UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

TEMA:

Sistema de reconocimiento facial para el área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil.

AUTOR:

Gómez Huacho, Franklin Geovany

Trabajo de Integración Curricular previo a la obtención del título de

INGENIERO EN SISTEMAS COMPUTACIONALES

TUTOR:

Ing. Erazo Ayón, José Miguel, MBA

Guayaquil, Ecuador

16 de febrero del 2024

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

CERTIFICACIÓN

Certificamos que el presente trabajo de Integración Curricular, fue realizado en su totalidad por **Gómez Huacho, Franklin Geovany**, como requerimiento para la obtención del título de **Ingeniero en Sistemas Computacionales**.

TUTOR

f. _____
Ing. Erazo Ayón, José Miguel, MBA

Guayaquil, a los 16 días del mes de febrero del año 2024

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Gómez Huacho, Franklin Geovany**

DECLARO QUE:

El Trabajo de Integración Curricular: **Sistema de reconocimiento facial para el área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil,** previo a la obtención del título de **Ingeniero en Sistemas Computacionales**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Integración Curricular referido.

Guayaquil, a los 16 días del mes de febrero del año 2024

EL AUTOR

f. _____
Gómez Huacho, Franklin Geovany

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

AUTORIZACIÓN

Yo, **Gómez Huacho, Franklin Geovany**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Integración Curricular: **Sistema de reconocimiento facial para el área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 16 días del mes de febrero del año 2024

EL AUTOR:

f. _____
Gómez Huacho, Franklin Geovany

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERIA

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

REPORTE COMPILATIO

TUTOR

f. _____

Ing. José Miguel, Erazo Ayón, MBA.

Carrera de Ingeniería en Sistemas Computacionales

AGRADECIMIENTO

Primeramente, quiero expresar mi más sincero agradecimiento a Dios por mantenerme con buena salud y con vida a mis padres por su ayuda económica y luego a cada uno de los docentes por tener la paciencia en compartir sus conocimientos en el transcurso de los estudios que he venido preparándome y así poder haber contribuido al éxito de este proyecto.

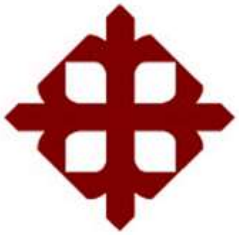
Agradezco profundamente el apoyo y la orientación de mi tutor, también quiero agradecer a todas las personas que participaron durante las entrevistas para lograr obtener resultados exitosos ya que sin su valiosa aportación este proyecto no habría sido posible. Por último, agradezco a mis amigos y familiares por su paciencia y ánimo durante este proceso.

El autor

DEDICATORIA

Dedico este proyecto a Dios y ah mis padres, por su amor incondicional, su constante apoyo y sacrificio para que pudiera alcanzar mis metas académicas. También quiero dedicar este trabajo a mis amigos, quienes siempre estuvieron presentes con palabras de aliento y momentos de distracción que me ayudaron a mantener el equilibrio durante este desafiante proceso. A todos ellos, gracias por ser mi fuente de inspiración y motivación.

El Autor



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

TRIBUNAL DE SUSTENTACIÓN

f. _____

Ing. Ana Isabel, Camacho Coronel, Mgs.

DIRECTORA (e) DE CARRERA

f. _____

Ing. Roberto García Sánchez, Mgs.

DOCENTE DE LA CARRERA

f. _____

Ing. Galo Enrique, Cornejo Gómez, Mgs.

OPONENTE

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El Diseño e implementación de una solución informática de reconocimiento facial para reforzar el nivel de acceso y seguridad en el área administrativa de la Facultad de Ingeniería de la UCSG, lleva las siguientes especificaciones: Revisar los recursos tecnológicos disponibles y utilizables para el diseño de un prototipo funcional de sistema de reconocimiento facial, determinar los requisitos de seguridad y acceso, desarrollar el prototipo para el control de seguridad y acceso, implementar el prototipo de reconocimiento facial en el área administrativa. se aplica el método cualitativo de la entrevista para dar aceptación e implementar el prototipo funcional. Previo a la implementación se diseñó la arquitectura de la solución que contiene servidores, un lector biométrico con reconocimiento facial, su software correspondiente y un componente para visualización de datos como Power BI.

Esta solución pretende facilitar al administrador una herramienta de control de accesos, a través de un cuadro de mando para fortalecer los procesos de seguridad física que se llevan en la Facultad de Ingeniería.

Palabras claves: *Reconocimiento Facial, Biométrico, Seguridad Física, Control de Acceso, Inteligencia de Negocios*

ABSTRACT

The design and implementation of a computerized facial recognition solution to enhance the level of access and security in the administrative area of the Faculty of Engineering at UCSG, entails the following specifications: Reviewing available and usable technological resources for designing a functional prototype of a facial recognition system, determining security and access requirements, developing the prototype for security and access control, implementing the facial recognition prototype in the administrative area. The qualitative interview method is applied to gain acceptance and implement the functional prototype. Prior to implementation, the solution architecture was designed, which includes servers, a biometric facial recognition reader, its corresponding software, and a component for data visualization such as Power BI.

This solution aims to provide administrators with an access control tool through a dashboard to strengthen the physical security processes carried out in the Faculty of Engineering.

Key words: *Facial Recognition, Biometric, Physical Security, Access Control, Business Intelligence*

INTRODUCCIÓN

La tecnología actual avanza de forma exponencial, cambiando de forma constante la calidad de vida de las personas y la forma como ésta se relaciona con su entorno. La innovación y surgimiento de nuevas herramientas ha permitido que el ser humano pueda vivir en sociedad de la forma más cómoda posible puesto que, por sus ventajas, puede acceder a conceptos que antes eran imposibles de conseguir. Acceso a la información, aprendizaje, comunicación inmediata, facilidad de realizar tareas, entre otras, son algunas de las propiedades de la tecnología que se encuentran al alcance de las personas para su uso (Santander Universidades, 2021). Esto implica la necesidad de estar a la vanguardia de los adelantos tecnológicos que se encuentran disponibles, ya que éstos se integran a las actividades diarias de las personas y de las organizaciones (Digixem 360, 2023).

El listado de tecnologías aumenta permanentemente. Inteligencia artificial (IA), aprendizaje automático (ML), internet de las cosas (IoT), robots, realidad aumentada, sistemas para control de acceso, comunicaciones entre máquinas, son tecnologías que tienen una evolución constante y pueden cambiar y mejorar la calidad de vida de las personas, y de los bienes y servicios que ofertan las empresas; su potencial permite la transformación de las organizaciones y, como se dijo, la vida de las personas (West, 2017).

Las aplicaciones de las herramientas tecnológicas que se encuentran disponibles para facilitar las actividades del ser humano, son innumerables. En educación, el uso de software para el aprendizaje, en salud, las herramientas para exámenes y diagnóstico de enfermedades, la biomedicina; en el tema de aplicaciones IoT se encuentran las oficinas inteligentes, sistemas para riego automatizados, recolección y adquisición de datos y desarrollo de software. En cuanto a las aplicaciones inteligentes se encuentra la lógica difusa, uso de redes neuronales para medición de temperatura, entre otras.

En el mismo contexto, en una sociedad impulosada por la tecnología y la información, un tema de importancia tanto para las personas como para las

organizaciones, es la seguridad, la misma que se ha convertido en un tema crítico. Es noticia diaria el nivel de inseguridad que actualmente se vive, sobre todo en Guayaquil, por lo que es tarea de todos los individuos buscar las mejores herramientas que resguarden su integridad; lo mismo sucede con las empresas, en las que la protección de la integridad de sus empleados y de la información que diariamente se genera, es de mucha importancia, y para esto se requiere de la elección de métodos eficientes para controlar el acceso de personas no autorizadas a lugares restringidos.

En este sentido, el control de acceso es un “mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos” (Tecno Seguro, s/f, párr. 1); de este modo, se pueden encontrar sistemas de control de acceso en diversas formas y para ser utilizados de distinta manera. Como sistema electrónico, limita o facilita el ingreso de personas o usuarios a determinadas áreas de una organización, reconociendo a quien accede al sitio por medio de la lectura de la identificación a través de clave, biometría o proximidad) y vigilando el medio por el cual se ingresa, que puede ser una puerta, reja o torniquete utilizando un dispositivo electrónico.

El control de acceso se puede constituir en una herramienta de colaboración para la seguridad en una empresa. Por medio de la implementación de estos sistemas, se puede facilitar o no el ingreso de personas a sus instalaciones o ciertas áreas no autorizadas; dependerá de cuáles son las necesidades de seguridad que tenga cada empresa para la implementación de un sistema de control de acceso determinado, el mismo que será el más apropiado para cumplir con las expectativas de protección (Kelio, 2020).

Existen algunos tipos de control de acceso que se encuentran disponibles en el mercado, tales como controles de acceso biométrico, con presencia y proximidad, biométrico con teclado, control de acceso y presencia por reconocimiento facial, para exteriores, con teclado externo (Kelio, 2020). En este contexto se pueden mencionar algunos sistemas de control de acceso biométrico con reconocimiento facial, como el realizado por Vaca Piña y Rivera Rodríguez (2022) para la academia Titanes Cuenca, cuya finalidad fue

ofrecer mayor seguridad a los deportistas de dicha academia, para que lleven a cabo sus prácticas deportivas de la mejor forma, para lo que se utilizó una cámara en los exteriores del establecimiento, que comparó los rostros de los miembros de la academia con el registro de éstos en una base de datos. Este problema se suscitó por cuanto no se disponía del personal suficiente (gerente y entrenador) y era muy complicado el acceso de los deportistas a las instalaciones.

De acuerdo al proyecto antes mencionado, cabe mencionarse que en el área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil se suscita un problema de similares características. El acceso a las oficinas de la administración se encuentra desprotegido y cualquier estudiante o individuo ajeno puede ingresar libremente, poniendo en riesgo la integridad de todos quienes conforman la Facultad y su trabajo; no se dispone de ninguna herramienta informática que controle la seguridad y el acceso a entornos a los que no se debería ingresar sin autorización. La seguridad es una prioridad constante y, en este sentido, el reconocimiento facial se presenta como una respuesta eficaz.

Para comprender de mejor manera los resultados de este proyecto, se ha dividido este trabajo en cuatro capítulos: el primer capítulo describe el problema de investigación, que comprende temas relacionados con la ubicación en un contexto, las causas y consecuencias, la delimitación, la formulación del problema, la evaluación, los objetivos, el alcance, la justificación e importancia, las preguntas y variables de investigación. En el segundo capítulo se investigan las tecnologías relacionadas al desarrollo del proyecto, con base en su aplicación en las diferentes actividades del ser humano; en el tercer capítulo se presenta la metodología de la investigación y desarrollo, que permiten la ejecución del proyecto y, en el cuarto capítulo se muestran la propuesta tecnológica. Finalmente, se muestran las conclusiones, recomendaciones y las referencias bibliográficas.

CAPÍTULO I
EL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

Ubicación del Problema en un Contexto

En los últimos años, la inseguridad se ha convertido en un tema preocupante tanto para los ciudadanos en general como para las autoridades de gobierno. De acuerdo con Prieto (2023) la inseguridad es la condición emocional que experimenta una persona cuando percibe que un escenario interno o externo a aquella puede llegar a afectarla. De este modo, la inseguridad puede surgir de hechos supuestos o reales, como por ejemplo transitar por una calle o barrio que no se conoce y sentir miedo por algún evento que pueda suceder.

En este sentido, se puede mencionar que existen algunos tipos de inseguridades, entre ella se encuentra la *externa*, que se refiere a aquel sentimiento que tienen las personas, de que existen riesgos o peligros distantes del ser humano y que son capaces de bloquear su bienestar personal (P. Prieto, 2023). Está directamente relacionada con el estado de inseguridad ciudadana que se vive en algunos países, siendo América Latina la región con un elevado índice delincuencial, demostrado en las más altas tasas de crímenes y mayores casos de eventos como secuestros, violencia, narcotráfico y su ajuste de cuentas, bandas criminales; esta situación tiene un impacto en la economía, la sociedad, en las instituciones gubernamentales y afecta a grupos vulnerables (Rettberg, 2020).

En el ámbito nacional, los niveles de inseguridad ciudadana están alcanzando niveles alarmantes. De acuerdo a lo expresado por López Lungo (2023) en el país, el índice de crímenes violentos por cada 100000 habitantes tuvo un incremento por cinco en solamente siete años, mencionándose que la limitación de las actividades diarias de los habitantes, como lo son la educación y el trabajo, parecería un nuevo confinamiento, por el nivel de violencia que se vive; el crecimiento del narcotráfico y las ineficientes disposiciones en materia de seguridad por parte del gobierno, son dos de las

causas principales que han permitido el avance descontrolado de la inseguridad.

Las cifras de las secuelas de la violencia son alarmantes. Se reportó alrededor de 3.500 muertes violentas en el país en los primeros seis meses del año, de las cuales 1.390 corresponden a Guayaquil, conocida en la actualidad como *la capital del crimen*. Se supo además que los ciudadanos, en un 60%, están convencidos que el problema más importante en 2023 es la inseguridad, frente al 22% que se percibía el año pasado (López Lungo, 2023).

Este nivel de violencia se ha extendido tanto, que los habitantes de los distintos barrios están en proceso de colocar mayor seguridades en sus residencias, en las calles peatonales, con el fin de aislar el sector y protegerlo, en lo que se pueda, de los altos niveles de inseguridad (Pachari Bravo, 2023). Actividades económicas se han visto afectadas por la delincuencia; asaltos a mano armada, disparos indiscriminados a personas o grupos y hasta las denominadas *vacunas* o extorsiones a los comercios están a la orden del día (Pachari Bravo, 2023). La educación no se queda atrás, con los ataques que han sufrido ciertas instituciones educativas en algunas zonas de la ciudad, lo que las ha obligado a ser intervenidas, y siendo los perjudicados tanto estudiantes como docentes y comunidad en general (Primicias, 2023c).

En este mismo contexto, en el ámbito universitario, según lo reportado por Primicias (2023e) tres universidades se acogieron a la modalidad virtual y teletrabajo para sus actividades en agosto de este año, debido a las medidas de seguridad adoptadas por el estado de excepción que decretó el gobierno y las precauciones tomadas para evitar reacciones violentas debido al traslado de un peligroso delincuente hacia otra cárcel. Una de éstas fue la Universidad Católica de Santiago de Guayaquil (UCSG), que se acogió a una semana de virtualidad; cabe mencionarse que la universidad, para hacer frente en lo posible a los posibles problemas de seguridad, estuvo gestionando un “plan de ingreso y egreso del campus universitario con mayor seguridad” (UCSG, 2023, párr. 1), que incluía buses para movilidad, aumento de cámaras de seguridad, mayor cantidad de guardias y personal policial en las inmediaciones del campus.

A pesar de estas medidas, aún faltaría por implementarse otras herramientas que complementen lo propuesto por la universidad, para

precautelar la seguridad. Los controles de acceso se pueden constituir en alternativas para evitar el ingreso de personas ajenas a lugares no públicos, como lo es el área administrativa de la Facultad de Ingeniería, en donde trabajan tanto autoridades como docentes y asistentes, en donde se gestiona la información de todos los estudiantes y demás actividades académicas. Sería menester limitar el acceso a dicha área, con la finalidad de precautelar no solamente el trabajo administrativo, sino la integridad de las personas que trabajan en este lugar y mejorar, de alguna manera, los métodos de seguridad que se hayan implementado, debido al alto índice de inseguridad que se vive en la ciudad y, por ende, en el país.

Causas y Consecuencias del Problema

En el área administrativa de la Facultad de Ingeniería de la UCSG no existe una herramienta o solución informática que registre y regule el control de acceso de personas ajenas que llegan a realizar algún trámite universitario, lo que significa que este proceso no se encuentra automatizado. El flujo de personas en las inmediaciones de la facultad puede ocasionar inconvenientes de seguridad para el personal docente y administrativo puesto que, al no identificarse a los individuos que ingresan a las oficinas, podrían infiltrarse personas de malos antecedentes a delinquir y poner en peligro la integridad de quienes ahí trabajan. Este problema genera la necesidad de desarrollar una solución que colabore con la institución para permitir o denegar la entrada de personas a la administración y así garantizar de mejor forma la seguridad interna.

Delimitación del Problema

Campo: Seguridad

Área: Control de acceso de personas

Aspecto: Se usará el análisis biométrico de personas para el reconocimiento de personas ajenas a la Facultad de Ingeniería, que ingresan al área administrativa.

Tema: Sistema de reconocimiento facial para el área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil

Formulación del Problema

¿El diseño de un prototipo de sistema de reconocimiento facial para el área administrativa de la Facultad de Ingeniería de la UCSG permitirá controlar el ingreso de personas ajenas a las oficinas y mejorar la seguridad?

Evaluación del Problema

Este proyecto es ***delimitado***, ya que el prototipo del sistema biométrico se orienta hacia la UCSG como herramienta para mejorar la seguridad interna. Por tal motivo, el diseño e implementación del sistema de reconocimiento facial, se puede convertir en una solución informática que permita identificar personas ajenas a la Facultad de Ingeniería que quieren acceder al área administrativa para realizar trámites universitarios.

Además, es ***evidente***, puesto que es fácil comprobar el ingreso sin restricciones de personas ajenas a la facultad para hacer algún trámite académico en las oficinas de la administración. Las personas llegan a la Facultad de Ingeniería, se acercan a control de cátedra en donde se encuentra el encargado, para averiguar si alguna autoridad o docente está disponible, o, en su defecto, ingresan hacia la secretaría para hablar directamente con las encargadas de los trámites universitarios de las dos carreras: Civil y Ciencias de la Computación, sin que se le solicite alguna identificación antes de entrar.

Es ***relevante***, ya que la solución informática busca la solución de un problema para la Facultad de Ingeniería de la UCSG, y se lo desarrollará con base en conocimientos científicos y académicos.

El proyecto es ***contextual***, ya que la herramienta a desarrollar es un trabajo colaborativo, que aportará utilidad a la comunidad universitaria para mejorar el nivel de seguridad.

También, el proyecto es ***factible***, puesto que se realizará la investigación de antecedentes, requerimientos, tecnologías, para diseñar e implementar una herramienta que sea apropiada para mejorar la seguridad en el área administrativa de la Facultad de Ingeniería.

Esta propuesta ***identifica los productos esperados***, lo que significa que la solución informática, desde que se plantea el proyecto, se identifica que el producto es un sistema de reconocimiento facial para el área administrativa de la Facultad de Ingeniería de la UCSG

Objetivos

Objetivo general

Diseñar e implementar una solución informática de reconocimiento facial para reforzar el nivel de acceso y seguridad en el área administrativa de la Facultad de Ingeniería de la UCSG

Objetivos específicos

- Revisar los recursos tecnológicos disponibles y utilizables para el diseño de un prototipo funcional de sistema de reconocimiento facial.
- Determinar los requisitos de seguridad y acceso al área administrativa de la Facultad de Ingeniería para el desarrollo del prototipo.
- Desarrollar el prototipo para el control de seguridad y acceso para el área administrativa de la Facultad de Ingeniería.
- Implementar el prototipo de reconocimiento facial en el área administrativa de la Facultad de Ingeniería

Alcances del problema

El proyecto se centrará en el desarrollo e implementación de un prototipo funcional de un sistema de control de acceso por reconocimiento facial para el área administrativa de la Facultad de Ingeniería de la UCSG, que se lo llevará a cabo durante el período correspondiente al semestre académico B-2023.

La herramienta se la desarrollará puesto en la facultad no existe una solución informática que registre e identifique las personas que ingresan a la administración, en donde se encuentran las asistentes que realizan los trámites universitarios de las dos carreras: Civil y Ciencias de la Computación. El acceso a esta área no tiene ninguna restricción para cualquier persona, por lo que la seguridad de quienes ahí se encuentran podría ser violentado en el momento que algún desconocido intente un acto delictivo, en vista de la grave situación de inseguridad que vive el país; más aún cuando se ha visto que instituciones educativas han sido blanco de ataques y universidades han debido acogerse a clases virtuales y teletrabajo para evitar posibles represalias de la delincuencia organizada.

El prototipo se probará y evaluará en un entorno controlado utilizando una base de datos limitada de usuarios autorizados; el alcance no incluirá la integración completa del sistema en un entorno de producción a gran escala.

En la actualidad, la facultad no realiza registro alguno de las personas que ingresan al área administrativa de la facultad.

Justificación e importancia

El beneficio de esta implementación está orientado a los integrantes de la Facultad de Ingeniería de la UCSG, es decir directivos, docentes y asistentes que laboran en estas dependencias, quienes podrán restringir el ingreso de personas ajenas a las oficinas por medio de una herramienta de reconocimiento facial.

También se beneficiará la comunidad universitaria en general, puesto que podrá considerarse como un modelo a ser implementado en otras facultades, para identificar a las personas que quieran realizar algún trámite académico en las respectivas carreras. Todo esto con el fin de mejorar el nivel de seguridad en la universidad, en vista de la ola delincuencial que se vive actualmente en la ciudad y en el Ecuador en general.

Preguntas científicas

¿Cuál es el estado de la seguridad en el área administrativa de la Facultad de Ingeniería de la UCSG?

¿Qué eventos que afectan la seguridad de las personas que trabajan en la Facultad de Ingeniería han sucedido en los últimos meses?

¿Existe un control de acceso para las personas que ingresan al área administrativa de la Facultad de Ingeniería de la UCSG?

