imagen de la misma cara en un conjunto de imágenes "conocidas", o imágenes de entrenamiento.⁴ La gran dificultad añadida es la de conseguir que este proceso se pueda realizar en tiempo real. El sistema identificará las caras presentes en imágenes o videos automáticamente. Puede operar en dos modos:

- Verificación o autenticación de caras: compara una imagen de la cara con otra imagen con la cara de la que queremos saber la identidad. El sistema confirmará o rechazará la identidad de la cara.
- Identificación o reconocimiento de caras: compara la imagen de una cara desconocida con todas las imágenes de caras conocidas que se encuentran en la base de datos para determinar su identidad.

El sistema de Análisis de distancias a puntos característicos es uno de los primeros sistemas de reconocimiento que se basa en la técnica a partir de puntos geométricos de la cara. A partir de la detección de diferentes puntos característicos se crean vectores que contienen datos de distancias entre los mismos. Cuantos más puntos característicos son detectados, mayor número de distancias permiten ser calculadas obteniendo así mejores resultados en el reconocimiento.

⁴ Cfr. Shonal Chaudhry (2017)

Reconocimiento facial según Jain, A. K., Ross, A., & Prabhakar, S (2004)

El reconocimiento de rostros es un método no intrusivo, y las imágenes faciales son probablemente las características biométricas más comunes utilizadas por los humanos para hacer un reconocimiento personal. Las aplicaciones de reconocimiento facial van desde una verificación estática y controlada hasta una identificación de rostro dinámica e incontrolada. en un contexto desordenado Los enfoques más populares para el reconocimiento de rostros se basan ya sea en 1) la ubicación y la forma de los atributos faciales, como los ojos, las cejas, la nariz, los labios y la barbilla, y sus relaciones espaciales, o el análisis general de la imagen de la cara que representa una cara como una combinación ponderada de varias caras canónicas. Si bien el rendimiento de verificación de los sistemas de reconocimiento de rostros que están disponibles en el mercado es razonable, imponen una serie de restricciones sobre cómo se obtienen las imágenes faciales, que a veces requieren un fondo fijo y simple o iluminación especial. Estos sistemas también tienen dificultades para reconocer una cara a partir de imágenes capturadas desde dos vistas drásticamente diferentes y bajo diferentes condiciones de iluminación. Es cuestionable si la cara en sí misma, con más información contextual, es una base suficiente para reconocer a una persona de un gran número de identidades con un nivel extremadamente alto de confianza.⁵ Para que un sistema de reconocimiento facial funcione bien en la práctica, debe automáticamente: 1) detectar si una cara está presente en la imagen adquirida; 2) ubicar la cara si hay una; y 3) reconocer la cara desde un punto de vista general (es decir, desde cualquier pose).

⁵ Cfr. Anil Jain (2004)

CAPÍTULO 5: DESARROLLO DEL PROYECTO

En este capítulo se explica el desarrollo del proyecto bajo los lineamientos de la metodología PMBOK (Project Management Body of Knowledge). El desarrollo se encuentra en fase de ejecución. Adicionalmente, se detalla los entregables del proyecto en sí y aquellos que aportaron valor dentro del mismo.

5.1. METODOLOGÍA APLICADA

El presente proyecto se está usando la metodología PMBOK y CCRA V4. Asimismo, se realiza el estudio de los siguientes puntos: Viabilidad del reconocimiento facial en el sector salud, Análisis Comparativo de las soluciones reconocimiento facial, Arquitectura de la solución.

5.2. VIABILIDAD DE RECONOCIMIENTO FACIAL PARA EL SECTOR SALUD

A continuación, se muestra la investigación que demuestra la viabilidad de reconocimiento facial para el sector salud. Se presenta el estudio realizado, definición del Sector, descripción de las funcionalidades del reconocimiento facial, procesos de machine learning, y el sustento del por qué el sector salud es el apto para la implementación de esta tecnología.

5.2.1. DEFINICIÓN DEL SECTOR SALUD

Salud Según ESSALUD:

Según el seguro social de salud (ESSALUD), el sector se define como la prestación servicios de salud en las regiones del Perú. Bajo las leyes establecidas, ESSALUD tiene por finalidad dar cobertura a los asegurados y sus derechohabientes, a través del otorgamiento de prestaciones de prevención, promoción, recuperación, rehabilitación, prestaciones económicas, y prestaciones sociales que corresponden al régimen contributivo de la Seguridad Social en Salud, así como otros seguros de riesgos humanos.

Sector Salud Según MINSA:

Según el ministerio de salud, el sector brinda salvaguardar, formular, ejecutar y dirigir el sistema general de seguridad social en salud en distritos sectores administrativos en el Perú. Dentro del ministerio se tiene la misión de proteger la dignidad personal del ciudadano integrando salud y condiciendo los lineamientos de políticas sanitarias con los sectores públicos.

Sector Salud Según SUSALUD:

La superintendencia Nacional de Salud (SUSALUD) define el sector como proteger y

defender los derechos de las personas a los servicios de salud en las regiones del Perú. Adicionalmente, para el sector describe la finalidad de supervisar las prestaciones de servicio con calidad y disponibilidad bajo las funciones administrativas, económicas y financieras en el sector.

En conclusión:

Al revisar las definiciones dentro del sector, se concluye que el sector salud ocupa brindar servicios de calidad y disponibilidad en salud; dando prestaciones económicas para la disponibilidad de la población en entidades establecidos.

5.2.2. DESCRIPCIÓN DE LAS FUNCIONALIDADES DE RECONOCIMIENTO FACIAL

Las funciones de reconocimiento facial están divididas en 4 módulos.

Detección de la cara

Este módulo detecta la cara en una imagen procesada. En los videos se realiza seguimiento del rostro en vivo.

Alineación de la cara:

Este módulo realiza transformaciones geométricas para la normalización de tamaño y posiciones. Se debe definir el tamaño de las imágenes y la gama de colores. Además, se realiza ecuaciones de histograma.

Extracción de características:

Realiza información para diferenciar los rostros según las variaciones geométricas.

Reconocimiento:

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

Ilustración 16: Secuencia de y codificación de los puntos biométricos

5.2.3. CASOS DE ÉXITO DE SECTORES QUE IMPLEMENTACIÓN RECONOCIMIENTO FACIAL

El reconocimiento facial ha sido implementado en distintas áreas y sectores en las cuales se centró en temas de seguridad. Para la presente investigación se tomó referencia casos de éxito en el año 2015-2017, con el objetivo de investigar la metodología usada por cada empresa y el servicio utilizado. Se presenta un cuadro en el cual se establece las empresas que implementaron el reconocimiento facial.

Tabla 5: Casos de éxitos que implementaron reconocimiento facial

Entidad	sector	aplicación específica	servicios
Tecsup	Educación	Biometría	IBM Cloud
UBER	Transporte	Biometría	Azure
KIA	automotriz	Control de acceso	AWS
Facebook	Redes Sociales	etiquetar usuario	facebook
Banco Industrial	Bancario	Tarjetas inteligentes	FacePhi
CaliBurger	Comida	Biometría	NeoFace NEC

Fuente: Elaboración Propia

5.3. ANÁLISIS COMPARATIVO DE LAS SOLUCIONES DE RECONOCIMIENTO FACIAL.

Este estudio abarca la comparación de las características entre las diversas herramientas de reconocimiento facial, describiendo cada una de ellas, y que se encuentran en los reportes de investigación de las firmas y empresas más influyentes en la actualidad como: Forrester o Gartner. Este análisis tiene como objetivo obtener el servicio de reconocimiento facial ideal para la implantación en el sector. Finalmente, se concluye que Azure es la herramienta óptima para el uso de identificación de pacientes.

Se realiza el análisis con los servicios de cloud con las empresas de Microsoft, Amazon e IBM.

Bluemix Por IBM:

La plataforma Bluemix de IBM tiene como servicio, en su categoría IA Watson, visual Recognition. El servicio ofrece reconocimiento de objetivos en imágenes para identificar objetos, escenas y caras con los objetivos de ser etiquetados y clasificados mediante algoritmos de machine learning. El proceso del servicio de visual recognition está estructurado de la siguiente manera:

- Preparación de imagen: Input de la imagen para procesar.
- Análisis de imágenes: realiza el análisis para determinar las capacidades.
- Preparación de datos de entrenamiento: prepara el ordenamiento de imágenes positivos o negativos.
- Entrenamiento y creación de nuevos modelos: insertar el entrenamiento de las nuevas imágenes de datos
- Vista de resultados: vista de resultados estadísticos.

