UNIVERSIDAD JOSÉ ANTONIO PÁEZ

SISTEMA DE ACCESO POR MEDIO DE UN DISPOSITIVO DE RECONOCIMIENTO FACIAL, PARA SISTEMAS INFORMÁTICOS

Autor:
Chirinos Jhorver

Urb. Yuma II, calle Nº 3. Municipio San Diego
Teléfono: (0241) 8714240 (master) – Fax: (0241) 8712394

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE COMPUTACION

SISTEMA DE ACCESO POR MEDIO DE UN DISPOSITIVO DE RECONOCIMIENTO FACIAL, PARA SISTEMAS INFORMÁTICOS

Proyecto del Trabajo de Grado para optar al título de

INGENIERO EN COMPUTACION

Autor:
Chirinos Jhorver
CI: 28359939
Tutor:
Wiston Espinoza
CI: 9885895

San Diego, Octubre de 2023

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
COORDINACIÓN DE PASANTÍA Y TRABAJO DE GRADO

ACTA DE APROBACIÓN

INFORME DE PASANTÍA ☐ **TRABAJO DE GRADO** ☑

El jurado designado por la Facultad de Ingeniería para la evaluación del **Informe de Pasantía o Trabajo de Grado** titulado:

Sistema de acceso por medio de un dispositivo de reconocimiento facial para sistemas informáticos

Realizado por el (la) Br. Jhorver Chirinos

C.I. Nº 28.359.939 cursante de la carrera de Computación

hace constar, después de haber analizado su contenido y oída la exposición oral, considera que el mismo ha sido:

APROBADO ☑ **NO APROBADO** ☐

El Jurado

Tutor Académico (Coordinador)
Nombre: Wilson Espinoza
C.I.: 9885895

Jurado
Nombre: Manuel Figueroa
C.I.: 17315996

Jurado
Nombre: María García
C.I.: 27724883

Fecha: 09 / 04 / 2024

UJAP

FI-C-007-2023-2CR-TG

San Diego, 01 de diciembre de 2023

Ciudadano(s):
CHIRINOS PADRÓN, JHORVER ALFREDO
C.I.: 28359939

Presente. -

Cumplo con informarle que la comisión de Trabajo de Grado y Pasantías de la Facultad de Ingeniería, en su reunión **N° 15-2023** de fecha **2/11/2023**, aprobó el proyecto de grado titulado:

SISTEMA DE ACCESO POR MEDIO DE UN DISPOSITIVO DE RECONOCIMIENTO FACIAL, PARA SISTEMAS INFORMÁTICOS

Presentado por usted(es) como requisito para optar al título de Ingeniero de Computación.

Se ratifica la designación del Tutor Académico que lo asesorará en el desarrollo de este proyecto al profesor Espinoza Hurtado, Wiston Alexander, titular de la cédula de identidad V-9885895.

Facultad de Ingeniería
UJAP
DECANATO

Atentamente,

Dra. Laura Aurora Sáenz Palencia
Decana de la Facultad de Ingeniería

c.c. Coordinación de Pasantía y Trabajo de Grado de la Facultad de Ingeniería

ÍNDICE GENERAL

CONTENIDO **pp.**

ÍNDICE DE CUADROS

DESCRIPCIÓN

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE COMPUTACION

SISTEMA DE ACCESO POR MEDIO DE UN DISPOSITIVODE RECONOCIMIENTO FACIAL, PARA SISTEMAS INFORMATICOS

Autor:

Chirinos Jhorver

Tutor:

Wiston Espinoza

Fecha: Abril 2024

RESUMEN

En el estudio de investigación su objetivo general se enfocó en el desarrollo de un sistemade acceso por medio de un dispositivo de reconocimiento facial para sistemas informáticos, que garantice la confidencialidad de los datos del usuario. Estas herramientas deben ser capaces de aplicar protecciones como el cifrado, el enmascaramiento de datos y el borrado de archivos confidenciales. La fundamentación parte de las herramientas que deben ofrecer la protección de los datos para facilitar las auditorías, satisfaciendo las exigencias normativas y previniendo los posibles errores de organización por fuga de datos. La línea de investigación utilizada fue el desarrollo de tecnología, el enfoque es cualitativo. El tipo de investigación es descriptiva y de proyecto especial, la técnica de recolección de datos fue la entrevista y el instrumento una guía de preguntas de 6 ítems y la técnica de observación una lista de cotejo. Se analizaron las distintas etapas de la investigación utilizando la metodología extreme programming (XP) para evaluar la eficacia del sistema de acceso propuesto mediante un dispositivo de reconocimiento facial en sistemas informáticos. Estas fases incluyeron el diagnóstico, la planificación, el diseño, el desarrollo y las pruebas, lo que permitió un desarrollo óptimo del sistema.

Descriptores: Sistema de escritorio, reconocimiento facial, seguridad informática, información confidencial, dispositivo de reconocimiento.

INTRODUCCIÓN

La seguridad informática es un aspecto fundamental para garantizar la confidencialidad de los datos de los usuarios de sistemas informáticos. Sin embargo, los métodos tradicionales de acceso, como las contraseñas o los códigos PIN, pueden ser vulnerados o extraviados, lo que compromete la integridad de la información. Por ello, se planteó el desarrollo de un sistema de acceso por medio de un dispositivo de reconocimiento facial, que permite identificar al usuario y aplicar las medidas de protección adecuadas a sus datos. El presente trabajo es una propuesta de un diseño para implementar dicho sistema, basándose en las herramientas y normativas existentes en el ámbito de la seguridad informática. Para ello, se realizó una investigación documental y de campo, con el fin de recabar los requisitos y las expectativas de los posibles usuarios del sistema. Asimismo, se utilizó el enfoque cualitativo para analizar los datos obtenidos y proponer una solución viable y eficiente.

El sistema de acceso por reconocimiento facial se fundamenta en el uso de algoritmos que permiten detectar y comparar las características faciales de una persona con una base de datos previamente registrada. De esta manera, se puede verificar la identidad del usuario y otorgarles el acceso a sus datos personales o restringirlo en caso contrario. El sistema también cuenta con mecanismos de seguridad adicionales, como la encriptación de los datos, el control de los intentos fallidos y la generación de alertas en caso de intrusión. El sistema se implementa mediante un programa de reconocimiento facial el cual está realizado en python. Él mismo se evaluó mediante pruebas técnicas y funcionales, así como mediante la aplicación de pruebas unitarias, de integración y de aceptación.

El siguiente trabajo de investigación se organizó de la siguiente manera: capítulo I se planteó el problema que se pretendía resolver, se formuló la pregunta de investigación, se establecieron los objetivos y la justificación del estudio. Capítulo II se revisa el marco teóricoque sustenta el tema de investigación, se analizaron los antecedentes y las principales corrientes conceptuales que lo abordan. Capítulo III se describió el marco metodológico que se emplea para realizar la investigación, se especificó el tipo de estudio, el diseño, la población y muestra, las técnicas e instrumentos de recolección de datos y el procedimiento de análisis. Capítulo IV se realizó el análisis de los resultados del diagnóstico. Capítulo V se presentaron los recursos humanos, materiales y financieros requeridos para llevar a cabo la investigación.

CAPITULO I EL PROBLEMA

Planteamiento de problema

El objetivo de la seguridad de datos es preservar la integridad, la confidencialidad y la disponibilidad de la información digital frente a posibles ataques, alteraciones o pérdidas durantetodo el tiempo que dure su tratamiento. Se trata de un concepto amplio que abarca todas las medidas de seguridad de la información, desde la protección física de los equipos y los medios de almacenamiento hasta los mecanismos de control y acceso, así como la seguridad de las aplicaciones informáticas. También implica las normas y los procesos de la organización.

La ejecución correcta de las estrategias de seguridad de datos sólidas posibilitará proteger los activos informativos de una organización frente a las actividades de los ciberdelincuentes, pero también frente a las amenazas internas y los errores humanos, que siguen siendo uno de los principales motivos de la infracción de datos. La seguridad de datos implica el uso de herramientas y tecnologías que ofrezcan mejoras a la organización en relación con la visibilidad sobre dónde se localizan los datos críticos y cómo se emplean.

En este orden de ideas, estas herramientas deben ser capaces de aplicar protecciones comoel cifrado, el enmascaramiento de datos y el borrado de archivos confidenciales, así como automatizar la generación de informes para simplificar las auditorías, cumplir las demandas normativas y controlar los posibles fallos de organización, que continúan siendo uno de los principales factores de riesgo para la violación de datos. La importancia de estas medidas se evidencia al revisar algunos de los casos más grandes de pérdida de información y robo de datos informáticos que han ocurrido en la historia. Por ejemplo, en 2009, el departamento de administración de archivos nacionales de EE. UU. Sufrió una gran pérdida de datos debido al robo de un disco duro que contenía toda la información personal de las personas que visitaron la Casa Blanca durante el mandato de Bill Clinton, García

(2003). En el mismo año, más de 800,000 usuarios del dispositivo Sidekick de Microsoft fueron víctimas de una grave pérdida de datos por una falla en el servidor que causó la pérdida de datos personales como contactos, fotos, eventos de calendario, entre otros García (2003). En 2016, Uber reveló que los datos fueron robados de 57 millones de usuarios y que tuvo que pagar $ 100,000 a los piratas informáticos que robaron la información para destruirla Uber (2016).

Estos son solo algunos ejemplos de las consecuencias devastadoras que puede tener una mala gestión o protección de los datos. Por ello, es fundamental contar con herramientas eficaces y actualizadas que garanticen la seguridad y la privacidad de la información.

Formulación del problema

¿De qué manera se podrá agregar una capa de seguridad al acceso en sistemas informáticos con un sistema de acceso por reconocimiento facial en la empresa IAM TECNOLOGIA, C.A.?

Objetivos de la investigación

Objetivo general

Desarrollar un sistema para el acceso a sistemas informáticos por medio de un dispositivo de reconocimiento facial en la empresa IAM TECNOLOGIA, C.A.

+9++9 8}

bjetivos específicos:

- Diagnosticar los métodos de control de acceso a sistemas informáticos
- Identificar los elementos funcionales y no funcionales de los sistemas de control de acceso a sistemas informáticos

- Diseñar un sistema de acceso por reconocimiento facial para sistemas informáticos empleando la metodología XP
- Desarrollar un sistema para el acceso a sistemas informáticos por medio de un dispositivo de reconocimiento facial a fin de garantizar la seguridad de la información confidencial de la empresa IAM TECNOLOGIA, C.A.

Justificación de la investigación

La confidencialidad de los datos del usuario es un tema de vital importancia en la actualidad debido a la gran cantidad de peligros y amenazas que hay del robo de la información privada. Con el aumento de la cantidad de información personal que se almacena en línea, es importante tener medidas de seguridad adecuadas para proteger los datos del usuario. El diseño de un sistema de acceso a través de un dispositivo de reconocimiento facial empleando la metodología XP, puede ser una solución efectiva para garantizar la seguridad y privacidad de los datos del usuario.

Es por ello que en la propuesta de investigación que se plantea, su objetivo general es crear un sistema para controlar el acceso a sistemas de información que impida el ingreso a personas no autorizadas, y que el mismo, sea solo accesible a través de un dispositivo de reconocimiento facial. Además, que en sus objetivos específicos se busca analizar la importancia de la confidencialidad de los datos, determinar los beneficios de un sistema que controle la información accesible a través de un dispositivo reconocimiento facial.

Este sistema pretende ofrecer una solución efectiva para garantizar la seguridad y privacidad de los datos del usuario, como información financiera, médica o de cualquier otro

campo que se almacene localmente. El reconocimiento facial es una tecnología que permite identificar a una persona mediante el análisis de las características biométricas de su rostro. Esta tecnología tiene múltiples beneficios, como la

rapidez, la seguridad y la fiabilidad de la identificación del usuario, así como la prevención de la falsificación y el robo de datos.

Alcance

El alcance de la investigación se limita a la creación de un sistema para el acceso a sistemas informáticos, accesible a través de un dispositivo de reconocimiento facial, que se pueda utilizar por cualquier persona o empresa que desee proteger su información.

