

UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

ESCUELA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

## INFORME FINAL DEL TRABAJO DE INTEGRACIÓN CURRICULAR TEMA:

**“USO DE DRONES CON RECONOCIMIENTO FACIAL COMO MECANISMO DE CONTROL DE SEGURIDAD EN LA FACULTAD DE CIENCIAS AGROPECUARIAS (FACIAG)”.**

## Autor:

**Aguirre Rosado Ken Michael Babahoyo – Los Ríos – Ecuador**

**2023**

# DEDICATORIA

Este proyecto va dedicado a mí continúo esfuerzo durante todos estos años.

# AGRADECIMIENTOS

Agradezco a mí continúo esfuerzo a pesar de las adversidades, además por haber logrado una de las metas de mi vida de obtener un título de tercer nivel. También agradezco el apoyo financiero de mis padres.

## CERTIFICACIÓN DE PORCENTAJE DE SIMILITUD CON OTRAS FUENTES EN EL SISTEMA DE ANTI-PLAGIO



ÍNDICE

[TEMA 6](#_TOC_250033)

[RESUMEN 6](#_TOC_250032)

[ABSTRACT 7](#_TOC_250031)

1. [INTRODUCCIÓN 8](#_TOC_250030)
	1. [Contextualización de la situación problemática 8](#_TOC_250029)
		1. [Contexto internacional 8](#_TOC_250028)
		2. [Contexto nacional 8](#_TOC_250027)
		3. [Contexto local 9](#_TOC_250026)
	2. [Planteamiento del problema 10](#_TOC_250025)
		1. [Pregunta de investigación 11](#_TOC_250024)
	3. [Justificación 11](#_TOC_250023)
	4. [Objetivos de investigación 12](#_TOC_250022)
		1. [Objetivo general 12](#_TOC_250021)
		2. [Objetivos específicos 12](#_TOC_250020)
	5. [Hipótesis 12](#_TOC_250019)
2. [MARCO TEÓRICO 12](#_TOC_250018)
	1. [Antecedentes 12](#_TOC_250017)
		1. [Internacionales 13](#_TOC_250016)
		2. [Nacionales 14](#_TOC_250015)
		3. [Locales 14](#_TOC_250014)
	2. [Bases teóricas 15](#_TOC_250013)
3. [METODOLOGÍA 30](#_TOC_250012)
	1. [Tipo y diseño de investigación 30](#_TOC_250011)
		1. [Tipo de investigación 30](#_TOC_250010)
		2. [Metodología 31](#_TOC_250009)
	2. [Operacionalización de variables 31](#_TOC_250008)
	3. Población y muestra de investigación 32
		1. Población 32
		2. Muestra 32
	4. Técnicas e instrumentos de medición 33
		1. Técnicas 33
		2. Instrumentos 33
	5. Procesamiento de datos 33
	6. Aspectos éticos 33
4. [PRESUPUESTO 34](#_TOC_250007)
5. [RESULTADOS Y DISCUSIÓN 36](#_TOC_250006)
	1. Resultados 36
	2. [Discusión 44](#_TOC_250005)
6. [CONCLUSIONES Y RECOMENDACIONES 45](#_TOC_250004)

[Conclusiones 45](#_TOC_250003)

[Recomendaciones 46](#_TOC_250002)

1. [BIBLIOGRAFÍA 46](#_TOC_250001)
2. [ANEXOS 48](#_TOC_250000)

# TEMA

“Uso de drones con reconocimiento facial como mecanismo de control de seguridad en la facultad de ciencias agropecuarias (FACIAG)”.

# RESUMEN

De acuerdo con los datos que el gobierno del Ecuador registra sobre los índices de criminalidad. Ha concluido que las provincias de Guayas, Manabí, Los Ríos, Esmeralda y El Oro son las más peligrosas. Entre estas se encuentra la ciudad de Babahoyo, capital de la provincia de Los Ríos, afectando la calidad de vida de su población, por lo que es necesario tomar las medidas correctivas antes esta situación, con base en la época de conocimiento e innovación en la que vivimos.