Ilustración 17: Proceso del servicio Visual Recognition

El servicio realiza los casos de usos en distintas industrias como:

- **Fabricación**: utilice imágenes de un entorno de fabricación para asegurarse de que los productos se colocan correctamente en una línea de montaje
- **Auditoría visual**: busque el cumplimiento visual o el deterioro en una flota de camiones, aviones o molinos de viento en el campo, entrene modelos personalizados para comprender qué defectos parecen
- **Seguro**: procesa rápidamente las reclamaciones mediante el uso de imágenes para clasificar las reclamaciones en diferentes categorías
- **social**: utilice imágenes de su línea de productos o su logotipo para rastrear el rumor sobre su empresa en las redes sociales
- **Comercio social**: use una imagen de un plato plateado para saber qué restaurante lo sirve y busque opiniones, use una foto de viaje para encontrar sugerencias de vacaciones basadas en experiencias similares.

- Venta minorista: tome una foto de su atuendo favorito para encontrar tiendas con esas prendas en existencia o en venta, use una imagen de viaje para encontrar sugerencias de venta minorista en esa área.

Azure por Microsoft:

La plataforma de Azure de Microsoft tiene como servicio Face API. Proporciona algoritmos faciales avanzados para detectar rostros con sus atributos y el reconocimiento facial. Se enfoca más a la detección biométrica del rostro de las personas para estudiar distintos indicadores. El servicio se centra en ofrecer distintos segmentos:

- Detección de Rostro: Bajo el proceso Face-dect, se detecta hasta 64 rostros en una imagen y determinar el género y edad de la persona.
- Reconocimiento facial: proceso identifica un rostro similar en un grupo de rostros y agrupa rostros ante una función bajo el proceso face-group. Se Identifica a las personas en función de una base de datos y personas detectadas (definida como LargePersonGroup / PersonGroup) que debe crearse con anticipación y puede editarse a lo largo del tiempo.

AWS de Amazon:

La plataforma de AWS de amazon tiene como servicio Amazon Rekognition. Proporciona reconocimiento y análisis facial. Puede detectar, analizar y comparar rostros para una amplia variedad de casos de uso de verificación de usuarios, catalogación, contabilización de personas y seguridad pública. AWS proporciona los siguientes beneficios:

- Detección de objetos: puede identificar miles de objetos al analizar videos. también puede identificar actividades específicas que ocurran en el fotograma.
- Reconocimiento Facial: capacidad de búsqueda precisa y ágil permite identificar una persona en una foto o video mediante el uso de su propio repositorio privado de imágenes faciales.

- **Análisis facial:** Puede analizar los atributos de los rostros que aparecen en imágenes y videos para determinar felicidad, rango de edad, apertura de ojos, lentes, vello facial, etc. En los videos, también es posible medir los cambios en los objetos con el transcurso del tiempo, como la reconstrucción de la cronología de las emociones de un actor.
- **Seguimiento de personas:** es posible seguir personas en un video, aunque sus rostros no estén visibles o aparezcan y desaparezcan de la escena. También puede identificar sus movimientos en el fotograma para determinar.

Los casos de uso más relevante dentro del servicio es la verificación de usuarios:

Ilustración 18: diagrama de verificación de usuario

Comparación entre los servicios:

Forrester:

En el primer trimestre de 2017, la empresa Forrester realizó un informe sobre análisis predictivo y machine learning. La empresa describe la evolución de esta tecnología. Se pronostica una tasa de crecimiento del 15% para el mercado PAML hasta el 2021.

Se evaluó 14 empresas en términos de estrategia, presencia en el mercado y oferta actual. Se visualiza los resultados en el siguiente cuadro:

Ilustración 19: cuadro Forrester

Mediante el cuadro Forrester se analiza la empresa IBM. La SPSS sigue siendo el núcleo de la plataforma de ciencia de datos de IBM, pero IBM también lanzó SystemML de sus inversiones en su Spark Technology Center e introdujo Data Science Experience para codificadores de ciencia de datos.

Microsoft ofrece Microsoft R para los científicos de datos que desean codificar en el lenguaje de programación R soportado por algoritmos ejecutables distribuidos por clúster. También ofrece Azure Machine Learning a los científicos de datos que desean una herramienta de desarrollo visual más tradicional.

Cuadrante mágico de Gartner:

Empresa líder dedicada a la investigación de tecnología en la información del mundo y consultoría. Gartner realiza anualmente un informe donde muestra el Magic Quadrant's Gartner o Cuadrante Mágico de Gartner que es la culminación de la investigación en un mercado específico, que le da una visión de gran angular de las posiciones relativas de los competidores del mercado. En este caso, se muestra en la ilustración 1 el cuadrante mágico de Gartner de Services Platforms. Este magic quadrant de un tratamiento gráfico y un

conjunto uniforme de criterios de evaluación sobre de los sevicios que se ofrecen y donde permite determinar rápidamente los principales proveedores de tecnología que son OpenText, Hyland, Microsoft, Mfiles, IBM, Oracle, SER Group, etc.

Ilustración 20: Cuadrante mágico de Gartner

Benchmarking:

Se realiza el bechmarking con los servicios de AWS, bluemix, Azure y Google. Se presenta un cuadro comparativo sobre los servicios de machine learning que fue presentado por la empresa altexsoft:

CLOUD MACHINE LEARNING SERVICES COMPARISON					
	Amazon ML	Amazon SageMaker*	Azure ML Studio	Google Prediction API	Google ML Engine**
Classification	✓	✓	✓	✓	✓
Regression	✓	✓	✓	✓	✓
Clustering	✗	✓	✓	✗	✓
Anomaly detection	✗	✓	✓	✗	✓
Recommendation	✗	✓	✓	✗	✓
Ranking	✗	✓	✓	✗	✓
Algorithms	unknown	10 built-in + custom available	100+ algorithms and modules	unknown	TensorFlow-based
Frameworks	✗	TensorFlow, MXNet	✗	✗	TensorFlow
Graphical interface	✗	✗	✓	✗	✗
Automation level	high	medium	low	high	low

*Both out-of-the-box features and possible custom-built features are marked as available in Amazon SageMaker

**The features available in TensorFlow are respectively marked as available in Google ML Engine.

Ilustración 21: Comparación de Servicios de Machine Learning según Altexsoft

Esta comparación nos indica que Azure cubre con las funcionalidades aplicadas. Por la comparación añadimos los requisitos que se necesitan en el servicio para la implantación del modelo:

Tabla 6: Benchmarking de reconocimiento Facial

				IBM Watson Visual Recognition API	Microsoft Face API	Amazon Rekognition
Nº	CARACTERÍSTICAS	SUB - CARACTERÍSTICAS	PESO	PUNTAJE		
1	Servicio de reconocimiento facial	Detección de rostros	5	5	5	5
		Reconocimiento facial (Imagen)	5	3	5	5
		Reconocimiento facial (Video)	2	1	3	3
		Profundidad de emocional	2	3	4	4
		Emociones presentes	2	4	4	3
		Año y género	4	3	4	5
		Seguimiento de múltiples rostros	3	5	5	5
		SDK	4	4	4	4
		API	5	5	5	5
		Etnicidad	3	3	3	4
2	Funcionalidad	Adecuación	3	3	4	4
		Exactitud	5	5	5	5
		Interoperabilidad	4	4	4	4
		Seguridad de Acceso	4	4	5	5
3	Fiabilidad	Madurez	5	4	4	5
		Tolerancia a fallos	4	3	3	3
		Capacidad de recuperación	3	3	4	3
4	Usabilidad	Capacidad para ser entendido	3	4	3	4

		Capacidad para ser aprendido	3	5	5	4
		Capacidad para ser operado	4	4	4	3
		Capacidad de atracción	1	3	3	3
5	Eficiencia	Comportamiento temporal	5	4	5	4
		Utilización de recursos	3	4	4	4
6	Mantenibilidad	Capacidad para ser analizado	3	3	3	3
		Capacidad para ser cambiado	2	5	4	3
		Capacidad para ser probado	4	5	5	1
7	Portabilidad	Adaptabilidad	5	5	4	4
		Instalabilidad	3	3	3	3
		Coexistencia	4	5	5	5
		Capacidad para ser reemplazado	2	4	4	4
TOTAL			419	430	428	

Fuente: Elaboración Propia

Se revisa al detalle en el anexo H.