No se abordarán otros aspectos relacionados con el reconocimiento facial, como su impacto social, político o cultural, ni se profundizará en los aspectos técnicos del algoritmo utilizado. Tampoco se considerarán otras formas de identificación biométrica, como el reconocimiento de voz, el reconocimiento de retina o iris o el reconocimiento vascular.

El Alcance del estudio de investigación se concreta en determinar los elementos funcionales y no funcionales; el diseño y desarrollo para el acceso a sistemas informáticos, accesible a través de un dispositivo de reconocimiento facial; la confidencialidad de los datos del usuario; y el proceso de evaluación final del funcionamiento.

Limitaciones y/o Delimitaciones

El sistema propuesto consiste en un dispositivo de reconocimiento facial que permite el acceso a sistemas informáticos que manejan datos sensibles o confidenciales, como bancos, empresas o instituciones públicas. Sin embargo, el sistema presenta algunas limitaciones, como la dependencia de la calidad y la iluminación de las imágenes capturadas por el dispositivo, la posibilidad de confusión entre personas con rasgos faciales similares o con cambios significativos en su apariencia, y la41 necesidad de una conexión a internet estable y segura para comunicarse conla aplicación web y la base de datos.

CAPÍTULO II

MARCO TEÓRICO

Antecedentes

Miró, M (2023) en su artículo de "seguridad informática: que es, tipos y características" habla sobre que la protección de los datos y sistemas de una compañía es una tarea fundamental para garantizar su continuidad y éxito a largo plazo, por lo que la seguridad informática se ha convertido en un tema cada vez más importante en el mundo empresarial. En este artículo, se aborda qué es la seguridad informática, los diferentes tipos de amenazas a los que se enfrentan las empresas y las características que deben tener los sistemas de protección. Este antecedente se extrajo del artículo publicado por Michel Miró, licenciado en ADE por la Universidad Politécnica de Valencia y Máster en MBA y Coaching por la Universidad Europea de Barcelona.

Este antecedente ratifica la necesidad del mundo empresarial de la seguridad informática para la prevención de las amenazas y es por ello su relación con el presente estudio que propone el diseño de un sistema de acceso por reconocimiento facial para la seguridad de los sistemas informáticos.

García, J. (2023). Este antecedente se extrajo del artículo publicado por José García, doctor en Ingeniería Informática por la Universidad de Granada y experto en ciberseguridad y gestión de riesgos. Ciberseguridad y gestión de riesgos. En este artículo, se analiza la importancia de la ciberseguridad como un factor clave para la gestión de riesgos en las organizaciones, especialmente en el contexto actual de transformación digital y aumento de los ciberataques. Se explica el concepto de ciberseguridad, sus dimensiones y objetivos, así como losprincipales desafíos y tendencias que enfrenta el sector. También se presentan algunas buenas prácticas y recomendaciones para mejorar la seguridad de la información y la resiliencia de las empresas ante posibles incidentes.

Su aporte a la investigación está en la importancia de la Ciberseguridad y gestión de riesgo en la información de las organizaciones, para el diagnostico de los métodos de control de acceso que facilita el sistema por reconocimiento facial propuesto.

AlSur (2022) define el reconocimiento facial como una tecnología que identifica a las personas por sus rasgos faciales, y destaca su utilidad para la vigilancia masiva en lugares públicos, aunque muchas veces sin el consentimiento de las personas observadas. El reconocimiento facial se originó en los años 60, pero ha cobrado mayor relevancia en los últimos tiempos gracias a los progresos en el manejo de imágenes, datos y algoritmos. Actualmente, el reconocimiento facial se usa para diversos fines, desde la seguridad de los dispositivos móviles hasta el análisis de las expresiones y sentimientos, una práctica que recuerda a la frenología del siglo XIX.

El aporte de AlSur al desarrollo de un sistema de acceso a sistema informático por medio de un dispositivo de reconocimiento facial propuesto, se sintetiza, en la utilidad de esta tecnología que ha cobrado relevancia en la actualidad.

Arguello, H. (2021) en su tesis de grado de la Universidad Industrial de Santander, Colombia. El autor describe las principales líneas de trabajo en la identificación de personas mediante imágenes faciales y presenta una síntesis de las técnicas matemáticas más recientes para extraer características en estos sistemas. Las técnicas más utilizadas para extraer características en sistemas de reconocimiento facial incluyen el análisis de componentes principales (PCA), análisis de discriminantes lineales de Fisher (FLD), conservación de proyecciones locales (LPP), proyecciones aleatorias (Randomfaces), redes neuronales artificiales (RN), análisis de componentes independientes (ICA), características locales o análisis de subregiones, correlación (CORR) y DCT. Arguello aclara que actualmente se han realizado muchas investigaciones sobre sistemas basados en modelos 3D de la cabeza de la personay esquemas que trabajan con señales de vídeo en lugar de imágenes fijas. Agrega que, para implementar un sistema de reconocimiento facial, se presentan seis etapas bien definidas: capturade la imagen, Preprocesamiento, localización, escalamiento y ajuste, extracción de características y, por último, clasificación y toma de decisiones. Este estudio fue promovido y financiado por la Universidad Industrial de Santander, Bucaramanga, Colombia, a nivel internacional.

El aporte de Arguello se resume en la importancia que tiene el uso de metodologías que garanticen la seguridad de la información basadas en la reducción de riesgos para el cumplimiento de las normas, políticas y procedimientos establecidos por la organización, lo cual está en los objetivos de la presente propuesta.

Álvarez, L. D. (2019) Estudiante de la Universidad Autónoma de Nuevo León, México. El autor expone los principales conceptos y metodologías para realizar una auditoría de sistemas informáticos y garantizar la seguridad de la información. Las auditorías de sistemas informáticos son procesos que evalúan el cumplimiento de las normas, políticas y procedimientos establecidos para el uso, administración y protección de los recursos informáticos. Las metodologías más

empleadas para realizar una auditoría de sistemas informáticos incluyen el análisis de riesgos, elcontrol interno, el marco COBIT, el estándar ISO 27001 y el modelo CMMI. Estas metodologíasse basan en la identificación, evaluación y mitigación de los riesgos asociados a la seguridad de la información. Álvarez aclara que actualmente se han desarrollado muchas herramientas y técnicas para facilitar y automatizar las tareas de auditoría, tales como software de análisis, pruebas de penetración, escaneo de vulnerabilidades y monitoreo de redes. Agrega que, para implementar una auditoría de sistemas informáticos, se deben seguir cinco fases bien definida planificación, ejecución, informe, seguimiento y cierre. Este estudio fue apoyado y financiado por la Universidad Autónoma de Nuevo León, Monterrey, México, a nivel nacional.). Álvarez aclara que actualmente se han desarrollado muchas herramientas y técnicas que protegen la información y es por ello que este trabajo considera dichos avances en el diseño de un sistema de reconocimiento facial como herramienta accesible que facilite el resguardo de datos confidenciales del usuario, a través de las fases planificación, ejecución, informe, seguimiento y cierre.

Bases teóricas Seguridad de Datos

La Información confidencial puede residir en repositorios de datos estructurados y no estructurados, como bases de datos, almacenes de datos, plataformas de big data y entornos de cloud. Las soluciones de detección y clasificación de datos automatizan el proceso de identificación de información confidencial, así como la evaluación y la corrección devulnerabilidades.

Los tres grandes conceptos de seguridad se resumen en:

- Confidencialidad: La clave es rechazar a quienes no deberían ver los contenidosrestringidos.
- Integridad: Garantizar que la información a la que se accede no se haya alterado, quesea confiable.

- Disponibilidad: Posibilidad de acceder a la información sin problema para eloperador.

Herramientas para la prevención de riesgos y vulnerabilidades

Las herramientas de análisis de riesgos y evaluación de vulnerabilidades facilitan el proceso de detección y mitigación de las mismas, como software obsoleto, configuraciones incorrectas o contraseñas débiles. Además, estas herramientas pueden identificar fuentes de datos con un mayor riesgo de exposición.

Las herramientas para la seguridad de la información son:

- **Autenticación:** La autenticación es el proceso de verificar la identidad de un usuario o de un sistema informático. La autenticación se basa en uno o más factores, como algoque el usuario sabe (una contraseña o un PIN), algo que el usuario tiene (una tarjeta oun token) o algo que el usuario es (una huella dactilar o un rostro). La autenticación permite controlar el acceso a los recursos y proteger la información de posibles ataques.
- **Cifrado:** El cifrado funciona como un proceso de codificación de datos en su transmisión o almacenamiento para que solo las personas autorizadas puedan leerlo
- **Firewall:** Un firewall se encarga de la gestión de tráfico de la red de la organización, estableciendo criterio para la entrada y salida de información.Existen dos tipos de firewall:
- **Firewall de hardware:** Se refiere a un dispositivo conectado a la red que filtra lospaquetes según un conjunto de reglas establecidas por la empresa
- **Firewall de software:** Este firewall se ejecuta en el sistema operativo e intercepta lospaquetes a medida que entran en el sistema.

Importancia de la Seguridad de Datos.

La seguridad de datos consiste en proteger información digital contra el acceso no autorizado. Por tanto, la importancia de la seguridad de la información contempla la seguridad física del hardware y los dispositivos de almacenamiento, así como, la seguridad lógica de aplicaciones de software, incluyendo las políticas y los procedimientos de la organización contra las actividades de Ciber-delincuentes, amenazas internas y errores humanos.

Reconocimiento facial.

Los sistemas de reconocimiento de identidad han utilizado distintas señales, entre ellas: imágenes de las huellas digitales, el iris de los ojos, la palma de la mano, el rostro, o por señales como la voz de una persona o su firma manual; sin embargo, ninguna de estas técnicas es confiable un 100% de las veces, de acuerdo a lo indicado por un estudio de Arguello H. (2011) publicado por la Universidad Industrial de Santander, Colombia.

Según Arguello (2011), en su artículo "Sistemas de reconocimiento basados en la imagen facial"menciona que los sistemas de reconocimiento por rostro son los que tienen las tasas más altas de falsa aceptación y falso rechazo, pero debido a su gran aceptación por parte del público, ya es un sistema menos invasivo y el sensor de captura es fácil de adquirir, haciendo este método de reconocimiento un mecanismo de autenticación bastante efectivo.

Fases del reconocimiento facial para su implementación.

Implementar el reconocimiento facial se debe cumplir con las 6 siguientes fases definidas:

- **Captura de imagen:** Selección de la cámara digital y las características de iluminación,controladas y no controladas.
- **Preprocesamiento:** Una vez la imagen es capturada, se incluye la selección del espacio de color o la extracción de la intensidad al utilizar la

escala de grises.

- **Localización:** luego de preprocesar la imagen obtenida, se determinan las coordenadas de la posición de la cara dentro de la escena, delimitando normalmente la zona de la cara formada por las orejas, la frente y el mentón.
- **Escalamiento y ajuste:** Realizando un escalado de imagen, se normaliza la informaciónobtenida de partes como los ojos, nariz u otras características.
- **Extracción de características:** La extracción de características utiliza cualquiera de las técnicas antes mencionadas o combinaciones de ellas. Esta operación produce un vector de características del individuo.
- **Clasificación y toma de la decisión:** En esta fase, se utiliza el vector de características del individuo obtenido en la fase anterior para compararlo con los vectores de características almacenados en la base de datos. La comparación se realiza mediante algoritmos de aprendizaje automático, que pueden ser supervisados o no supervisados, y se determina si la persona es reconocida o no. Si la persona es reconocida, se toma una decisión basada en el propósito del sistema de reconocimiento facial.

Bases Legales

Bases legales de la Seguridad de Datos.

La seguridad de la información digital es un aspecto fundamental para garantizar el respeto y la protección de los derechos humanos, especialmente el derecho a la privacidad, en el contexto de las tecnologías nuevas y emergentes. Existen diversas normas internacionales y nacionales que regulan este ámbito, estableciendo principios, obligaciones y medidas para prevenir y sancionar las injerencias arbitrarias o ilegales en la vida privada, la familia, el domicilio o la correspondencia de las personas, así como los ataques ilegales a su honra y reputación.

Entre las normas internacionales más relevantes se encuentran el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, que consagran el derecho a la privacidad como un derecho humano fundamental. Asimismo, la Asamblea General de las Naciones Unidas y el Consejo de Derechos Humanos han aprobado numerosas resoluciones sobre el derecho a la privacidad en la era digital, que contienen recomendaciones a los Estados Miembros y las empresas para garantizar el respetoy la protección del derecho a la privacidad en la era digital.