¿Los sistemas biométricos de reconocimiento facial son las mejores opciones para el control de acceso de personas?

Variables de la investigación

Variable independiente: Ingreso de personas al área administrativa de la Facultad de Ingeniería.

Variable dependiente: Sistema biométrico de reconocimiento facial.

CAPÍTULO II
MARCO TEÓRICO

Con el fin de tener un contexto teórico del problema que se pretende resolver, a continuación, se presenta la investigación correspondiente a los aspectos más relevantes en cuanto a temas sobre seguridad e inseguridad, la tecnología al servicio de la seguridad, en donde se tratarán los sistemas de control de acceso, los sistemas biométricos, los algoritmos de reconocimiento facial, las herramientas de desarrollo, el contexto en donde se va a desarrollar el proyecto y las normativas existentes que lo enmarcan. En los párrafos siguientes se realiza la descripción de cada uno de los temas mencionados.

La seguridad

De forma general, el término *seguridad* se deriva del latín *seguritas*, lo que significa que tiene su distintivo de *seguro*, esto es, se destaca la cualidad de que algo no tiene ningún tipo de amenazas, perjuicios, riesgos o peligros; una situación segura es algo que tiene solidez, es indiscutible y cierta. Es así, que la seguridad podría entenderse como una garantía, y se encuentra estrechamente vinculado con la confianza que la persona pueda tener y también con la precaución, cuyo significado podrían cambiar según la perspectiva del área de conocimiento que se analice (Equipo Editorial Etecé, 2020; Pérez Porto & Gardey, 2021).

La seguridad es, de acuerdo con Prieto (2023, párr. 6) “el sistema o conjunto de sistemas de protección usados para prevenir y evitar cualquier riesgo o peligro externo o interno que pueda tener un impacto negativo en la vida de una persona o, dependiendo del campo, animal”. Esto se refiere a la situación de tranquilidad que el ser humano entiende cuando se siente a salvo de cualquier tipo de riesgo. Según el mismo autor, la seguridad es una de las siete necesidades básicas del ser humano de acuerdo a la pirámide de Maslow, que deben ser satisfechas y su consecución se consigue por medio de acciones a ejecutarse en el entorno en donde se desarrolla la vida de una persona o también su comportamiento, lo que significa que cualquier situación que sea capaz de provocar perjuicio emocional, físico, mentales o materiales pueden dominarse suficientemente como para que la idea que se tiene sobre

los riesgos sea aceptable y salvaguardar así la salud del individuo y su entorno.

Según el Plan Estratégico de Seguridad Pública y Ciudadana (Ministerio del Interior, 2019), existen algunas amenazas y retos a la seguridad, que poco a poco han adquirido importancia en los programas gubernamentales locales e internacionales, debido a las graves implicaciones en la política, economía, finanzas, sociedad, etc. (ver Tabla 1):

Tabla 1.
Problemas relacionados con la seguridad

Fenómenos de alcance global	Alcance
Terrorismo	Afecta directamente la vida y seguridad de las personas, debilitando las entidades gubernamentales y arriesgando intereses primordiales y claves, suministros, servicios críticos y suministros.
Delincuencia organizada transnacional	Se caracteriza por ser transaccional, opacidad, flexibilidad, capacidad de adaptación y de recuperación, además de movilidad. A esto se suma el lavado de activos y corrupción, que mina la estabilidad de un estado, impidiendo el crecimiento de la economía y la democracia.
Vulnerabilidad energética	La seguridad energética depende la correcta oferta a precios razonables, la seguridad de los lugares de producción y redes de transporte y la sostenibilidad del medio ambiente.
Flujos migratorios irregulares	Aumenta el flujo irregular de movilidad por las fronteras de un país, aumentando el riesgo en los controles de frontera, sin excluir en su totalidad núcleos de conflictos potenciales al interior de la nación.
Vulnerabilidad del espacio marítimo	El mar es el espacio con menos regulaciones y de más fácil acceso. Esto convierte al espacio marítimo en un conductor de riesgos y amenazas a la seguridad, pudiendo esparcirse fácil y rápidamente.
Desastres naturales: catástrofes	Las variaciones ambientales (olas de calor, inundaciones, lluvias, sequías o incendios forestales) pueden ser medio de presión para la migración, provocando conflictos en las franjas de tránsito, destino e inclusive fragilidad de ciertas naciones.
Desequilibrios demográficos: cambio climático	Es el mayor reto ambiental y socioeconómico del siglo XXI. Sus desafíos más importantes que influyen en la seguridad son la escasez de agua potable, modificaciones en la forma de producción, competencia indiscriminada por los recursos energéticos.

Fuente: Adaptado de Ministerio del Interior (2019)

Tipos de seguridad

La seguridad es un criterio bastante extenso, que abarca un completo soporte, por lo que se podría referirse a la seguridad en distintos ámbitos de la vida del ser humano. Entre éstas se encuentran:

- Seguridad en el trabajo
- Seguridad nacional
- Seguridad informática
- Seguridad vial
- Seguridad jurídica
- Seguridad ambiental
- Seguridad ciudadana (Navicelli, 2022)

En el apartado siguiente, se hace referencia a la *seguridad ciudadana*, como un aspecto de relevancia para este proyecto.

La seguridad ciudadana (Vázquez Campos, 2017)

De acuerdo con el Programa de Naciones Unidas para el Desarrollo Humano, la seguridad ciudadana:

> Es el proceso de establecer, fortalecer y proteger el orden civil democrático, eliminando las amenazas de violencia en la población y permitiendo una coexistencia segura y pacífica. Se le considera un bien público e implica la salvaguarda eficaz de los derechos humanos inherentes a la persona, especialmente el derecho a la vida, la integridad personal, la inviolabilidad del domicilio y la libertad de movimiento. (PNUD, 2013, p. 1).

La seguridad ciudadana abarca mucho más que una disminución de los crímenes cometidos por los delincuentes, sino de minuciosas y diversificadas políticas que permitan acrecentar la calidad de vida de las personas, de planes comunitarios que prevengan el auge delincuencial, de la participación a sistemas de justicia equitativos y eficientes, y de la implementación de una educación sustentada en valores, respeto a normativas vigentes y respeto (PNUD, 2013).

La misma fuente señaló que las causas para que exista violencia e inseguridad son variados y, por lo general, bastante complicados, pero se pueden mencionar algunos como:

- Episodios acaecidos recientemente de conflictos o violencia.
- Situaciones conflictivas de carácter interno, tales como elevados niveles de desempleo en la población joven, economías de guerra, desigualdades sociales y ostensible inequidad.
- Situaciones de conflictos provenientes del porte ilegal de armas, migraciones, crecimiento de la criminalidad, tráfico de drogas, guerras internas por control de territorio de carteles de droga.
- Crecimiento urbano indiscriminado, generando cinturones de pobreza.
- Conflictos presentes y desavenencias por temas políticos, religiosos o de raza, desigualdades sociales y repartición desigual de los recursos.
- Ambiente de irresponsabilidad y corrupción, sobre todo de las instituciones gubernamentales y de justicia, que motiva a crisis de gobernabilidad y debilidad institucional y que no permite enfrentar o prevenir la delincuencia organizada (PNUD, 2013).

La idea de seguridad ciudadana tiene relación con el buen estado de los habitantes de una nación, visto desde un amplio espectro, pero es a partir del ámbito de la seguridad que se pueden analizar los cambios que ha pasado el sistema penal y penitenciario, y la esfera policial. Se concibe a la seguridad ciudadana como un propósito de acción, propuesto para reducir la inseguridad partiendo de cambios en las instituciones involucradas, con el fin de plantear nuevas políticas de protección de los derechos humanos y todo lo que las personas necesitan (Vázquez Campos, 2017).

La seguridad ciudadana significa el momento en el que se pueden cambiar las tácticas de intervención con las cuales hacer frente a la violencia enquistada en la sociedad, puesto que destaca la definición y cumplimiento de la prevención a través de actividades alejadas de respuestas violentas, tales como negociar y construir la paz, en contraposición a la utilización de acciones que promuevan la utilización de la fuerza (Vázquez Campos, 2017).

La falta de seguridad ciudadana, en algunos países, puede ser considerada como el más grande limitante social, económico y político. La eficiencia para prevenir el cometimiento de los delitos, se considera como requerimiento para la disminución de la pobreza y el desarrollo de los países (PNUD, 2013).

En el mismo contexto, según con el Ministerio del Interior, la seguridad ciudadana es:

> El conjunto de acciones que tienen por finalidad consolidar la convivencia pacífica, el respeto a los derechos humanos y la prevención de todo tipo de violencia a través de la interacción de actores públicos, privados, con la participación activa de la ciudadanía. (Ministerio del Interior, 2019, p. 23).

De acuerdo con Álvarez Velasco (2023) y referenciando al Programa de Naciones Unidas para el desarrollo (PNUD), la seguridad ciudadana es una circunstancia requerida para el desarrollo de las personas. Se lo valora como un bien de carácter público y es deber del estado proporcionarla a los ciudadanos y se fortalece mediante la presencia de instituciones y modos de vida democráticos, por medio de los cuales se permita brindar protección efectiva y alineada a los derechos humanos. En este contexto, las expresiones de la violencia obstaculizan el fortalecimiento de las vías para el desarrollo de las naciones y personas, señalándose cuatro indicadores de violencia por los que atraviesa el país:

- *Muertes violentas*, que han crecido de forma exponencial en los últimos cinco años. Este indicador es el que presenta cómo se ha desgastado la seguridad ciudadana. Las muertes violentas son causantes de resquebrajamiento económico, puesto que se debe invertir en investigaciones, condena de casos, gastos de medicina forense y la baja de personas que trabajan.
- *Muertes violentas con armas de fuego*, considerada como la más alta causa de muerte. Las estadísticas señalan que, a nivel de Latinoamérica, las muertes por ese medio llegan al 75%, en tanto que en el país son del 80%.

- *Extorsión*, que es un delito por medio del que un individuo o grupo obliga a otro a llevar a cabo actividades que no quiere hacer. Por lo general, cuando hay un delito por extorsión, se demandan pagos en dinero para no hacer daño a la persona víctima de la extorsión y a todo su entorno.
- *Robos*, delito que ha crecido en todas sus variantes, exceptuando los ocurridos en domicilios y carreteras (Álvarez Velasco, 2023).

Violencia urbana, como parte de la batalla de la seguridad ciudadana

En palabras de Vázquez Campos (2017) la violencia es un problema que es parte de la historia del hombre y entender las causas que la motivan es una práctica obligatoria. El crecimiento acelerado de los centros urbanos ha provocado modificaciones en la lógica de las ciudades, influenciando en el aumento de la delincuencia y la violencia, que son dos hechos que desgastan a los pobladores y se caracteriza por ser indefinida, universal y tener como inicio, causas diversas: situaciones biológicas y sicológicas, hasta las que suceden a partir del contacto persona a persona y éstas con sus propios entornos.

La violencia puede ser clasificada en varias categorías, aunque para poder entender esta manifestación en el contexto urbano, se toman en consideración dos: 1) *violencia objetiva*, relacionada con los sucesos específicos de la violencia, es decir, la actividad delictiva que se puede cuantificar, y comprende acciones delictivas en contra del patrimonio y las personas, y que significa la utilización de la fuerza física con el fin de perjudicar el patrimonio, hacer daño o matar a otra persona o a sí mismo, y 2) *violencia subjetiva*, o aquella que se orienta en la apreciación que tienen las personas sobre la inseguridad, en cuanto al miedo y la forma de interpretar personalmente el hecho del concepto social del miedo que se crea por la violencia directa o indirecta.

La percepción que se tiene de los centros urbanos se concentra en las posibilidades de progreso que éstos ofrecen, cuya realidad demuestra que el concepto que la ciudad ideal que se tiene disminuye conforme no se

encuentren los medios necesarios para un desarrollo sostenido. Cabe mencionarse que en la ciudad converge los aspectos sociales, económicos y políticos, que podrían acrecentar las dificultades en el entorno urbano; estas dificultades se hacen más visibles en algunas áreas urbanas, en las que se encuentran agrupaciones sociales en situación de vulnerabilidad, las mismas que suelen *disculpar* los nexos que existen entre violencia y pobreza. Este nexo marca los espacios en donde confluye la exclusión y segregación de las personas en las urbes que, de acuerdo con la percepción que se tiene, se identifican como inseguros, generando el escenario ideal para que la violencia interior se exprese de acuerdo con la experiencia de los individuos y por medio de rumores y representaciones de lo que sucedido; esto origina una sensación dividida de la violencia como tal: una violencia que se presenta en las ciudades a través del miedo ciudadano en las calles, que obliga a resguardarse en la más profunda seguridad y que convierten a los hogares en lugares herméticamente cerrados, a los que deberán cuidar las compañías de seguridad que surgen como resultado de este fenómeno.

Como efecto de la violencia urbana se encuentra el desgaste de los nexos creados por la interacción de las personas, reflejado en la poca credibilidad y confianza que se le tiene a la autoridad competente. Asimismo, la manifestación de la violencia conlleva a que los espacios públicos sean abandonados. Calles, veredas, parques, áreas verdes son los espacios que poco a poco se van abandonando, por lo que disminuye las zonas de interacción entre personas, provocando que se señalen estos lugares como peligrosos, no solamente por quienes se encuentran alrededor, sino por las noticias que se generan en los medios de comunicación, que señalan los sitios más peligrosos en donde se producen los hechos delincuenciales.

La seguridad ciudadana se relaciona con la violencia, por los planes que se desarrollan y que tienen la finalidad de prevenir los delitos, junto con la participación y convivencia de los ciudadanos, para conseguir un mejor control social informal y que las políticas que se planteen se legalicen y se lleven a cabo localmente (Vázquez Campos, 2017).

La seguridad en las instituciones educativas y su importancia

Las instituciones educativas se han convertido en el entorno obligado para niños y jóvenes, puesto que es aquí en donde pasan largas horas, confraternizando con otros congéneres, en donde no solamente adquieren su instrucción, sino que aprenden nuevas experiencias, además de socializar, transmitir saberes y culturas, entre otros (Florenciañez, 2022). La seguridad en estos centros de estudio es de suma importancia, puesto que los estudiantes necesitan sentir protección a su llegada a la institución y mientras cumplen su labor de aprendizaje; un ambiente tranquilo es muy importante para los estudiantes, puesto que así pueden orientarse hacia su progreso personal y profesional. Junto a la tranquilidad a la que tienen derecho los alumnos, se encuentra la seguridad, que ofrece la certeza de que la institución educativa tiene implementadas acciones de protección y prevención de incidentes (Cohen, 2023a).

Las instituciones educativas están sujetas a una variedad de peligros y riesgos y es parte importante de la parte directiva, docentes, administrativos y todos los que las conforman, tengan la sensación de protección, al mismo tiempo sentirse relajados, de manera que las actividades que realizan puedan ser ejecutadas con total tranquilidad. Por tal motivo, la seguridad es una de las bases principales al momento de realizar la planificación, tomando en cuenta los costos que en ella se invertirían (Protek Seguridad, 2022).

En las instituciones educativas de cualquier tipo, se encuentran en la mira de la delincuencia, registrándose hurtos y otras acciones delictivas, no solamente de personas ajenas sino dentro del propio recinto, por parte de los propios empleados y trabajadores. En la mayoría de las ocasiones, los robos tienen relación con los bienes materiales de la institución, como equipos tecnológicos, o también objetos pertenecientes a docentes y/o estudiantes (Protek Seguridad, 2022).

La gran afluencia de personas a los centros de estudios cuando se desarrolla algún evento, facilita la presencia de los delincuentes. La primera recomendación para disminuir los índices de inseguridad sería contratar a mayor cantidad de guardias de seguridad para que vigilen la institución; lo

segundo a implementar debería ser la instalación de cámaras de seguridad en los accesos y en las áreas comunes, de manera que las autoridades se mantengan en conocimiento de lo que sucede en el recinto. También se podría sugerir que se mantenga un registro de las personas que acceden al centro de estudios para tener una base de datos con la información básica y, en caso de algún incidente, tener la constancia para realizar cualquier reclamo (Protek Seguridad, 2022).

La inseguridad ciudadana

Definiendo el término inseguridad, de acuerdo con el Centro de Psicología Clínica y Psiquiatría Manuel Escudero (2023, párr. 1) es "la dificultad para escoger entre diferentes opciones para conseguir un objetivo determinado". La sensación de inestabilidad o vulnerabilidad que puede afectar los sentimientos de autoestima y percepción propia podría ocasionar ansiedad, incomodidad o nerviosismo en situaciones diversas; un individuo inseguro no confía en su propio valor y capacidad, creyendo que las demás personas, en algún momento lo defraudarán.

Como fenómeno social, la delincuencia se edifica con base en el rechazo mayoritario que se comparte hacia ciertas conductas, el mismo que se presenta en una petición a la acción como una respuesta decisiva hacia ellas. Los actos delictivos o la justicia se erigen bajo esta demanda, al mismo tiempo que representan la materialización de valores e ideas construidas y construyendo en el entorno social la idea de utilizar la fuerza de parte de los gobiernos. "Tanto la existencia de esta demanda de acción política como su traducción en leyes penales, cuerpos policiales, juzgados o prisiones hacen necesario que se disponga de información acerca de cuánta y cuál es la delincuencia conocida" (Caro Cabrera, et al., 2020, p. 11).

Tener una idea clara de la criminalidad es importante para que la justicia la pueda controlar. Asimismo, el control ejercido por las instituciones de seguridad, la justicia y las cárceles, crea información relacionada con los actos delincuenciales y, por ende, en todo lo relacionado con el control. De este modo se puede comprender todo lo relacionado con la criminalidad; las

acciones planeadas para atacar a la delincuencia son las que generan los datos de las penitenciarías, de los órganos judiciales o de la policía.

En América Latina

Todos los días, semanas y meses aumentan las víctimas mortales debido a la delincuencia en América Latina, convirtiéndola en la región más violenta del mundo, en donde se cuenta con los más altos índices de asesinatos, de acuerdo a reportes de organismos internacionales, cifras alarmantes a pesar de que en esta región del planeta se ubica solamente el 8% del total mundial de la población. La cantidad de homicidios registrados podría ser considerada como una epidemia, según se menciona en un informe de la ONU contra la Droga y el Delito (Lissardy, 2019).

Los brotes de violencia generalizada podrían atribuirse a algunos factores, siendo el primero la presencia del crimen organizado, el mismo que a partir de la década de 2000 origina el mismo número de fallecidos alrededor del mundo, que las guerras, afectando de manera particular a los países de Latinoamérica. En esta región el crimen organizado y las pandillas se caracterizan por su extrema violencia, que se asocian a las luchas por el territorio para un lucrativo negocio: el narcotráfico, ya que es en América Latina que se fabrica cocaína; por ganarse un lugar en ese mercado se encuentran los carteles de la droga colombianos y mexicanos, y las maras centroamericanas, lo que ha motivado que los gobiernos declaren una guerra contra el expendio y tráfico de drogas, provocando el aumento de la violencia y descomposición en sus propias instituciones de seguridad A estos problemas se debe añadir la facilidad con la que se pueden adquirir las armas de fuego que, de acuerdo con estudios, se han utilizado en tres de cuatro muertes violentas, un promedio muy superior al global (Lissardy, 2019).

La violencia y el crimen organizado han crecido de tal forma en Latinoamérica, que han obligado a las naciones a buscar alternativas efectivas para tratar de controlarlos. Aunque en la actualidad los índices de asesinatos se encuentran entre los más altos del mundo, las estadísticas de aquellos se han equilibrado y tienen reducación en países particularmente en donde la violencia es más agresiva, como El Salvador y Colombia, el horizonte se

mantiene deprimente. Aproximadamente un tercio de los niveles de crímenes en todo el mundo, se originan en Latinoamérica, atribuyéndose la gran mayoría de aquellos a la operación de la delincuencia organizada. La violencia de género ha crecido; el accionar criminal de las bandas delincuenciales ha provocado y empeorado las crisis humanitarias presentes en la población, como lo son las migraciones (International Crisis Group, 2023).

A pesar de que los actores de la violencia son de diversa índole, se pueden mencionar tres tipos que

En Ecuador

En el Ecuador, el nivel de violencia e inseguridad es alarmante, ya que los índices de crímenes violentos atentan con los derechos humanos. Junto a los ataques a personas, el crimen tiene su impacto directo en el gasto público, puesto que luchar contra ellas es trabajo adicional para las fuerzas del orden. A partir de 2018 el Ecuador ya no se lo considera como uno de los países con mayor seguridad, pasando a convertirse en el más violento en 2022. En el contexto de la actual inseguridad que vive el país, el gobierno entrante deberá enfrentar el problema creando planes que permitan detener el dominio que tiene el crimen organizado a nivel nacional que, con el transcurso de los días, va en aumento exponencial y de este modo poder reforzar “las capacidades técnicas, de inteligencia, de seguridad y de administración de justicia en el país” (Álvarez Velasco, 2023, p. 1)

Según una publicación de Primicias (2023b), el organismo Iniciativa Global Contra el Crimen Organizado Transnacional (Gitoc) que estudia el crimen, anunció que “Ecuador se ha convertido en un país clave en el mercado internacional de las drogas” (párr. 1). Además, ya integra la lista del top 10 de los países que registran la más alta tasa de crímenes a nivel mundial en 2023, liderada por “Myanmar, seguida de Colombia México, Paraguay, República del Congo, Nigeria, Sudáfrica, Iraq, Afganistán y Líbano (que tienen un empate) y Ecuador” (Primicias, 2023b, párr. 5).