Se concluye bajo los requerimientos que se necesitan el servicio Face API de Azure cumple con las expectativas.

5.4. MODELOS DE REFERENCIA PARA LA IMPLEMENTACIÓN DE UNA SOLUCIÓN PARA LA IDENTIFICACIÓN DE PACIENTES EN EL SECTOR SALUD

Se describe distintos modelos o sistemas de solución para identificar a los pacientes en el sector salud peruana.

5.4.1. MODELO DE VERIFICACIÓN DE IDENTIDAD DEL PACIENTE BASADA EN FUSIÓN DE SEÑAL FISIOLÓGICA

Una de las soluciones que se implementó para la identificación de pacientes es un sistema

de señales fisiológicas comunes (signos vitales) ya recopiladas de los pacientes. La idea es fusionar dos señales fisiológicas electrocardiograma (ECG) con presión arterial (ABP) para identificar a un paciente individual. Las soluciones existentes de identificación / autenticación basadas en señales cardíacas se han probado principalmente en pacientes sanos cuyas señales exhiben ritmo y morfología normativos.

Ilustración 22: Modelo de verificación de identidad del paciente basada en fusión de señal fisiológica

La fusión de múltiples ECG y ABP, en el modelo, permite asegurar la identificación del paciente incluso cuando los pacientes tienen dolencias que afectan sus ritmos cardíacos. Una evaluación mostró que es más del 97% de precisión en la identificación de pacientes con ritmos cardíacos no normativos y morfología con más del 99% de precisión para pacientes cuyos ritmos cardíacos son normativos. Basado en la fusión ECG y ABP, el modelo logra una precisión superior al 97% en la identificación del usuario con el que se despliega el sistema en 3 segundos.

5.4.2. SISTEMA BASADO EN RFID Y AGENTES MÚLTIPLES PARA MEJORAR LA EFICIENCIA EN LA IDENTIFICACIÓN Y EL CONTROL DE LOS PACIENTES

Se propuso un sistema basado en RFID (llamado SIMOPAC) que integra tecnologías de RFID y agentes múltiples en el cuidado de la salud para hacer que la atención de emergencia del paciente sea lo más eficiente y libre de riesgos posible, proporcionando a los médicos tanta información sobre un paciente como lo más rápido posible. Todos los hospitales podrían usar SIMOPAC con su sistema existente para promover la seguridad del paciente y optimizar el flujo de trabajo del hospital. el sistema se usa en la atención de emergencia para identificar a los pacientes y obtener información en tiempo real sobre los datos biométricos de los pacientes, que podrían usarse en diferentes puntos del sistema de salud (laboratorio, médico de familia, etc.).

Ilustración 23: Sistema basado en RFID y agentes múltiples para la identificación y control de pacientes

5.5. MODELO TECNOLÓGICO DE RECONOCIMIENTO FACIAL PARA LA IDENTIFICACIÓN DE PACIENTES EN EL SECTOR SALUD

En esta sección, se presenta el enfoque utilizado para identificar a los pacientes mediante reconocimiento facial. El objetivo es desarrollar un modelo que complete las soluciones de identificación de pacientes de manera confiable y eficiente. La estructura del modelo se divide en 3 fases: entrada, proceso y salida. Bajo el método utilizado, la tecnología se utiliza el aprendizaje automático en servicios en la nube. Se basa en una disciplina en el campo de la inteligencia artificial. Se crean sistemas que desarrollan el aprendizaje automático para identificar patrones complejos de datos requeridos.

5.5.1. DESCRIPCIÓN DEL MODELO

Entrada:

En la fase de entrada, se requieren los datos básicos del paciente de una base de datos existente y una imagen de su rostro. Esta información se encuentra dentro del proceso de admisión de un paciente en el centro médico. La imagen se envía a la fase de proceso por medio de la nube para realizar los análisis cognitivos para la detección de rostros y almacenar en la base de datos. La información del paciente se almacena en la base de datos.

Proceso:

Esta fase se desarrolla en el entorno de la nube. Se divide en 4 subprocesos: detección de rostros, identificación facial, gestión de bases de datos y notificación de mensajes. Bajo la plataforma en la nube PaaS y SaaS, los servicios cognitivos de detección facial e identificación facial se utilizan a través del aprendizaje automático. El servicio de detección facial usa una serie de algoritmos para detectar la cara en una imagen baja en un nivel de predefinición. Luego, el servicio de reconocimiento facial realiza el aprendizaje automático bajo el sistema de red neuronal para interpretar la imagen y detectar a un solo paciente.

a) Detección de la cara:

La imagen cargada en la nube PaaS pasa por el proceso de análisis facial. Su función del

servicio es detectar las caras de una imagen. Realiza diferentes algoritmos biométricos para determinar la característica facial. Para el modelo, solo se necesita la cara del paciente. La selección de la cara requerida se solicita en función de los detectados. Una vez que se selecciona la cara, el servicio transforma la foto en un archivo json y realiza un análisis facial para detectar los atributos de edad y sexo. Una vez que se completa el proceso, la información de la cara se envía al proceso de identificación facial para conocer la cara o identificarla en la base de datos. Si una cara no está identificada en la imagen, el proceso no le permite continuar con el flujo del modelo y se solicita otra imagen.

b) Identificación facial

El proceso recopila información de la cara para ejecutar el servicio de identificación facial en Cloud PaaS. El análisis realiza los algoritmos cognitivos del reconocimiento facial del aprendizaje profundo. El servicio aprende los puntos biométricos, junto con sus atributos, para que el paciente pueda identificarse al buscar rostros. La información aprendida se registra con una ID y se almacena en la base de datos.

Si el paciente necesita ser identificado, el proceso realiza la comparación de las características faciales aprendidas. Al encontrar el mayor porcentaje de coincidencia de rostros, se llama a la ID de la base de datos para obtener la información del paciente. Finalmente, se genera un aprendizaje profundo del rostro que se ha comparado y se genera un nuevo archivo json que se almacena en la base de datos. Esta última función se da para evitar la reducción del porcentaje de autenticidad.

c) Notificación de mensajes

La administración de almacenamiento es responsable de almacenar los archivos del paciente. Guarda los archivos json para comparar el reconocimiento facial. Realice una alimentación proactiva en cada visita al paciente dentro del centro médico. Asigna el acceso en la entrada y salida de la información a las solicitudes solicitadas en el proceso de identificación facial. La distribución de la base de datos se divide en información e imágenes del paciente. Solo la información del paciente se puede desarrollar localmente.

d) Notificación de mensajes

Cuando se identifica al paciente, el proceso de notificación envía un mensaje de texto al número del familiar registrado en la base de datos. El proceso se realiza para la experiencia del usuario en torno al modelo. Si no se identifica al usuario, se le solicita a la Identificación Nacional que identifique al paciente en la base de datos y consulte su número de teléfono para notificar mediante un mensaje de texto el propósito de la atención del paciente en el centro de salud.

Salida:

La fase de salida muestra la identificación del paciente con la información principal. Simultáneamente, se envía una notificación por SMS al teléfono móvil del paciente o familiar con la notificación del intento de asistir al centro médico.

Privacidad y seguridad de datos:

La fase de privacidad y seguridad de datos describe las medidas de seguridad asignadas en el modelo. Asigna la creación de perfiles y roles para la autenticación del modelo. A nivel de servicios carga de datos, se ejecuta

Ilustración 24: Modelo tecnológico de reconocimiento facial para la identificación de pacientes en el sector salud

5.5.2. FASES

5.5.2.1. ANÁLISIS DE LA EMPRESA

para realizar demostrar la validez del modelo, se utilizó como caso de uso la clínica UROGINEC. Se realiza el conocimiento de la situación actual de la empresa, con la finalidad de obtener información clave para indicar si la empresa está apta para la implementación de la solución. Se propone una serie de actividades dadas en la siguiente tabla:

Tabla 7: Situación actual de la clínica

Actividades	Para
Organización de la Empresa	Conocer cómo está organizada la empresa. (organigrama)

Estrategia: Misión y Visión	El conocimiento de sus metas a corto, mediano y largo plazo.
Análisis de la Competencia	Conocer si los competidores directos ya cuentan con sistemas de identificación de pacientes
Infraestructura de TI	Saber los recursos con los que dispone la clínica
Diseño de los Procesos ASIS	Conocer los procesos core de la empresa.
Indicadores de la Empresa	Saber cuáles son los resultados que tiene la empresa.
Análisis Digital	Saber si cuenta con herramientas Digitales. (Facebook, Google Adword, etc)
Canales de Venta	Conocer los canales de venta con la que cuentan en la actualidad.
Análisis Financiero	Saber cuánto es el límite de gasto para implementar un sistema de identificación de pacientes

Fuente: Elaboración Propia

Una vez se tenga la información de la organización, es necesario realizar la evaluación de situación actual de la clínica. Esta evaluación es el resultado de la investigación realizada de los factores de adopción para la implementación de identificación de pacientes.