En el ámbito internacional, existen diferentes leyes que, de una forma u otra, complementan el concepto general de seguridad de la información digital. Entre ellas se destacan la Ley Orgánica 15/1999 española de Protección de Datos de Carácter Personal y su Reglamento de desarrollo, que establecen una serie de medidas de seguridad tanto para ficheros automatizados como en papel que contengan datos personales; la Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico, que regula las obligaciones de los prestadores de servicios en Internet y las comunicaciones comerciales por vía electrónica; el Real Decreto 1/1996 de Propiedad Intelectual, que reconoce los derechos morales y de explotación sobre las obras originales.

El cumplimiento de estas normas es esencial para asegurar un nivel adecuado de seguridad de la información digital, así como para minimizar y conocer los riesgos con los que se puede encontrar. La seguridad de la información digital no solo implica aspectos técnicos, sino tambiénjurídicos, éticos y sociales, que deben ser considerados por todas las organizaciones que manejeninformación sensible o relevante.

La Constitución de la República Bolivariana de Venezuela, que establece en su artículo 28 el derecho de toda persona a acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como el derecho a conocer el uso

que se haga de los mismos.

Asimismo, el artículo 60 reconoce el derecho a la protección de la vida privada, sin injerencias arbitrarias, y el artículo 61 consagra el derecho al honor, a la reputación y a la propiaimagen.

La Ley Especial contra los Delitos Informáticos, que tipifica como delitos las conductas que atenten contra la seguridad, la integridad o el funcionamiento de los sistemas que utilicen tecnologías de información, así como las que afecten la confidencialidad, la integridad o la disponibilidad de los datos o información contenidos en dichos sistemas. Esta ley también establece las medidas preventivas y cautelares que pueden adoptar las autoridades judiciales para investigar y sancionar estos delitos.

La Ley Orgánica de Telecomunicaciones, que regula el servicio público de telecomunicaciones y las actividades conexas, incluyendo el uso del espectro radioeléctrico y el acceso a las redes e infraestructuras. Esta ley también define los derechos y obligaciones de los prestadores de servicios de telecomunicaciones, entre los que se encuentran los proveedores de servicios de internet, así como los derechos y deberes de los usuarios y las usuarias.

La Ley sobre Mensajes de Datos y Firmas Electrónicas, que reconoce la validez y eficacia jurídica de los mensajes de datos y las firmas electrónicas, así como los principios y requisitos para su generación, envío, recepción, almacenamiento y conservación. Esta ley también regula la actividad de los proveedores de servicios de certificación y las entidades de registro y verificación.

Bases legales del Reconocimiento facial

El reconocimiento facial es una tecnología que permite identificar a una persona mediante el análisis de las características de su rostro. Esta tecnología plantea una serie de desafíos jurídicos

y éticos, ya que puede afectar a la privacidad, la seguridad y los derechos humanos de las personas. Por ello, es necesario establecer unas bases legales que regulen su uso y garanticen el respeto a los principios de proporcionalidad, necesidad y transparencia.

En el ámbito europeo, el reconocimiento facial se rige por el Reglamento General de Protección de Datos (RGPD), que establece que el tratamiento de datos biométricos para identificar a una persona debe basarse en una de las siguientes bases legítimas: el consentimiento explícito del interesado, el cumplimiento de una obligación legal, la protección de intereses vitales, la realización de una tarea de interés público o el ejercicio de poderes públicos. Además, el RGPD exige que se realice una evaluación de impacto previa al uso del reconocimiento facial y que se apliquen medidas técnicas y organizativas adecuadas para proteger los datos.

En Venezuela, no existe una legislación específica que regule el uso del reconocimiento facial, ni tampoco una autoridad independiente que supervise su aplicación. Sin embargo, existen algunas normas generales que podrían aplicarse al tratamiento de datos personales obtenidos por esta tecnología, como la Constitución, el Código Civil, la Ley Orgánica de Telecomunicaciones, la Ley Especial contra los Delitos Informáticos y la Ley Orgánica de Protección del Niño, Niña y Adolescente.

Estas normas establecen principios como el respeto a la intimidad, la inviolabilidad de las comunicaciones, el consentimiento informado, la finalidad y proporcionalidad del tratamiento, la seguridad y confidencialidad de los datos y el derecho de acceso, rectificación y oposición por parte de los titulares de los datos. Sin embargo, estas normas son insuficientes para regular adecuadamente el uso del reconocimiento facial, ya que no contemplan aspectos como la calidad y exactitud de los datos, el plazo de conservación, la transferencia internacional, la responsabilidad de los operadores o las garantías frente a posibles abusos o discriminaciones.

Definición de Términos Básicos

- **Big Data:**Big Data se refiere al conjunto de datos que son tan grandes, complejos diversos que requieren técnicas especiales de procesamiento, análisis y almacenamiento. El término también se usa para describir las aplicaciones y tecnologías que permiten manejar estos datos, así como los conocimientos y habilidades necesarios para ello.
- **Ciberseguridad:** Es el conjunto de medidas, técnicas y buenas prácticas que se emplean para proteger los activos digitales de una organización o individuo frente a amenazas cibernéticas.
- **Cloud:** El cloud es un conjunto de recursos informáticos que se pueden acceder y utilizar través de Internet o de una red privada. Estos recursos pueden incluir servidores, almacenamiento, aplicaciones, bases de datos, redes, software y otros servicios.
- **Dispositivo de reconocimiento:** Es un aparato sistema que permite identificar a unapersona o entidad mediante el análisis de sus características físicas.
- **Identificación biométrica:** Es un tipo de reconocimiento basado en el uso de rasgosbiológicos únicos e intransferibles, como la huella dactilar, el iris, la voz o el rostro.
- **Información confidencial:** Es aquella información que tiene un valor estratégico, comercial, legal o personal y que debe ser resguardada de accesos no autorizados odivulgaciones indebidas.
- **Metodología XP:** Es una metodología ágil de desarrollo de software que se basa en principios como la comunicación, el feedback, la simplicidad, el valor y el respeto. Su objetivo es entregar software de calidad que satisfaga las necesidades del cliente en tiempos cortos y con cambios frecuentes.
- **Multicloud:** Multicloud es una estrategia de computación en la nube que consiste en utilizar múltiples proveedores de servicios de nube pública o

privada para satisfacer lasnecesidades de una organización.

- **Reconocimiento facial:** Es una técnica de identificación biométrica que utiliza el análisisde las características faciales de una persona para verificar su identidad o detectar su presencia.
- **Sistema de escritorio:** Es un tipo de sistema operativo que se ejecuta en un ordenador personal y que ofrece una interfaz gráfica de usuario para facilitar la interacción con elusuario.

CAPÍTULO III

MARCO METODOLÓGICO

Enfoque de la Investigación:

Según Hernández, Fernández y Baptista (2014), el enfoque cuantitativo utiliza la recolección de datos para descubrir o afinar preguntas de investigación en el proceso de interpretación.

Tipo de Investigación

|El tipo de investigación según Arias (2006), se enfoca en un proyecto especial, en la modalidad de propuesta factible y sistemática dirigida a buscar la solución a un problema concreto y a corto plazo para responder a las necesidades específicas de un determinado cliente; En este caso es la propuesta de un sistema de acceso por medio de un dispositivo de reconocimiento facial, para sistemas informáticos.

Diseño de la Investigación

El diseño de la investigación es Cuasiexperimental, según Hernández, Fernández y Baptista (2014), se asemeja al diseño experimental, pero no se asignan aleatoriamente los sujetos a los grupos experimentales, sino que se aprovechan grupos naturales o preexistentes. Este tipo de diseño reduce el control sobre las variables extrañas y la validez interna del estudio" (p. 235). **Nivel de**

Investigación

La investigación de carácter descriptivo es aquella que tiene como objetivo principal describir las características, propiedades o atributos de un fenómeno, una población o una muestra. Este tipo de investigación no busca establecer relaciones causales entre variables, sino simplemente observar y registrar los hechos tal como ocurren. La aplicabilidad de la investigación descriptiva es amplia, ya que puede servir para explorar un tema poco conocido, para identificar problemas o necesidades, para evaluar programas o políticas, o para proporcionar información básica para estudios posteriores de mayor complejidad (Arias, 2006). Por ello el

estudio pretende describir las fases para agregar una capa de seguridad al acceso de informaciónen sistemas informáticos a través del reconocimiento facial.

El nivel de investigación es un criterio que permite clasificar los estudios científicos según el grado de profundidad con que se aborda un fenómeno u objeto de estudio según Arias (2006). La investigación opta por los siguientes niveles de investigación: descriptivo y el proyecto especial.

El nivel descriptivo se enfoca en describir las características, propiedades y relaciones de las variables y el nivel de proyecto especial, en la modalidad de propuesta factible y sistemática, está dirigida a buscar la solución a un problema concreto y a corto plazo por medio de un dispositivo de reconocimientofacial, para sistemas informáticos.

13

Población y muestra

- **Población:** La población está definida por el objeto de estudio y es la variable principal en el título: "Sistemas de acceso para sistemas informáticos". Según Hernández S, Fernández C, Batista L (2014), la define como el conjunto de elementos con características afines. Se estableció como población para el estudio de investigación: Sistema de control de acceso digital

.

Muestra: La muestra está definida por la característica específica que define la variable: "Sistemas de acceso para sistemas informáticos mediante reconocimiento facial". La muestra es un subconjunto o parte de población que se selecciona para representar las características de interés del conjunto mayor. Según Hernández S, Fernández C, Batista L (2014), existen diferentes criterios para determinar el tamaño y la composición de la muestra, dependiendo del tipo de investigación y del diseño metodológico. La muestra seleccionada es: Sistema de control de acceso digital con reconocimiento facial.

Técnicas e Instrumentos de recolección de datos.

La técnica de recolección de datos es el conjunto de métodos y herramientas que se utilizan para obtener, registrar y analizar la información necesaria para una investigación Hernández S, Fernández C, Batista L (2014). En la investigación se utilizará las siguientes técnicas de recolección de datos: la observación, las entrevistas y el análisis documental.

La observación según Hernández S, Fernández C, Batista L (2014). Consiste en el registro sistemático y objetivo de los hechos, fenómenos o comportamientos que ocurren en un contexto determinado. El investigador puede ser un observador participante, que interactúa con los sujetos o el entorno de estudio, o un observador no participante, que se limita a observar sin intervenir. La observación puede ser directa, cuando se realiza en el momento y lugar donde ocurren los hechos, o indirecta, cuando se utiliza algún medio auxiliar como una cámara o un grabador.

Las entrevistas según Hernández Sampieri (2014). Son conversaciones dirigidas entre el investigador y los informantes, con el fin de obtener información relevante para la investigación.

Las entrevistas pueden ser estructuradas, cuando se sigue un guion preestablecido de preguntas cerradas, semi-estructuradas, cuando se combinan preguntas cerradas y abiertas, o no estructuradas, cuando se plantean preguntas abiertas y flexibles según el desarrollo del a conversación.

El análisis documental según arias (2006) es el examen crítico y sistemático de las fuentes escritas o gráficas que contienen información relacionada con el objeto de estudio. El investigador debe seleccionar, clasificar, interpretar y evaluar los documentos según su pertinencia, validez y fiabilidad. Los documentos pueden ser primarios, cuando son producidos por los protagonistas o testigos directos de los hechos, o secundarios, cuando son elaborados por personas que no participaron directamente en los hechos.