Guayaquil está considerada actualmente como una de las 10 ciudades con mayor índice de violencia a nivel internacional, motivado por la encarnizada lucha de territorios de los grupos narcodelictivos que poco a poco

se han tomado el país (Primicias, 2023d). La ola de inseguridad que se vive ha obligado a que los ciudadanos empiecen a tomar medidas extremas para protegerse de la embestida de la delincuencia que, en un hecho sin precedentes, aumenta día a día; estas precauciones incluyen la *bunkerización* o proceso de encierro forzado en un búnker para evitar el ingreso de personas ajenas a sus casas, barrios o ciudadelas (Pachari Bravo, 2023).

En la Tabla 2 se muestra el ranking 2022 de las ciudades más violentas, en donde se puede apreciar que Durán es otra de las ciudades más golpeadas por la delincuencia.

Tabla 2:
Ranking 2022 de las ciudades más violentas del mundo (sin un conflicto bélico)

Posición	Población	País	Homicidios	Habitantes	Tasa
1	Colima	México	601	330 329	182
2	Zamora	México	552	310 575	178
3	Ciudad Obregón	México	454	328 430	138
4	Zacatecas	México	490	363 996	135
5	Tijuana	México	2 177	2 070 875	106
6	Celaya	México	740	742 662	100
7	Uruapan	México	282	360 338	78
	Durán	Ecuador	222	303910	73
8	New Orleans	Estados Unidos	266	376 971	71
9	Juárez	México	1 034	1 527 482	68
10	Acapulco	México	513	782 661	66
11	Mossoró	Brasil	167	264	63
12	Cape Town	Sudáfrica	2 998	4 758 405	63
	Guayaquil	Ecuador	1703	2746403	62
13	Irapuato	México	539	874 977	62
14	Cuernavaca	México	410	681 086	60
15	Durban	Sudáfrica	2 405	4 050 968	59

Fuente: Primicias (2023a)

La violencia ha alcanzado niveles exorbitantes. Según datos proporcionados por la Policía Nacional, en el primer semestre de este año, se ha incrementado en 657 los hechos delictivos, de los cuales “el 94,6% corresponde a violencia criminal, 5,1% interpersonal y 0,3% sociopolítica” (Policía Nacional del Ecuador, 2023, párr. 1), superior a la cifra registrada en 2022; crímenes ocurridos en meses anteriores, como el de un candidato a la presidencia y un alcalde, evidencian lo vulnerable que se encuentra la sociedad frente a la delincuencia (Solano & Molina, 2023). La inseguridad generalizada en todo el país y sobre todo en Guayaquil, ha obligado a los ciudadanos a colocar puertas y cerramientos en sus barrios o ciudadelas, además de sistemas biométricos con lectores de huellas para identificación (Primicias, 2022).

El combate a la delincuencia no está dando resultados positivos. El gobierno de turno se encuentra en la lucha por detener los niveles de inseguridad, mediante el uso de la fuerza y la incorporación de nuevo personal policial (DW, 2023), además de la provisión de nuevo material que fortalezca a las fuerzas armadas en su capacidad de operación frente al crimen y delincuencia, que está sometiendo al país (Xinhua Español, 2023). Los ciudadanos deben protegerse de cualquier forma, ya que la seguridad se pone en riesgo hasta en sus lugares de trabajo por lo que, si no se colabora con estrategias propias de protección, será muy difícil, incluso imposible, mantener una existencia lejos de la preocupación de ser víctima en algún momento de algún hecho violento.

En otro contexto, la ola de violencia se ha extendido a las instituciones educativas. En agosto se conoció del secuestro y posterior rescate de una autoridad de la Universidad de Guayaquil (The San Diego Union-Tribune, 2023); los primeros días de noviembre se conoció del asesinato de miembros policiales y coches bomba colocados en distintos lugares de la ciudad, motivando a que las universidades anuncien la suspensión de las clases presenciales para precautelar la integridad de sus integrantes: la Universidad Laica Vicente Rocafuerte, Ecotec, UCSG, la Tecnológica Empresarial, la Escuela Superior Politécnica del Litoral, la Politécnica Salesiana, la Casa

Grande, la Especialidades Espíritu Santo pasaron a clases virtuales y suspensión de actividades administrativas.

Todo lo anterior demuestra que es prioridad de los establecimientos educativos buscar alternativas que permitan mantener la seguridad e integridad de los estudiantes, docentes, administrativos y demás involucrados en el proceso educativo. Dentro de estas alternativas está la tecnología, con nuevas herramientas para detección de personas, cámaras de vigilancia, sistemas biométricos que, de ser implementados, serían de gran ayuda.

La tecnología al servicio de la seguridad

Los avances tecnológicos han permitido la evolución del paradigma de las empresas, manifestándose como un punto elemental para la renovación industrial, como lo es la seguridad. Inteligencia Artificial, IoT o ML, son algunas de los mayores cambios tecnológicos que se han hecho presentes en la actualidad y que su presencia será duradera. Las ventajas están presentes en la automatización de los procesos industriales y agilización de labores de seguridad, con las cuales se ha mejorado su eficiencia (Prosegur, 2023).

Es constante en el ámbito tecnológico los temas de IoT o Transformación digital. En la seguridad, estos temas han facilitado el desarrollo de nuevos sistemas que han convertido en un adecuado complemento para quienes gestionan los procesos de seguridad. El más claro ejemplo de evolución tecnológica en seguridad es el desarrollo de aplicaciones móviles, cuya utilización puede servir para realizar el monitoreo en tiempo real de cualquier lugar en donde se aplique, para alertar a la empresa proveedora del servicio de cualquier evento sospechoso y tomar acciones en forma rápida. Otra aplicación de la tecnología en el campo de la seguridad es la biometría, que combina lo tecnológico con las características físicas del ser humano; el reconocimiento facial, lectura de iris o de huella digital se pueden mencionar como ejemplos que se aplican en las empresas para mejorar la seguridad (Omnitempus, 2020).

En los apartados a continuación, se presentan algunos temas relacionados con la seguridad, los sistemas de seguridad, sistemas de control

de acceso, controles de acceso y sus tipos, sistemas biométricos y su clasificación, y los algoritmos de reconocimiento facial.

Seguridad electrónica y seguridad física

Con la evolución de las tecnologías de la información y comunicación (TIC), la seguridad ha tenido un significativo avance en cuanto a lo que puedan brindar las empresas dedicadas a este tipo de servicio; dentro de esto se encuentra la seguridad electrónica, la misma que utiliza equipos electrónicos, con el fin de detectar posibles intrusiones de personas ajenas a un determinado entorno y prevenir, en lo posible, actos de violencia o robo (Martínez García, 2023).

Se entiende por *seguridad electrónica* "es la capacidad de determinados sistemas avanzados de realizar operaciones de seguridad. Entre estas operaciones de seguridad se pueden encontrar: controles de acceso, televisores de circuido cerrado, alarmas...etc." (Martínez García, 2023, párr. 3).

La seguridad electrónica se refiere a los productos y/o servicios que se ofrecen, a través de la instalación de los distintos dispositivos electrónicos, cuya función es proporcionar información automatizada y controles con mayor rigurosidad, que sirvan para servir de apoyo a los métodos tradicionales de seguridad, que se diseñan con anticipación. Los sistemas de seguridad electrónica, por lo tanto, son aquellos artefactos electrónicos que pueden ejecutar procedimientos de seguridad como controles de acceso, vigilancia, circuito cerrado de televisión (CCTV) y otras alternativas electrónicas (Secatel, 2019).

El uso de los sistemas de seguridad electrónica puede ser para:

- Seguridad para instituciones, empresas o eventos, mediante el control de acceso, para observar la confluencia de las personas que ingresan por medio de tarjetas magnéticas, fichas y otras formas de acceso.
- Seguridad en hogares, con sistemas de detección de intrusos, para minimizar el riesgo de robos.
- Detección de incendios, que contienen, de manera general, sensores de humo y pueden ser alarmas que se comunican con la estación de

bomberos más cercana, o pueden activar riego automático para disminuir, en lo posible, los daños ocasionados por el flagelo

- Seguridad para cadenas de producción.
- Sistemas de seguridad para instituciones de gobierno (Martínez García, 2023; Secatel, 2019, párr. 3).

Los elementos de un sistema de seguridad electrónico son:

- Unidad central de control
- Interfaz de usuario
- Sensores
- Fuente de alimentación
- Red de conexión
- Respaldo de energía
- Señalizador
- Central receptora (Laarcom, s/f).

Cabe mencionarse que los sistemas de seguridad electrónica pueden emitir señales como luces, ruidos o notificaciones al centro de monitoreo, por medio de los sensores inalámbricos o cableados. Este sistema de alarmas también facilita la práctica de medidas de contingencia para la reducción de los riesgos asociados a la emergencia (Laarcom, s/f).

Por otro lado, la *seguridad física* se refiere al tratamiento que se les brinda a los sistemas para protegerlos de peligros físicos, por medio de "barreras físicas y procedimientos de control, como medidas de prevención y contramedidas, ante amenazas a los recursos e informaciones confidenciales" (GSITIC, 2018, párr. 8). Eventos como intrusiones o delitos internos y externos entre otros, se encuentran dentro de la seguridad física.

La seguridad física constituye una de las partes integrantes en la elaboración de un plan de seguridad, que servirá para vigilar un entorno especificado con la finalidad de prevenir cualquier percance y reducir peligros. Un buen servicio de seguridad consiste en poder reconocer cuáles podrían ser las amenazas y riesgos que pueden existir en el lugar, y tratar de buscar los dispositivos físicos que puedan ser utilizados para mejorar los mecanismos de protección. Los peligros que pueden ser detenidos por medio de los

componentes de la seguridad física, y se refieren a robos, suplantación de identidad, secuestros, robo de información, que pueden ser catalogados como probable, altamente probable, poco probable y escasamente probable (Frevinco, 2021).

Sistemas de seguridad

Un sistema de seguridad es un grupo de dispositivos que se encuentran instalados y que se comunican entre sí, para realizar la prevención, detección y ejecución de acciones frente a accesos no autorizados, tentativas de atracos o algún otro tipo de evento de seguridad, como una emergencia o incendio (Verisure, 2023).

Los sistemas de seguridad eficiente son aquellos que pueden responder a la protección de los negocios contra posibles eventualidades como robos, ingresos no autorizados o actos delictivos; asimismo, son efectivos como persuasión a los criminales, puesto que no estarán totalmente en calma al saber que se sienten vigilados y que alguna tentativa de atraco será detectada en el momento preciso (Cohen, 2023b).

Un sistema de seguridad para una empresa se refiere al

> Conjunto de medidas organizativas (que se componen a su vez de medidas y métodos) y medios técnicos interconectados, unidos por canales de comunicación que garantizan el mantenimiento de un estado seguro de la instalación, además de la detección y eliminación de la lista más completa o compleja de amenazas a la vida, la salud, el hábitat, la propiedad y la información, a través de medios comunes de recopilación y procesamiento de información y gestión. (RecFaces, 2021b, párr. 2).

Como función principal de un sistema de seguridad se menciona la *alerta temprana de accesos no autorizados*, ya que su diseño está desarrollado para realizar el monitoreo permanente de un determinado lugar o empresa en caso de presentarse cualquier movimiento inusual, con el fin de

adoptar procedimientos inmediatos y, de esta forma, prevenir daños (Cohen, 2023b). Estos sistemas son variados

Otra característica de los sistemas de seguridad es la *vigilancia y monitoreo*, mediante la instalación de cámaras en puntos estratégicos del lugar a vigilar, para realizar el seguimiento de todos los acontecimientos que suceden a diario en la empresa y poder establecer los involucrados en el supuesto caso que suceda algún incidente de seguridad (Cohen, 2023b). Además de las cámaras, también se pueden instalar intercomunicadores de audio y video en las entradas de los hogares, instituciones, hospitales y otros sitios de interés; detectores de metales y escáneres de explosivos, mediante los cuales se pueden identificar componentes y elementos peligrosos, y que pueden atentar contra las demás personas que se encuentren en el entorno (aeropuertos, estados, instituciones gubernamentales, que tienen concentración de individuos); torniquetes, cerraduras electrónicas colocadas en las puertas y otros, que están creados para la gestión de la entrada de visitantes por medio de mecanismos de identificación (RecFaces, 2021b).

Los sistemas de seguridad también se caracterizan por la *protección contra incendios y emergencias*, ya que otra de las funciones que desempeña es la detección de humo y calor por medio de sensores, lo que permite alertar de un incendio cuando recién se está iniciando, de manera que la respuesta sea inmediata y tratar de reducir los posibles daños (Cohen, 2023b).

Sistemas de control de acceso

El control de acceso es una parte fundamental de los planes de seguridad que diseña una organización, que sirve para establecer qué personas tienen acceso a un determinado lugar. Un sistema de control de acceso puede ser entendido desde dos ángulos: el **físico**, que consiste en los dispositivos o instrumentos que permiten el ingreso de personas o automotores a lugares específicos; y desde la óptica de la **seguridad informática**, que significa “el control de acceso como medida de ciberseguridad” (Grupo Atico34, 2023, párr. 4) en cuyo caso se determinan las soluciones o herramientas informáticas, con la finalidad de determinar el

personal que tendrá autorización para su acceso a los sistemas informáticos y la información que en ellos se gestiona.

Los sistemas de control de acceso son aquellos que facilitan o bloquean el ingreso de personas o automotores a entornos o perímetros específicos. Buscan “garantizar la seguridad y facilitar la organización” (Seguritecnia, 2022, párr. 1). Un sistema de control de acceso se refiere al mecanismo que, mediante la identificación y autenticación, tiene acceso a información u otro tipo de recursos; “es un sistema electrónico que restringe o permite el acceso de un usuario a un área específica validando la identificación por medio de diferentes tipos de lectura (…) y a su vez controlando el recurso (…) por medio de un dispositivo eléctrico” (Tecno Seguro, s/f, párr. 5).

Tiene como objetivo:

- El acceso o restricción de personas a ciertos sitios de una organización.
- El acceso o restricción a sistemas informáticos, bases de datos y otros servicios.
- La protección de bienes físicos, equipos o información de la empresa, para evitar accesos no autorizados o robos.
- La detección de accesos que no están autorizados y la aplicación de planes de seguridad para prevenirlos.
- El registro y revisión de incidentes de criticidad elevada cometidos por los usuarios de los sistemas.
- La posibilidad de que la empresa se organice de mejor forma y controle a sus empleados (Grupo Atico34, 2023).

Sus funciones son: **identificar**, se refiere al reconocimiento de la persona que busca el acceso a un determinado lugar o instalación, por medio de algunos métodos, puesto que la identificación de la persona es importante cuando se quiere conocer si reúne los requisitos para su ingreso al sitio; **autenticar**, lo que significa verificar a los individuos o vehículos que buscan un acceso a un sitio específico, desde una base de datos o si reúne los requisitos exigidos para su ingreso; **autorizar**, que por medio del software del sistema comprueba y ordena que se abra o no un determinado acceso; y

trazabilidad, mediante la que se consigue una lista de todas personas que se encuentran en un sitio específico, almacenadas en un repositorio, de manera que se puede llevar un control, tanto de la frecuencia de ingreso como de tiempo de estancia de las personas en el sitio (NÜO Planet, 2019; Viatek, 2022).

La implementación de los controles de acceso en las organizaciones genera algunos desafíos previos, entre los que se pueden mencionar:

- *Comprender los requerimientos necesarios para la seguridad*, para establecer un árbol de control de accesos, que facilitará el diseño de los permisos más adecuados para el ingreso; “se incluye la identificación de los datos sensibles, determinar quiénes van a tener acceso, y establecer diferentes procedimientos para manejar y proteger toda la información” (Fernández, 2023, párr. 7).
- *Proteger de las contraseñas*, puesto que, al ser una manera habitual de autenticación, se deberá determinar cuáles serán las reglas de seguridad para las contraseñas, que pueden estar formadas de una cantidad mínima de caracteres y su frecuencia de renovación puede ser periódica.
- *Cumplir los estándares necesarios*, para el tratamiento, protección y uso de los datos. La regulación de los datos obliga a las organizaciones a adoptar medidas de seguridad pertinentes que permitan el cumplimiento de los requerimientos de seguridad.
- *Gestión de accesos remotos*, sobre todo en los últimos tiempos, en donde el teletrabajo es una tendencia en las organizaciones, puesto que ha obligado a centralizar esta forma de actividades. Esto obliga a mantener una revisión permanente de los accesos a los sistemas e información confidencial que se procesa en aquellos.
- *Monitoreo y auditorías*, que mantiene a los gestores de los sistemas a estar prevenidos en caso de suceder algún incidente de seguridad y poder prevenirlos (Fernández, 2023).

Existen algunos tipos de control de acceso, de acuerdo a la disposición del sistema y sus componentes. Éstos son:

Autónomos

Se caracterizan porque no tienen ninguna conexión a sistemas centrales: son lectores conectados a las puertas, con la capacidad de “dar de alta a ciertos usuarios y permitir su acceso” (NÜO Planet, 2019, párr. 11). Aunque es sencillo, este sistema tiene algunas limitaciones: 1) no almacena un archivo de los accesos y cualquier evento sucedido, y 2) no todos estos sistemas están capacitados para restringir los ingresos de acuerdo a horarios establecidos o centralizar otros sistemas colocados en las puertas.

Centralizados

Los sistemas centralizados son únicos, capaces de controlar los accesos y eventos que confluyen de varios puntos de acceso, lo que significa “que los diferentes lectores para identificación, autenticación y autorización están conectados entre sí” (NÜO Planet, 2019, párr. 12).

Distribuidos

Los sistemas distribuidos pueden controlar varias puertas de acceso desde un único punto. Estos sistemas pueden poner en funcionamiento sistemas cableados, ya que el acceso por medio de cable tiene algunas ventajas, como el registro de los datos de los accesos en tiempo real, la información que se comparte para generar ecosistemas inteligentes, en donde la información están seguros (NÜO Planet, 2019).

Sistemas biométricos

Son aquellos sistemas tecnológicos que recogen, registran y comparan la información biométrica o rasgos de las personas, para autenticarla y/o identificarla. Están compuestos de: “hardware (por ejemplo, un lector de huellas y un ordenador conectado al mismo) y un software a través del cual operar para reconocer los rasgos biométricos programados (por ejemplo, la huella dactilar o el iris)” (Grupo Atico34, 2023, párr. 3). Los sistemas biométricos de mayor utilización es la identificación biométrica, puesto que su operatividad y la información que requieren son de muy difícil alteración, casi imposible, y perduran en el tiempo, convirtiéndolos en una forma de verificación segura y fiable.

El funcionamiento de estos sistemas requiere del registro de los rasgos biológicos de la persona que servirá para identificación y/o autenticación. Por medio de un algoritmo, el rasgo se convierte “un patrón digital (o plantilla biométrica), que se almacena en una base de datos” (Grupo Atico34, 2023, párr. 4); luego de la creación de la base de datos, el sistema realizará, otra vez, la captura el rasgo biométrico y lo comparará con los registros de la base de datos para encontrar si existe o no coincidencia y verificar la similitud de los datos con la persona a identificar; la comparación se realizará “de uno a uno (1:1, autenticación) o de uno a muchos (1:N, identificación)” (Grupo Atico34, 2023, párr. 6), tomando en consideración que en la opción primera se realiza la verificación de la persona y en la segunda se identifica positivamente a un desconocido.

Existen algunos tipos de sistemas biométricos, que son los de mayor utilización. En los párrafos a continuación se revisan algunos.

Escaneo de huellas dactilares

El reconocimiento dactilar es utilizado en los sistemas biométricos para identificación de las personas, mediante el cual se pueden autentificar datos (RecFaces, 2021a). Se pueden dividir en tres subtipos: 1) los que transforman una huella digital en un código digital, por medio del uso de un sensor óptico, 2) los que convierten la impresión por medio de un sensor lineal térmico, y 3) la transformación de una huella digital con un sensor capacitivo de autenticación (RecFaces, 2021a, párr. 11). Aunque estos sistemas ofrecen una variedad de formas de autenticación de las personas, para el usuario final lo único que difiere entre ellos los pasos que deberán ejecutar con el escáner.

Escáner del iris

Tanto el escaneo del iris como de la retina son métodos de identificación bastante confiables, de acuerdo con el entorno ambiental y la función que van a cumplir luego de su implementación. Las dos características físicas de la persona usan escáneres sin ningún contacto, aunque sí difiere notablemente uno del otro; mientras el iris es una forma de biometría no invasiva, la exploración de la retina lo es en gran medida, puesto que el ojo se

expone al ingreso de rayos de luz visible mientras verifica la identidad de la persona.

El escaneo del iris no requiere contacto, el reconocimiento es bastante rápido, es bastante preciso y puede ser utilizado a lo lejos. Utiliza un equipo especial, pero con los avances de la biometría, la tecnología de reconocimiento por medio del iris es más accesible en cuanto a costos y se ha convertido en una herramienta bastante aceptada (RecFaces, 2021c).

Geometría de la mano

Los sistemas que se basan en la geometría de la mano son utilizados generalmente para realizar un control físico de acceso por medio de aplicaciones, aunque también se los utiliza en combinación con otras. Tienen su base en las particularidades geométricas de la mano, tales como los dedos y sus dimensiones, amplitud de la palma, entre otras. Este método de reconocimiento se inicia con un pre-procesado (con la ayuda de filtros para reducir las interferencias, conversión binaria de las imágenes y localización de bordes en la imagen) para luego extraer el contorno de la mano. Esos sistemas son considerados como los más veloces dentro del grupo de la biometría, con tasa de error razonable (un segundo se necesita para establecer si una persona dice ser lo que es (EcuRed, 2017, párr. 1).