Tabla 8: Evaluación del entorno de la clínica

Agrupación	Factor	Descripción	Pregunta	Cumple
	Recursos de la	Personal de la empresa que se involucrarán en la administración del	¿Tiene los recursos suficientes para la implementación del	1 - 3

	empresa	sistema	sistema.?	
Organizacional	Infraestructura de Negocio	Procesos de Negocio que se involucrarán con el sistema.	¿La empresa cuenta con procesos que pueden involucrarse con el sistema?	1 - 3
	Educación y conciencia	Educación necesaria para una correcta adopción	¿Los empleados de la organización conocen lo que es un sistema?	1 - 3
	Productos y Servicios	Productos que se involucrarán con el sistema.	¿La empresa cuenta con la cantidad de productos necesarios para un sistema?	1 - 3
	Canales de Venta	Canales de venta con los que cuenta la empresa	¿La empresa cuenta con más de un canal de ventas?	1 - 3
	Soporte del CEO	Interés de parte de la administración de la empresa por el sistema.	¿El comercio electrónico está dentro de los objetivos estratégicos?	1 - 3
	Capacidad Financiera	Recursos financieros destinados a la adopción	¿La empresa cuenta con los recursos necesarios para la implementación?	1 - 3
Entorno	Industria	Rubro de la empresa	¿El rubro se encuentra en crecimiento?	1 - 3
	Competencia	sistema en la competencia	¿La competencia cuenta con soluciones de comercio electrónico?	1 - 3
	Presión de los Compradores / Proveedores	El sistema debe satisfacer las necesidades de estos usuarios	¿Los clientes o proveedores necesitan una solución de sistema por parte de la empresa?	1 - 3
Tecnológico	Infraestructura de TI	Infraestructura que soporta a la solución sistema	¿La empresa cuenta con la infraestructura de TI necesaria para la implementación?	1 - 3
	Skill en IT y	Experiencia necesaria para la adopción al	¿Los empleados de la empresa tienen la experiencia necesaria	1 - 3

	experiencia	sistema	para utilizar el sistema?	
--	-------------	---------	---------------------------	--

Fuente: Elaboración Propia

Se valora en un rango de uno a tres el nivel de cumplimiento de los factores de adopción para implementar el sistema de identificación de pacientes. Los valores que se localizan en uno significan que la empresa no cuenta con el factor de adopción para la implementación. Si se localiza en dos significa que la empresa cuenta parcialmente; por último, se localiza en tres si cuenta con las condiciones del factor. Para que la empresa esté apta para la implementación del sistema, el puntaje total de los factores debe ser mayor a la mitad (18).

5.5.2.2. MODELADO DE NEGOCIO

Es la siguiente Fase a partir de si la clínica está apta para implementar la solución, el modelado de negocio es mejorar lo que brinda la clínica directamente a sus pacientes. En esta fase se debe tener criterio como:

- **Evaluación de Plataformas.** Para la evaluación de la mejor plataforma e-para la clínica, se debe realizar los criterios principales de selección; tales como: Precios de las Plataformas de servicios cognitivos, Descripción General de las Plataformas, Requerimientos Técnicos de las Plataformas y Evaluación de Funcionalidades de sistema de reconocimiento facial vs Plataformas.
- **Transformación del Negocio.** Se refiere a realizar cambios en relación de lo que tiene la empresa respecto al negocio. Todo ello, conlleva a repotenciar el área que va a ser impactada con la ayuda de entregables como: Diseño de los procesos ToBe, Infraestructura de TI ToBe y Diagrama de Casos de Uso. Con la finalidad de asignar funciones y cargos que permitan a la empresa adaptarse a la solución.

5.5.2.3. IMPLEMENTACIÓN

En esta fase posibilita la implementación del sistema en la clínica, para ello debe tener en cuenta aspectos como desarrollo de la implementación y las pruebas que se realizan antes de

la puesta en marcha.

Para el desarrollo de la implementación, se propone identificar actividades como: Alojamiento de la Plataforma Cloud, desarrollo de la aplicación, Asignación de Usuarios, Diseño de la aplicación e Instalación de la aplicación. Todo ello, permite que el sistema tenga las funcionalidades necesarias para su puesta en marcha.

Antes de la puesta en marcha de la plataforma, es necesario realizar pruebas a la plataforma tales como las que se muestran a continuación:

- **Pruebas Funcionales.** Se refiere analizar que la aplicación cumpla con todas las especificaciones requeridas correctamente.
- **Pruebas de Desempeño.** Se refiere analizar el tiempo de respuesta para las transacciones o las funcionalidades de la aplicación.
- **Pruebas de Stress.** Se refiere analizar si la aplicación funciona apropiadamente y sin errores.

Ilustración 25: Flujo de identificación de pacientes por aplicativo desarrollado

5.5.2.4. RESULTADOS

Para el recojo de resultados luego de la implementación de la solución, se debe identificar indicadores de éxito como: Indicadores de posibles suplantaciones, Satisfacción de Cliente e indicadores de costo sanitario. Por último, en base a los resultados de la solución, es necesario brindar a la clínica una retroalimentación. Además, de entregarle un documento de posibles mejoras a futuro de la solución, que depende si la empresa desea mejorar la solución a corto, mediano o largo plazo.

CAPÍTULO 6: RESULTADOS DEL PROYECTO

En este capítulo se explica los resultados del análisis de la validación del modelo tecnológico de reconocimiento facial para la identificación de pacientes en el sector salud. Los resultados se basaron en la implementación en una clínica privada.

6.1. VALIDACIÓN DEL MODELO

6.1.1. COMPARACIÓN CON LA LITERATURA

A partir de la investigación se encontraron distintas metodologías y formas del uso de reconocimiento facial en el sector salud. Se compararon los resultados de los de la identificación de pacientes de manera eficientes en las distintas tecnologías aplicadas. Esta comparación permite la validación del modelo. La literatura a comparar con sus resultados fueron los siguientes:

Tabla 9: Distintos sistemas para la identificación de pacientes

N°	Título
1	Evaluation of electrocardiogram for biometric authentication
2	EGC Authentication for mobile devices
3	Patient Identity Verification based on Physiological Signal Fusion
4	An RFID and Multi-agent Based System for Improving Efficiency in Patient Identification and Monitoring

Fuente: Elaboración Propia

Estas literaturas fueron escogidas por identificar a los pacientes en distintas instituciones médicas. Evaluation of electrocardiogram for biometric authentication describe un sistema que identifica el paciente bajo un electrocardiograma. El sistema lee los resultados que brinda el electrocardiograma y bajo el algoritmo desarrollado determina el paciente con los ritmos cardiacos registrados.

EGC Authentication for mobile devices desarrolla una app que lee los resultados de un electrocardiograma. Al leer los resultados, aprende de ello para determinar a la identidad del paciente. La identificación del paciente aparece en la aplicación.

Patient Identity Verification based on Physiological Signal Fusion desarrolla un Sistema para detectar en señales electrocardiogramas y presión arterial para identificar al paciente. Esta solución permite autenticar y detectar a los pacientes dentro de la institución médica. Bajo el enfoque que tienen para identificar a los pacientes es el tiempo reducido en 3 segundos de aproximación.

An RFID and Multi-agent Based System for Improving Efficiency in Patient Identification and Monitoring desarrolla una arquitectura implementando un Sistema de RFID para contralar e identificar a los pacientes. Los pacientes se les asigna un brazalete con tecnología RFID para el monitoreo. La tecnología se utilizó para el área de emergencia para obtener información en tiempo real para utilizar en distintos sistemas de salud.