Para los fines de la investigación, la técnica que se utilizará será la entrevista, y el instrumento será una guía de 6 preguntas cerradas aplicadas a 6 empleados para conocer el Método de acceso a información, elementos funcionales y no funcionales, sistema informático e identificación del usuario, empleado por la muestra seleccionada para el estudio de investigación (IAM TECNOLOGIA, C.A.)(ver Apéndice A); con relación a la técnica de observación directa se utilizará una lista de cotejo que contemplará los siguientes aspectos del proceso: identificación del usuario, acceso al sistema, reconocimiento facial (ver Apéndice

B). **Validación del Instrumento**

Los criterios de validación y confiabilidad aplicados a cada instrumento para la recolección de datos, pretenden medir resultados consistentes y estables. Se utilizará la validación de experto, que consiste en someter los instrumentos que se aplicarán en el estudio de investigación a la revisión y el juicio de personas con experiencia y conocimiento en el tema, los cuales pueden evaluar la pertinencia, claridad y adecuación de las preguntas. La validación de experto se realiza mediante una matriz de validación, que contiene los criterios e indicadoresque se utilizarán para valorar cada pregunta. La matriz de validación es la siguiente:(ver Apéndice C)

| Criterio | Indicador | Valoración |

| Pertinencia | La pregunta se relaciona con el objetivo del estudio

| Claridad | La pregunta se expresa de forma sencilla y comprensible

| Adecuación | La pregunta tiene una sola respuesta correcta y las opciones de respuestason coherentes

| Criterio | Indicador | Valoración |

| Pertinencia | La pregunta se relaciona con el objetivo del estudio

| Claridad | La pregunta se expresa de forma sencilla y comprensible

|Adecuación | La pregunta tiene una sola respuesta correcta y las opciones de respuestason coherentes

Fases de la investigación

La metodología XP (eXtremeProgramming) es una forma de desarrollar software basada en valores como la simplicidad, la comunicación, el feedback y el coraje. Las fases de la metodología XP son las siguientes:

Fase I

Diagnóstico de los métodos de control de acceso a sistemas informáticos: Esta

fase consisteen analizar los requisitos del cliente y elaborar las historias de usuario, que son descripciones breves de las funcionalidades que se quieren implementar en el sistema. También se evalúa la situación actual de la organización en cuanto a la seguridad de los datos, identificando los problemas y las oportunidades de mejora.

Objetivo Específico: Diagnosticar los métodos de control de acceso a sistemas informáticos.

Fase II

Identificación de los elementos funcionales y no funcionales de los sistemas de control de acceso a sistemas informáticos: Esta fase consiste en priorizar las historias de usuario y asignarlas a iteraciones, que son ciclos cortos de desarrollo. También se identifican y definen las necesidadesque debe cumplir el sistema, tanto desde el punto de vista funcional (lo que hace el sistema) comono funcional (cómo lo hace el sistema).

Objetivo específico: identificar los elementos funcionales y no funcionales de los sistemas de control de acceso a sistemas informáticos.

Fase III

Diseño de un sistema de acceso por reconocimiento facial para sistemas informáticos empleando la metodología XP: Esta fase consiste en desarrollar el software siguiendo los principios y las prácticas de la metodología XP, que se basa en la comunicación, la simplicidad, laretroalimentación y el coraje. La metodología XP utiliza técnicas como el desarrollo guiado por pruebas, la integración continua, el diseño simple, la refactorización, la programación en parejas, la propiedad colectiva del código, los estándares de codificación, el ritmo sostenible y las metáforas.

Objetivo Específico: Diseñar un sistema de acceso por reconocimiento facial parasistemas informáticos empleando la metodología XP

Cuadro 1 Técnico Metodológico

OBJETIVO GENERAL	Desarrollar un sistema para el acceso por medio de un dispositivo de reconocimiento facial para sistemas informáticos.				
OBJETIVO ESPECÍFICO 1	**VARIABLES**	**DEFINICIÓN**	**INDICADORES**	**ÍTEMS**	**FUENTE DE INFORMACIÓN**
1. Diagnosticar los métodos de control de acceso a sistemas informáticos 2. Identificar los elementos funcionales y no funcionales de los sistemas de control de accesoa sistemas informáticos	**Sistema de acceso a datos**	El sistema de control de acceso es un mecanismoque utiliza la informática para autenticar o identificar a un usuario y permitirle acceder a información o a un lugar específico. Es una medida de seguridad que utiliza medios informáticos para proteger la información y los recursos	• Método de acceso a información • Elementos funcionales y no funcionales • Sistema informático	1,2,3,4,5,6	Técnica De Entrevista Instrumento Guía de Preguntas
3. Diseñar un sistema de acceso por reconocimiento facialpara sistemas informáticos empleando la metodología XP	**Autenticació n a través de un dispositivo de reconocimien to facial**	La autenticación es el proceso de verificar la identidad de un usuario o dispositivo. Si la información es correcta, el usuario se autentica y se le permite acceder al sistema. La autenticación se basa en uno o más factores, como algo que el usuario sabe o algo que el usuario es **(un rostro)**.	• Identidad del usuario • Accesoal sistema • Reconocimiento facial	1,2,3,4,5,6	Técnica de Observación Instrumento Lista de Cotejo

Fuente: Jhorver Chirinos

CAPÍTULO IV

ANALISÍS DE INTERPRETACION DE LOS RESULTADOS.

Se evaluaron las diferentes fases de la investigación con la utilización de la metodología XP Extreme Programming para verificar la efectividad del sistema de acceso por medio de un dispositivo de reconocimiento facial para sistemas informáticos propuesto. Dichas faces se conformaron por el diagnóstico, planificación, diseño, desarrollo y pruebas, las cuales permitieron el óptimo desarrollo del sistema.

Fase I Diagnóstico: Realización de encuesta

Para el diagnóstico de los métodos de control de acceso a sistemas informáticos, se utilizó los instrumentos correspondientes para aplicar las diferentes técnicas de recolección de datos, analizar los requisitos del cliente y elaborar las historias de usuario, que fueron descripciones breves de las funcionalidades implementar en el sistema. También se evaluó la situación actual de la organización en cuanto a la seguridad de los datos, identificando los problemas y las oportunidades de mejora para el análisis respectivo de los datos.

Análisis de la encuesta:

Muestra: 6 empleados

Guía de preguntas: 6 preguntas

Pregunta 1: ¿Utiliza un método de control para el acceso a los datos?

Pregunta 2: ¿El método para el resguardo que utiliza actualmente garantiza la confidencialidad de los datos?

Pregunta 3: ¿Aplican medidas técnicas, organizativas y jurídicas que eviten elacceso no autorizado, la alteración, la pérdida o el uso indebido de la información?

Pregunta 4: ¿La organización necesita mejorar las herramientas para el acceso a la información?

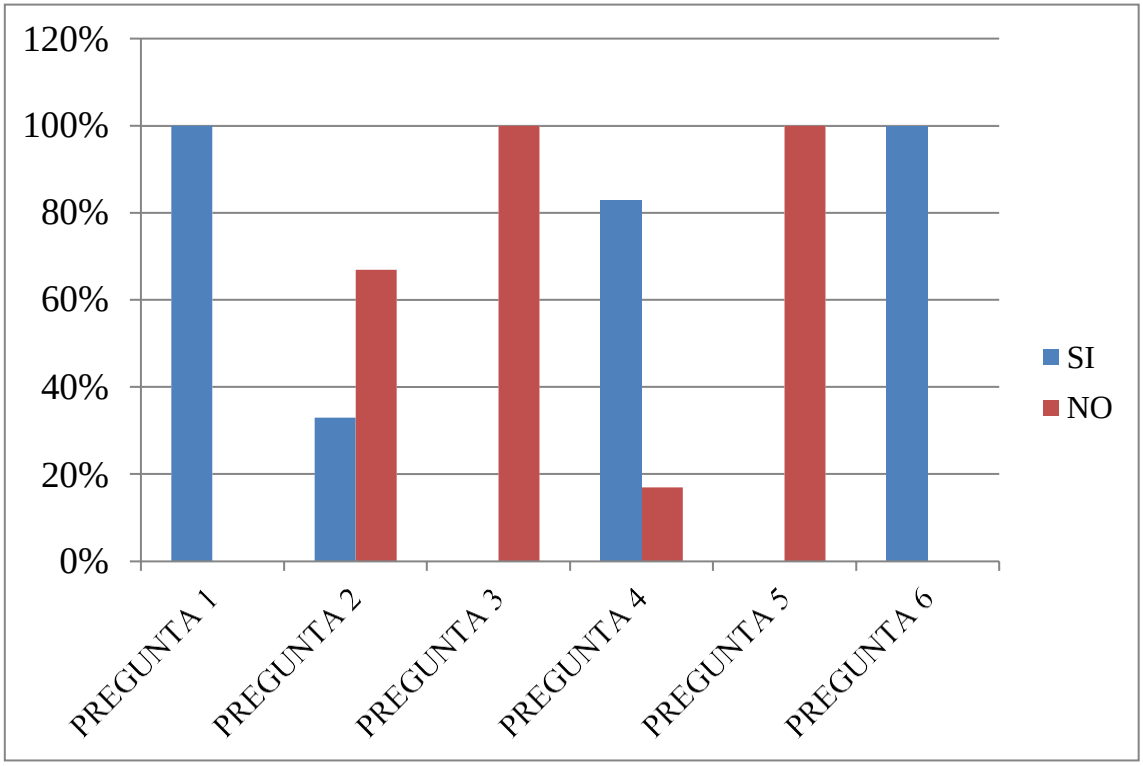
Pregunta 5: ¿El nivel de satisfacción, el rendimiento y el impacto de las herramientas existentes, las consideras óptimas para el funcionamiento

de la empresa?

Pregunta 6: ¿Considera Factible el uso de un sistema de reconocimiento facial para garantizar la confidencialidad de los datos?

Pregunta	1		2		3		4		5		6	
Muestra	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO
1	X		X			X	X		X		X	
2	X			X		X	X		X		X	
3	X			X		X	X		X		X	
4	X		X			X	X		X		X	
5	X			X		X		X	X		X	
6	X			X		X	X		X		X	
Total	6	0	2	4	0	6	5	1	6	0	6	0
%	100%	0%	33%	67%	0%	100%	83%	17%	100%	0%	100%	0%

Resultados del Diagnóstico de la guía de encuesta



Análisis de resultados del diagnostico de la guía de encuesta.

Pregunta 1: El 100% de la muestra indicó que si utilizan un método de control para el acceso a datos.

Pregunta 2: El 33% de la muestra indica que si utiliza actualmente un método de resguardo de información, y un 67% indicó que no se utiliza.

Pregunta 3: El 100% de la muestra indicó que no utilizan medidas organizativas y jurídicas que eviten elacceso no autorizado, la alteración, la pérdida o el uso indebido dela información.

Pregunta 4: Un 83% de la muestra dijo que la organización si necesita mejorar las herramientas para el acceso a la información y un 17% dijo que no.

Pregunta 5: El 100% de la muestra indicó que no es satisfactorio, el rendimiento yel impacto de las herramientas existentes.

Pregunta 6: El 100% de la muestra indicó que si considera factible el uso de un sistema de reconocimiento facial para garantizar la confidencialidad de los datos.

Analizando los resultados, se puede observar que la organización IAM TECNOLOGÍA, necesita mejorar las herramientas para el acceso a la información y que el uso de un sistema de reconocimiento facial es factible para garantizar la confidencialidad de los datos. Además, se evidencia que el método para el resguardo que utiliza actualmente no garantiza la confidencialidad de los datos y que no se aplican medidas técnicas, organizativas y jurídicas que eviten el acceso no autorizado, la alteración, la pérdida o el uso indebido de la información. Por último, se concluye que el nivel de satisfacción, el rendimiento y el impacto de las herramientas existentes no son óptimos para el funcionamiento de la empresa. A continuación se presentan los resultados obtenidos con la aplicación de la guía de preguntas a los empleados de IAM Tecnología.