Esta investigación está orientada al estudio de como el uso de drones con inteligencia artificial, aplicando el reconocimiento facial como mecanismo de seguridad en la Facultad de Ciencias Agropecuarias (FACIAG), además de todos los recursos necesarios para su uso, reduciendo los riesgos de incidentes como robos; mejorando así, la respuesta ante situaciones de emergencia. A través de esta investigación es posible determinar el impacto positivo que ya se ha demostrado en tipo de sistema de seguridad, para así, poder aplicarlo a la realidad presentada en la FACIAG.

**Palabras clave:** Seguridad, Drones, Sistema de seguridad, Infraestructura tecnológica, Inteligencia artificial, Reconocimiento facial, Redes neuronales.

# ABSTRACT

According to the data collected by the Ecuadorian government on crime rates, it has been concluded that the provinces of Guayas, Manabi, Los Rios, Esmeraldas, and El Oro are the most dangerous. Among them is the city of Babahoyo, the capital of the province of Los Rios, which is affecting the quality of life of its population. It is necessary to take corrective measures before this situation, based on the era of knowledge and innovation in which we live.

This research is aimed at studying the use of drones with artificial intelligence, applying facial recognition as a security mechanism in the Faculty of Agricultural Sciences (FACIAG), in addition to all the necessary resources for their use, reducing the risks of incidents such as theft and improving the response to emergency situations. Through this research, it is possible to determine the positive impact that has already been demonstrated in this type of security system, in order to apply it to the reality presented in FACIAG.

**Keywords:** Security, Drones, Security system, Technological infrastructure, Artificial intelligence, Facial recognition, Neural networks.

# INTRODUCCIÓN

## Contextualización de la situación problemática

### Contexto internacional

En los últimos años, el uso de drones ha crecido en popularidad en todo el mundo, tanto en la industria como en la investigación. Uno de los usos más comunes de los drones es en la seguridad y vigilancia, especialmente en lugares donde la seguridad es crucial, como aeropuertos, instalaciones militares y grandes eventos.

En algunos países, el uso de drones con reconocimiento facial para la seguridad ha sido implementado en aeropuertos, estadios y zonas de alta seguridad. Por ejemplo, en el aeropuerto de Schiphol en Ámsterdam, se utiliza un sistema de drones equipados con cámaras de reconocimiento facial para patrullar la pista de aterrizaje y detectar cualquier actividad sospechosa.

En China, la policía ha utilizado drones con reconocimiento facial para buscar delincuentes y criminales en grandes multitudes, como en festivales y eventos deportivos. En Estados Unidos, algunos departamentos de policía han comenzado a utilizar drones equipados con cámaras de alta resolución y reconocimiento facial para buscar a personas desaparecidas o sospechosas de haber cometido delitos.

### Contexto nacional

La utilización de sistemas de vigilancia no es una práctica novedosa, puesto que se está empleando con mayor frecuencia en diversos ámbitos que ya han sido mencionados. Varios países están adoptando estas medidas como lo menciona

(Agudelo, 2019) “China, Estados Unidos y Alemania son los países con la mayor cantidad de cámaras de vigilancia del mundo”.

Según lo que Agudelo ha expuesto, es posible afirmar que estos países son los principales desarrolladores de estas tecnologías, por lo que no es sorprendente que lideren en este sector. Aunque hay otros países que también están incursionando en el uso de estas tecnologías, pero en menor medida.

En el Ecuador, el mayor sistema de vigilancia es el ECU911 el cual comprende casi la totalidad del país, pero aún presenta fallos logísticos como también su limitación dentro de las organizaciones. Además, desde el año dos mil veinte, se han creado regulaciones a este tipo de dispositivo tecnológico y a su peso y los lugares restringidos como: helipuertos, zonas de seguridad del estado, zonas intangibles, entre otros.