6.1.2. JUICIO DE EXPERTOS

Para la validación adicional al modelo tecnológico se realizó una validación por juicio de expertos. Para este caso se contactó al experto en desarrollo en PaaS a Roberto Zubiaur, quien ocupa el puesto de gerente en el área de Plataforma Windows en la empresa Falabella. También, se contactó con el experto Henry Mendoza catedrático en las carreras de Ingeniería de Software e Ingeniería de Computación y Sistemas de la universidad Privada Antenor Orrego.

Se realizó una evaluación sobre los criterios y fases que contiene el modelo. Esta evaluación se realizó de la siguiente manera:

Tabla 10: Evaluación de criterios

Nº	Criterios	Puntuación
1	Seguridad	
2	Precisión	
3	Adaptabilidad	
4	Administrable	

5	Escalabilidad
6	Funcionabilidad
7	Fiabilidad
8	Mantenibilidad
9	Portabilidad
Total	

Fuente: Elaboración Propia

Colocando una puntuación de 0 a 9 siendo el 9 como el máximo puntaje en el que cumple satisfactoriamente. La puntuación fue de 92.24% de la media de consideraciones aprobada ante la evaluación de los dos expertos.

6.2. CASO DE USO

6.2.1. PRESENTACIÓN DE EMPRESA

Para validar el modelo tecnológico, se implementó en la clínica UROGINEC. Se dedica a la especialización de servicios en urología y ginecología obstetricia. La clínica cuenta con ingresos mensuales de S/. 65,000.00 aproximadamente. Tiene más de 10 años de funcionamiento.

Ilustración 26: Logo de la clínica Uroginec

La clínica cuenta con un problema de problemas en registros indebidos provocando quejas en los pacientes. Además, por parte del seguro se obliga a pagar por los servicios brindados, reduciendo las ganancias en un 12%. La clínica tiene en sospechas de posibles suplantaciones de identidad por parte de los pacientes.

6.2.2. IMPLEMENTACIÓN

Para implementación se tomó por obligación que la información del paciente esté de manera local. El dataset de las imágenes se desarrolló en la nube. Para esto se utilizó el servidor de la clínica. Para este caso se agregó tablas dentro de la base de datos para la integración y consultas de los pacientes. Para la estructura de la nube, se crea una cuenta en Azure para el servicio de reconocimiento facial. El uso del servicio genera un dataset para el almacenamiento de las imágenes.

Ilustración 27: Servicio de reconocimiento facial en Azure

El API del servicio cloud de Azure será integrado a la aplicación móvil. Luego, la aplicación se ejecutará dentro del entorno de la clínica. Para la primera fase, se utilizó en el área de admisión.

Ilustración 28: Decodificación de la aplicación

Ilustración 29: Inicio de sesión de la aplicación

Se puede ver al detalle la instalación en el anexo J.

6.2.3. RESULTADOS

Al mencionar los sistemas de las literaturas mencionadas, se describe los resultados de cada uno. Para detallar los resultados, evidencia un resume en la siguiente tabla de cada literatura. Bajo los resultados medidos comparamos los resultados medidos en el modelo tecnológico.

Tabla 11: Resultados de las métricas de los sistemas según su literatura

Nº	Exactitud	Tasa de falsos positivos	Tiempo de entrenamiento	Tiempo de identificación	Satisfacción del cliente
1	82%	7%	30 segundos	30 segundos	No medido
2	84.93%	1.29%	30 segundos	4 segundos	No medido
3	95.36%	4.49%	20 minutos	3 segundos	No medido
4	87.2%	5.23%	No entrena	No entrena	86.2%

Fuente: Elaboración Propia

Tabla 12: Resultados del modelo tecnológico de reconocimiento facial

Nº	Exactitud	Tasa de falsos positivos	Tiempo de entrenamiento	Tiempo de identificación	Satisfacción del cliente
M5	95.82%	4.18%	7 segundos	2.75 segundos	95%

Fuente: Elaboración Propia

Se concluye que el modelo soporte las mediciones solicitadas para la identificación de pacientes en la clínica.

6.2.4. BENEFICIO

Al implementar el modelo, la clínica logró que los pacientes se identifiquen de manera eficiente y segura. Se realizó una comparación sobre las posibles suplantaciones dentro del entorno de la clínica. Se redujo un 10% al igual que la cantidad de quejas de malos registros.

Bajo este escenario se estimó un cuadro de retorno de inversión por el desarrollo e implementación del modelo. Se estima que la recuperación de las ganancias registradas como pérdida se recupera en un plazo de 12 meses.

Gastos de servicio					
	Cantidad	Precio unitario	Precio Mensual (S/.)	Costo anual	
1. Implementación de la herramienta					
precios de servicio					
Presuntos pacientes suplantados	5	S/ 25.00	S/ 125.00	S/ 1,500.00	
Venta de fármacos	14	S/ 3.00	S/ 42.00	S/ 504.00	
Cirugías	2	S/ 3,600.00	S/ 7,200.00	S/ 86,400.00	
Total			S/ 7,367.00	S/ 88,404.00	

Retorno de Inversión	
Inversión	S/69,607.50
Ingreso Neto por la inversión	S/ 7,367.00
ROI	10.58%

Total de meses a recuperar	9.44855436
----------------------------	------------

Ilustración 30: Cuadro de retorno de Inversión

6.2.5. PLAN DE CONTINUIDAD

SLA

Definición

El SLA (Service Level Agreement) es un acuerdo entre un proveedor y el cliente quien va a consumir el servicio. El acuerdo tiene como objetivo fijar el nivel acordado de la calidad de la entrega del servicio. Esta entrega debe cubrir temas como el tiempo de respuesta,

disponibilidad horaria, documentación disponible o personal asignado al servicio. Además, realiza un punto de referencia para el proceso de mejora continua.

Ilustración 31: Acuerdos entre cliente y proveedor

SLA en Azure

SLA para servicios cognitivos:

Este es un acuerdo a nivel de servicios de Microsoft Online Services. Se aplica a los Servicios en línea de Microsoft detallados en este documento (un "Servicio" o los "Servicios"), pero no se aplica a los servicios de marca por separado disponibles con o conectados a los Servicios o a cualquier software local que sea parte de cualquier Servicio.

Intentos de transacciones totales:

Cantidad total de solicitudes API autenticadas por el Cliente durante un mes de facturación para una API de Servicios Cognitivos dada. Los intentos totales de transacción no incluyen solicitudes API que devuelven un código de error que se repiten continuamente dentro de una ventana de cinco minutos después de que se recibe el primer código de error.

Transacciones Fallidas:

Conjunto de todas las solicitudes a la API de Servicios Cognitivos dentro de Intentos de Transacción Total que devuelven un Código de Error. Los intentos fallidos de transacción no incluyen solicitudes API que devuelven un código de error que se repiten continuamente

dentro de una ventana de cinco minutos después de que se recibe el primer código de error. Se realiza el cálculo de tiempo de actividad mensual en la siguiente fórmula:

Tiempo de Actividad Mensual

$$= \frac{\text{Total de Intentos de Transacción} - \text{Transacciones Fallidas}}{\text{Total de Intentos de Transacción}} \times 100$$

Ilustración 32: Formula para la disponibilidad operativa en transacciones

Al realizar los cálculos, se declara que el servicio garantiza la disponibilidad del servicio al menos es 99.9% mensual. En el caso que se incumpla con este acuerdo, se establece brindar un porcentaje del crédito del monto facturado como se muestra en la siguiente tabla:

Tabla 13: Porcentajes de Tiempo

PORCENTAJE DE TIEMPO DE ACTIVIDAD MENSUAL	CRÉDITO DE SERVICIO
<99.9%	10%
<99%	25%

Fuente: Microsoft Azure

SOPORTE TÉCNICO

Soporte en la aplicación

Para realizar una mejora continua se desarrolla un soporte de la aplicación móvil para ejecutar una mejora continua.

Actualización de la aplicación:

Se estima actualizaciones trimestrales para dar mejoras de la aplicación. Bajo el acuerdo se estima mejorar indicadores de usabilidad, funcionabilidad, desempeño e interoperabilidad.

Servicio de soporte:

Bajo la gestión de servicio de TI se asigna el servicio de soporte para ejecutar consultas o incidentes no previstos ante la aplicación. Se responderá todos los reclamos y consultas que tenga al cliente con respecto a la aplicación. Los objetivos específicos para el presente de son detallados a continuación:

- Permitir identificar planes de acción a contingencias.
- Permitir identificar responsables frente a contingencia.
- Permitir identificar acciones para la ejecución del sistema.
- Garantizar la operabilidad del software de manera efectiva.