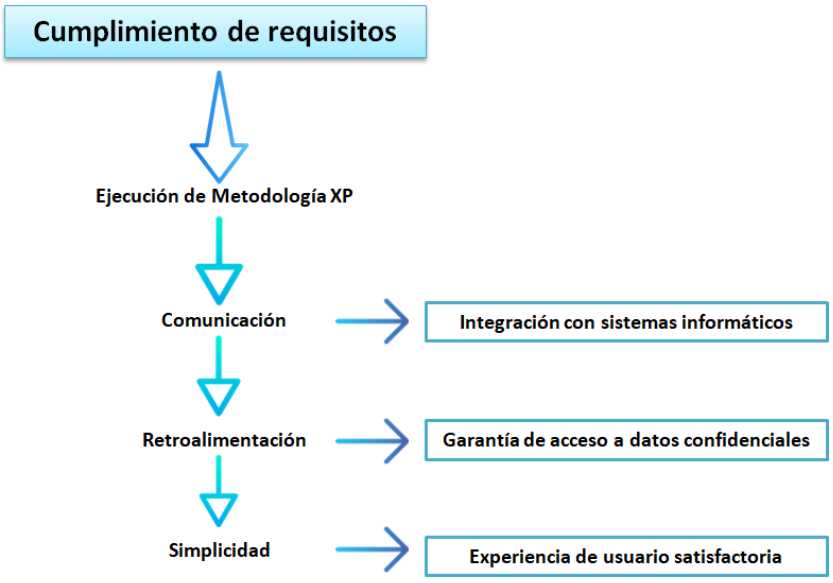
Fase II Planificación: Identificación de los elementos funcionales y no funcionales

En la fase de identificación de los elementos funcionales y no funcionales de los sistemas de control de acceso a sistemas informáticos, realizada a través de la lista de cotejo (4.4.2.4 Lista de cotejo), se priorizaron las historias de usuario y se asignaron a iteraciones, que son ciclos cortos de

desarrollo. Además, se identificaron y definieron las necesidades que debía cumplir el sistema, tanto desde el punto de vista funcional (lo que hace el sistema) como no funcional (cómo lo hace el sistema).

- **Elementos funcionales:**
  1. Registro de usuario
  2. Autenticación
  3. Interfaz gráfica
- **Elementos no funcionales**
  1. Seguridad
  2. Rendimiento
  3. Usabilidad
  4. Accesibilidad

Gráfica de cumplimiento de la metodología XP



Fase III Diseño: Desarrollo del sistema

El software del sistema de acceso por reconocimiento facial para sistemas informáticos se desarrolló siguiendo los principios y las prácticas de la metodología XP, la cual se basa en la comunicación, la simplicidad, la retroalimentación y el coraje. La metodología XP utiliza técnicas como el desarrollo guiado por pruebas, la integración continua, el diseño simple, la refactorización, la programación en parejas, la propiedad colectiva del código, los estándares de codificación, el ritmo sostenible y las metáforas.

En esta fase se presentó el desarrollo de un sistema de reconocimiento facial parael acceso a información privada, se utilizó Python y diversas librerías para la creación del modulo de reconocimiento facial, el cual consta de dos programas independientes: uno para el registro (REGISTRO_ID) y otro para el inicio de sesión (LOGIN_ID). Ambos programas necesitan de una carpeta llamada DataBase, la cual tiene una carpeta llamada faces, donde el programa de registro almacena la imagen del rostro identificada con el nombre del usuario, y en una base de datos Access se almacena la información del usuario (nombre, usuario de acceso, contraseña). El programa de inicio de sesión verificó la identidad del usuario mediante el reconocimiento facial, y permitió acceder a los datos confidenciales y la autenticación fue exitosa. Para el desarrollo del sistema se utilizaron las siguientes librerías: opencv, mediapipe, face-recognition, tkinter y librerías condicionales. Estas librerías facilitan el procesamiento de imágenes, la detección y el reconocimiento de rostros, y la creación de interfaces gráficas y el manejo de condiciones lógicas. El sistema para validar se realizó con una persona la que estaba al frente de la pantalla requería un pestañeo del usuario validó el registro y se dio inicio a la sesión.

Para la creación del entorno donde se almacenaba la información se utilizó Visual Basic Su simplicidad de uso con Windows permitió la creación de una interfaz que leyó la base de datos de la información del usuario,

validó la autenticación y permitió encriptar los archivos almacenados dentro del sistema para una mayor seguridad, a esta parte se le llamó “Interfaz de Usuario”.

Base de datos

La base de datos se compuso por 3 tablas: DOC tabla donde se almacenó la información del usuario (archivos y documentos), en la tabla Usuarios, se generó el ID de cada usuario, además de que se guardó los datos del mismo (nombre, usuario de acceso, contraseña).

Tabla DOC: Las tabla de archivos tiene los siguientes Atributos:

- **ID:** Número entero autonumerico que identifica de forma única cada archivo.
- **USUARIO:** Nombre del usuario que ha subido el archivo.
- **NOMBRE:** Nombre del archivo original definido por el usuario.
- **FECHA:** Fecha en la que se subió el archivo.
- **ARCHIVO:** Tipo de archivo (binario largo).
- **RUTA:** Ruta completa donde se encuentra almacenado el archivo en el servidor.
- **NOMBRE_AI:** Nombre generado por el sistema para el archivo.
- **Tabla USUARIO:**
- **ID:** Número entero autonumerico que identifica de forma única cada usuario.
- **USUARIO:** Nombre de usuario único para acceder al sistema.
- **CLAVE:** Contraseña del usuario.
- **Tabla ACTIVADO_COL:**
- **ID:** Número entero autonumerico que identifica de forma única cada registro.
- **USUARIO:** Nombre del usuario al que se aplica la configuración.
- **ACTIVADO:** Nombre de la columna que indica que usuario esta activado.

Proceso de registro biométrico

El proceso se registró y gestionó la identidad de las personas utilizando la tecnología de reconocimiento facial para identificar y verificar a las personas, con las siguientes funciones principales:

- **Registro de primer usuario:** Si la base de datos no tiene usuarios, el programa permitió la creación de un usuario máster, el cual dio acceso a la creación de nuevos usuario. Capturando su imagen facial y los datos de acceso (nombre, usuario de acceso, contraseña) almacenándola en una base de datos.
- **Registro de usuarios:** El programa permitió registrar a los usuarios, capturando su imagen facial y los datos del cliente (nombre, usuario de acceso, contraseña) almacenándola en una base de datos.
- **Verificación de identidad:** El programa verificó la identidad de las personas comparando su imagen facial con las imágenes almacenadas en la base de datos, si no existe, procede a crear el registro del nuevo usuario.
- **Control de acceso:** A los usuarios registrados en la base de datos, se les permitió acceder exclusivamente a los archivos de su perfil.

Diseño del registro biométrico:

Interfaz gráfica:

El programa contó con una interfaz gráfica sencilla que permitió al usuario registrarse e iniciar sesión en el sistema. La interfaz gráfica estuvó desarrollada con la librería Tkinter y presenta los siguientes elementos:

Formulario de registro: El formulario de registro solicitó de que él usuario que ingrese su nombre, usuario y contraseña. Estos datos se validan para garantizar que sean correctos y seguros.

Botón de registro: El botón de registro guardó los datos del usuario en a base de datos y la imagen facial del usuario en la subcarpeta "Faces".

Captura de imagen facial

El programa utilizó la librería OpenCV para capturar la imagen facial del usuario.

La captura de la imagen facial se realizó en tiempo real y se muestró en la interfaz gráfica. El programa utilizó una serie de técnicas para mejorar la calidad de la imagen facial capturada, como:

Corrección de la iluminación: Se ajustó la iluminación de la imagen facial paraque sea uniforme.

Normalización del tamaño: Se normalizó el tamaño de la imagen facial para que fuese compatible con el algoritmo de reconocimiento facial.

Segmentación de la cara: Se segmentó la cara del resto de la imagen para mejorar la precisión de la extracción de características faciales.

Extracción de características faciales

El programa utilizó la librería dlib para extraer características faciales de la imagen facial del usuario. Las características faciales fueron puntos clave faciales que se encontraron en lugares específicos del rostro, como los ojos, la nariz, la boca, etc.

Codificación de la imagen facial

El programa utilizó la librería face_recognition para codificar la imagen facial del usuario en un vector de características. Este vector de características es una representación matemática de la imagen facial del usuario.

Comparación de imágenes faciales

- **Algoritmo Cosine Similarity:** El algoritmo Cosine Similarity se utilizó para comparar dos vectores de características. El algoritmo calculó el coseno del ángulo entre los dos vectores. El coseno del ángulo es una medida de la similitud entre dos vectores. Cuanto más cercano sea el valor del coseno del ángulo a 1, más similares son los dos vectores. Hubo similitud entre el vector de características de la imagen facial del usuario y el vector de características almacenado en la base de datos fue mayor que un umbral predefinido, por lo tanto el usuario fue autenticado correctamente.

- **Umbral de similitud:** El valor del umbral de similitud determinó la similitud de un vector de características a otro para ser iguales. Un valor de umbral más bajo significó que los vectores de características deben ser más similares para que se consideren iguales. Un valor de umbral más alto significó que los vectores de características pueden ser menos similares para que se consideren iguales. El valor del umbral de similitud se elegió en función de la aplicación específica. En una aplicación de seguridad, se puede usar un valor de umbral bajo para garantizar un alto nivel de seguridad. En una aplicación de comparación de fotos, se puede usar un valor de umbral más alto para permitir una mayor flexibilidad.
- **Optimización del rendimiento: Para l**a comparación de imágenes faciales, a pesar de ser un proceso computacionalmente costoso, se utilizaron una serie de técnicas para optimizar el rendimiento del proceso de comparación,como:
- **Reducción de dimensionalidad:** Se pudo reducir la dimensionalidad de los vectores de características antes de compararlos. Esto redujo la cantidad de tiempo que se necesitó para calcular la similitud entre dos vectores de características.
- **Indexación de vecinos más cercanos:** Se utilizó un algoritmode indexación de vecinos más cercanos para encontrar los vectores de características más similares a un vector de características dado. Esto redujo la cantidad de tiempo que se necesitó para buscar el vector de características más similar a un vector de características dado.

Procedimiento del registro biométrico

El procedimiento del registro biométrico es el siguiente

1. El usuario introdujo sus datos (nombre, usuario, contraseña) en la interfazgráfica.
2. Se verificó si el usuario ya existe en la base de datos.
3. Si el usuario no existe, se registró en la base de datos y se

guardó su imagenfacial en la subcarpeta "Faces".

4. Se inició la captura de la imagen facial del usuario.
5. Se comparó la imagen facial del usuario con la información biométrica almacenada en la base de datos.
6. Si la comparación fue exitosa, se le dio acceso al usuario.
7. Si la comparación no fue exitosa, se le negó el acceso al usuario.

Proceso de inicio de sesión biométrico

El proceso de inicio de sesión biométrico comparó los datos recibidos por la cámara con los de la base de datos verificando si existe un usuario asociado a sus datos biométricos permitiendo a los usuarios iniciar sesión en un sistema utilizando su rostro. El programa utilizó las siguientes funciones:

- **Code_Face(images):** La función tomó una lista de imágenes en formato RGB como entrada y genera una matriz con los códigos de las imágenes como salida. En primer lugar, las imágenes se convirtieron a formato RGB si es necesario. A continuación, se utilizó la función face_recognition.face_encodings para

- codificar las imágenes. Finalmente, la función retornó a una matriz con los códigos de las imágenes.
- **Close_Windows2():** La función no tuvo entrada ni salida, y su objetivo fue cerrar la ventana actual. Esta función se utilizó tanto para la ventana de registro facial como para la ventana principal. El mecanismo que utilizó para cerrar la ventana es la función tkinter.Tk.destroy ().
- **Profile(UserName):** Esta función recibó el nombre de usuario como argumento y verifica el acceso al perfil del cliente en el sistema. Además, actualizó la base de datos para indicar que el usuario está activo.
- **Sign_Biometric():** Esta función capturó video en tiempo real, detectó rostros en el video y realizó el reconocimiento facial utilizando la matriz de códigos de las imágenes registradas. Si el reconocimiento facial es exitoso, llamó a la función Profile para mostrar la información del usuario. La función utilizó la función opencv2.VideoCapture para capturar video en tiempo real. Luego, se utilizó la función face_recognition.face_locations para detectar rostros en el video. Finalmente, utilizó la función face_recognition.compare_faces para realizar el reconocimiento facial.
- **Sign():** Esta función abrió la ventana para el registro facial. Cargó las imágenes de los rostros registrados, creó la matriz de códigos de las imágenes registradas y llamó a la función Sign_Biometric para iniciar el reconocimientofacial. La función utilizó la función tkinter.Tk para abrir la
- ventana. Luego, utilizó la función tkinter. Finalmente, llamó a la función Sign_Biometric para iniciar el reconocimiento facial.

Flujo del programa:

El programa de inicio de sesión se realizó a través de las siguientes fases

Apertura del Programa: Al ejecutar el programa, se muestró la ventana principal en la pantalla.