### Contexto local

La Universidad Técnica de Babahoyo, ubicada en la capital fluminense (Babahoyo) cuenta con su respectiva facultad dedicada a los ámbitos agropecuarios, medicina veterinaria, zootecnia, entre otros. La ubicación de esta facultad es distante a su matriz, por lo que logísticamente representa ya por si misma un riesgo, debido a que los estudiantes, personal administrativo y docente son propensos a ser víctimas de algún tipo de atentado.

Si bien, la matriz cuenta con un sistema de vigilancia básico, no es el caso de la FACIAG, por lo que es imperante que la facultad ya disponga de medias de seguridad, y como no, es la oportunidad para hacer uso de tecnología y así brindar una seguridad de calidad a los que asisten a esta facultad.

## Planteamiento del problema

La inseguridad en Ecuador es un problema que afecta a muchas personas en todo el país. La delincuencia en las calles, robos, hurtos y la violencia son algunos de los problemas más comunes que los ciudadanos tienen que enfrentar diariamente. El aumento del crimen en las ciudades es un reflejo de la falta de inversión en seguridad pública y la falta de políticas públicas efectivas para abordar esta situación. La inseguridad afecta a todas las clases sociales, pero es especialmente grave para las personas más vulnerables, como los residentes de barrios pobres, que a menudo carecen de recursos para protegerse.

A lo largo de las provincias del Ecuador, la inseguridad ha alcanzado niveles alarmantes entre los años 2021-2022 como lo explica (UNIVERSO, EL UNIVERSO, 2022) “Durante todo el 2021 se registraron 25.389 robos a personas a nivel nacional” siendo estas cifras altas pero las cifras del año siguiente según (UNIVERSO, EL UNIVERSO, 2022) “de enero a mayo de este 2022 ya se habían registrado 12.548, es decir, casi la mitad en cinco meses”; caracterizada por un aumento en muertes violentas, robos y extorsiones.

Pese a los controles y estados de excepción emitidas por el gobierno con la participación de los militares para combatir este problema, la actividad criminal no ha disminuido y por el contrario los ciudadanos se ven obligados a implementar diferentes medidas para protegerse. La Facultad de Ciencias Agropecuarias (FACIAG) de la Universidad Técnica de Babahoyo (UTB) por las características de sus actividades diarias existe un gran tráfico de personas y vehículos, además la distribución de las instalaciones torna complicado controlar la presencia de personas ajenas a la institución con el riesgo de pérdida de bienes de la población perteneciente a la facultad en general.

La falta de medidas de seguridad en la Facultad de Ciencias Agropecuarias de la Universidad Técnica de Babahoyo expone a estudiantes, personal docente y administrativo a situaciones de riesgo e incluso poner en peligro su integridad física y material. La FACIAG, como también la matriz, no cuentan con un sistema de vigilancia de drones con inteligencia artificial, por lo que es imperante empezar a modernizar los mecanismos de seguridad de la Universidad Técnica de Babahoyo.

### Pregunta de investigación

¿Cómo el uso de drones con reconocimiento facial como mecanismo de control de seguridad mejorará la seguridad en la Facultad de Ciencias Agropecuarias (FACIAG) actualmente?

## Justificación

Dado a lo mencionado en los puntos anteriores, es necesario establecer un plan de seguridad para los estudiantes, personal administrativo y bienes, para lo cual se propone el estudio del uso de drones como mecanismo de seguridad para mejorar la seguridad en la FACIAG.

La novedad de esta investigación yace en el uso de tecnologías como el reconocimiento facial para la detección de personas no pertenecientes a la institución, reduciendo los riesgos que se puedan presentar como los robos u otro tipo de siniestros, gracias a la constante vigilancia con los drones y apoyados por la tecnología de reconocimiento facial, los cuales sobrevolarán las zonas con mayor concurrencia de la FACIAG.