Reconocimiento de voz

Reconocimiento de habla o de voz “es una rama de la inteligencia artificial cuya finalidad es posibilitar la comunicación entre humanos y sistemas informáticos” (CEUPE Magazine, s/f, párr. 5); puede detectar y entender lo que pronuncia naturalmente un ser humano.

Su forma de operar es un tanto compleja, pero se podría resumir de la siguiente manera:

- Se detectan las palabras pronunciadas por las personas.
- Se transforman las palabras a un formato que la máquina pueda leer y lo convierte en mensaje.

- El sistema reacciona al mensaje que recibe en forma de una orden a cumplir, una contestación a un tema, o mantener una conversación fluida.

Tiene algunas aplicaciones: sistemas de coche, dictado de voz, control por comandos, entorno telefónico, dispositivos inteligentes, sistemas para personas discapacitadas (CEUPE Magazine, s/f).

Reconocimiento de escritura

Es la capacidad que tiene una computadora para la recepción de entradas de escritura incomprensible de distintos orígenes (documentos, fotos, pantallas táctiles, otros dispositivos) y transformarla a texto. Lo que se extrae del texto se puede presentar de dos maneras: *fuera de línea*, proveniente de una hoja de papel con texto escrito, que se escanea mediante un lector óptico o un reconocimiento inteligente de palabras, y *en línea*, cuando el texto ingresa al sistema por medio de la punta de un lápiz de una pantalla táctil; esta última por lo general más fácil, ya que existen más pistas a disposición del usuario. Los sistemas de reconocimiento de texto escrito segmenta en caracteres y busca las palabras que mejor se asocien a lo que se quiere reconocer (AcademiaLab, 2023; Alegsa, 2023).

Reconocimiento de venas

Este tipo de biometría es algo nueva, puesto que su uso a nivel mundial es reducido en la actualidad (alrededor del 3%). El dispositivo que realizará el escaneo de la palma de la mano utiliza una luz infrarroja que leerá el reflejo. “La hemoglobina en las venas absorbe parte de la radiación, lo que se traduce en un reflejo que muestra un patrón de líneas oscuras que constituyen una red de vasos sanguíneos subcutáneos” (RecFaces, 2021a, párr. 24). El código digital que se genera resulta de la aplicación de algoritmos matemáticos para la conversión del patrón y luego ser empaquetado en un archivo de patrón cifrado. El escaneo de la palma de la mano de la persona se realiza por medio del dispositivo, sin que tenga contacto con la palma y lo compara con la información que tiene en la base de datos (RecFaces, 2021a).

Reconocimiento facial

Por último, se menciona el reconocimiento facial como parte de los sistemas biométricos, y se manifiesta que es la “manera de identificar o confirmar la identidad de una persona mediante su rostro. Los sistemas de reconocimiento facial se pueden utilizar para identificar a las personas en fotos, videos o en tiempo real (Kaspersky, 2023, párr. 1). Es una escala de la seguridad biométrica.

En los párrafos a continuación, se revisa con más detalle la tecnología de reconocimiento facial, que es el tema central de este proyecto, para implementarse en el área administrativa de la Facultad de Ingeniería de la UCSG.

Tecnología de reconocimiento facial

De acuerdo con Cedeño Navarrete y Párraga Vera (2017) el reconocimiento facial es “una aplicación dirigida por ordenador que identifica automáticamente a una persona en una imagen digital” (p. 7). Se lo realiza porque se lleva a cabo un examen de las particularidades faciales de la persona que se las obtiene de una foto o imagen principal extraída de un video y luego comparada con las que se encuentran en una base de datos. Este tipo de biometría es segura y confiable para identificar a personas, ya que inclusive se pueden detectar estados de ánimo o emociones, que permitan descubrir alguna situación fuera de lugar.

El reconocimiento facial para su funcionamiento requiere de **tres etapas**: detección, análisis o extracción de características y reconocimiento.

Figura 1. *Etapas del reconocimiento facial*

Fuente: Tomado de Orozco Analuiza (2022)

La **detección** significa reconocer, en una imagen, el rostro de una persona, es decir, la localización. Por medio de la visión artificial, esta

tecnología es capaz de realizar una detección e identificación individual de rostros, teniendo únicamente una imagen que tenga como contenido un rostro; detecta los datos faciales en perfiles frontales y laterales faciales. La *visión artificial* se utiliza en los equipos para la identificación de las personas, entornos y elementos que se encuentran en las imágenes más precisas, similar a la precisión del ser humano, con mayor eficacia y velocidad más altas (AWS, 2023; Orozco Analuiza, 2022). Gracias a la IA, esta tecnología realiza la automatización de "la extracción, el análisis, la clasificación y la comprensión de la información útil a partir de los datos de las imágenes" (AWS, 2023, párr. 7). La información de la imagen se puede presentar de algunas formas: "imágenes individuales, secuencias de video, visualizaciones de varias cámaras, datos tridimensionales (AWS, 2023, párr. 8).

Existen algoritmos con sus variantes que no permiten especificar cuántos métodos para detección de rostros existen. En apartados siguientes se mencionarán algunos que operan con el reconocimiento facial en sistemas biométricos.

Figura 2. *Ejemplo de detección de rostro*

Fuente: Tomado de Orozco Analuiza (2022)

El *análisis* de la imagen del rostro es el siguiente paso. "Asigna y lee la geometría del rostro y las expresiones faciales. Identifica los puntos de referencia faciales que son clave para distinguir un rostro de otros objetos" (AWS, 2023, párr. 10). Los parámetros del reconocimiento facial son, por lo general, los siguientes: 1) distancia entre ojos, de la frente a la barbilla, entre nariz y boca, 2) fondo del cuenco del ojo, 3) anatomía de los pómulos, 4) perfil de barbilla, labios y orejas.

Posteriormente se convierten los datos obtenidos del reconocimiento en la huella facial, que no es otra cosa sino una cadena de puntos o números, siendo para cada persona una huella facial única. Con los datos obtenidos del reconocimiento facial también se puede reconstruir el rostro de un individuo, si se los utiliza de forma inversa.

Por último, el *reconocimiento*, permite llevar a cabo una comparación de las caras de algunas imágenes y analizar si tienen coincidencias o no. Con esto se podrían reconocer documentos de identidad, licencias de conducir, fotos de pasaportes, revisando esas imágenes y contrastando, por ejemplo, con una foto tomada en un dispositivo móvil (AWS, 2023).

El reconocimiento facial tiene su aplicación en algunos ámbitos:

- Legal y de seguridad: análisis forense, encontrar personas extraviadas o que son víctimas de explotación, identificación de criminales, seguridad en aeropuertos, tareas de vigilancia, entre otros.
- Salud: detección de enfermedades, rastreo de medicamentos utilizados, entre otros.
- Banca y marketing: encontrar nuevos usuarios de productos, campañas publicitarias, controles de acceso, entre otros.
- Para desbloquear dispositivos inteligentes (celulares o relojes), controles de asistencia, inicio de sesiones en cuentas, etiquetado de fotos en redes sociales, entre otras muchas aplicaciones (LISA Institute, 2023).

Se pueden mencionar algunas técnicas para implementar el reconocimiento facial:

- *Holísticas*: los rostros son creados por medio de la extracción de los rasgos más sobresalientes y son representados por un vector de pesos, que son comparados con las imágenes que se almacenaron en una base de datos para ver si existe alguna coincidencia de la identidad o no de la persona que se quiere verificar.
- *Geométricas*: se representa la imagen por medio de una estructura geométrica, como líneas, puntos o curvas, para crear una plantilla con estadísticas con el propósito de realizar comparaciones; esto se utiliza,

por lo general, en el reconocimiento facial 2D. En el 3D, la información que se obtiene de la anatomía del rostro se lo compara con los metadatos que se hayan obtenido para determinar si existe o no coincidencia, tomando todos los elementos que se encuentran almacenados en la base de datos.

- *Análisis de la textura de la piel*, consiste en tomar las características de la apariencia para realizar un análisis del espacio; no influye el uso de imágenes de baja calidad, pero sí necesita de varias para realizar la comparación. La variación en la iluminación y las expresiones faciales son importantes en el momento de llevar a cabo el análisis.
- *Basadas en videos*, se realiza la identificación de un individuo entre varios que se encuentran en un video o grabación, con base en el la información facial; la imagen es dinámica y obtiene las expresiones faciales adecuadamente. Se puede crear modelos 3D y examinar las particularidades de las imágenes de la persona y las variaciones que haya tenido; su utilidad primera es la vigilancia(LISA Institute, 2023).

Entre las ventajas del reconocimiento facial se pueden mencionar las siguientes:

- Seguridad más eficiente, puesto que la verificación de la persona se realiza de manera eficaz y rápida, en comparación con otros métodos de biometría, tales como el escaneo de retina o la geometría de la mano. Los puntos de contacto para verificar la identidad de la persona son menores que cuando se introduce una contraseña; también se puede realizar la autenticación de otros factores, aumentando el nivel de seguridad.
- Más precisión, ya que identifica con mayor exactitud a las personas, en comparación con otras formas de reconocimiento, como un número móvil, dirección de correo, dirección IP, entre otras maneras.
- Mayor facilidad de integración, puesto que tiene mayor compatibilidad y se pueden integrar con otros softwares de seguridad (AWS, 2023).

Algoritmos de detección facial

Tanto los algoritmos y las técnicas que se emplean para detectar e identificar el rostro humano surgen de una intensa investigación en el área de las matemáticas, a fin de determinar el más adecuado para los ordenadores en el ámbito de la visión artificial. Entre éstos se encuentran los mencionados a continuación:

Eigenfaces (Caras Propias)

Utiliza el análisis de componentes principales (PCA) para representar las caras en un espacio dimensional reducido. Son vectores que extraen las características para reconocer los rostros, los mismos que se obtienen "a partir de una matriz de covarianza de distribución de probabilidad sobre el espacio vectorial de la imagen del rostro, mediante la posición de cada imagen representa un propio vector denominado eigenface" (Garcés Núñez, 2017, p. 36), formando un conjunto ortogonal para encontrar la imagen proyectada. Esta técnica reduce la dimensionalidad que es un método de reducción del volumen. Al momento de ejecutar este método "la matriz de covarianza se descompone en sus eigenvectores o vectores propios" (Riofrio Villamar, 2023, p. 27). Al referirse a imágenes faciales, los pixeles que la forman son diversificaciones de luminosidad, con variaciones de 0 a 255. El algoritmo Eigenfaces sigue el siguiente proceso:

- Se preparan los datos.
- Se calcula el rostro medio del conjunto de entrenamiento.
- Se calcula la matriz de covarianza.
- Se seleccionan los principales componentes.
- Se clasifican los rostros.
- Se comparan una nueva imagen de rostro con otra (Riofrio Villamar, 2023).

Fisherfaces (Caras de Fisher)

Similar a Eigenfaces, pero utiliza el análisis discriminante de Fisher en lugar de la técnica PCA, lo que puede mejorar la capacidad de discriminación; este discriminante es LDA (Análisis Discriminante Linia) y toma algunas

funcionalidades como lo son “la velocidad del sistema, la eficiencia y capacidad de operar en muchas caras en muy poco tiempo” (Granja Heredia, 2018, p. 171). Fisherfaces tiene menos sensibilidad a los cambios en la iluminación y los bordes de los rostros que se ven en las imágenes.(Granja et al., 2020).

Patrones binarios locales (LBPH Local Binary Pattern Histograms)

Este algoritmo es un descriptor que se basa en la textura facial que se encuentran en las imágenes y utiliza patrones binarios locales para describir las características faciales. Etiqueta y examina cada pixel con el próximo (de su vecino) por medio de un umbral que será un numero binario (1 o 0), “determinando si el valor de intensidad de un pixel es mayor o menor que el valor de intensidad de pixel a analizar, si el valor es mayor se asigna un (1), caso contrario se asigna un (0)” (Granja Heredia, 2018, p. 13). Son utilizados varios descriptores locales, los que fusionarán con uno de carácter global.

Redes Neuronales Convolucionales (CNN)

Las CNN son populares en reconocimiento facial debido a su capacidad para aprender características jerárquicas. Son una subárea del ML y se constituyen en la parte medular de los algoritmos de aprendizaje profundo (DEL). Se componen de:

> Capas de nodos, que contienen una capa de entrada, una o más capas ocultas y una capa de salida. Cada nodo se conecta a otro y tiene un peso y umbral asociados. Si la salida de cualquier nodo individual está por encima del valor del umbral especificado, ese nodo se activa y envía datos a la siguiente capa de la red. De lo contrario, no se pasa ningún dato a la siguiente capa de la red. (IBM, s/f, párr. 1).

El uso de las CNN se orienta hacia las tareas de clasificación de imágenes y visión artificial. Tienen una perspectiva evolutiva en cuanto a las tareas de clasificación y reconocimiento de objetos, “aprovechando principios del álgebra lineal, específicamente la multiplicación de matrices, para identificar patrones dentro de una imagen. Sin embargo, pueden ser muy

exigentes desde el punto de vista informático, ya que requieren unidades de procesamiento gráfico (GPU) para entrenar los modelos" (IBM, s/f, párr. 2).

DeepFace

Desarrollado por Facebook, utiliza una red neuronal profunda para identificar y verificar caras en imágenes, y así superar el búfer que se crea por el agujero en cuanto al rendimiento. Este modelo requiere de un entrenamiento con un gran volumen de datos de rostros, muy diferente a los grupos de datos que se utilizan para la construcción de puntos de referencia que servirán para evaluación, y es capaz de ser más eficiente que los marcos que actualmente existen, con muy pocas adaptaciones. Las representaciones de los rostros de DeepFace son compactas comparadas con otros sistemas que originan un alto volumen de particularidades de la apariencia del rostro (Kejriwal, 2023).

Detección y Reconocimiento de Puntos de Referencia Faciales

Estos algoritmos identifican puntos clave en la cara y utilizan esta información para crear una representación única.

Detectores de caras

La selección de los detectores de caras va a depender, entre otras cosas, de la herramienta que se va a utilizar, para así poder especificar la librería requerida, y la precisión del algoritmo y su dificultad. Existen algunos detectores, entre los que se pueden mencionar:

- **RetinaFace**, que aporta en la detección, los rostros difíciles; se "puede ejecutar en tiempo real en un solo núcleo de CPU para una imagen de resolución VGA" (Fernández Ordejón et al., 2021, p. 11).
- **Dual Shot Face Detection** (DSFD), se basa en SSD y aporta: mejor aprendizaje de características, diseño de pérdida progresiva, aumento de datos con base en especificación de anchor.
- **PyramidBox**, permite la selección de las caras muy pequeñas, borrosas o que pueden estar tapadas, por medio de la información proporcionada por el entorno (Fernández Ordejón et al., 2021).

- **Selective Refinement Network (SRN)**, “introduce novedosas operaciones de clasificación y regresión de dos pasos de forma selectiva para reducir los falosos positivos y mejorar la precisión de la localización” (Fernández Ordejón et al., 2021, p. 12).
- **Light and Fast Face Detector (LFFD)**, “detector de una etapa, de rostros ligeros y eficiente para dispositivos de borde” (Fernández Ordejón et al., 2021, p. 13). Especial importancia se le otorga “al campo receptivo (RF) y al campo receptivo efectivo (ERF) en la detección de las caras” (Fernández Ordejón et al., 2021, p. 13).

Herramientas informáticas

En cuanto a las herramientas informáticas, se revisarán algunos lenguajes de desarrollo y bases de datos. En los párrafos a continuación, se presenta esta investigación.

PHP

“PHP (acrónimo recursivo de PHP: Hypertext Preprocessor) es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML” (PHP.net, 2024b, párr. 1); es rápido, experto y flexible, y se ejecuta del lado del servidor (IONOS Digital Guide, 2023b; PHP.net, 2024a). Este lenguaje, conforme ha pasado el tiempo, se ha establecido como una parte esencial de algunas tecnologías web y páginas web más actuales; a pesar de estos avances, para los programadores que se encuentran en el aprendizaje de este lenguaje puede ser un desafío (IONOS Digital Guide, 2023b).

Entre las características de este lenguaje son:

- Gratuito y código abierto.
- Orientado a objetos, facilitando el procesamiento de datos.
- Permite la manipulación de datos mientras otros son estáticos.
- Código estable y limpio.
- Dispone de una comunidad grande, para compartir información y conocimientos.

- Facilita el desarrollo de páginas web dinámicas y de mayor complejidad.
- Su ejecución se puede realizar en cualquier servidor o sistema operativo.
- Versátil.
- El procesamiento de los datos puede ser manejado de mejor forma (K. Ortega, 2023).

Otra característica de PHP incluye el manejo de varios tipos de datos: integer, double, string, boolean, object, array, null, y resource (K. Ortega, 2023).

Java

De acuerdo con el sitio web de Java

> Java is a programming language and computing platform first released by Sun Microsystems in 1995. It has evolved from humble beginnings to power a large share of today's digital world, by providing the reliable platform upon which many services and applications are built. (Java, 2024, párr. 1).

Java es un lenguaje de desarrollo y plataforma informática que apareció en 1995 por la empresa Sun Microsystems. Desde entonces, ha ido evolucionando hasta convertirse en parte importante del entorno digital que actualmente existe, convirtiéndose en una plataforma confiable utilizada por numerosos servicios y aplicaciones (traducción propuesta por el autor).

Entre las características de este lenguaje se encuentran:

- Lenguaje del lado del cliente.
- Tipado estático.
- Orientado a objetos: permite encapsulación, herencia y polimorfismo.
- Portable, lo que permite que las aplicaciones puedan ejecutarse en varios sistemas operativos, sin que se recurra a modificaciones notorias.

- Lenguaje compilado, lo que significa que su código se traduce a un código de bytes para su posterior interpretación por la máquina virtual de Java (JMV).
- Concurrencia a nivel de lenguaje, para ejecutar simultáneamente partes del programa y aprovechar los recursos de manera más eficiente (Palma González, 2023).

Comparativa Java-PHP

En la Tabla 3 se presenta algunas características, fortalezas y debilidades de Java y PHP.

Tabla 3. *Comparativa Java-PHP*

Idioma	Características	Fortalezas	Debilidades	Comentario
Java	Orientado a objetos Multiplataforma	Modularización Creación de aplicaciones de escritorio Tiene soporte a desarrollo de aplicaciones móviles y web	Lenguaje interpretado, relativamente lento en comparación con otros lenguajes	Bastante documentado y fácil de aprender, contiene librerías, tiene alternativas de estructura para un desarrollo más fácil y creación de aplicaciones robustas
PHP	Para páginas web dinámicas Se ejecuta en el servidor Los usuarios no pueden ver el código PHP, solo recibir en su código de navegador HTML Las páginas que genera son visibles para cualquier navegador y computadora, dispositivos móviles que puedan interpretar el HTML. No se necesita la instalación de PHP en el lado del cliente. Versiones resistentes permiten la POO Lenguaje alto nivel	Sintaxis muy similar a otros lenguajes. Fácil de aprender Lenguaje muy popular, tiene una comunidad muy grande Rápido Multiplataforma No requiere definición de variables Puede ser combinado junto a HTML Tiene muchos marcos que facilitan el desarrollo en este lenguaje.	Necesita un servidor para funcionar La POO es deficiente para aplicaciones grandes Todo el trabajo y realiza en el servidor y mucha información o solicitudes pueden ser ineficiente	Lenguaje muy bien documentado y se pueden encontrar ejemplos y tutoriales lo cual lo hace una muy buena opción para aprender y conocer sobre la programación

Fuente: Adaptado de Course Hero (2018)

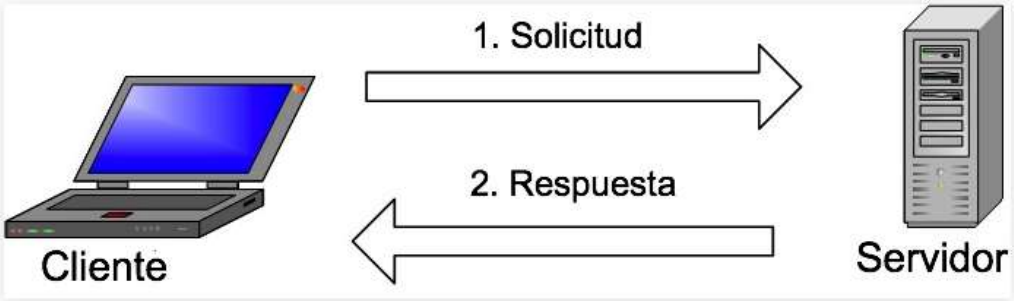
MySQL

Sistema gestor de bases de datos relacionales de Oracle, utilizada para almacenar datos de servicios web, de código abierto. Los datos son gestionados y presentados en tablas; es un sistema cliente-servidor: la base

de datos es el servidor de almacenamiento de la información de mayor importancia, mientras que el software funciona como cliente; tiene alta independencia de la plataforma que se utilice (IONOS Digital Guide, 2023b).

En la Figura 3 se presenta cómo funciona MySQL.

Figura 3. *Funcionamiento de MySQL*



Fuente: Hostinger (2023)

La Figura 3 ofrece una explicación básica del funcionamiento de la arquitectura cliente-servidor. El o los clientes pueden efectuar una solicitud desde la interfaz gráfica y el servidor ejecutará la salida requerida (Hostinguer, 2023).