1. **Reconocimiento Facial:** Se inició el proceso de captura de video en tiempo real. La función Sign_Biometric() detectó los rostros en el video y los comparó con la matriz de códigos que almacena las características faciales de los usuarios registrados. Al coincidir el rostro con alguno de los códigos, se llamó a la función Profile.

2. **Activación de usuario:** Una vez que el sistema de reconocimiento facial confirmó la identidad del usuario, se generó un registro de usuario activo enla base de datos que indicó la hora y fecha de inicio de sesión.

Interfaz de Usuario

La interfaz de usuario desarrollada en visual basic, permitió gestionar información privada de diferentes usuarios mediante el reconocimiento facial. Para ello, se utilizó el programa para inicio de sesión biométrico (LOGIN_ID), que se ejecutó al iniciar la interfaz y realizó la identificación biométrica de forma rápida y segura. Si el usuario es el administrador, pudo acceder a un botón de registro que cerró el programa de inicio de sesión y abrió el programa de registro biométrico (REGISTRO_ID) para liberar la cámara, que permitió registrar nuevos usuarios con sus datos faciales, en caso de no existir usuarios anteriormente, el botón de registro quedó habilitado para registrar al usuario máster el cual permitió el registro de nuevos usuarios. La interfaz de usuario consta de tres formularios, siendo el primero FrmLogin, que se encargó de conectar los programas de reconocimiento facial y facilitó el acceso o el registro de los usuarios al sistema. El segundo formulario es Form1 encargado de mostrar los archivos privadosdel usuario, permitió la modificación, y adición de nuevos archivos y el último form2 el cual se es un subformulario donde se ejecutó la función de modificar de form1.

Formulario de inicio de sesión FrmLogin

Para acceder a la aplicación, los usuarios iniciaron sesión de las dos formas posibles: mediante reconocimiento facial y mediante usuario y contraseña. La autenticación por reconocimiento facial proviene de LOGIN_ID para identificar a los usuarios. El rostro capturado coincidió con alguno de los rostros registrados, el programa LOGIN_ID permitió el acceso a la aplicación. La aplicación verificó que la información ingresada era correcta y coincidió con la información almacenada en la basede datos y verificó que el usuario se activo a través de LOGIN_ID. Si la información ingresada fue correcta, la aplicación permitió el acceso. Una vez que el usuario inició sesión exitosamente, se muestró el formulario Form1 que contiene la información privada del usuario (figura2 esquema de FrmLogin). El programa también utilizó las siguientes funcionalidades:

- **Mostrar información personal:** Esta funcionalidad mostró en la parte superior del formulario los datos personales del usuario, tales como su imagen, nombre, fecha de nacimiento, nacionalidad, ocupación Y última conexión. Estos datos se obtuvieron de la base de datos donde se almacenan la información de los usuarios registrados (figura1, interfaz de usuario formulario para el inicio de sesión).
- **Modificar información personal:** Esta funcionalidad permitió al usuario modificar algunos de sus datos personales, como la fecha de nacimiento, la nacionalidad y la ocupación. Al hacerlo, se habilitaron los campos correspondientes para que el usuario pueda editarlos. Una vez que el usuario ha introducido los cambios deseados, presionando la tecla “enter” se modificaron los valores.

- **Modificar imagen de Usuario:** Después del inicio de sesión, permitió modificar la imagen de la cuenta, es un aspecto visual que añadió confort al uso del sistema,debido a que permitió personalizar la experiencia.

Figura1: interfaz de usuario formulario para el inicio de sesión

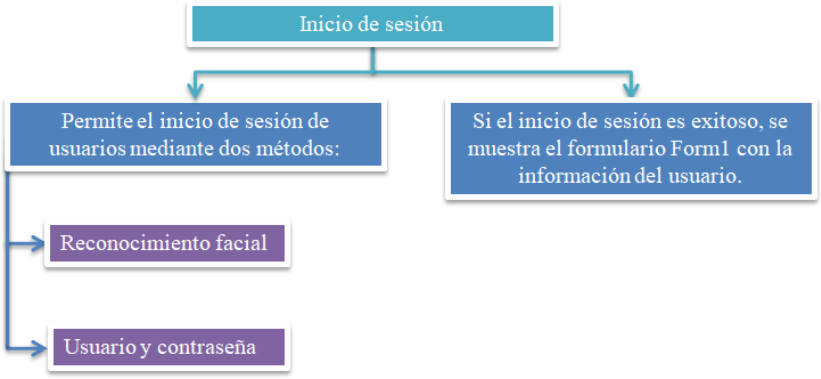


Figura 2: Esquema formulario para el inicio de sesión

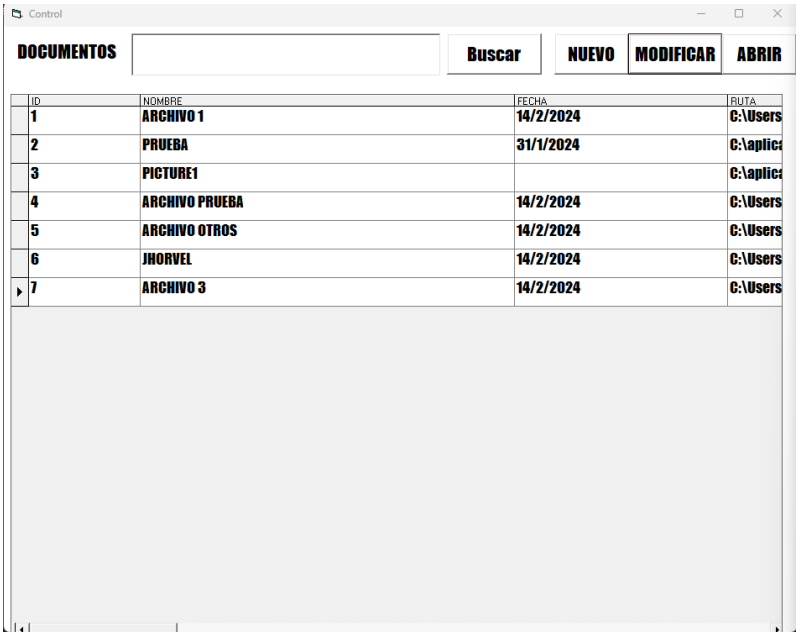
Formulario de archivos confidenciales

El formulario Form1 es un componente de la aplicación que permitió al usuario gestionar su información personal y sus archivos privados. A continuación se describen las funcionalidades que ofreció este formulario (figura 3. Interfaz de archivos confidenciales):

- **Abrir archivos privados:** Esta funcionalidad permitió al usuario abrir uno de sus archivos privados usando la aplicación predeterminada del sistema para ese tipo de archivo. Cada archivo tiene un nombre, una fecha y una ruta que indicó dónde se mostró el archivo, luego al cerrar la vista del archivo, el programa eliminó el archivo de la ruta donde se había cargado (figura 4. Abrir archivo).
- **Agregar archivos privados:** Esta funcionalidad permitió al usuario agregar nuevos archivos privados a su lista al presionar el botón de nuevo, donde ejecutó el form2 permitiendo elegir el nombre del archivo, luego al presionar aceptar mostró una ventana de Windows para buscar el archivo que se quería cargar. Al hacerlo, se abrió un explorador de archivos para que el usuario pueda seleccionar el archivo que deseaba subir. Una vez que el usuario seleccionó el archivo, hizo clic en el botón "Abrir" e inició la subida del archivo al servidor. El contenido del archivo se guardó en la base de datos y se añadió a la lista con su nombre, fecha y ruta (Figura 5. Agregar archivo, Figura 6 ventana de windows).
- **Modificar archivos privados:** Esta funcionalidad permitió al usuario modificar el nombre de uno de sus archivos privados. Para ello, el usuario debe hacer clic en el botón "Modificar". Al hacerlo, se abrió el formulario Form2, que es un cuadro de

diálogo que solicita al usuario introducir el nuevo nombre del archivo.El nombre debe ser único y no debe contener caracteres especiales. Una vez que el usuario introdujo el nuevo nombre, hizo clic en el botón "Aceptar" y se actualizó el nombre del archivo en la base de datos abriendo una ventana de windows donde permitió buscar otro archivo (figura 7. Modificar archivo).

Figura 3: Interfaz de archivos confidenciales



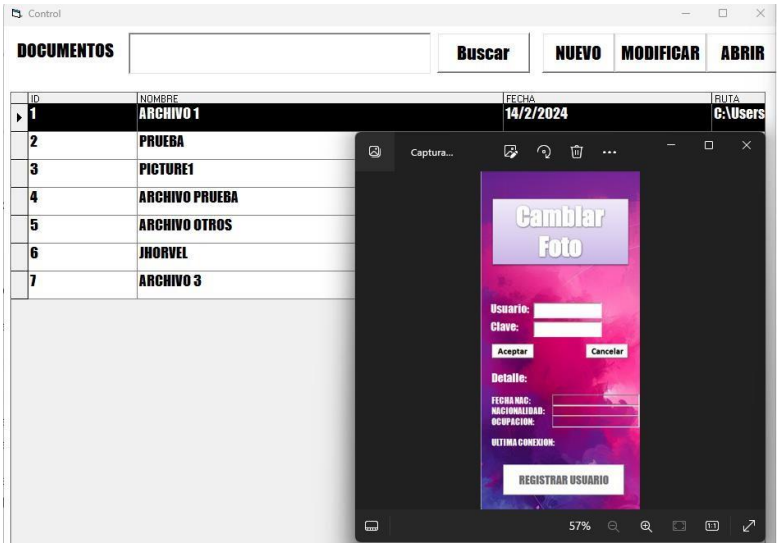


Figura 4: Abrir archivo.