Si se utilizan drones con reconocimiento facial mejorará la seguridad en la Facultad de Ciencias Agropecuarias (FACIAG) actualmente, porque al existir una vigilancia más precisa en tiempo real de las personas que ingresan y transitan en la

facultad, lo que permitirá a reducir los riesgos de robos u otros delitos en la zona, siendo los estudiantes, personal docente y administrativo de la FACIAG los beneficiarios directos

## Objetivos de investigación

### Objetivo general

Investigar el potencial del uso de drones con reconocimiento facial como mecanismo de control de seguridad en la FACIAG.

### Objetivos específicos

* + - 1. Identificar los riesgos de seguridad a los que se enfrentan los estudiantes, docentes y personal administrativo de la FACIAG.
			2. Establecer las necesidades específicas de seguridad en la FACIAG, considerando su tamaño y ubicación.
			3. Evaluar las soluciones tecnológicas disponibles en el mercado para seleccionar las pertinentes a la situación de la FACIAG.

## Hipótesis

Si se utilizan drones con reconocimiento facial mejorará la seguridad en la Facultad de Ciencias Agropecuarias (FACIAG) actualmente, porque al existir una vigilancia más precisa en tiempo real de las personas que ingresan y transitan en la facultad, lo que permitirá a reducir los riesgos de robos u otros delitos en la zona.

# MARCO TEÓRICO

## Antecedentes

Los sistemas de vigilancia son importantes como eficaces dependiendo como se los utilice, pero su actual importancia es la fusión con la inteligencia artificial. La inteligencia artificial, es actualmente la herramienta de la que más ha dado de hablar, debido a sus ventajas, desventajas, polémicas y ética. Aunque, tiene sus desventajas, como ya se mencionó; la inteligencia artificial puede reducir (siendo optimistas) los niveles de criminalidad que azotan el mundo.

Para brindar más información sobre antecedentes relacionados a este tema lo clasificaremos en internacionales, nacionales y locales.

### Internacionales

Según (Mundo, 2017) “China está construyendo lo que se ha llamado "la red de videovigilancia más grande y más sofisticada del mundo". Actualmente hay 170 millones de cámaras de circuito cerrado desplegadas por todo el país para vigilar a sus

1.300 millones habitantes”.

China es actualmente, el país puntero en el desarrollo de tecnología en base a la inteligencia artificial, y como cita BBC Mundo, en el anterior párrafo China desarrolla una enorme red, hay quienes lo cuestionan llamándolo “El gran hermano chino”, pero aun así no deja de ser sorprendente las posibilidades con la inteligencia artificial.

Dentro del marco de lo que es la seguridad y la vigilancia, entra lo que son los drones. Ya existen en el mercado este tipo de proyectos como lo menciona (Agular, 2021) “AnyVision ha registrado una patente que ayudará a los dispositivos voladores no tripulados a conseguir el mejor ángulo para obtener imágenes de alta calidad y de todo el rostro de los ciudadanos que tengan que ser identificados”.

Otros casos son de proyectos de drones con reconocimiento facial son:

El Pentágono ha adjudicado a la firma RealNetworks, con sede en Seattle, un proyecto de implementación del reconocimiento facial en drones autónomos de pequeño tamaño para la identificación y la recopilación de inteligencia, según figura en la página web del fondo del Gobierno estadounidense destinado a fomentar la innovación y la transferencia de tecnología en pequeñas y medianas empresas. (lapatilla, 2023)

### Nacionales

Al ser una tecnología relativamente nueva, Ecuador, no ha incursionado fuertemente en este tema, aunque existen evidencias de que a los drones se les ha dado uso agrícola, entretenimiento dentro del país. Con este evidente uso de este tipo de aparatos tecnológicos, no se ha dado uso para la vigilancia de seguridad ciudadana. En el país el referente respecto a seguridad es el ECU911 el cual posee un sistema actualizado a consecuencia de la pandemia del Covid-19 en 2020.