Por medio del software, los usuarios están en la facultad de “formular diversas consultas, denominadas “queries”, en el lenguaje de consulta SQL y enviarlas al sistema de base de datos. Estos son procesados por MySQL, por lo que el acceso a los datos es también una parte importante” (IONOS Digital Guide, 2023a).

MariaDB

MariaDB es un fork de MySQL, que fue creado para mantener la estructura y características de MySQL, por cuanto Oracle, la empresa que era la mayor competidora de MySQL hasta ese momento, comprometiera la base de datos. Para cada nueva versión de MariaDB, los desarrolladores se aseguran que tenga compatibilidad con la versión de MySQL; MariaDB, aparte de adaptar los archivos de definición de datos y tablas de MySQL, hace uso de “protocolos de cliente, API de cliente, puertos y sockets idénticos. El objetivo es que los usuarios de MySQL puedan cambiar a MariaDB sin problemas” (Hostinguer, 2023, párr. 11).

De la misma manera que lo hace MySQL, MariaDB puede modificarse por medio de instrucciones SQL (Hostinguer, 2023).

Comparativa MySQL-MariaDB

En la Tabla 4 se muestra una comparativa de las bases de datos MySQL y MariaDB.

Tabla 4. *Comparativa de bases de datos*

	MySQL	MariaDB
¿Qué es?	Gestor de bases de datos, más usado y reconocido en el mercado, orientada especialmente a desarrollo web, de código abierto	Gestor de bases de datos, muy relacionado con MySQL. El objetivo de su desarrollo fue mantener el software de gestión de base de datos con software libre.
Características	Permite escoger múltiples motores de almacenamiento para cada tabla. Ofrece seguridad en la conectividad. Amplio subconjunto del lenguaje SQL.	Mejoras en la velocidad. Extensiones. Alertas y detección de errores. Amplia documentación y ayuda.
Compatibilidad	Linux. Mac. Windows.	Unix. Windows. Solaris. Linux. OS X. BSD
Ventajas	Uso libre y gratuito. Licencia GPL. Facilidad de instalación y configuración.	Nuevos motores de almacenamiento más eficientes. Estadísticas para índices y tablas que pueden ayudar para la optimización de la base de datos.
Desventajas	Muchas de sus utilidades no tienen documentación. Se debe controlar y/o monitorear el rendimiento de las aplicaciones en busca de fallos.	La migración.

Fuente: Raya Camacho (2022)

Software de administración de dispositivos de seguridad electrónica

De la misma forma que en otros sectores, el ámbito de la seguridad electrónica ha sufrido cambios en años recientes. Las normas de seguridad en las organizaciones se han tornado más rigurosas, puesto que exigen celeridad y capacidad de respuesta. Estas situaciones involucran dos situaciones importantes:

- Las empresas que ofrecen sistemas de seguridad están en la obligación de garantizar a sus usuarios, “productos, soluciones y procesos de atención y soporte son de alta calidad. La inversión en I + D no es una opción, sino un requisito imprescindible, así como la formación adecuada, regular y renovada de los profesionales” (Praxedo, 2023, párr. 10).
- Ofrecer soluciones diferenciadoras es un punto clave dentro del competitivo mercado tecnológico, puesto que el servicio a brindar a los clientes debe ser primordial, para garantizar su fidelidad.

Por tales motivos, las empresas que quieran permanecer en el mercado y evolucionar en estas condiciones, deberán considerar la viabilidad de su modelo de negocio, buscar invertir en nuevos desarrollos tecnológicos que les permitan mejorar su trabajo y convertirla en una empresa más competitiva (Praxedo, 2023).

Importancia de invertir en sistemas de seguridad en el Ecuador

La seguridad de los ciudadanos está relacionada con las actividades e ideas que se orientan hacia la prevención y disminución de los índices de violencia, favoreciendo la seguridad pública, además de fortaleciendo el compromiso de los ciudadanos y el estado. “Conjuntamente, la seguridad ciudadana implica establecer lineamientos de seguridad pública efectiva en relación a reglamentos democráticos más amplios” (Salas et al., 2022, p. 113).

En los países latinoamericanos, no obstante que cada uno está regido bajo su sistema económico y metas a alcanzar, tienen en común un reto, que es el de tratar de orientar ese crecimiento hacia un desarrollo para todos sus pobladores. En ese reto se encuentra inmersa la seguridad, que es quizás la brecha de mayor importancia que deben solucionar; esto se demuestra en las

estadísticas que colocan a América Latina y el Caribe como la región con mayores índices de violencia a nivel mundial (K. M. Ortega & Pino, 2021).

En el Ecuador, la seguridad se ha convertido en una de las debilidades más grandes. Los reportes de violencia, asesinatos y otro tipo de delitos ha aumentado en los últimos años, lo que ha tenido un impacto social y económico bastante alto; delitos que afectan a la seguridad ciudadana, tales como homicidios, drogas, narcotráfico, han deteriorado la percepción de la seguridad ciudadana (K. M. Ortega & Pino, 2021). A nivel social, la inseguridad afecta en la pérdida de capital social, pérdida de vidas humanas y pobreza, migración forzada; las empresas y el sector privado se han visto en la necesidad de cambiar su accionar debido a la violencia: en casos extremos, sobre todos los más pequeños, tienen la opción de convertirse en informales para poder cuidar su trabajo y sus ganancias para no llamar tanto la atención y no ser el centro de atención de los criminales.

En este escenario de cosas, para las empresas se convierte en una necesidad la inversión en proyectos de sistemas de seguridad, puesto que se requiere precautelar la integridad de todos los ciudadanos, que se encuentran afectados por la alta ola delincuencial. Las empresas dedicadas a ofrecer seguridad, están en la obligación de mantenerse a la vanguardia en las nuevas herramientas tecnológicas, y ofrecer productos y/o servicios que se conviertan en instrumentos de apoyo de personas y organizaciones que los utilicen; de esta forma el ciudadano puede sentir mayor protección frente a la inseguridad que se vive actualmente en el país.

Contexto del proyecto

El estudio se lleva a cabo en la UCSG, institución de estudios superiores que se creó en 1962, como un pedido de la junta pro universidad católica, presidida por el arzobispo de Guayaquil y otras autoridades. El acuerdo ejecutivo 936, emitido por el entonces presidente de la república, fue aprobado y el Ministerio de Educación, mediante la resolución 1158, autorizó la entrada en funcionamiento de la universidad.

A los 19 días de expedido el acuerdo ministerial, se dio inicio al primer período de clases en las facultades de “Jurisprudencia, Ciencias Sociales y

Políticas, Filosofía, Letras y Ciencias de la Educación y Ciencias Físicas y Matemáticas (Escuelas de Ingeniería Civil y Arquitectura)" (UCSG, s/f-d, párr. 3) en el colegio nocturno jesuita 20 de abril, cuyos cursos se mantuvieron hasta 1966, que fue la inauguración del edificio principal en el campus universitario en donde se encuentra actualmente.

Se crearon algunas facultades en años siguientes: en 1963 la Escuela de Economía, aprobándose en 1965 la Facultad de Economía; en 1965, Arquitectura, en 1967-1968 se crearon el Instituto de Educación Técnica para el Desarrollo (Facultad desde 1977), con las Escuelas de Zootecnia y Electricidad y Telecomunicaciones, y la Facultad de Medicina; en 1969 la Escuela de Trabajo Social, en 1970 el Instituto de Artes Aplicadas. En 1973 la Facultad de Ciencias Médicas, en 1985 la Escuela de Ingeniería en Sistemas Computacionales, en 2003 la Facultad de Especialidades Empresariales y en 2005 la Facultad de Artes y Humanidades (UCSG, s/f-d).

Misión

"Generar, promover, difundir y preservar la ciencia, la tecnología, el arte y la cultura, formando personas competentes y profesionales socialmente responsables para el desarrollo sustentable del país, inspirados en la fe cristiana de la Iglesia Católica" (UCSG, s/f-b, párr. 1).

Visión

"Ser una Universidad Católica, emprendedora y con liderazgo académico dentro y fuera de las fronteras patrias, que incida en la construcción de una sociedad nacional e internacional, eficiente, justa y sustentable" (UCSG, s/f-e, párr. 1).

Objetivos

La principal meta de la UCSG es la formación de profesionales responsables con la sociedad, con base en "la investigación, conservación, promoción y difusión de la ciencia y de la cultura" (UCSG, s/f-c, párr. 1), resaltando sus propios valores, con la finalidad de que el ciudadano encuentre su superación personal. El cumplimiento de estos objetivos se llevará a cabo porque la universidad:

- Se responsabilizará de su papel de responsabilidad social como institución.
- Vigilará el cumplimiento objetivo de “la investigación, conservación, promoción y difusión de la ciencia, la técnica y la cultura” (UCSG, s/f-c, párr. 2).
- Favorecerá la igualdad de oportunidades en la educación, de acuerdo con los planes de la institución, los mismos que se encuentran en constante crecimiento.
- Se orientará hacia la formación científica, técnica y con atención al ser humano en todos los ámbitos de su existencia.
- Tratará de mantener un equilibrio entre ciencia y fe.
- Se preocupará por mantener el autoanálisis para el mejoramiento personal e institucional (UCSG, s/f-c).

Área administrativo académica

El área administrativa académica en la que se va a desarrollar el proyecto, se refiere a la Facultad de Ingeniería. Su historia de creación se remonta a 1977, cuando el consejo universitario dio su aprobación para la nueva conformación de la estructura de la universidad, que se constituyeron en Facultades entre ellas la de Ingeniería “con la Escuela de Ingeniería Civil. Se aclaró que se entiende por Facultad a un ente administrativo-académico, semiautónomo, que está constituido por Escuelas. Las Escuelas son unidades independientes de la Facultad, para la enseñanza de materias afines previa la concesión de títulos profesionales y académicos (UCSG, s/f-a, párr. 5).

En el año 1985 el consejo universitario se iniciaron las actividades de la Escuela de Sistemas Computacionales de la Facultad de Ingeniería. A partir de 1973 la Facultad de Ingeniería tiene sus propias instalaciones, y desde entonces se ha incorporado nuevas construcciones o rediseños conforme las nuevas necesidades de estudio y de espacio físico, dependiendo de las circunstancias.

En sus instalaciones se encuentra un auditorio, la asociación de estudiantes de Ingeniería en Sistemas Computacionales, las aulas de clases, la sala de profesores, el decanato, las direcciones de carrera y la coordinación,

además de otros edificios para Ingeniería Civil (UCSG, s/f-a). El área administrativo académica está conformada por la secretaría general, en donde se atienden los asuntos académicos de las dos carreras.

Normativas que rigen el uso de la tecnología para la seguridad

De acuerdo a una investigación realizada por Almeida et al. (2021) quienes llevaron a cabo un diagnóstico de la videovigilancia, reconocimiento facial y las violaciones de los derechos de los ciudadanos, se refirió la importancia que tiene el derecho a la privacidad de las personas en el cumplimiento de otros derechos humanos como "la libertad de expresión, libertad de asociación y reunión, hasta el acceso y goce de los derechos económicos sociales y culturales" (Almeida et al., 2021, p. 10). La privacidad es un derecho de las personas que es aplicados a todos por igual; las diferencias que pueden existir en referencia al respeto a este derecho no tienen compatibilidad con el derecho a la igualdad y no discriminación, que se encuentra estipulado en **artículo 26** del **Pacto Internacional de Derechos Civiles y Políticos.**

En concordancia con lo anterior, se entiende que la privacidad, de acuerdo con las normativas internacionales es un entorno de evolución independiente, en donde la interactividad se lleva a cabo de forma libre, sin que exista injerencia de las autoridades de gobierno ni la intromisión de otras personas; todo lo anterior en cuanto a aplicarse a espacios de orden público, ya que la privacidad solamente se daría en espacios privados (Almeida et al., 2021).

La evolución constante de la tecnología ha conducido a que la privacidad de las personas se encuentre al descubierto cuando los gobiernos por medio de los sistemas de vigilancia, para identificar, rastrear, determinar perfiles, realizar reconocimiento facial; este tipo de actividades representan intrusión y vulneración del derecho de las personas a la privacidad y la libre práctica de otros derechos. Cabe resaltarse que el uso adecuado, legítimo y legal de los sistemas de vigilancia, están en la capacidad de ofrecer una garantía en identificar actos de violencia, mas cuando su utilización es ilegítima, se pueden convertir en herramientas para cometer cualquier acto

que vulnere los derechos de las personas. Un ejemplo de esto es la implementación de sistemas de vigilancia mediante reconocimiento facial (Almeida et al., 2021).

El reconocimiento facial compara la captura digital de la imagen de una persona con otras almacenadas en una base de datos, de manera que se pueda determinar la posibilidad de la identificación del individuo de acuerdo con el criterio de quien use el sistema. Es así que esta herramienta puede convertirse en un riesgo para el ejercicio de algunos derechos, puesto que se puede señalar de forma equivocada a personas que hayan cometido algún delito, se amplíe la discriminación de grupos desprotegidos o en ambiente de desigualdad social, además de vulnerar la libertad de expresión y asociación pacífica.

A nivel nacional, la **Constitución de la República**, en su **artículo 66** numeral 19 se refiere a que todas las personas tienen el derecho a que se protejan sus datos personales, incluyendo el acceso a los mismo, cualquier decisión que se tenga sobre aquellos y su respectiva protección. Cualquier actividad que con ellos se lleve a cabo, deberá estar autorizada por su titular o la decisión de la ley (Asamblea Nacional, 2008).

En el **artículo 92** se menciona que las personas tuenen derecho a "conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico" (Asamblea Nacional, 2008, p. 67), así como a conocer cuál será el uso que a aquellos se les dé.

Una de las leyes que rige para el uso de la tecnología, en este caso, el reconocimiento facial, es la **Ley de protección de datos**, que en su **artículo 1** Objeto y finalidad, se refiere a que se deberá "garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección…" (Asamblea Nacional, 2021, p. 5).

El **artículo 2** Ámbito de aplicación material, se refiere a que su aplicación será de “cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior” (Asamblea Nacional, 2021, p. 5).

Dentro de los términos y definiciones del **artículo 4** se mencionan:

- Base de datos o fichero, es un conjunto de datos estructurado de cualquier forma, modo de creación, almacenamiento, tipo de soporte, localización, tratamiento o repartición.
- Consentimiento, es decir, la autorización del titular de los datos para su tratamiento a la persona autorizada para su manejo.
- Dato biométrico, es aquel “dato personal único (…) que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros” (Asamblea Nacional, 2021, p. 6).
- Dato personal, es aquel que permite la identificación de una persona natural, de forma directa o indirecta.

El **artículo 8** se refiere al consentimiento sobre el tratamiento y comunicación de los datos personales, cuando exista la voluntad del titular para que se haga ese proceso (Asamblea Nacional, 2021).

A pesar de que esta ley se encuentra vigente, se han reportado casos de vulneración de sus mandatos por una indiscriminada videovigilancia, la divulgación de imágenes para publicidad y la inexistencia de “transparencia en los protocolos de manejo y archivo de la información recopilada” (Almeida et al., 2021, p. 12).

CAPÍTULO III
METODOLOGÍA

Para llevar a cabo la ejecución de este proyecto, se requiere el planteamiento de la metodología determinándose dentro de la metodología de la investigación el tipo, enfoque, población y muestra, las técnicas e instrumentos de recolección de información y el análisis de los resultados; para complementar este apartado, se hace referencia a la metodología de desarrollo que se utilizó para la creación de la solución informática.

Tipo de investigación

Este proyecto es *descriptivo*, puesto que este tipo de investigación detalla todas las particularidades o puntos característicos de un hecho o situación que se está estudiando. Se lo considera uno de los procedimientos de mayor uso en el área de la investigación, ya que facilita la narración de todos los aspectos que distinguen las personas, hechos, problemas, situaciones o cosas, es decir, las cualidades que los distinguen frente a los demás (Bernal Torres, 2016, p. 156).

Por lo tanto, esta investigación es descriptiva, porque se conocen las características del problema que presenta el área administrativa de la Facultad de Ingeniería, en cuanto al ingreso de personas ajenas a la Universidad para realizar algún trámite estudiantil, ya que este suceso se da porque el acceso a las oficinas se encuentra desprotegido, facilitando que cualquier persona ingrese sin ninguna restricción y ponga en un posible riesgo la integridad de todas las personas de la Facultad, sobre todo a entornos que deberían estar aislados y resguardados.

Enfoque metodológico

Según lo manifestado por Gallardo Echenique (2017) dentro de los paradigmas de la investigación se encuentran diferentes enfoques, es decir, la forma cómo el investigador entiende algún problema y plantea la resolución del mismo, siempre en contexto con los lineamientos conceptuales. Dentro de estos paradigmas de encuentran el cuantitativo (positivista), cualitativo (interpretativo) y mixto.

Para el desarrollo de este proyecto, se requirió del enfoque metodológico *cualitativo*, en donde el trabajo de la persona que investiga el problema es realizar un estudio del proceso que siguen los actores sociales para interpretar la realidad; esto significa que el investigador deberá asignar un determinado significado al problema motivo de investigación (Gallardo Echenique, 2017).

Por otro lado, Hernández-Sampieri y Mendoza Torres (2018) mencionaron que este enfoque realiza un estudio de los hechos, fenómenos o problemas de forma sistemática. El investigador inicia el proceso revisando y estudiando los hechos entre sí y estudios previos al tema, acciones que deberán realizarse a la par, con el fin de forjar una teoría que sea consecuente con la observación de lo que está sucediendo.

En el mismo tema, Bernal Torres (2016) el enfoque cualitativo busca examinar casos específicos más no generalizar. No se preocupa exactamente de medir, sino de “cualificar, describir e interpretar el fenómeno (situación o sujeto) social a partir de rasgos determinantes, según sean percibidos por los elementos que están dentro de la situación estudiada” (Bernal Torres, 2016, p. 72). El uso de este paradigma en la investigación permite entender un problema como un conjunto, considerando siempre sus particularidades y dinámica.

Por lo anotado anteriormente, se justificó el enfoque cualitativo de este proyecto, porque se analizó la situación del problema de la inseguridad que en la actualidad se vive en el Ecuador y su repercusión en la ciudadanía en general, particularmente en el ámbito académico de la UCSG y en el área administrativa de la Facultad de Ingeniería. En este sentido, se revisó la literatura relacionada con la violencia a nivel de la ciudad de Guayaquil, y cómo se está viviendo el tenso ambiente de los hechos delictivos en las instituciones educativas. Complementa este análisis las entrevistas realizadas a directivos, docentes y personal administrativo sobre la necesidad de implementar mayor seguridad interna con una herramienta tecnológica de control de acceso.

Población y muestra

Para este proyecto, la población está dada por todos los sujetos que participan en el estudio. Al ser éste un estudio de enfoque cualitativo, no es necesario la estimación de la población; por lo tanto, el cálculo de la muestra como tal tampoco es requerido, pero se realizará un *muestreo intencional*, que seleccionará a los informantes clave de quienes conforman la Facultad de Ingeniería, es decir autoridades, docentes y asistentes administrativas, para obtener información valiosa que servirá para conocer opiniones sobre la implementación del proyecto.

El *muestreo intencional* es parte de la clasificación del muestro no probabilístico, y se refiere a que la elección de los elementos se realizará con base en el juicio que tenga el investigador para determinar la importancia de la fuente a seleccionar (Arias, 2016).

Técnicas e instrumentos de recolección de datos

En cuanto a las técnicas de recolección de datos, se puede mencionar que se refieren a las variadas formas que el investigador consigue la información que busca para el análisis de su proyecto. Entre las técnicas que existen se encuentran la entrevista, observación, encuesta, análisis documental, entre otras (Arias, 2016). La entrevista consiste en recopilar información de interés público o, investigar un tema o cuestión en desarrollo. Las entrevistas nos permiten recopilar información sobre un tema, situación o persona a partir de testimonios de primera mano o de expertos en la materia (Martínez, 2023).

Para este proyecto, se aplicará la *entrevista* a cinco miembros de la Facultad de Ingeniería, que serán los informantes clave, los mismos que ofrecerán información importante de la situación actual de seguridad interna, para que aporten conocimiento que permita proponer la herramienta tecnológica que ayude a mejorar el tema de la seguridad.

Sobre los instrumentos, “los medios materiales que se emplean para recoger y almacenar lo información” (Arias, 2016, p. 111). Entre éstos se pueden mencionar los cuestionarios de entrevista, lista de cotejo, grabador,

etc. Como instrumento de la entrevista, se utilizará el *cuestionario* para la formulación de las preguntas a los informantes.

Metodología de desarrollo

La metodología utilizada fue el *prototipado*, que "permite realizar y materializar diversas ideas de soluciones propuestas en un proyecto de diseño o rediseño de productos y servicios. (…) puede estar vinculado al recorrido completo de un servicio o bien a un punto de contacto específico" (Gerea, 2021, párrs. 5–6). De cualquier forma, se deberá representar escenificar la solución con el fin de que los usuarios finales participen en dicho proceso.

El prototipado sirve para:

- Validación de ideas, cuando se diseñan productos y/o servicios nuevos.
- Testeo oportuno de ideas antes de realizar el despliegue.
- Desarrollo de distintos tipos de opciones para soluciones
- Definición de criterios antes del planteamiento del diseño último del producto.
- Modelar y concretar una idea para una solución de un producto y/o servicio.
- Participar de las experiencias de los usuarios, para conseguir sus respuestas sobre el modelo que se está diseñando.
- Anticipar los resultados de las ideas de la solución.
- Ahorro de recursos, porque se puede validar el producto antes de que no responda a las necesidades del cliente (Gerea, 2021).