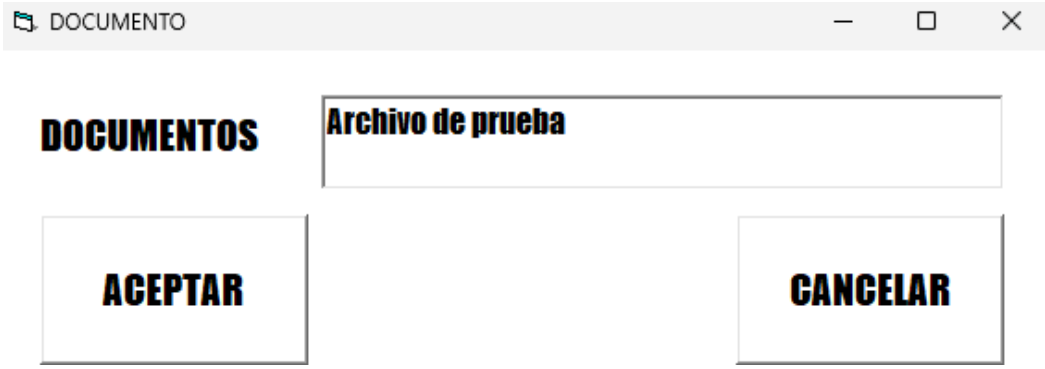


Figura 5. Agregar archivo

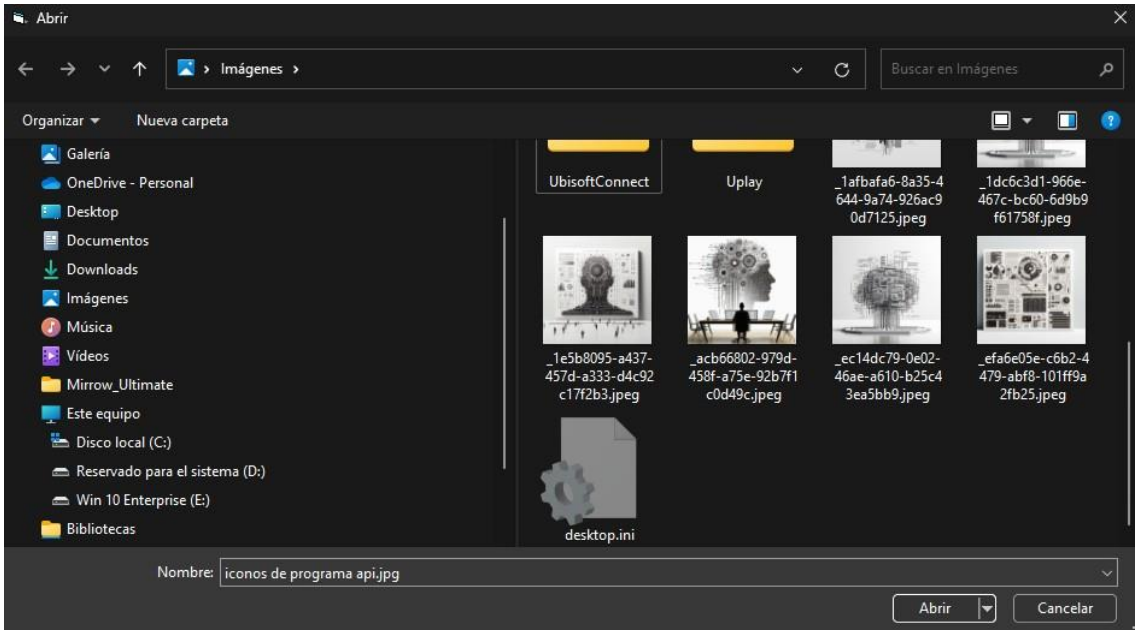


Figura 6: Ventana de Windows

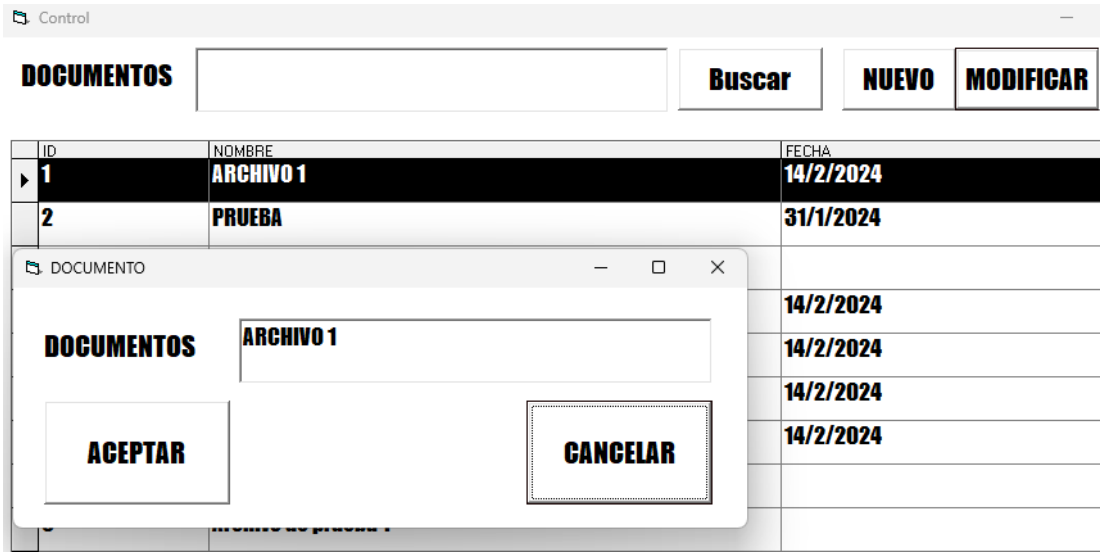


Figura 7. Modificar archivo

Fase IV Análisis de resultados

En esta fase se analizaron e interpretaron los datos obtenidos de la investigación, se aplicó una matriz FODA para medir la efectividad del sistema de acceso por reconocimiento facial para sistemas informáticos; consiste en analizar e interpretar los resultados con criterios objetivos y rigurosos.

Análisis FODA del sistema de acceso por reconocimiento facial aplicada a la empresa IAM TECNOLOGIA:

- **Seguridad:** El sistema de reconocimiento facial ofreció una mayor seguridad que los métodos tradicionales utilizados para el control de acceso.
- **Eficiencia:** El sistema de reconocimiento facial resultó ser rápido y eficiente. Los usuarios pueden acceder a la información de forma rápida y sencilla.
- **Comodidad:** El sistema de reconocimiento facial fue cómodo para los usuarios.

Oportunidades:

- **Integración con otros sistemas:** El sistema de reconocimiento facial se pudo integrar con otros sistemas, como sistemas de seguridad o sistemas de control de acceso. Esto mejoró la seguridad y la eficiencia de la organización.
- **Personalización:** El sistema de reconocimiento facial se pudo personalizar para satisfacer las necesidades específicas de la organización. Esto significó que la empresa pudo elegir las características y funcionalidades que mejor se adapten a sus necesidades.

Debilidades:

- **Precisión:** La precisión del sistema de reconocimiento facial pudo verse afectada por una serie de factores, como la

iluminación, el ángulo de la cámara ylas expresiones faciales.

- **Sesgo:** Los sistemas de reconocimiento facial pueden ser sesgados, lo que significa que pueden tener más dificultades para identificar a personas.

Amenazas:

- **Competencia:** La competencia en el mercado de sistemas de reconocimiento facial es intensa. La competitividad se dará en términos de precio, calidad y servicio.
- **Avances tecnológicos:** Los avances en la tecnología de reconocimiento facial debe estar preparadas para actualizar sus sistemas con regularidad.

Pruebas unitarias, de integración y de aceptación

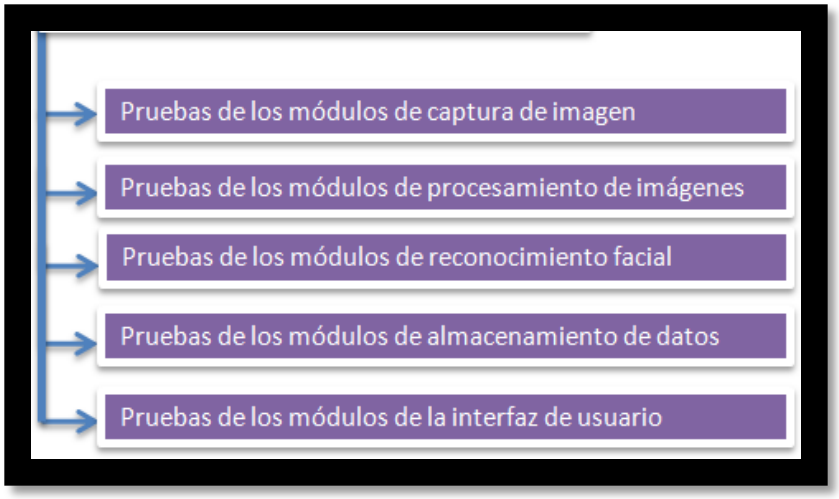
4.4.2.1Pruebas de Caja Negra

En la prueba realizada con respecto a la caja negra, se centró en la captura de la imagen, procesamiento de imágenes, reconocimiento facial, interfaz del usuario, almacenamiento de datos

Objetivo: Evaluar el funcionamiento de cada módulo del sistema de forma individual.

Metodología:

- Se diseñaron casos de prueba para cada unidad funcional del sistema.
- Se verificaron los resultados de las pruebas para asegurar que



cada unidadfuncione según lo esperado.

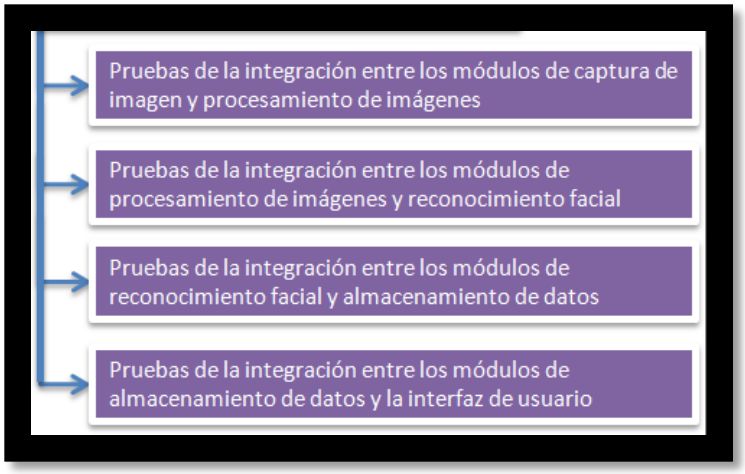
Pruebas de Caja Blanca:

Los pasos tomados fueron la selección de las pruebas de integración entre módulos de captura y procesamiento de imágenes, reconocimiento facial con procesamiento de imagen; reconocimiento facial con almacenamiento de datos; interfaz de usuario con almacenamiento de datos. Esto con relación a la interacción de los módulos del sistema.

Objetivo: Evaluar la interacción entre los diferentes módulos del sistema.

Metodología:

- Se diseñaron casos de prueba para evaluar la interacción entre diferentesmódulos del sistema.
- Se verificaron los resultados de las pruebas para asegurar que los diferentesmódulos del sistema se integran correctamente.

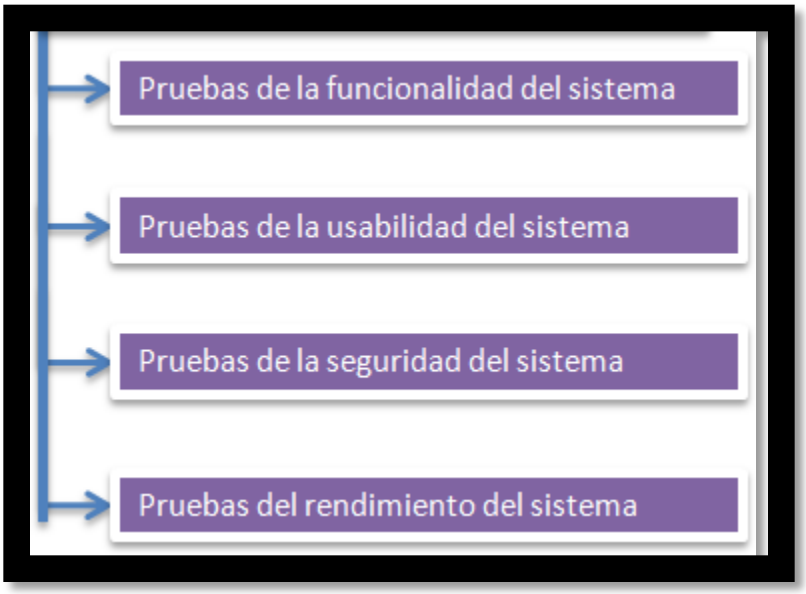


Los pasos tomados para la evaluación del sistema a la comprobación de los requisitos de los usuarios fueron casos de prueba: en base a los requisitos de los usuarios finales; pruebas de grupo de usuarios finales de aceptación y verificación de los resultados de las pruebas

Objetivo: Evaluar si el sistema cumple con los requisitos de los usuarios finales.

Metodología:

- Se diseñaron casos de prueba en base a los requisitos de los usuarios finales.
- Se ejecutaron las pruebas con un grupo de usuarios finales de aceptación.
- Se verificaron los resultados de las pruebas para asegurar que el sistema cumplecon los requisitos de los usuarios finales.



Lista de cotejo: Análisis de resultados

N#	LISTA DE COTEJO	SI	NO
1	¿El sistema de reconocimiento facial cumple con los requisitos funcionales y no funcionales especificados por el cliente?	✓	
2	¿Los criterios e indicadores establecidos para el desarrollo del sistema de reconocimiento facial son factibles?	✓	
3	¿El sistema de reconocimiento facial se ha integrado correctamente con los sistemas informáticos a los que da acceso, sin causar conflictos ni errores?	✓	
4	¿El sistema de reconocimiento facial respeta los principios y prácticas de la metodología XP, tales como la comunicación, la simplicidad, la retroalimentación y el coraje?	✓	
5	¿El sistema de reconocimiento facial garantiza con los criterios e indicadores establecidos sobre el acceso a datos confidenciales?	✓	
6	¿El sistema de reconocimiento facial ofrece una experiencia de usuario satisfactoria, tanto en términos de velocidad como de precisión?	✓	

Item 1: El sistema de reconocimiento facial cumple con los requisitos funcionales y no funcionales especificados por el cliente, evidenciado a través de los siguientes pasos.