Para la ejecución de soporte se emplea el modelo de ITIL para una óptima gestión. Para ello se emplea los niveles para la elaboración de buenas prácticas.

Ilustración 33: Mejora Continua del Servicio

DRP

definición

El DRP (Disaster Recovery Plan) es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que el negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos sin ser interrumpidos. Esto también debería incluir proyectos para enfrentarse a la pérdida inesperada o repentina de personal clave con el propósito de la protección de datos. Los escenarios que puede sufrir un negocio son los siguientes:

- Catástrofes.
- Fuego.
- Fallos en el suministro eléctrico.
- Ataques terroristas.
- Interrupciones organizadas o deliberadas.
- Sistema y/o fallos del equipo.
- Error humano.
- Virus, amenazas y ataques informáticos.
- Cuestiones legales.
- Huelgas de empleados.
- Conmoción social o disturbios.

DRP en Azure

Site recovery de azure se enfoca en reducir costos de infraestructura locales para hacer negocios durante las interrupciones. Elimina los costos de centros de datos totales y configurar la recuperación ante desastres entre regiones de Azure. Puede evaluar previamente la red, el almacenamiento y los recursos de procesos necesarios para replicar las aplicaciones desde las instalaciones locales en Azure y pagar solo los recursos de procesos y almacenamiento necesarios para ejecutar las aplicaciones en Azure durante las interrupciones.

Azure Site Recovery cuenta con un respaldo de un Acuerdo de Nivel de Servicio del 99,9% y soporte técnico ininterrumpido para que su empresa funcione sin problemas. Con el objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación (RTO) mejores en su clase.

En el caso que se presente una incidencia crítica en el servicio de Azure se plantea la migración al servicio de AWS. Para ello se plantea la solución de la multi-Cloud.

Ilustración 34: Servicio Cloud DRaaS

certificaciones en azure

La Certificación CSA STAR involucre una rigurosa asesoría de terceros de la postura de seguridad de un proveedor de nube que combina la certificación ISO 27001 con criterios especificados en CSA Cloud Controls Matrix. Azure mantiene el Gold Award más alto posible por la madurez de su capacidad de evaluación de la Certificación CSA STAR, y como se mencionó con anterioridad, ahora está disponible en la nube de Azure Government.

Azure cuenta con los siguientes certificados:

Tabla 14: Certificaciones e ISO en Azure

Certification	Azure	Azure Government
CSA STAR Certification	✓	✓ (new)
ISO 27001:2013	✓	✓ (new)
ISO 27017:2015	✓	✓ (new)
ISO 27018:2014	✓	✓ (new)
ISO 20000-1:2011	✓ (new)	✓ (new)
ISO 22301:2012	✓	✓
ISO 9001:2015	✓	

Fuente: Microsoft Azure

Back ups

definición

Los backups son copias de archivos de datos digitales para resguardar la información con el

fin de disponer de un medio para recuperarlos en caso de su pérdida.

Ejecución en el proyecto

Para establecer una garantía de la continuidad del proyecto. Se realizan políticas de respaldo para evitar la pérdida de la información:

- Se ejecutan backups de la data set de manera automática por cada fin de semana.
- Se habilita la opción de tail-log para los backups para evitar la pérdida de trabajo y para mantener intacta la cadena de registro.
- Se ejecuta la notificación del administrador de TI ante las copias de seguridad realizados.
- Los respaldos pueden ser destruidos al pasar un periodo de 5 años desde su creación.

CAPÍTULO 7: GESTIÓN DEL PROYECTO

En este capítulo se explica a detalle la gestión del proyecto bajo los lineamientos de la metodología PMBOK. Se describen los planes de gestión, matrices, entre otros documentos necesarios para el desarrollo del proyecto.

7.1 PRODUCTO FINAL

Para el presente proyecto se establecieron determinados entregables, los cuales se listan a continuación.

- Modelo tecnológico como apoyo a la identificación de pacientes en el sector de salud en el Perú
- Plantilla de Levantamiento de Información de las Cargas de Trabajo
- Plantilla de Requerimientos del Cliente
- Plantilla de Benchmarking
- Plantilla de Estudio de Viabilidad

El producto final del proyecto es el modelo tecnológico como apoyo a la identificación de pacientes en el sector de salud en el Perú, en el cual será evaluado por juicio de expertos.

.

7.2 REGISTRO DE INTERESADOS

En este documento se presenta la información de todos los interesados, así como su influencia e impacto en el desarrollo del proyecto. A continuación, se presenta el registro de interesados.

Tabla 15: Registro de Interesados

Nombres y Apellidos	Organización	Cargo	Información del contacto	Requerimientos sobre el Producto	Influencia					Influencia sobre el proyecto	Impacto el proyecto	Tipo de interés
					I	P	E	S	C			
Diego La Madrid Arroyo	IT Research	Jefe de Proyecto	U201012614@upc.edu.pe	Analizar, ejecutar y supervisar el desarrollo del proyecto con el fin de cumplir los objetivos en las fechas indicadas.	☒	☒	☒	☐	☒	Favorable	Alto	Conseguir toda la información requerida para el desarrollo exitoso del proyecto.

Martín Barriga Rivera	IT Research	Jefe de proyecto	201211625@upc.edu.pe	Analizar, ejecutar y supervisar el desarrollo del proyecto con el fin de cumplir los objetivos en las fechas indicadas.	☒	☒	☒	☒	☒	Favorable	Alto	Conseguir toda la información requerida para el desarrollo exitoso del proyecto.
Rosario Villalta Jimmy Armas Pedro Shiguihara Luis Vives Garnique	UPC	Comité	<u>rosario.villalta@upc.edu.pe</u> <u>jimmy.armas@upc.edu.pe</u> <u>pedro.shiguihara@upc.edu.pe</u> <u>Luis.vives@upc.edu.pe</u>	Evaluar el proyecto bajo los estándares establecidos de la EISC de la UPC	☒	☐	☐	☒	☐	Favorable	Alto	Formar profesionales que cumplan los Students Outcomes por el cual se rige la EISC

Luis Canaval	IT Research	Profesor Gerente	luis.canaval@upc.edu.pe	Brindar apoyo y asesoría durante el desarrollo del proyecto	☒	☒	☒	☒	☒	Favorable	Regular	Culminación de todos los proyectos pertenecientes a la empresa virtual IT Research
Juan Manuel Cuya	UPC	Profesor Cliente	pcsijcuy@upc.edu.pe	Brindar apoyo y asesoría durante el desarrollo del proyecto	☒	☐	☐	☒	☒	Favorable	Alto	Solución de dudas y asesoramiento durante el desarrollo del proyecto
Alfredo Barrientos	Empresas Virtuales	Gerente general	pcsieher@upc.edu.pe	Evaluar el proyecto, bajo los estándares establecidos de la EISC de la UPC	☒	☐	☐	☒	☒	Favorable	Regular	Gestión de los proyectos de las empresas virtuales

Influencia I: Inicio; P: Planificación; E: Ejecución; S: Supervisión y Control; C: Cierre

7.3 MATRIZ DE TRAZABILIDAD DE REQUERIMIENTOS

A continuación, se muestra un análisis de la matriz de trazabilidad de requerimientos, esta matriz vincula los requerimientos del proyecto con los objetivos y entregables a desarrollar.

Tabla 16: Matriz de Trazabilidad de Requerimientos

ID	Requerimiento	Justificación	Prioridad/ Categoría	Propósitos u Objetivos del proyecto	Código EDT	Método de Revisión	Verificación de Alcance / Validación	Estado Actual	Fecha
RQ01	Se requiere analizar el proceso de atención de pacientes y documentos registrados dentro del proceso	Es necesario entender cómo funciona el proceso de atención.	Alta	OE1: Analizar la cobertura disponible, servicios cognitivos de reconocimiento facial y procesos de atención en el sector salud.		Presencial	Cumplido	Cerrado	24/10/2017
RQ02	Se requiere diseñar un modelo de reconocimiento	El modelo permite un conjunto de pasos y buenas	Alta	OE2: Diseñar un modelo tecnológico para identificar y notificar la atención		Presencial	Cumplido	Cerrado	24/10/2017

	facial para identificar a los pacientes.	prácticas para que cualquier organización identificar a las personas después de un evento		de los pacientes en el sector salud.					
RQ03	Se requiere implementar el diseño para realizar la validación	El modelo debe ser validado para garantizar que funciona correctamente	Alta	<p>OE3: Validar el funcionamiento del modelo tecnológico para identificar y notificar la atención de los pacientes en el sector salud.</p> <p>OE4: Elaborar un plan de continuidad acorde al modelo tecnológico validado para una alta disponibilidad y usabilidad.</p>		Presencial	Cumplido	Cerrado	24/10/2017

Fuente: Elaboración Propia

7.4 MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

A continuación, se presenta la matriz de asignación de responsabilidades de todos los involucrados del proyecto, estas responsabilidades son designadas en función al entregable respectivo.