Para el diseño e implementación de un prototipo, se deben seguir algunas fases:

- **Definición de los requerimientos**, establecer cuál es la finalidad del prototipo, a qué ámbito pertenece, cuáles son los elementos necesarios para su diseño.
- **Diseño del prototipo de la idea**: se determina el tipo de prototipo que se ajusta a las necesidades del cliente y también "factores como el

diseño, montaje, ergonomía, materiales, formas, dimensiones, entre otros” (Gerea, 2021, párr. 17)**.**

- **Analizar los resultados y aprendizaje**, se perfecciona la definición del producto y su desempeño, luego de haber realizado la definición del mismo.
- **Implementación del prototipo**, luego de haber analizado los resultados, para su funcionamiento.

Análisis de resultados

Aplicación de la Entrevista

Entrevistado: Ing. Galo Cornejo, Mgs.

1. **¿Conoce Ud. si en la UCSG o en sus inmediaciones, se ha registrado algún evento de seguridad?**

   Algunos. Sin embargo, es común que las instituciones educativas implementen medidas de seguridad para proteger a su comunidad universitaria.

2. **¿Qué medidas conoce Ud. que la UCSG ha implementado para mejorar la seguridad interna y precautelar la vida de toda la comunidad universitaria?**

   La Universidad Católica de Santiago de Guayaquil ha implementado diversas medidas, como la instalación de cámaras de seguridad, la contratación de personal de seguridad, la implementación de sistemas de control de acceso y la realización de capacitaciones en seguridad para la comunidad universitaria.

3. **¿Qué tecnologías conoce Ud. que existen para restringir el acceso de personas?**

   Algunas tecnologías para restringir el acceso de personas incluyen sistemas de identificación biométrica, tarjetas de acceso, sistemas de reconocimiento facial, sistemas de reconocimiento de huellas dactilares y sistemas de reconocimiento de voz.

4. **¿Tiene conocimiento si en la UCSG se ha implementado algún sistema de reconocimiento facial para restringir el acceso de personas y mejorar la seguridad interna?**

   No tengo acceso a información específica sobre la implementación de tecnologías de seguridad en la UCSG. Sin embargo, la implementación de un sistema de reconocimiento facial podría ser una medida efectiva para mejorar la seguridad interna de la institución.

5. **¿Qué ventajas considera Ud. que tienen los sistemas biométricos de reconocimiento facial?**

   Algunas ventajas de los sistemas biométricos de reconocimiento facial incluyen su rapidez y precisión en la identificación de personas, su capacidad para operar en tiempo real, su facilidad de uso y su capacidad para funcionar en diversos entornos y condiciones de iluminación.

6. **¿Cuáles serían las desventajas de los sistemas de reconocimiento facial?**

   Algunas desventajas de los sistemas de reconocimiento facial incluyen posibles problemas de privacidad y seguridad de datos, la posibilidad de errores de identificación, la susceptibilidad al sesgo algorítmico y la necesidad de una infraestructura tecnológica costosa.

7. **¿Cómo se controla el acceso de las personas al área administrativa de la Facultad de Ingeniería?**

   El acceso al área administrativa de la Facultad de Ingeniería podría controlarse mediante la implementación de medidas de seguridad físicas, como la instalación de cerraduras, la asignación de tarjetas de acceso y la supervisión por parte del personal de seguridad.

8. **¿Estaría de acuerdo con la lectura de rostro de las personas para acceder al área administrativa de la Facultad de Ingeniería?**

   La opinión sobre la lectura facial para acceder al área administrativa puede variar según las preferencias personales y las preocupaciones éticas y de privacidad de cada individuo.

9. **¿En qué ayudaría la implementación de un sistema biométrico de reconocimiento facial en la Facultad de Ingeniería?**

   La implementación de un sistema biométrico de reconocimiento facial en la Facultad de Ingeniería podría ayudar a mejorar la seguridad

interna al controlar el acceso de personas autorizadas, agilizar los procesos de identificación y registro y reducir los riesgos asociados con el acceso no autorizado.

Entrevistado: Ing. José Lumbano

1. **¿Conoce Ud. si en la UCSG o en sus inmediaciones, se ha registrado algún evento de seguridad?**

   La verdad que no conozco algún evento así en la universidad

2. **¿Qué medidas conoce Ud. que la UCSG ha implementado para mejorar la seguridad interna y precautelar la vida de toda la comunidad universitaria?**

   No, el acceso se lo hace a través de un código QR generado periódicamente, y el acceso a las áreas administrativas es controlado por el agente de seguridad asignado a los puntos correspondientes.

3. **¿Qué tecnologías conoce Ud. que existen para restringir el acceso de personas?**

   Herramientas de IOT como biometricos, cámara de seguridad.

4. **¿Tiene conocimiento si en la UCSG se ha implementado algún sistema de reconocimiento facial para restringir el acceso de personas y mejorar la seguridad interna?**

   No, desconozco, pero sería muy factible que se implemente esta herramienta para mejorar la seguridad.

5. **¿Qué ventajas considera Ud. que tienen los sistemas biométricos de reconocimiento facial?**

   Considero que ofrecen mayor rapidez para el usuario al ingresar al área administrativa así dando una mayor seguridad a los usuarios.

6. **¿Cuáles serían las desventajas de los sistemas de reconocimiento facial?**

   Algunos sistemas dependen de electricidad y a veces se ven afectados por cortes de luz.

7. **¿Cómo se controla el acceso de las personas al área administrativa de la Facultad de Ingeniería?**

Para tener acceso las personas al área administrativa dependen de la supervisión de un agente de seguridad.

8. **¿Estaría de acuerdo con la lectura de rostro de las personas para acceder al área administrativa de la Facultad de Ingeniería?**

   Si, para lograr tener mayor seguridad dentro del área administrativa.

9. **¿En qué ayudaría la implementación de un sistema biométrico de reconocimiento facial en la Facultad de Ingeniería?**

   Ayudaría a mejorar la seguridad al controlar de manera más efectiva también se podrá agilizar los procesos de identificación al personal administrativo, docentes y estudiantes.

Posterior a las entrevistas realizados a expertos, se lleva a la conclusión que es importante la implementación de un sistema de seguridad que permita llevar un control del personal que ingresa al área administrativa de la Facultad de Ingeniería, considerando el alto nivel de inseguridad que existe en la ciudad de Guayaquil al momento de la escritura de este documento.

Se sugiere el uso de dispositivos que integren algoritmos de reconocimiento facial, garantizando la calidad del servicio, al aprovechar la experiencia que tienen los fabricantes en sistemas de seguridad que utilizan características personales de los usuarios como su rostro, retina, huellas dactilares para la identificación de los mismos.

Durante el proceso de investigación, se entrevistó a un profesional experto en el campo de seguridad física, quien ocupa el cargo de jefe de seguridad en una empresa de seguridad del sector privado, quien ha sugerido un manual de procedimientos de acceso aplicado a un área administrativa, basado en un control de acceso biométrico y contando con agentes de seguridad, dicho procedimiento es descrito a continuación.

Procedimiento de Acceso a Área Administrativa

Administrativo:

- **Registro del Rostro Biométrico:**

- Todo el personal administrativo debe registrar su rostro en el sistema de control de acceso biométrico. Este registro debe incluir la captura y almacenamiento de imágenes faciales para su posterior verificación, este requerimiento debe estar a cargo de una persona asignada por la administración.

- **Ingreso al Área Administrativa:**
  - Al llegar al área administrativa, el personal administrativo debe dirigirse al punto de acceso biométrico designado.
  - El personal se posiciona frente al dispositivo de reconocimiento facial para que su rostro sea escaneado.
  - Si el rostro del personal coincide con los registros almacenados, se autoriza el acceso al área administrativa.

Guardia:

- **Asignación de Tarjeta RFID:**
  - Se asigna la tarjeta RFID al guardia de turno para su identificación.
  - La tarjeta RFID debe estar programada con la información de acceso necesaria y vinculada al sistema de control de acceso.
- **Ingreso al Área Administrativa:**
  - El guardia de turno se acerca al lector de tarjetas RFID instalado en el punto de acceso al área administrativa.
  - El lector de tarjetas RFID verifica la identidad del guardia comparando la información de la tarjeta con los registros almacenados en el sistema.
  - Si la identificación es válida, se autoriza el acceso al área administrativa.

Consideraciones Generales:

- **Seguridad de Datos:**
  - Todos los datos biométricos y de identificación personal deben almacenarse de manera segura y cumplir con las regulaciones de privacidad y protección de datos.
- **Mantenimiento del Sistema:**

- Se debe realizar un mantenimiento regular del sistema de control de acceso biométrico y los lectores de tarjetas RFID para garantizar su correcto funcionamiento.

- **Capacitación del Personal:**
  - El personal administrativo y el guardia de turno deben recibir capacitación sobre el uso adecuado del sistema de control de acceso y las medidas de seguridad asociadas.
- **Auditoría y Monitoreo:**
  - Se deben realizar auditorías periódicas del sistema para garantizar su integridad y seguridad.
  - Se puede implementar un sistema de monitoreo para registrar los accesos y detectar posibles anomalías o intentos de acceso no autorizados.

CAPÍTULO IV
PROPUESTA TECNOLOGICA

Este capítulo hace referencia a la implementación del sistema biométrico de reconocimiento facial utilizado para solucionar el sistema de seguridad dentro del área administrativo de la Facultad de Ingeniería de la UCSG. El objetivo de la implementación del sistema es la automatización del proceso de ingreso del personal administrativo, docente y estudiantes, que tengan autorizado el acceso; las personas que no están registradas deberán habilitar su acceso con el agente de seguridad encargado.

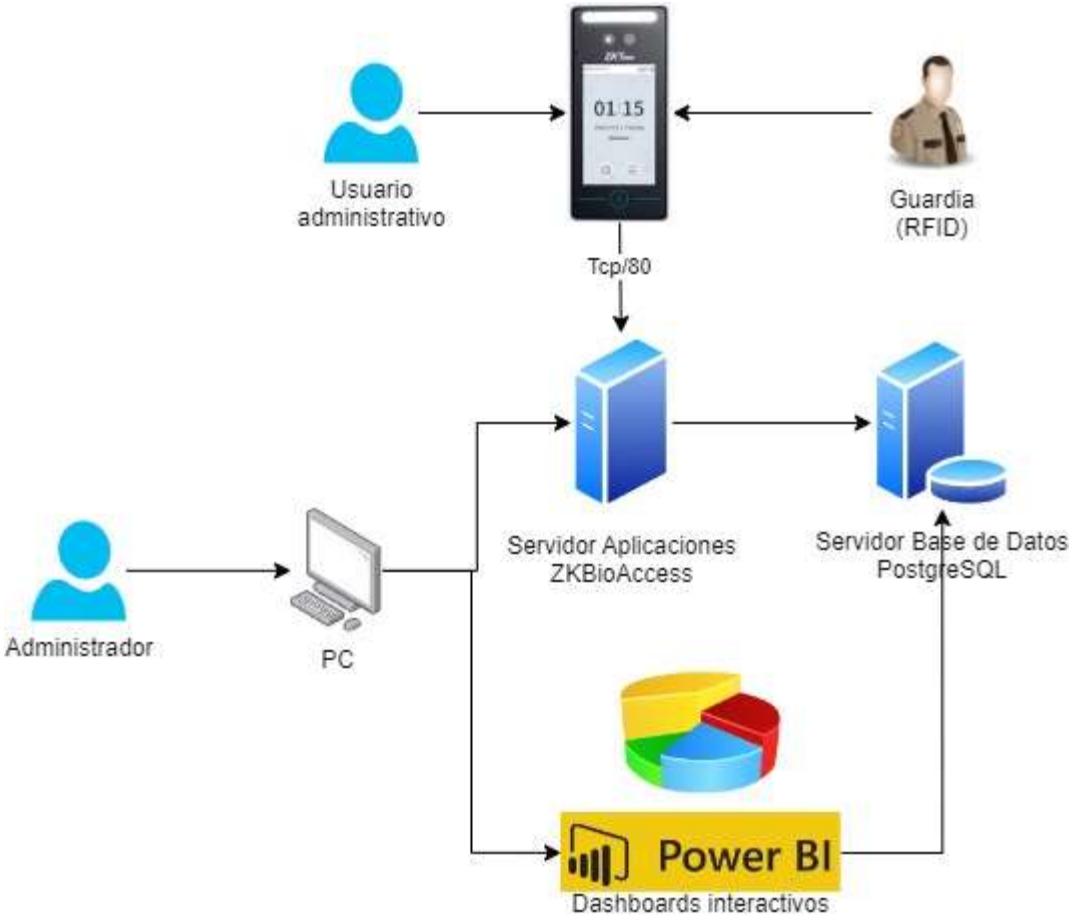
Para la Facultad de Ingeniería, la solución permitirá identificar al individuo al colocarse frente a la pantalla del biométrico, donde tomará imagen de su rostro, posterior será identificado y automáticamente se desbloqueará la puerta habilitando el acceso correspondiente.

A continuación, se presenta el proceso de desarrollo de la herramienta tecnológica

Arquitectura Solución

La arquitectura solución detalla los componentes tanto de hardware como de software que son partes de la propuesta, esta soporta el siguiente proceso: un usuario administrativo ingresa con la identificación de su rostro y el agente de seguridad con la Tarjeta RFID asignada al puesto, la parametrización se encuentra registrada en el software ZKBioAccess. El administrador visualiza los registros de eventos de acceso de entrada y salida. ZKBioAccess utiliza una base de datos en PostgreSQL, a la cual se conecta un módulo de Power BI, para obtención de los datos y presentación de la información en cuadros de mandos ejecutivos, cabe recalcar que esta arquitectura funciona sobre la infraestructura tecnológica de la UCSG.

Figura 4. *Arquitectura Solución del Sistema propuesto*



Fuente: El Autor

Infraestructura tecnológica

Hardware

Tabla 5: *Especificaciones del Dispositivo ZK-SpeedFace-4VL*

	ZK-SpeedFace-4VL
Capacidad:	**Número Rostros:** 800 **Número Palma:** 800 **Número Tarjetas:** 1000
Lector de Tarjeta:	RFID
Pantalla	Pantalla Táctil de 4”
Conexión	TCP/IP, Wi-Fi(2.4 Ghz), USB, RS485

Fuente de Alimentación	12v 3A

Fuente: El Autor

Software

Tabla 6*: Especificaciones de PostgreSQL*

PostgreSQL	
Última Versión:	16.2 - 8 de febrero de 2024
Soporte en Lenguajes de programación	C, C#, Perl, PHP, Haskell, Python. Ruby, Java.
Escalabilidad:	Aceptado
Script del lado de servidor:	Solo funciones personalizadas en modo Usuario
Tipo de Seguridad:	Alta
Nivel de Consumo de Recursos:	Alto

Fuente: El Autor

La base de datos. Para el software. ¿Qué conecta con el dispositivo biométrico? Debe ser. PostgreSql, el gestor. Sí soporta. La compatibilidad con el lenguaje de programación PHP. En ambiente web.

Tabla 7: *Especificaciones de ZKBio CVAccess*

ZKBio CVAccess	
Ultima Versión:	4.0.1
Lenguajes de programación:	PHP, Python
Tipo de Marcación	Reconocimiento Facial Reconocimiento de Palma Reconocimiento por Tarjeta RFID
Cantidad de Credenciales:	Múltiple

Soporte de Base de Datos:	Por defecto: PostgreSQL Opcionales: MS SQL Server, MySQL y Oracle
Licenciamiento:	Estándar Gratuito

Fuente: El Autor

Esta herramienta es una aplicación web. Que está ejecutada. En el lenguaje de programación PHP Y se conecta. con la base de datos PostgreSQL. Esta aplicación se integra mediante un servidor propio De tipo local. Para ejecutar De manera funcional.

Tabla 8: *Especificaciones de Power BI*

Power BI	
Framework:	.NET Framework 4.8
Almacenamiento:	**Disco Duro:** 1Gb Mínimo **Memora RAM:** 1Gb Mínimo – 4Gb Recomendado
Sistema Operativo:	• Windows Server 2022 • Windows Server 2019 Datacenter • Windows Server 2019 Standard • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows 10 Home • Windows 10 Professional • Windows 10 Enterprise
Soporte de Base de Datos:	PostgreSQL, MySQL, MS SQL Server y Oracle
Conexión principal:	Microsoft Office 365

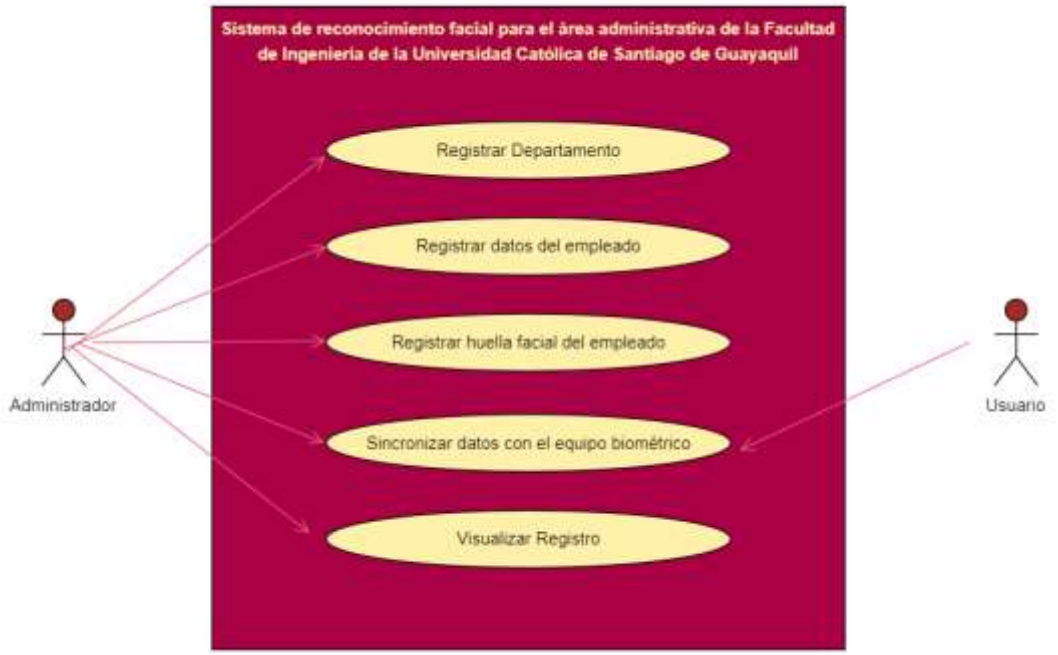
Licenciamiento:	Estándar Gratuito

Fuente: El Autor

Administración de usuarios: El usuario administrador será quien ingresará a los nuevos usuarios al sistema y también tendrá el acceso de eliminar del sistema quien ya no esté laborando dentro del área administrativo.