- **Análisis de la lista de cotejo:** El sistema de reconocimiento facial cumplió con todos los criterios e indicadores establecidos para su desarrollo.
- **Integración con otros sistemas:** El sistema se integró correctamente conlos sistemas informáticos a los que da acceso, sin causar conflictos ni errores.
- **Metodología XP:** El sistema se desarrolló siguiendo los principios y prácticas de la metodología XP, tales como la comunicación, la simplicidad, la retroalimentación y el coraje.
- **Seguridad y privacidad:** El sistema garantiza la seguridad y privacidad de los datos confidenciales.

El análisis de los resultados de la lista de cotejo, junto con la evidencia de la integración con otros sistemas, la metodología XP, la seguridad y privacidad, y la experiencia de usuario**,** confirmaron que el

sistema de reconocimiento facial cumple con los requisitos establecidos por el cliente.

Item 2: los criterios e indicadores establecidos para el desarrollo del sistema de reconocimiento facial son factibles. El análisis de la lista de cotejo arrojó resultados positivos en todos los aspectos relevantes:

- **Acceso a datos:** El sistema protege los datos confidenciales según los criterios establecidos.
- **Experiencia de usuario:** La velocidad y precisión del sistema fue satisfactoria.

En conjunto, estos resultados confirman que los criterios e indicadores establecidos para el desarrollo del sistema de reconocimiento facial son factibles y se han cumplido satisfactoriamente.

Item 3: el sistema de reconocimiento facial se integró correctamente con los sistemas informáticos a los que da acceso, sin causar conflictos ni errores.

- **Ausencia de conflictos y errores:** No se encontraron errores o conflictosdurante la integración del sistema de reconocimiento facial con los demássistemas.

En base a la evidencia disponible, se pudo concluir, con un alto grado de confianza, que el sistema de reconocimiento facial se ha integrado correctamente con los sistemas informáticos a los que da acceso, sin causar conflictos ni errores.

Item 4: el sistema de reconocimiento facial respetó los principios y prácticas de lametodología XP.

- **Comunicación:** la integración exitosa con otros sistemas

informáticos demuestró una comunicación efectiva entre los diferentes componentes delproyecto.

- **Respecto a la simplicidad**: el diseño del sistema se centró en la facilidad deuso, tanto para los desarrolladores como para los usuarios finales.
- **Retroalimentación:** Los resultados de la lista de cotejo, junto con las pruebas yla evaluación de la experiencia de usuario, proporcionaron información valiosa para la mejora continua del sistema.
- **Coraje:** La metodología XP permitió al equipo tomar decisiones rápidas yasumir riesgos calculados para alcanzar los objetivos del proyecto.

El sistema de reconocimiento facial se ajustó a los principios y prácticas de la metodología XP, lo que se traduce en un proyecto bien planificado, desarrollado y evaluado, con un alto grado de satisfacción para el cliente.

Item 5: El sistema de reconocimiento facial cumplió con los criterios e indicadoresestablecidos para el acceso a datos confidenciales ya que el sistema de reconocimiento facial se diseñó y desarrolló con la seguridad como una prioridad fundamental. Se implementaron medidas para proteger los datos confidenciales, siguiendo los criterios e indicadores establecidos. Se verificó que el sistema cumple con los requisitos funcionales y no funcionales, incluyendo la seguridad y la protección de datos confidenciales.

Item 6: El sistema de reconocimiento facial ofreció una experiencia de usuario satisfactoria, tanto en términos de velocidad como de precisión.

- **Cumplimiento de requisitos:** El sistema cumplió con los requisitosfuncionales y no funcionales especificados por el cliente.
- **Integración exitosa:** Se integró correctamente con los sistemas informáticosexistentes sin causar problemas.
- **Metodología XP:** Se desarrolló siguiendo los principios de la metodologíaXP, lo que asegura una buena experiencia de usuario.
- **Acceso a datos confidenciales:** Cumplió con los criterios de seguridad parael acceso a datos confidenciales.
- **Velocidad y precisión:** Ofreció una experiencia de usuario rápida y precisa.

En el análisis de los resultados de la lista de cotejo, se pudo observar que el sistema de reconocimiento facial cumplió con los requisitos funcionales y no funcionales especificados por el cliente, y que los criterios e indicadores establecidos para el desarrollo del sistema son factibles. Además, se evidenció que el sistema de reconocimiento facial se integra correctamente con los sistemas informáticos a los que da acceso, sin causar conflictos ni errores. También se concluyó que el sistema de reconocimiento facial respeta los principios y prácticas de la metodología XP, tales como la comunicación, la simplicidad, la retroalimentación y el coraje. Por último, se puede afirmar que el sistema de reconocimiento facial garantizó su efectividad con los criterios e indicadores establecidos sobre el acceso a datos confidenciales y ofreciendo una experiencia de usuario satisfactoria, tanto en términos de velocidad como de precisión.

CONCLUSIONES Y RECOMENDACIONES

Como resultado del proyecto se presentan las siguientes conclusiones y recomendaciones del sistema de reconocimiento facial, el cual logró desarrollar una aplicación de reconocimiento facial que cumplió con todos los requisitos funcionales y no funcionales planteados. Mediante la metodología XP,se pudo crear un software flexible y adaptable a los cambios, capaz de reconocer las identidades de los usuarios y proteger sus archivos de forma eficiente y confiable. Además, la herramienta garantizó la seguridad y privacidad de los datos de los usuarios, y ofreció una experiencia de usuario satisfactoria, con una interfaz amigable y fácil de usar.

Conclusiones:

- El sistema de reconocimiento facial cumple con todos los requisitos funcionales y nofuncionales especificados por el cliente.
- Los criterios e indicadores establecidos para el desarrollo del sistema son factibles y se hancumplido satisfactoriamente.
- El sistema se integró correctamente con los demás sistemas informáticos sin causar conflictos nierrores.
- Se respetaron los principios y prácticas de la metodología XP durante el desarrollo del sistema.
- El sistema cumple con los criterios de seguridad para el acceso a datos confidenciales.
- El sistema ofrece una experiencia de usuario satisfactoria en términos de velocidad y precisión.

Recomendaciones:

- Realizar pruebas de usuario con un grupo amplio y diverso para obtener comentarios ysugerencias sobre la experiencia de usuario.
- Documentar detalladamente el sistema para facilitar su mantenimiento y futuras mejoras.

- Considerar la implementación de medidas de seguridad adicionales para proteger los datosconfidenciales.
- Investigar y evaluar nuevas tecnologías de reconocimiento facial para mejorar el rendimientodel sistema.
- Planificar la expansión del sistema a otros departamentos o áreas de la organización.
- Es recomendable realizar un seguimiento continuo del rendimiento del sistema y realizar ajustesy mejoras según sea necesario.

REFERENCIAS

Onu (1948). declaración universal de los derechos humanos. parís: nacionesunidas.

Onu (1966). pacto internacional de derechos civiles y políticos. nueva york:naciones unidas.

Congreso nacional (1982). código civil. gaceta oficial n° 2.990 extraordinario del26/07/1982.

Onu (1988). convenio 108 del consejo de europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. estrasburgo: consejo de europa.

Asamblea nacional constituyente (1999). constitución de la república bolivariana de venezuela. gaceta oficial n° 36.860 del 30/12/1999.

Asamblea nacional (2000). ley orgánica de telecomunicaciones. gaceta oficial n° 37.013 del 12/06/2000.

Asamblea nacional (2001). ley especial contra los delitos informáticos. Gacetaoficial n° 37.313 del 30/10/2001.

Arias, f. (2006). el proyecto de investigación6ta edición. 2012 editorial episteme, c.a. república bolivariana de venezuela, caracas.

Asamblea nacional (2007). ley orgánica para la protección del niño, niña y adolescente. gaceta oficial n° 38.573 del 10/12/2007.

Arguello f h. (2021). Sistemas de re c o n o c i m i e n t o facia l basado en la imagen fa c i a l . universidad industrial de santander, facultad de ingenierías físico-mecánicas, colombia**.**

Hernández, Fernández, y Baptista (2014). Metodología de la investigación (6a ed.).

mcgraw-hill / interamericana editores.

García, a. (2018). la protección de datos personales en el derecho internacional y europeo.madrid: tecnos.

Onu (2018). resolución 73/179 sobre el derecho a la privacidad en la era digital.nueva york: naciones unidas.

Martínez, j. (2020). seguridad de la información y protección de datos: aspectos jurídicos y técnicos.barcelona: uoc.

Raeburn, a. (2022). sitio web asana. la programación extrema (xp) produce resultados, pero ¿es la metodología adecuada para ti?

García, J. (2023). Ciberseguridad y gestión de riesgos. [Libro electrónico].

Editorial: Universidad de Granada.

Ibm. (2023). data security. ¿por qué es importante la seguridad de datos?

Miró, m. (2023, 16 de mayo). seguridad informática: qué es, tipos y características.

APENDICE

Apéndice A Instrumento de Recolección de Datos

REPUBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JOSE ANTONIO PAEZ FACULTAD DE INGENIERIA

ESCUELA DE COMPUTACION

EMPRESA: IAM TECNOLOGIA, C.A.

ENTREVISTADO: _____

INSTRUCCIONES PARA LA GUIA DE PREGUNTAS
• **Lea detenidamente cada pregunta.** • **Conteste con sí o no con una X en la casilla correspondiente.** • **Sea sincero en sus respuestas.** • **En caso de dudas, consulte con la persona encargada de la aplicación del cuestionario.**

N#	Guía de Preguntas	SI	NO
1	¿Utiliza un método de control para el acceso a los datos?		
2	¿El método para el resguardo que utiliza actualmente garantiza la confidencialidad de los datos?		
3	¿Aplican medidas técnicas, organizativas y jurídicas que eviten el acceso no autorizado, la alteración, la pérdida o el uso indebido de la información?		
4	¿La organización necesita mejorar las herramientas para el acceso a la información?		
5	¿El nivel de satisfacción, el rendimiento y el impacto de las herramientas existentes, las consideras óptimas para elfuncionamiento de la empresa?		
6	¿Considera Factible el uso de un sistema de reconocimiento facial para garantizar la confidencialidad de los datos?		

Apéndice B Instrumento de Recolección de Datos

REPUBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JOSE ANTONIO PAEZ FACULTAD DE INGENIERIA

ESCUELA DE COMPUTACION

EMPRESA: IAM TECNOLOGIA, C.A.

GERENTE/CLIENTE: Jonás Álvarez

INVESTIGADOR: Jhorver Chirinos

LISTA DE COTEJO PARA LA VERIFICACION DEL DESARROLLO DEL SISTEMA PARA EL ACCESO A LA INFORMACION POR MEDIO DE UN DISPOSITIVO DE RECONOCIMIENTO FACIAL.
Una lista de cotejo es un instrumento que facilita la evaluación del grado de cumplimiento de determinados criterios o indicadores en una actividad. En este caso, se elabora una lista de cotejo para comprobar el adecuado funcionamiento mediante la técnica de observación directa al sistema de reconocimiento facial, considerando los siguientes aspectos:

N#	LISTA DE COTEJO	SI	NO
1	**¿El sistema de reconocimiento facial cumple con los requisitos funcionales y no funcionales especificados por el cliente?**		
2	**¿Los criterios e indicadores establecidos para el desarrollo del sistema de reconocimiento facial son factibles?**		
3	**¿El sistema de reconocimiento facial se ha integrado correctamente con los sistemas informáticos a los que da acceso, Sin causar conflictos ni errores?**		
4	**¿El sistema de reconocimiento facial respeta los principios y Prácticas de la metodología XP, tales como la comunicación, la simplicidad, la retroalimentación y el coraje?**		
5	**¿El sistema de reconocimiento facial garantiza con los criterios e indicadores establecidos sobre el acceso a datos confidenciales?**		
6	**¿El sistema de reconocimiento facial ofrece una experiencia de usuario satisfactoria, tanto en términos de velocidad como de precisión?**		

FECHA:__/__/_____ _____ _____

Firma del Cliente **Firma del Investigador**

Apéndice C Instrumento de Recolección de Datos

REPUBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JOSE ANTONIO PAEZ FACULTAD DE INGENIERIA

ESCUELA DE COMPUTACION

ítems	Redacción de Ítems			Pertinencia de los objetivos		Observaciones
	Clara	Confusa	Tendenciosa	Pertinente	No Pertinente	
1						
2						
3						
4						
5						
6						

Fecha: ___/___/_____

_____

Firma del Especialista

Breve descripción del perfil académico del Especialista	