Este software usa imágenes de las cámaras para medir el distanciamiento, si se detectan concentraciones, se genera una ficha y se remite a las instituciones de control. El software lo desarrolló el BID y el ECU 911 apoyó para integrarlo al sistema de videovigilancia, ejecutar pruebas, ajustes y modificaciones. El

mecanismo genera alertas que van a la Sala de Videovigilancia y a través de Megafonía IP se solicitará cumplir esta norma para evitar contagios en esta ‘nueva normalidad’, es una herramienta tecnológica preventiva al servicio de las instituciones que trabajan en territorio. (ecu911, 2020)

### Locales

La ciudad de Babahoyo, se encuentra ubicada en la provincia de Los Ríos, la cual está catalogada como zona agrícola, este es un precedente para abarcar el tema del desarrollo tecnológico en esta zona del país. Debido a la categorización de zona agrícola, se ha invertido mayores recursos de tiempo en investigaciones y dinero para desarrollar esta área, dejando a un lado el desarrollo de nuevas tecnologías.

En términos de seguridad, la ciudad de Babahoyo cuenta con el mismo sistema de vigilancia que brinda el ECU-911, porque (como ya se mencionó anteriormente) es el sistema mayormente integrado en el país con los diferentes sectores como: policías, militares, cuerpo de bomberos, hospitales, entre otros, lo que en la práctica significa eficacia.

En lo que respeta a la UTB (Universidad Técnica de Babahoyo), específicamente en la facultad de la FACIAG su sistema de seguridad, no está actualizado a las tendencias actuales en el área, por lo que aún no cuenta con un sistema de vigilancia sea con cámaras estáticas o drones con las tecnologías actuales.

## Bases teóricas

**¿Qué es un sistema de vigilancia?**

Los sistemas de vigilancia son utilizados ampliamente por todo tipo de instituciones para precautelar la integridad de trabajadores, civiles y bienes. Según (Benito, 2023) “los sistemas de videovigilancia son elementos que, mediante la grabación de audio y vídeo, tratan de garantizar la seguridad de una determinada propiedad” para lo cual utilizan varios componentes como cámaras de videovigilancia, drones, el cableado respectivo con cables de red, grabadores de videos, alarmas, sensores, etc.

Los sistemas de vigilancia actuales, cuentan con avanzadas características como: mejoras en la calidad de video, la inteligencia artificial (reconocimiento facial, detención de objetos, análisis de datos, automatización, entre otros), conexión inalámbrica. A lo antes mencionado podemos categorizarlos en: Sistemas de vigilancia cerrados y Sistemas de vigilancia IP.

## Sistema de vigilancia cerrado

Según [“l](https://www.leroymerlin.es/ideas-y-consejos/consejos/sistemas-de-vigilancia-caracteristicas-y-tipos.html#sistemas-de-vigilancia-cerrados)os sistemas cerrados consisten en un tipo de vigilancia compuesto por una cámara, un monitor y un grabador, siendo este último innecesario si simplemente queremos ver la imagen en tiempo real y no queremos almacenarla”. Es decir, un tipo de sistema en el cual no es necesario una conexión wifi como lo es en el sistema de vigilancia IP, presentando una ventaja al requerir menos componentes, pero, de ser necesario, se puede aplicar de forma inalámbrica.

## Sistemas de seguridad IP

Este tipo de sistemas parte del sistema de seguridad cerrado con la clara diferencia de su versatilidad, con base en lo que escribe (*leroymerlin.es*, s. f.) “permiten ver en todo momento y lugar lo que la cámara está viendo a través de un smartphone, tablet o un ordenador, y la mayoría poseen una app para sistemas Android o Apple”.

Estos sistemas, además, integran muy bien tecnologías como IoT (Internet of Things o Internet de las Cosas), como también el almacenamiento en la nube en caso de almacenar las grabaciones o audios, por lo que cabe mencionar algunas de las características que tienen los sistemas de seguridad modernos:

1. Reconocimiento facial.
2. Rotación trescientos sesenta grados.
3. Detección de movimiento.
4. Visión nocturna y aptas para exteriores.
5. Habla y escucha.
6. Modo privacidad.
7. Compatibilidad con sistemas de alarmas.
8. Grabación y visión en mosaico.
9. Grabación incorporada. (*leroymerlin.es*, s. f.)