Función que realiza el rol en el entregable:

R (Es el responsable del entregable), **C** (Coordina actividades del entregable), **P** (Participa en la construcción/elaboración del entregable), **A** (Aprueba entregable), **V** (Participa en el control de calidad del entregable), **F** (El entregable requiere su firma).

Tabla 17:Matriz de asignación de Responsabilidades

Código EDT	Entregable	Jefe Proyecto	de	Comité de Proyectos	Profesor Gerente	Profesor Cliente	Recursos de IT Service
1.1	Inicio						
1.1.1	Project Charter	R		A	A,C,F,V	A,C,F,V	V
1.2	Planificación						
1.2.1	Cronograma	R		A	A,C,F	V	V

1.2.2	Diccionario EDT	R	A	A,C,F	V	V
1.2.3	Plan de gestión del alcance	R	A	A,C,F	V	V
1.2.4	Plan de gestión de RRHH	R	A	A,C,F	V	V
1.2.5	Plan de gestión de comunicaciones	R	A	A,C,F	V	V
1.2.6	Registro de interesados	R	A	A,C,F	V	V
1.2.7	Plan de gestión de riesgo	R	A	A,C,F	V	V
1.2.8	Descripción de roles y responsabilidades	R	A	A,C,F	V	V
1.2.9	Plan de gestión	R	A	A,C,F	V	V

	del cronograma					
1.2.10	Plan de gestión de calidad	R	A	A,C,F	V	V
1.2.11	Matriz RAM	R	A	A,C,F	V	V
1.2.12	Matriz de trazabilidad de requerimientos	R	A	A,C,F	V	V
1.2.13	Matriz de riesgos	R	A	A,C,F	V	V
1.2.14	Matriz de comunicaciones	R	A	A,C,F	V	V
1.3	Análisis y diseño					
1.3.1	Procesos de negocio	R	A	A,C,F	V	V
1.3.2	Driver e Negocio	R	A	A,C,F	V	V

1.3.3	Benchmarking	R	A	A,C,F	V	V
1.3.4	Client Conversation Plan	R	A	A,C,F	V	V
1.3.5	Entorno actual de TI	R	A	A,C,F	V	V
1.3.6	Requerimientos No Funcionales	R	A	A,C,F	V	V
1.3.7	Visión general del proyecto	R	A	A,C,F	V	V
1.4	Implementación					
1.4.1	Decisiones de la arquitectura	R	A	A,C,F	V	V
1.4.2	Modelo Operacional	R	A	A,C,F	V	V
1.4.3	Roadmap	R	A	A,C,F	V	V

1.4.4	Pruebas de aceptación	R	A	A,C,F	V	V
1.5	Cierre	R	A	A,C,F	V	V
1.5.1	Memoria del proyecto	R	A	A,C,F	V	V
1.5.2	Paper	R	A	A,C,F	V	V
1.5.3	Plan de continuidad	R	A	A,C,F	V	V

Fuente: Elaboración Propia

7.5 PLAN DE GESTIÓN DE CALIDAD

Se estableció un Plan de Gestión de Calidad para asegurar la calidad del proyecto durante todas sus fases. A continuación, se detallan los puntos descritos en el plan.

7.5.1 ROLES Y RESPONSABILIDADES

Comité de Proyectos

- Aprobar proyectos profesionales
- Evaluar el avance del proyecto
- Decidir continuidad de proyectos

Cliente

- Evaluar y dar seguimiento a los avances del proyecto
- Aprobar los resultados del proyecto
- Asesorar a los jefes de proyecto

Gerente Profesor

- Dar seguimiento a los proyectos de la empresa
- Facilitar comunicación entre las empresas virtuales involucradas
- Aprobar los documentos de gestión

Jefe de Proyecto

- Gestionar el proyecto
- Gestionar los recursos
- Definir el alcance del proyecto
- Coordinar con las autoridades involucradas en el proyecto

7.5.2 PROCEDIMIENTOS

1. Procedimiento para la Planificación de la Calidad

- Definir aquellos entregables que deberán pasar por el control de calidad, los responsables de este control y como se realizara dicho proceso.

- Definir aquellos certificados con los que debe contar el proyecto para validar que ha pasado por un proceso de control de calidad.
- Definir los recursos necesarios para las pruebas de control de calidad.
- Definir las fechas en el cronograma de cuando se realizarán estas pruebas de calidad.

2. Procedimiento para Aseguramiento de la Calidad

- Se realiza un monitoreo semanal de las fechas establecidas en el cronograma para asegurar el cumplimiento de las actividades.
- Asegurar la asignación de recursos de la empresa virtual QS para el aseguramiento de la calidad de los entregables.
- Evaluar el impacto de algún cambio dentro del proyecto (alcance, objetivos, tiempos, etc.) con respecto a la calidad.

3. Procedimiento para el Control de la Calidad

- El control de calidad se inicia revisando los entregables y la matriz de incidencias encontradas por el Analista de QS.
- Se analizan las mejoras y acciones correctivas para los entregables del proyecto.

7.6 PLAN DE GESTIÓN DE RIESGOS

A continuación, se presenta un cuadro resumen de los riesgos establecidos para el proyecto y su análisis en relación a la probabilidad e impacto en el desarrollo del proyecto.

Tabla 18: Gestión de Riesgos

Identificación					Análisis			
Cód. Riesgo	Fecha de registro	Categoría - Origen	Descripción del Riesgo	Disparador	Probabilidad	Impacto (HH)	Impacto	Exp al Riesgo (Horas)
R001	24/10/2017	Ext - Proveedor	No contar con una señal de internet necesaria para la implementación y validación del proyecto	Incapacidad de enviar la foto tomada por la app	70%-Alta	20	4 Alta	14.00
R002	25/10/2017	Ext - Usuarios	No contar con espacio en la nube a tiempo	Incapacidad de usar el sistema por no contar con espacio en la nube	70%-Alta	20	4 Alta	14.00
R003	27/10/2017	Int - El proyecto	No contar con la aprobación del cliente en	Rechazo de algún entregable	30% Baja	20	4 Alta	6.00

			algún entregable	por parte del cliente				
R004	28/10/2017	Int - Equipo de trabajo	Estimación errónea de tiempo	Retraso en alguna actividad	50% Media	20	4 Alta	10.00
R005	29/10/2017	Ext - Usuarios	Cambios en el calendario del Comité de Proyectos.	Informe de cambio de fechas por parte del comité de proyectos	10% Muy baja	20	4 Alta	2.00
R006	30/10/2017	Ext - Usuarios	Modificación del alcance por el Comité de Proyectos.	Cambio de alcance por el comité	30% Baja	20	4 Alta	6.00

Fuente: Elaboración Propia

El siguiente cuadro representa las estrategias de respuesta y monitoreo de los riesgos antes presentados.