Caso de uso

Figura 5. Caso de uso el Sistema Propuesto



Fuente: El Autor

Descripción de Caso de uso

Tabla 9: *Descripción de Caso de uso*

CASO DE USO		**Sistema de reconocimiento facial para el área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil**			
ID	**NOMBRE**	**DESCRIPCIÓN**	**LIMITACIONES**	**ACTOR PRINCIPAL**	**ACTOR SECUNDARIO**
U1	Registrar Departamento	Este caso de uso permite registrar el departamento para integrar al personal que labora el área administrativa en la que pertenece	1) Registrar Departamento Administrativo	Administrador	
U2	Registrar datos del empleado	Este caso de uso realiza el registro del personal administrativo en el dispositivo biométrico cumpliendo con los requerimientos funciónales dentro del Sistema	1) Registrar datos del empleado	Administrador	
U3	Registrar huella facial del empleado	Este caso de uso registra sólo la huella facial para facilitar el acceso que identifica cada usuario registrado dentro del área administrativa	1) Registrar la Huella facial del Empleado administrativo	Administrador	Usuario
U4	Sincronizar datos con el equipo biométrico	Este caso de uso conecta los datos registrados en el Sistema Biométrico con su respectiva huella Facial para realizar marcaciones de acceso de manera correcta	1) Sincronizar conexión de los datos con el Sistema Biométrico	Administrador	

U5	Visualizar Registro	Este caso de uso visualiza quien está registrado y qué tipo de acceso identifica dentro del Sistema o en el Sistema Biométrico	1) Visualizar Consulta general de los usuarios registrados	Administrador

Fuente: El Autor

Descripción de Actores

Tabla 10. *Descripción de Actores*

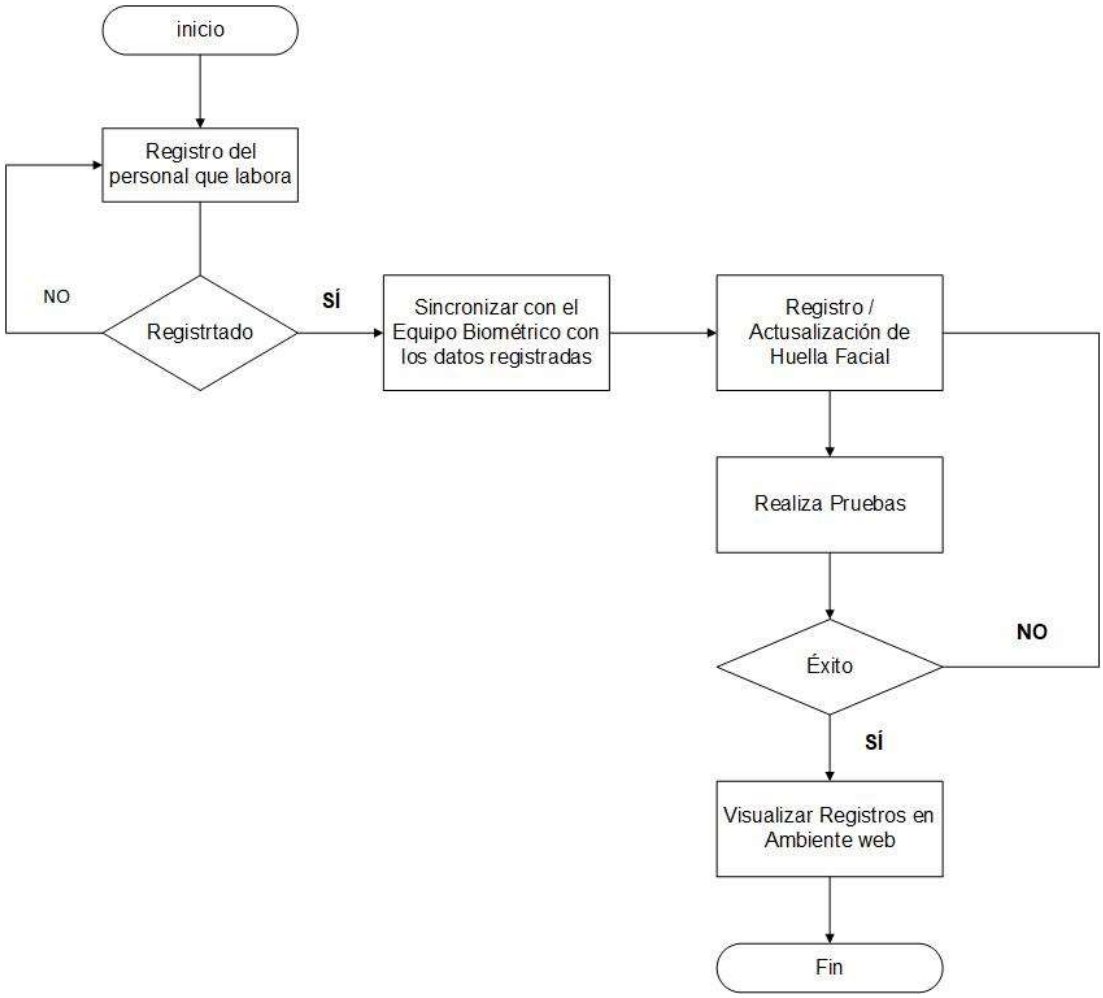
CASO DE USO		**Sistema de reconocimiento facial para el área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil**		
N°	**NOMBRE**	**DESCRIPCIÓN**	**TIPO ACTOR**	**LIMITACIONES**
1	Administrador	Se encarga de manejar el Dispositivo Biométrico y la aplicación que conecta al Sistema, el Administrador es la Coordinadora Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil.	Actor Principal	1. Registrar Departamento 2. Registrar datos del empleado 3. Registrar huella facial del empleado 4. Sincronizar datos con el equipo biométrico 5. Visualizar Registro
2	Usuario	Se encarga de enrolarse para facilitar el acceso al Área Administrativa, los usuarios son el personal que labora en la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil.	Actor Secundario	1. Registrar huella facial del empleado

Fuente: El Autor

Diagrama de Flujo de Procesos

Se pretende detallar Cómo funciona el proceso de registro del usuario en forma secuencial para facilitar el acceso al área administrativa

Figura 6. *Diagrama de Flujo de Procesos del Sistema Propuesto*



Fuente: El Autor

El proceso se inicia con el registro del usuario del personal que labora, en caso de haberse registrado puede. sincronizar. con el equipo biométrico con los datos registrados, caso contrario, se realiza un nuevo registro. Cuando los datos del usuario se encuentran en el sistema. se realiza un registro o actualización de la huella facial qué identifica al usuario. Después se realiza pruebas de validación, en caso de ser exitoso, se encuentra en el registro dentro de un ambiente web, caso contrario, vuelve a actualizar para registrar en el sistema de manera Correcta.

Implementación del prototipo

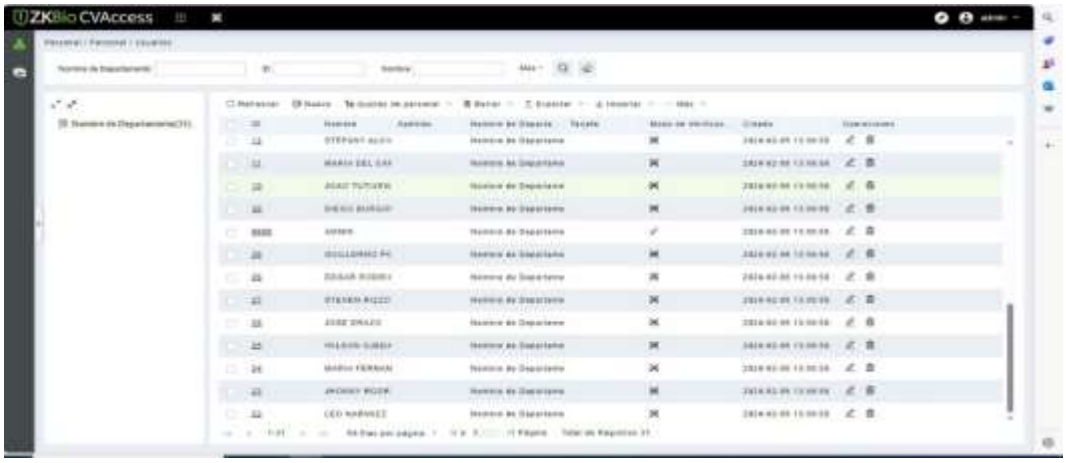
Luego de haber realizado la implementación física del equipo biométrico, se comprobó la funcionalidad del mismo mediante el software proporcionado por el fabricante.

Figura 7. *Pantalla principal*

Fuente: El Autor

De Acuerdo con la Figura 7, para acceder a la aplicación del Sistema Biométrico, se lo hace a través de un browser, por lo que la página principal es un módulo de Login con credenciales para ingresar usuario y contraseña, en caso de estar correctos enlaza al panel de control.

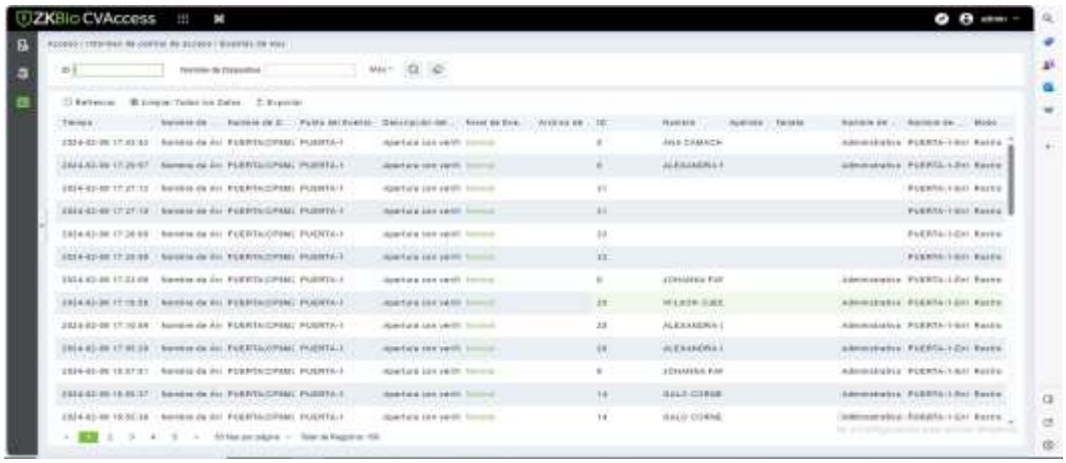
Figura 8. Módulo de consulta de usuarios registrados



Fuente: El Autor

De Acuerdo con la Figura 8, este es el módulo de consulta de usuarios registrados del dispositivo biométrico para acceder al área administrativa se desbloquea la puerta de acceso en modo entrada y salida Mediante Huella Facial, Palma o tarjeta. Los usuarios son el personal que labora en el área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil.

Figura 9. *Módulo de Eventos de marcaciones de entrada y salida*



Fuente: El Autor

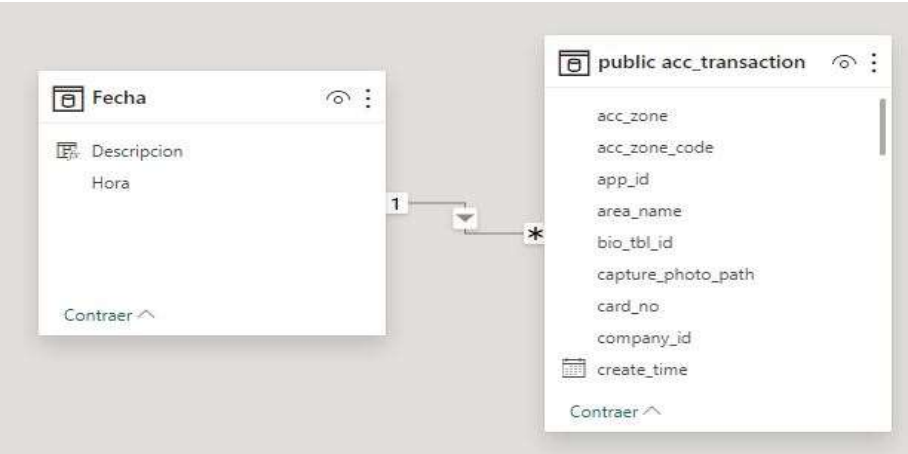
De Acuerdo con la Figura 8, este es el módulo de historial de Eventos de marcaciones de entrada y salida que accedieron al área administrativa Mediante Huella Facial, Palma o tarjeta. Los usuarios en blanco para efectos de prueba.

Modelado de datos de Power BI

Están conformada por dos tablas:

- Fecha
- Public acc_trnsction

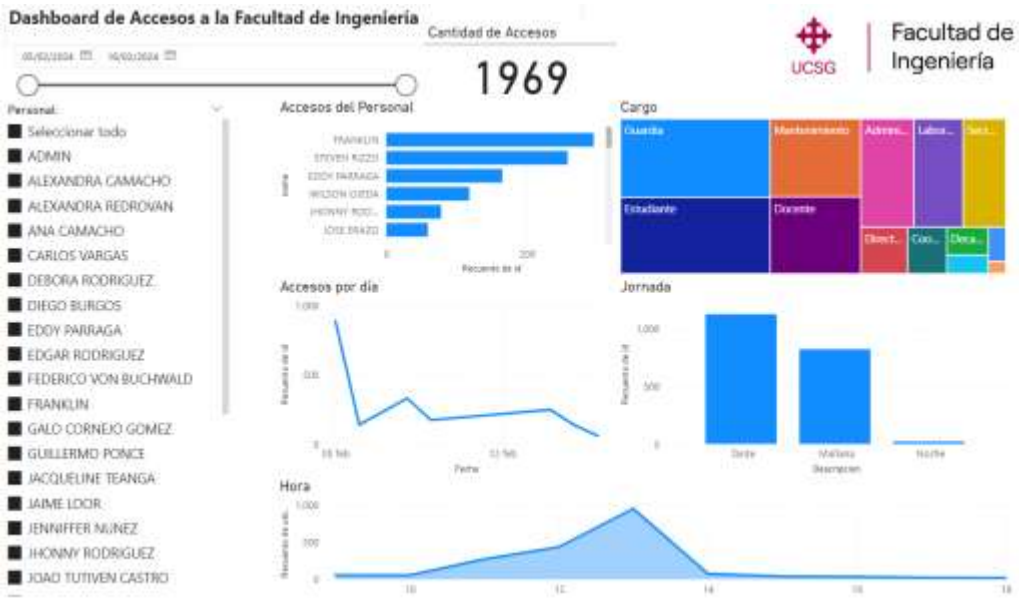
Figura 10. *Modelado de datos en Power BI*



Fuente: El Autor

Dashboard Estadístico del Control de Acceso

Figura 11. *Dashboard del Control de Acceso de la Facultad de Ingeniería*



Fuente: El Autor

De acuerdo a la Figura 11, es la descripción estadística sobre el control de acceso de la Facultad de Ingeniería, conlleva el registro del personal administrativo, como base principal genera resultado de manera gráfica:

- **Acceso del personal:** Frecuencia en donde quien accede cada persona cuantas veces ingresa o sale.
- **Cargo:** Colores que representa los roles dentro del personal administrativo
- **Acceso por día:** Promedio de la cantidad de acceso por día
- **Jornada:** número de acceso por da por tarde y de noche mostrando cada frecuencia en el control de acceso.
- **Hora:** Frecuencia para mostrar la hora que accede con más frecuencia.

Análisis costo-beneficio

La inversión realizada corre de parte del autor, por lo que para la Facultad de Ingeniería y, por consiguiente, a la UCSG no tuvo ningún costo.

Los valores presentados en la Tabla 5 sirven de referente para cualquier futura implementación en algún otro sitio de interés de la universidad, con el fin de mejorar la seguridad interna.

Tabla 11. *Costo de equipos para la implementación de la solución*

EQUIPO	VALOR
Biométrico ZK-SpeedFace-4VL	$170,00
Caja metálica	$15,00
Botón don't touch	$15,00
Fuente	$12,00
UPS	$70,00
TOTAL	$282,00

Fuente: El Autor

CONCLUSIONES

- Se instalaron los componentes necesarios para el funcionamiento del biométrico, luego se realizaron pruebas para garantizar su funcionamiento, se logró la operatividad del sistema para optimizar la seguridad del control del acceso. La implementación del Sistema de reconocimiento facial para el área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil contribuyó a la optimización de procesos manuales para reforzar restricciones de entrada y salida al sitio.
- Para el desarrollo del prototipo, se evaluó un diagnóstico con respecto a la situación actual que surgen a los procesos en el control de acceso de manera libre en la Facultad de Ingeniería, por lo que se expone a riesgos a las oficinas ubicadas en el sitio. La implementación del sistema según los expertos, es una solución valida para restringir el libre acceso a las instalaciones y beneficia al personal otorgando mayor seguridad en las oficinas.
- Se instaló el software de control de acceso para conectar con el dispositivo de reconocimiento facial con el software del fabricante, el cual se conecta a una base de datos PostgreSQL, lo cual contribuye a la visualización de registros y eventos de accesos a los usuarios que pertenece al área administrativa.
- Se utilizó el lenguaje DAX para el proceso de limpieza de datos antes de la implementación de los dashboards en la herramienta de visualización de datos.
- El biométrico se encuentra instalado al lado izquierdo de la oficina de control de cátedra de la Facultad de Ingeniería, para facilitar su uso a los usuarios.

RECOMENDACIONES

- Se debe instalar otro dispositivo biométrico para el control de acceso de salida, que genere registros del personal que labora.
- Se sugiere realizar un mantenimiento o Soporte periódico cada tres (3) meses, por el estado de portabilidad del dispositivo instalado funcionalmente.
- Se pretende instalar cámaras de seguridad con sensores de detección corporal para identificar en el control de acceso a todas las personas que se encuentran transitando.
- Se sugiere el manejo de procesos de respaldo de la información, para evitar la pérdida de datos.

REFERENCIAS

AcademiaLab. (2023). *Reconocimiento de escritura a mano*. https://academia-lab.com/enciclopedia/reconocimiento-de-escritura-a-mano/

Alegsa, L. (2023). *Definición de Reconocimiento de escritura*. Alegsa.com.ar. https://www.alegsa.com.ar/Dic/reconocimiento_de_escritura.php

Almeida, M., Romero, S., & Thiel, D. (2021). *La videovigilancia en Ecuador vulnera derechos ciudadanos*. Derechos Digitales. https://www.fundamedios.org.ec/wp-content/uploads/2021/12/Inf.-Videovigilancia_01-1.pdf

Álvarez Velasco, C. (2023). *Seguridad ciudadana y violencia*. https://ecuador-decide.org/wp-content/uploads/2023/08/Seguridad-y-violencia-ciudadana.pdf

Arias, F. G. (2016). *El proyecto de investigación. Introducción a la metodología científica* (Séptima). El Pasillo. https://es.slideshare.net/SheilaGalindez1/el-proyectodeinvestigacionfidiasarias7maedic2016pdf-compress

Asamblea Nacional. (2008). *Constitución de la República del Ecuador* [Entrevista]. https://www.asambleanacional.gob.ec/sites/default/files/documents/old/constitucion_de_bolosillo.pdf

Asamblea Nacional. (2021). *Ley Orgánica de Protección de Datos Personales* [Entrevista]. https://www.finanzaspopulares.gob.ec/wp-

content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

AWS. (2023). *¿Qué es el reconocimiento facial?* Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/facial-recognition/

Bernal Torres, C. (2016). *Metodología de la Investigación* (Cuarta). Pearson Educación de Colombia S.A.S. https://www.academia.edu/44228601/Metodologia_De_La_Investigaci%C3%B3n_Bernal_4ta_edicion

Caro Cabrera, J., Pozo Cuevas, F., López Menchón, A., & Navarro Ardoy, L. (2020). *Encuestas de seguridad ciudadana* (Primera). CIS. https://bit.ly/47xsCY6

Cedeño Navarrete, J., & Párraga Vera, C. (2017). *Sistema biométrico de control de acceso para el laboratorio de cómputo de la Unidad Ecuativa Francisco González Álava* [Título de Ingeniero en Informática, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López]. https://repositorio.espam.edu.ec/bitstream/42000/479/1/TC109.pdf

CEUPE Magazine. (s/f). *¿Qué es el Reconocimiento de voz y cómo funciona?* Ceupe. Recuperado el 29 de diciembre de 2023, de https://www.ceupe.com/blog/reconocimiento-de-voz.html

Cohen, A. (2023a). *¿Cuál es la importancia de la seguridad privada en las escuelas?* https://es.linkedin.com/pulose/cu%C3%A1l-es-la-importancia-de-seguridad-privada-en-las-escuelas-cohen-1e

Cohen, A. (2023b). *¿Cuáles son las funciones de un sistema de seguridad?* https://es.linkedin.com/pulose/cuales-son-las-funciones-de-un-sistema-seguridad-ariel-cohen

Course Hero. (2018). *Cuadro comparativo Java—PHP*. https://www.coursehero.com/file/32165429/Cuadro-Comparativodocx/

Digixem 360. (2023). *¿Cuáles son los avances tecnológicos actuales?* IT Masters Mag. https://www.itmastersmag.com/noticias-analisis/cuales-son-los-avances-tecnologicos-actuales/

DW. (2023). *Ecuador incorpora 8.000 nuevos policías ante criminalidad*. dw.com. https://www.dw.com/es/ecuador-incorpora-8000-nuevos-policias-para-enfrentar-criminalidad/a-65877048

EcuRed. (2017). *Geometría de la mano*. https://www.ecured.cu/Geometr'a_de_la_mano

Equipo Editorial Etecé. (2020). *Seguridad*. concepto. https://concepto.de/seguridad/

Fernández, L. (2023). *Control de acceso: Qué es y cómo ayuda a proteger nuestros datos*. RedesZone. https://www.redeszone.net/tutoriales/seguridad/control-de-acceso-que-es/

Fernández Ordejón, M. H., Baulema Molina, L., & Prados Torreblanca, A. (2021). *Alineación de caras en imágenes a partir de datasets heterogéneos* [Grado de Ingeniería Informática, Universidad Politécnica de Madrid].

https://oa.upm.es/68454/1/TFG_MARIA_HENAR_FERNANDEZ_ORDEJON.pdf

Florenciañez, O. (2022). *Seguridad en Instituciones Educativas*. https://es.linkedin.com/pulose/seguridad-en-instituciones-educativas-osmar-florencia%C3%B1ez

Frevinco. (2021). *¿Qué es la Seguridad Física?* Frevinco. https://frevinco.com.ec/blog/institucional/que-es-la-seguridad-fisica/

Gallardo Echenique, E. (2017). *Metodología de la Investigación. Manual Autoformativo Interactivo* (Primera). Universidad Continental. https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_UC_EG_MAI_UC0584_2018.pdf

Garcés Núñez, A. (2017). *Sistema de reconocimiento facial con visión artificial para apoyar el ECU-911 con la identificación de personas en la lista de los más buscados* [Título de Ingeniero en Electrónica y Comunicaciones, Universidad Técnica de Ambato]. https://repositorio.uta.edu.ec/bitstream/123456789/24490/3/Tesis_t1189ec.pdf

Gerea, C. (2021). *Prototipo: Qué es y para qué sirve*. FREED TOOLOS. https://freed.toolos/blogs/ux-cx/prototipo

Granja Heredia, D. I. (2018). *Procesamiento de imágenes para la identificación de personas como sisitema de seguridad en zonas domiciliarias de la ciudad de Riobamba* [Magíster en Sistemas de Telecomunicaciones, Escuela Superior Politécnica de Chimborazo].

http://dspace.espoch.edu.ec/bitstream/123456789/9281/1/20T01109.PDF

Granja, I., Moreno, D., Cabrera, F., & Valle, P. (2020). *Procesamiento de imágenes para la identificación de personas como sistema de seguridad en zonas domiciliarias*. 164--186. https://doi.org/10.18502/keg.v5i2.6233