## ¿Qué son los drones?

El siguiente autor indica que:

El término drone generalmente se refiere a cualquier aeronave no tripulada. A veces llamados vehículos aéreos no tripulados (UAV), estas aeronaves pueden llevar a cabo una impresionante variedad de tareas, desde operaciones militares hasta la entrega de paquetes. Los drones pueden ser tan grandes como una

aeronave o tan pequeños como la palma de tu mano. (Daley, 2022)

Basándonos en lo que Daley expone, podemos argumentar que los drones son herramientas versátiles, las cueles pueden ocupar muchas zonas de trabajo o en seguridad, inclusive llegando a colarse en las filas militares como parte de reconocimiento o ataques en enjambres; teniendo diferentes formas y tamaños, lo que la hace muy atractiva para una variedad de industrias y aplicaciones como en el caso de Amazon y su servicio de entrega a domicilio utilizando esta tecnología.

## Ventajas y desventaja del uso de drones

Como bien ya se ha explicado que los drones están teniendo un auge; agregando además el hecho de que se ve integrada con nuevas y mejores tecnologías como lo es la inteligencia artificial en la aplicación del reconocimiento facial, se ve envuelta en la dicotomía de sus ventajas y desventajas. Por ello, se presentarán las ventajas y desventajas del uso de estos aparatos:

Como ventajas, estos aparatos brindan; como principales ventajas como:

1. Aumentar niveles de seguridad.
2. Costos disminuidos ante años anteriores debido a la investigación en este tipo de dispositivos.
3. Imágenes de calidad y vigilancia en vivo.
4. Fácil manejo.
5. Llegan a zonas de difícil acceso.

El impacto que estos dispositivos no únicamente es positivo, sino que, también presenta aspectos negativos, como los son:

1. Pueden existir vulneraciones a la privacidad.
2. Vulnerables a ataques de animales en entornos donde los haya.
3. Agujeros legales en su uso.
4. Tiempo de autonomía.
5. Probabilidades de hackeo.