Tabla 19: Estrategias de Respuesta

Identificación		Estrategia de respuesta						Monitoreo	
Cód. Riesgo	Tipo de Estrategia	Descripción de la estrategia planteada	Rol responsable	Nombre Responsable	Acciones realizadas	Situación de la estrategia	Plan de Contingencia	Estado	Fecha de cambio de estado
R001	Mitigar	Ubicaciones de zonas con mejor cobertura de internet.	Jefe	Diego La Madrid / Martín Barriga	Se informa que el modelo no se llega a validar	No iniciado	Los stakeholders aceptaran el modelo sin la validación	No Incurrido	N/A
R002	Mitigar	Solicitar ampliación de espacio	Jefe	Diego La Madrid / Martín Barriga	Crear una cuenta gratuita de prueba	No iniciado	Se hará uso de una cuenta de prueba de estudiante para la validación, y solo se usará hasta el límite de la misma (sin incurrir en gastos adicionales).	No Incurrido	N/A
R003	Mitigar	Coordinar reuniones periódicas con el cliente a fin de evaluar el avance.	Jefe	Diego La Madrid / Martín Barriga	Proponer nueva fecha de entrega	No iniciado	El equipo propondrá una nueva fecha de entrega para la corrección. Serán horas de trabajo adicionales que no comprometan el desarrollo continuo.	No Incurrido	N/A

R004	Mitigar	Realizar seguimiento constante al cronograma a fin de realizar cambios necesarios.	Jefe	Diego La Madrid / Martín Barriga	Informar el retraso al cliente	No iniciado	El equipo informa sobre el retraso de un entregable en las reuniones para reorganizar los siguientes y no cometer el mismo error.	No Incurrido	N/A
R005	Mitigar	Coordinar con el gerente profesor para tomar las medidas necesarias si en caso perjudique de manera directa a nuestro proyecto.	Jefe	Diego La Madrid / Martín Barriga	Coordinar con el gerente profesor	No iniciado	Coordinar con el gerente profesor para tomar las medidas necesarias si en caso perjudique de manera directa a nuestro proyecto.	No Incurrido	N/A
R006	Mitigar	Modificar todos los documentos de gestión y la aprobación del gerente profesor.	Jefe	Diego La Madrid / Martín Barriga	Actualizar los documentos correspondientes	No iniciado	Modificar todos los documentos de gestión y la aprobación del gerente profesor.	No Incurrido	N/A

Fuente: Elaboración Propia

CONCLUSIONES

- Se desarrolló un análisis de los servicios cognitivos de reconocimiento facial en la nube y procesos de atención en el sector salud en el cual permitió cumplir con el objetivo 1.
- Bajo el análisis desarrollado se identificó a Azure como el servicio de reconocimiento facial adecuado por factores de eficiencia, usabilidad, SLAs, seguridad y certificaciones ISO.
- Se diseñó un modelo tecnológico para la identificación y notificación de la atención de los pacientes en base al método CCRA V4: Cloud Computing Reference Architecture, lo cual permitió cumplir con el objetivo 2.
- Se validó el funcionamiento del modelo tecnológico en una clínica en el proceso de atención, lo cual permitió cumplir el objetivo 3.
- Se elaboró un plan de continuidad acorde al modelo tecnológico validado para una alta disponibilidad y usabilidad, lo cual permitió cumplir con el objetivo 4.
- Se convalidó el funcionamiento de la aplicación para la ejecución de pruebas de concepto. Lo cual fue certificado por IT Services.

RECOMENDACIONES

- Para el proyecto se recomienda establecer un baseline para el costo del uso del servicio de la nube. Debido a que es más factible el control por el uso del servicio sin evitar salir del consumo diario.
- Se recomienda investigar herramientas adicionales en las cuales se pueda adaptar al modelo para evitar incompatibilidad en la integración con los sistemas establecidos en las empresas.
- Se recomienda contar con herramientas alternativas de servicios cognitivos en caso de que sea necesario, debido a que se puede dar el caso que algunas políticas de estas cambien e impacten negativamente al proyecto.

- Se recomienda colocar “AccessPoint” en puntos estratégicos para la estabilidad y cobertura de conexión a internet. De tal forma, no disminuye la comunicación de redes dentro de la empresa y la información no se perderá.
- Por último, se recomienda generar estrategias de continuidad no sólo para la empresa, sino también para el modelo tecnológico.

BIBLIOGRAFÍA

Chaudhry, S., & Chandra, R. (2017). Face detection and recognition in an unconstrained environment for mobile visual assistive system. *Applied Soft Computing*, 53, 168-180.

CIO Perú (2014) ¿Es ya el momento del reconocimiento facial? Recuperado de <https://cioperu.pe/articulo/15865/es-ya-el-momento-del-reconocimiento-facial/>

We live SSecurity (2015) ¿Cómo funciona la tecnología de reconocimiento facial? Recuperado de <https://www.welivesecurity.com/la-es/2015/08/27/tecnologia-de-reconocimiento-facial/>

Forrester (2018) Predictive Analytics And Machine Learning Solutions. Recuperado de <https://www.forrester.com/report/Now+Tech+Predictive+Analytics+And+Machine+Learning+Solutions+Q2+2018/-/E-RES141392>

Bost, R., Popa, R. A., Tu, S., & Goldwasser, S. (2015, February). Machine learning classification over encrypted data. In *NDSS* (Vol. 4324, p. 4325).

Gartner (2018). Neural Net or Neural Network. Recuperado de <https://blogs.gartner.com/it-glossary/neural-net-or-neural-network/>

Ravi, D., Wong, C., Deligianni, F., Berthelot, M., Andreu-Perez, J., Lo, B., & Yang, G. Z. (2017). Deep learning for health informatics. *IEEE journal of biomedical and health informatics*, 21(1), 4-21.

Wang, P., Lin, W. H., Chao, K. M., & Lo, C. C. (2017, November). A Face-Recognition Approach Using Deep Reinforcement Learning Approach for User Authentication. In *2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)*(pp. 183-188). IEEE.

- Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, 14(1), 4-20.
- Agrawal, A. K., & Singh, Y. N. (2015). Evaluation of Face Recognition Methods in Unconstrained Environments. *Procedia Computer Science*, 48, 644-651.
- Hassan, G., & Elgazzar, K. (2016, April). The case of face recognition on mobile devices. In *Wireless Communications and Networking Conference (WCNC), 2016 IEEE* (pp. 1-6). IEEE.
- Amos, B., Ludwiczuk, B., & Satyanarayanan, M. (2016). Openface: A general-purpose face recognition library with mobile applications. *CMU School of Computer Science*.
- Cui, D., Zhang, G., Hu, K., Han, W., & Huang, G. B. (2017). Face recognition using total loss function on face database with ID photos. *Optics & Laser Technology*.
- Lu, S., Ranjan, R., & Strazdins, P. (2015). Reporting an experience on design and implementation of e-Health systems on Azure cloud. *Concurrency and Computation: Practice and Experience*, 27(10), 2602-2615.
- Hossain, M. S., & Muhammad, G. (2015). Cloud-assisted speech and face recognition framework for health monitoring. *Mobile Networks and Applications*, 20(3), 391-399.
- Singh, D., & Verma, H. K. (2016, March). A new framework for cloud storage confidentiality to ensure information security. In *Colossal Data Analysis and Networking (CDAN), Symposium on* (pp. 1-5). IEEE.
- Knorr, K., & Aspinall, D. (2015, April). Security testing for Android mHealth apps. In *Software Testing, Verification and Validation Workshops (ICSTW), 2015 IEEE Eighth International Conference on* (pp. 1-8). IEEE.
- Karim, M. Y., Kagdi, H., & Di Penta, M. (2016, March). Mining android apps to recommend permissions. In *Software Analysis, Evolution, and Reengineering (SANER), 2016 IEEE 23rd International Conference on* (Vol. 1, pp. 427-437). IEEE.
- Hussein, Z., Oon, S. W., & Fikry, A. (2017). Consumer Attitude: Does It Influencing the Intention to Use mHealth? *Procedia Computer Science*, 105, 340-344.

GLOSARIO

C

- **CCRA v4:** Arquitectura para el desarrollo de proyectos en entorno de Cloud Computing.

E

- **Entregable:** Artefacto documentado.

M

- **Metodología:** Estándar de pasos a seguir para lograr un objetivo.

R

- **Riesgo:** Evento que puede afectar el desarrollo del proyecto.
- **Reconocimiento Facial:** Tecnología para la identificación de rostros.
- **ROI:** Retorno de la Inversión.

S

- **Software:** Conjunto que engloba todos los elementos (documentación, procedimientos e información procesada) de un sistema informático.
- **Stakeholder:** Grupo de personas o individuos a quienes les puede afectar o son afectados por las actividades de una empresa; pueden ser internos o externos a esta.
- **Student Outcomes:** Puntos que debe cumplir el perfil del egresado de la carrera de Ingeniería de Sistemas de Información de la UPC.

P

- **PMBOK:** Libro que describe los conocimientos y de prácticas aplicables a cualquier situación que requiera formular ante una gestión de proyectos.
- **PaaS:** Encapsulación de una abstracción de un ambiente de desarrollo y el empaquetamiento de una serie de módulos o complementos que proporcionan, normalmente, una funcionalidad horizontal.