Grupo Atico34. (2023). *Sistemas biométricos: Qué son, tipos, ejemplos y ventajas*. Grupo Atico34. https://protecciondatos-lopd.com/empresas/sistemas-biometricos/

GSITIC. (2018). *Seguridad física y lógica de un sistema de información. Riesgos, amenazas y vulnerabilidades. Medidas de protección y aseguramiento. Auditoría de seguridad física.* GSITIC. https://gsitic.wordpress.com/2018/01/19/bii13-seguridad-fisica-y-logica-de-un-sistema-de-informacion-riesgos-amenazas-y-vulnerabilidades-medidas-de-proteccion-y-aseguramiento-auditoria-de-seguridad-fisica/

Hernández-Sampieri, R., & Mendoza Torres, C. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta* (Primera). McGRAW-HILL INTERAMERICANA EDITORES, S.A. de C. V. http://repositorio.uasb.edu.bo:8080/bitstream/54000/1292/1/Hernandez-%20Metodologia%20de%20la%20investigaci%c3%b3n.pdf

Hostinguer. (2023). *¿Qué es MySQL? Explicación detallada para principiantes*. Tutoriales Hostinger. https://www.hostinger.es/tutoriales/que-es-mysql

IBM. (s/f). *¿Qué son las redes neuronales convolucionales?* Recuperado el 31 de diciembre de 2023, de https://www.ibm.com/mx-es/topics/convolutional-neural-networks

International Crisis Group. (2023). *América Latina lucha contra una nueva ola de criminalidad*. https://www.crisisgroup.org/es/latin-america-caribbean/latin-america-wrestles-new-crime-wave

IONOS Digital Guide. (2023a). *¿Qué es MySQL?* IONOS Digital Guide. https://www.ionos.es/digitalguide/servidores/know-how/que-es-mysql/

IONOS Digital Guide. (2023b). *¿Qué es PHP? Tutorial para principiantes*. IONOS Digital Guide. https://www.ionos.es/digitalguide/paginas-web/creacion-de-paginas-web/tutorial-de-php-fundamentos-basicos-para-principiantes/

Java. (2024). *What is Java and why do I need it?* https://www.java.com/en/download/help/whatis_java.html

Kaspersky. (2023). *Reconocimiento facial: Definición y explicación*. latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-facial-recognition

Kejriwal, K. (2023). *DeepFace para reconocimiento facial avanzado*. https://www.unite.ai/es/Deepface-para-reconocimiento-facial-avanzado/

Kelio. (2020). *Descubre los diferentes tipos de control de accesos*. https://www.kelio.es/empresa/noticias/322-descubre-los-diferentes-tipos-de-control-de-accesos.html

Laarcom. (s/f). *¿Qué es la seguridad electrónica?* Laarcom.com. Recuperado el 24 de diciembre de 2023, de https://www.laarcom.com/que-es-la-seguridad-electronica

LISA Institute. (2023). *Reconocimiento facial: Descubre cómo funciona y quién (y para qué) lo utiliza*. LISA Institute. https://www.lisainstitute.com/blogs/blog/reconocimiento-facial-como-funciona-quien-utiliza

Lissardy, G. (2019). Por qué América Latina es la región más violenta del mundo (y qué lecciones puede tomar de la historia de Europa). *BBC News Mundo*. https://www.bbc.com/mundo/noticias-america-latina-48960255

López Lungo, L. I. (2023). *¿Qué hay detrás del auge de la violencia en Ecuador?* France 24. https://www.france24.com/es/am%C3%A9rica-latina/20230811-qu%C3%A9-hay-detr-del-auge-de-violencia-en-ecuador

Manage Engine. (2023). *Soluciones de seguridad de TI*. https://www.manageengine.com/latam/herramientas-administracion-seguridad-ti.html

Martínez García, L. (2023). *Seguridad Electrónica*. Euroinnova Business School. https://www.euroinnova.ec/blog/seguridad-electronica

Ministerio del Interior. (2019). *Plan específico de Seguridad Pública y Ciudadana 2019-2023*. https://www.defensa.gob.ec/wp-

content/uploads/downloads/2019/07/plan-nacional-min-interior-web.pdf

Navicelli, V. (2022). *Definición de seguridad*. https://definicion.com/seguridad/#tipos-de-seguridad

NÜO Planet. (2019). *Tipos de control de acceso: Qué son, tipos y diferencias*. https://blog.nuoplanet.com/tipos-control-acceso

Omnitempus. (2020). *Avances de tecnología en seguridad*. https://omnitempus.com/2019/tecnologia-en-seguridad/

Orozco Analuiza, C. (2022). *Algoritmos de procesamiento de señales para el reconocimiento facial y de voz empleando redes neuronales* [Título de Ingeniero en Electrónica y Comunicación, Universidad Técnica de Ambato]. https://repositorio.uta.edu.ec/bitstream/123456789/36410/1/t2088ec.pdf

Ortega, K. (2023). *¿Qué es el lenguaje de programación PHP?* Saint Leo University. https://worldcampus.saintleo.edu/noticias/sistemas-computacionales-que-es-el-lenguaje-de-programacion-php

Ortega, K. M., & Pino, S. L. (2021). Impacto social y económico de los factores de riesgo que afectan la seguridad ciudadana en Ecuador. *Espacios*, *42*(23), 52–70. https://doi.org/10.48082/espacios-a21v42n21p04

Pachari Bravo, D. (2023). *Barrios de Guayaquil se encierran por inseguridad*. https://www.elmercurio.com.ec/2023/07/19/guayaquil-barrios-encerrados-inseguridad/

Palma González, Y. A. (2023). *Timeline compartivo de JAVA y PHP*. Genially. https://view.genial.ly/6515b509ecdc90001193bede/interactive-content-timeline-comparativo-de-java-y-php

Pérez Porto, J., & Gardey, A. (2021). *Seguridad*. Definición.de. https://definicion.de/seguridad/

PHP.net. (2024a). *PHP*. https://www.php.net/index.php

PHP.net. (2024b). *¿Qué es PHP?* https://www.php.net/manual/es/intro-whatis.php

PNUD. (2013). *Sinopsis: Seguridad ciudadana*. https://www.undp.org/sites/g/files/zskgke326/files/publications/08022013_citizen_security_issue_brief-(spanish).pdf

Policía Nacional del Ecuador. (2023). *La Policía entrega estadísticas de las muertes violentas y la productividad alcanzada en el 2023 en la Zona 8*. https://www.policia.gob.ec/la-policia-sincera-las-estadisticas-de-las-muertes-violentas-y-la-productividad-alcanzada-en-el-2023-en-la-zona-8/

Praxedo. (2023). *Instalación y mantenimiento de sistemas de seguridad electrónica, hacia un modelo competitivo y diferenciador a través de la tecnología*. Praxedo. https://www.praxedo.es/blog/instalacion-mantenimiento-sistemas-de-seguridad-electronica/

Prieto, B. (2023). *Los 10 tipos de Seguridad (y sus características)*. https://medicoplus.com/ciencia/tipos-seguridad

Prieto, P. (2023). *Los 10 tipos de Inseguridades (y sus características)*. https://medicoplus.com/psicologia/tipos-inseguridades

Primicias. (2022). *Ciudadelas de Guayaquil se encierran ante la inseguridad*. Primicias. https://www.primicias.ec/noticias/sucesos/guayaquil-inseguridad-ciudadelas-encerradas/

Primicias. (2023a). *Durán, al nivel de las 10 ciudades más violentas del mundo*. Primicias. https://www.primicias.ec/noticias/seguridad/duran-criminalidad-ciudades-violencia-inseguridad/

Primicias. (2023b). *Ecuador, en el "top 10" de los países con mayor criminalidad del mundo*. Primicias. https://www.primicias.ec/noticias/seguridad/ecuador-paises-mayor-criminalidad-mundo/

Primicias. (2023c). *Escuelas de Guayaquil serán intervenidas por sicariato y extorsión*. Primicias. https://www.primicias.ec/noticias/sucesos/escuelas-guayaquil-intervenidas-sicariato-extorsion/

Primicias. (2023d). *Guayaquil y Durán se disputan el top 10 de ciudades más violentas del mundo*. Primicias. https://www.primicias.ec/noticias/seguridad/guayaquil-duran-violencia-inseguridad-ecuador/

Primicias. (2023e). *Universidades de Guayaquil aplican clases virtuales por inseguridad*. Primicias. https://www.primicias.ec/noticias/sucesos/universidades-guayaquil-clases-virtuales-inseguridad/

Prosegur. (2023). *Los beneficios de los avances tecnológicos en el ámbito de la seguridad*. Prosegur España. https://www.prosegur.es/blog/seguridad/tecnologia-seguridad

Protek Seguridad. (2022). *¿Qué importancia tiene la seguridad en las instituciones educativas?* Protek. https://www.protek.com.py/novedades/que-importancia-tiene-la-seguridad-en-las-instituciones-educativas/

Raya Camacho, M. J. (2022). *Cuadro comparativo SGBD*. https://www.studocu.com/es-mx/document/instituto-tecnologico-de-zacatepec/diseno-asistido-por-computadora/raya-camacho-maria-jose-actividad-2-cuadro-comparativo/33076421

RecFaces. (2021a). *8 tipos de sistemas biométricos más significativos*. RecFaces. https://recfaces.com/articles/tipos-de-identificacion-biometrica

RecFaces. (2021b). *Los 5 mejores sistemas de seguridad*. RecFaces. https://recfaces.com/articles/que-es-sistemas-de-seguridad

RecFaces. (2021c). *¿Qué es el escáner de iris y de retina y cómo funcionan?* RecFaces. https://recfaces.com/articles/escaner-de-iris

Rettberg, A. (2020). Violencia en América Latina hoy: Manifestaciones e impactos. *Revista de Estudios Sociales*, *73*. https://doi.org/10.7440/res73.2020.01

Riofrio Villamar, S. (2023). *Análisis comparativo de los algoritmos Eingenface y Fisherface de reconocimiento facial para la seguridad de los sistemas*

de información [Título de Ingeniero en Sistemas de Información, Universidad Técnica de Babahoyo]. http://dspace.utb.edu.ec/bitstream/handele/49000/14248/E-UTB-FAFI-SIST.INF-000137.pdf?sequence=1&isAllowed=y

Salas, Y., Leandro, P., & Sifuentes, N. (2022). Importancia de la inversión en proyectos de seguridad ciudadana. *Gestionar: revista de empresa y gobierno*, *3*(1), Article 1. https://doi.org/10.35622/j.rg.2023.01.008

Santander Universidades. (2021). *¿Cuáles son las ventajas y desventajas de la tecnología actual?* https://www.becas-santander.com/es/blog/ventajas-y-desventajas-de-la-tecnologia.html

Secatel. (2019). *¿Qué es la Seguridad Electrónica?* Secatel SCC. https://secatel.com/que-es-la-seguridad-electronica/

Seguritecnia. (2022). *Sistema de control de acceso: Qué es*. Seguritecnia. https://www.seguritecnia.es/actualidad/que-es-un-sistema-de-control-de-acceso_20220808.html

Solano, G., & Molina, G. (2023). *Violencia, miedo y dificultades económicas, el país que le espera al próximo presidente de Ecuador*. Los Angeles Times en Español. https://www.latimes.com/espanol/politica/articulo/2023-08-17/violencia-miedo-y-dificultades-economicas-el-pais-que-le-espera-al-proximo-presidente-de-ecuador

Tecno Seguro. (s/f). *¿Qué es un Sistema de Control de Acceso?* Recuperado el 5 de noviembre de 2023, de

https://www.tecnoseguro.com/faqs/control-de-acceso/que-es-un-control-de-acceso

The San Diego Union-Tribune. (2023). *Ecuador: Secuestran a decana de universidad estatal de Guayaquil, policía la libera horas después*. San Diego Union-Tribune en Español. https://www.sandiegouniontribune.com/en-espanol/noticias/story/2023-08-09/ecuador-secuestran-a-decana-de-universidad-de-guayaquil-policia-la-libera-horas-despues

UCSG. (s/f-a). *Historia de la Facultad*. Recuperado el 18 de noviembre de 2023, de https://www.ucsg.edu.ec/ing/historia-facultad/

UCSG. (s/f-b). *Misión*. Recuperado el 18 de noviembre de 2023, de https://www.ucsg.edu.ec/la-universidad/mision/

UCSG. (s/f-c). *Objetivos*. Recuperado el 19 de junio de 2023, de https://www.ucsg.edu.ec/la-universidad/objetivos-ucsg/

UCSG. (s/f-d). *Reseña Histórica*. Recuperado el 19 de junio de 2023, de https://www.ucsg.edu.ec/la-universidad/

UCSG. (s/f-e). *Visión*. Recuperado el 19 de junio de 2023, de https://www.ucsg.edu.ec/la-universidad/vision-ucsg/

UCSG. (2023). *La UCSG Trabaja para Precautelar la Seguridad de toda la Comunidad*. https://www.ucsg.edu.ec/la-ucsg-trabaja-para-precautelar-la-seguridad-de-toda-la-comunidad/

Vaca Piña, F., & Rivera Rodríguez, F. (2022). *Diseño e implementación de un sistema de control de acceso mediante reconocimiento facial para la academia Titanes Cuenca* [Título de Ingeniero Electrónico, Universidad Politécnica Salesiana]. https://dspace.ups.edu.ec/bitstream/123456789/24611/1/UPS-CT010421.pdf

Vázquez Campos, M. (2017). *La Seguridad Ciudadana y la influencia de la participación ciudadana en las estrategias de prevención del delito. El caso del barrio de San Juan, Quito, Ecuador, 2009-2014* [Titulo de Maestría en Estudios Urbanos, Facultad Latinoamericana de Ciencias Sociales, FLACSO Ecuador]. https://repositorio.flacsoandes.edu.ec/bitstream/10469/12023/14/TFLACSO-2017MFVC.pdf

Verisure. (2023). *Sistemas de seguridad: Qué son y tipos*. Alarmas Verisure Perú. https://www.verisure.pe/consejos-y-ayuda/preguntas-frecuentes/que-son-sistemas-de-seguridad

Viatek. (2022). *Sistemas de control de acceso. Qué son y tipos*. Grupo Viatek. https://grupoviatek.com/sistemas-de-control-de-acceso/

West, D. (2017). Avance tecnológico: Riesgos y desafíos. En *El próximo paso: La vida exponencial*. https://www.bbvaopenmind.com/wp-content/uploads/2017/01/BBVA-OpenMind-libro-El-proximo-paso-vida-exponencial1.pdf

Xinhua Español. (2023). *Lasso entrega equipo a Fuerzas Armadas para fortalecer combate al crimen organizado en Ecuador*. https://spanish.news.cn/20230809/19cc3f589d364ceda5f39dfe753548ad/c.html

ANEXOS

Anexo A: Modelo de la Entrevista

Modelo de la Entrevista	
Entrevistado:	
Fecha	
Desarrollo de preguntas	

1. ¿Conoce Ud. si en la UCSG o en sus inmediaciones, se ha registrado algún evento de seguridad?

2. ¿Qué medidas conoce Ud. que la UCSG ha implementado para mejorar la seguridad interna y precautelar la vida de toda la comunidad universitaria?

3. ¿Qué tecnologías conoce Ud. que existen para restringir el acceso de personas?

4. ¿Tiene conocimiento si en la UCSG se ha implementado algún sistema de reconocimiento facial para restringir el acceso de personas y mejorar la seguridad interna?

5. ¿Qué ventajas considera Ud. que tienen los sistemas biométricos de reconocimiento facial?

6. ¿Cuáles serían las desventajas de los sistemas de reconocimiento facial?

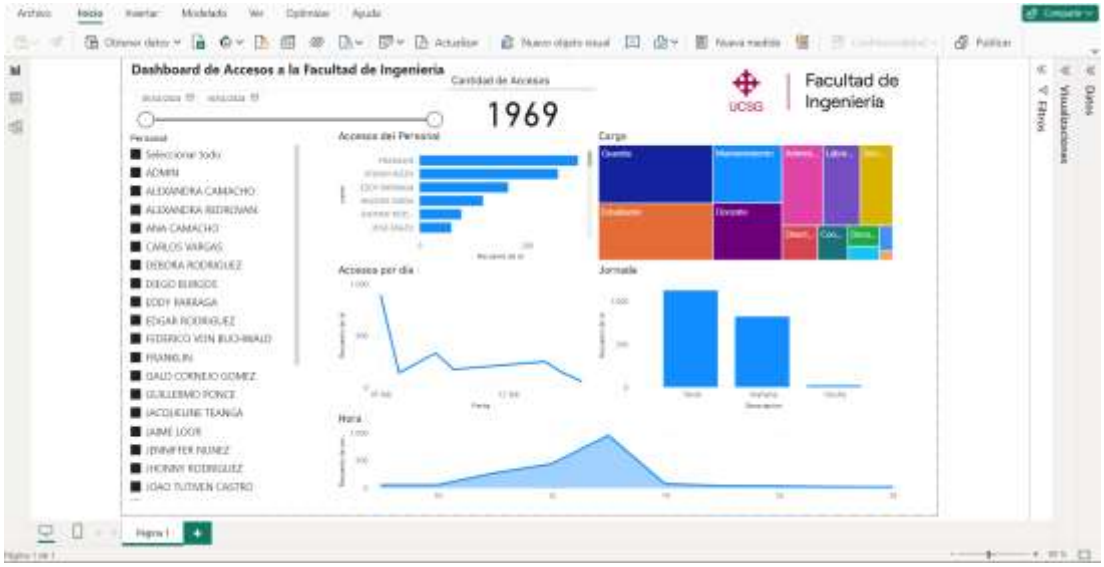
7. ¿Cómo se controla el acceso de las personas al área administrativa de la Facultad de Ingeniería?

8. ¿Estaría de acuerdo con la lectura de rostro de las personas para acceder al área administrativa de la Facultad de Ingeniería?

9. ¿En qué ayudaría la implementación de un sistema biométrico de reconocimiento facial en la Facultad de Ingeniería?

Elaborado por: Franklin Gómez Huacho

Anexo B: Evidencia del progreso de la implementación


Dashboard de Accesos a la Facultad de Ingeniería
Cantidad de Accesos
1969
UCSG
Facultad de Ingeniería
Personal
Seleccionar todo
ADMIN
ALEXANDRA CAMACHO
ALEXANDRA REDROVAN
ANA CAMACHO
CARLOS VARGAS
DEBORA RODRIGUEZ
DIEGO BURGOS
EDDY BARRAGA
EDGAR RODRIGUEZ
FEDERICO WEIN BUCHWALD
FRANKLIN
GALO CORNEJO GOMEZ
GUILLERMO PONCE
JACQUELINE TEANIGA
JAIME LOOR
JENNIFFER NUNEZ
JHONNY RODRIGUEZ
JOAO TUTIVEN CASTRO
Accesos del Personal
Carga
Accesos por día
Jornada
Hora
Página 1

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Gómez Huacho, Franklin Geovany**, con C.C: # **0201839156** autor del trabajo de titulación: **Sistema de reconocimiento facial para el área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil,** previo a la obtención del título de **Ingeniero en Ciencias de la Computación** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 16 de febrero del 2024

_____

Nombre: **Gómez Huacho, Franklin Geovany**

C.C: **0201839156**

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TEMA Y SUBTEMA:	**Sistema de reconocimiento facial para el área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil.**		
AUTOR(ES)	Gómez Huacho, Franklin Geovany		
REVISOR(ES)/TUTOR(ES)	**Ing. Erazo Ayón, José Miguel, Mgs.**		
INSTITUCIÓN:	**Universidad Católica de Santiago de Guayaquil**		
FACULTAD:	**Ingeniería**		
CARRERA:	**Ingeniería en sistemas computacionales**		
TITULO OBTENIDO:	**Ingeniero en sistemas computacionales**		
FECHA DE PUBLICACIÓN:	**16 de febrero del 2024**	**No. DE PÁGINAS:**	97
ÁREAS TEMÁTICAS:	**Biométrico RID, facial, Enrolamiento al personal, Control de Acceso**		
PALABRAS CLAVES/ KEYWORDS:	*Reconocimiento Facial, Biométrico, Seguridad Física, Control de Acceso, Inteligencia de Negocios*		

RESUMEN:

El Diseño e implementación de una solución informática de reconocimiento facial para reforzar el nivel de acceso y seguridad en el área administrativa de la Facultad de Ingeniería de la UCSG, lleva las siguientes especificaciones: Revisar los recursos tecnológicos disponibles y utilizables para el diseño de un prototipo funcional de sistema de reconocimiento facial, determinar los requisitos de seguridad y acceso, desarrollar el prototipo para el control de seguridad y acceso, implementar el prototipo de reconocimiento facial en el área administrativa. se aplica el método cualitativo de la entrevista para dar aceptación e implementar el prototipo funcional. Previo a la implementación se diseñó la arquitectura de la solución que contiene servidores, un lector biométrico con reconocimiento facial, su software correspondiente y un componente para visualización de datos como Power BI.

Esta solución pretende facilitar al administrador una herramienta de control de accesos, a través de un cuadro de mando para fortalecer los procesos de seguridad física que se llevan en la Facultad de Ingeniería.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:**+593-983527095	E-mail: **franklingomez669@gmail.com**
CONTACTO CON LA INSTITUCIÓN(C00RDINADOR DEL PROCESO UTE)::	**Toala Quimí, Edison José**	
	Teléfono: +593-990-976776	
	E-mail: edison.toala@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	