**Tabla comparativa de drones**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No. | Nombre del Drone | Precio Aproximado | Autonomía de Vuelo | Característic as Técnicas | Uso Ideal |
| 1 | DJI Mavic 2 Pro | $1,599 | Hasta 31 minutos | Sensor CMOS de 1pulgada, resolución de video 4K, rango de transmisión de hasta 8 km | Fotografía y video profesional |
| 2 | DJI Phantom 4 Pro V2.0 | $1,799 | Hasta 30 minutos | Sensor CMOS de 1pulgada, resolución de video 4K, rango de transmisión de hasta 7 km | Fotografía y video profesional |
| 3 | Parrot Bebop 2 Power | $599 | Hasta 30 minutos | Resolución de video Full HD, rango de | Entretenimie nto y recreación |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  | transmisión de hasta 2 km |  |
| 4 | Yuneec Typhoon H Plus | $1,899 | Hasta 28 minutos | Sensor CMOS de 1pulgada, resolución de video 4K, rango de transmisión de hasta 1.6 km | Fotografía y video profesional |
| 5 | Autel Robotics EVO II | $1,495 | Hasta 40 minutos | Sensor CMOS de 1pulgada, resolución de video 8K, rango de transmisión de hasta 9 km | Fotografía y video profesional |
| 6 | DJI Mini 2 | $449 | Hasta 31 minutos | Resolución de video 4K, | Viajes y aventuras al |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  | rango de transmisión de hasta 10 km | aire libre |
| 7 | Holy Stone HS100D | $249 | Hasta 15 minutos | Resolución de video 1080p, rango de transmisión de hasta 500 m | Entretenimie nto y recreación |
| 8 | Potensic T18 | $179 | Hasta 10 minutos | Resolución de video 1080p, rango de transmisión de hasta 300 m | Entretenimie nto y recreación |
| 9 | Ryze Tech Tello | $99 | Hasta 13 minutos | Resolución de video 720p, rango de transmisión | Aprendizaje y experimenta ción con drones |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  | de hasta 100 m |  |
| 10 | Hubsan H107D+ | $149 | Hasta 8 minutos | Resolución de video 720p, rango de transmisión de hasta 100 m | Entretenimie nto y recreación |
| 11 | DJI Matrice 300 RTK | $6,500 | Hasta 55 minutos | Cámara de zoom óptico, rango de transmisión de hasta 15 km, capacidad de vuelo con condiciones climáticas adversas | Vigilancia y operaciones de rescate |
| 12 | Skydio 2 | $1,999 | Hasta 23 minutos | Cámara de 12megapíxeles, | Seguimiento de personas y objetos en |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  | capacidad de evitar obstáculos automáticam ente | movimiento |
| 13 | Autel Robotics Dragonfish | $13,999 | Hasta 120 minutos | Cámara térmica y óptica, capacidad de operar en ambientes marinos y acuáticos | Vigilancia |
| 14 | DJI Mavic 2 Enterprise Dual | $2,699 | 31 minutos | Cámara dual (visual y térmica), sensor de obstáculos, sistema de transmisión de video en vivo, luces de advertencia y altavoz integrados | Búsqueda y rescate, seguridad pública |
| 15 | Yuneec H520E RTK | $3,999 | 28 minutos | Cámara 4K, sensor RTK de alta precisión, sistema de transmisión de video en vivo, modos | Inspección y monitoreo en servicios públicos y de seguridad |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  | de vuelo autónomo |  |
| 16 | Parrot Anafi USA | $7,000 | 32 minutos | Cámara 4K HDR, zoom óptico 32x, sistema de transmisión de video en vivo, modo de vuelo autónomo, resistencia a condiciones climáticas adversas | Vigilancia y monitoreo en entornos de seguridad pública |

## Eficiencia de los drones en la seguridad pública

Los drones, al ser una tecnología relativamente nueva, tiene que ser sometida a rigurosas pruebas para verificar su eficiencia en determinada área; en el caso de la seguridad pública, aún no existen los estudios técnicos suficientes para validar en un cien por ciento su eficacia, pero existen casos de su uso donde su rol fue decisivo al salvar vidas como en el siguiente caso:

En el año 2017 un sospechoso armado se atrinchero en el interior de una casa en Illinois, Estados Unidos tras abrir fuego contra policías, la situación empeoró debido a que era un exsoldado experimentado, por lo que al momento de negocias y debido a que el sospechoso se quedaba sin baterías, se optó por usar un dron para darle un celular al secuestrador para comunicarse y momentos después se entregó. (EXPANSION, 2019)

En este caso se puede apreciar la versatilidad que se le puede dar un dron, siendo que, sirvió como apoyo para la policía local en una situación donde pudo haber victimas

fatales, pero gracias al profesionalismo del personal policial, sumado al dron, se logró apaciguar la situación con éxito. Otro ejemplo es:

En el año 2016 en una operación de búsqueda y rescate por el Departamento de Lynwood. El jefe de bomberos John Cobb inicio la operación cuando un vehículo con dos personas se salió de la carretera y cayó a un lago, aunque solicitaron el equipo necesario como el de buceo, la búsqueda no tuvo suerte ni la búsqueda por helicóptero porque se quedaba sin combustible, por lo que optaron por usar un dron hasta donde el helicóptero había llegado, pero detuvieron la búsqueda porque ya era de noche, al día siguiente mapearon la zona con un dron y determinaron posibles ubicaciones dando resultados positivos. (EXPANSION, 2019)

En este otro ejemplo de como un dron puede ser útil, ahora no solo por su videovigilancia, sino porque puede ser una herramienta eficaz para realizar otro tipo de actividades como mapear un área en este caso.

## ¿Qué es una infraestructura tecnológica y sus tipos?

Una infraestructura tecnológica es vital en toda organización, aunque sea pequeña necesita de una infraestructura para funcionar, la cual está compuesta de diferentes elementos dependiendo del tipo que sea. Los tipos de infraestructura tecnológica son:

* Infraestructura de transporte: incluye carreteras, puentes, túneles, aeropuertos, ferrocarriles, puertos, etc.
* Infraestructura de energía: incluye la generación, transmisión y distribución de energía eléctrica, así como la extracción, transporte y refinación de petróleo y gas.
* Infraestructura de comunicaciones: incluye redes de telefonía fija y móvil, internet, satélites, televisión, radio, etc.
* Infraestructura de agua: incluye represas, embalses, acueductos, plantas de tratamiento de aguas, etc.
* Infraestructura de saneamiento: incluye sistemas de alcantarillado, plantas de tratamiento de aguas residuales, etc.
* Infraestructura social: incluye escuelas, hospitales, centros comunitarios, parques, etc.
* Infraestructura de tecnología: incluye centros de datos, servidores, redes de computadoras, software, etc.
* Infraestructura de seguridad: incluye sistemas de vigilancia, cámaras de seguridad, controles de acceso, alarmas, etc.
* Infraestructura financiera: incluye bancos, cajeros automáticos, sistemas de pago, etc.

## ¿Qué es la inteligencia artificial?

La definición de inteligencia artificial varía dependiendo el autor o desde la perspectiva de se estudie, como:

No existe una definición aceptada por todos los expertos de lo que significa la inteligencia artificial. Primero, porque es una ciencia bastante nueva, cambiante y experimental. Y segundo, porque ni siquiera podemos definir con exactitud qué es la inteligencia humana. (Estapé, 2022)

En su análisis, Estapé aborda la definición de la inteligencia artificial desde una perspectiva filosófica debido a la falta de una definición clara de la inteligencia. Esta dificultad hace que definir la inteligencia artificial sea complicado y requiere una sólida

comprensión de la inteligencia humana. La perspectiva de Estapé destaca la necesidad de seguir investigando y reflexionando sobre la definición de la inteligencia y la inteligencia artificial.

Por otra parte, otros autores como (IBM Cloud Education, 2020) plantea que la inteligencia artificial “es un campo que combina la ciencia informática y los conjuntos de datos robustos para permitir la resolución de problemas. También abarca los subcampos del machine learning y el deep learning, que se mencionan frecuentemente junto con la inteligencia artificial.”

En su análisis, IBM sostiene que la inteligencia artificial se compone de datos robustos para solucionar problemas y contribuir a la toma de decisiones. Asimismo, destaca que la forma de entrenar los diferentes tipos de IA varía según el tipo y alcance que se desee.

## ¿Qué es el reconocimiento facial?

La inteligencia artificial tiene diferentes aplicaciones, una de ellas es el reconocimiento facial. El reconocimiento facial, según (Kellett, 2023) “es una tecnología utilizada para mapear, identificar o verificar la estructura facial de una persona” y quien continúa explicando lo métodos que existen en esta tecnología, los que son:

* Reconocimiento facial tradicional: Detección, Análisis e Identificación.
* Reconocimiento facial 3D: Detección, Alineamiento, Medición, Representación, Emparejamiento e Identificación.
* Reconocimiento facial biométrico.

## Algoritmos utilizados en el reconocimiento facial.

Dentro de lo que es el reconocimiento facial, hay varias maneras de entrenar a estas redes neuronales, entre ellas tenemos:

## Eigenface (caras propias):

Basándonos en lo dicho por (JPL, 1991), “los eigenfaces se refieren a un enfoque sobre el [reconocimiento de rostros](https://proyectoidis.org/fisiognomia/) que busca capturar la variación en una colección de imágenes de [rostros](https://proyectoidis.org/zach-blas/) y utilizar esta información para codificar y comparar imágenes de rostros individuales de una manera holística (en contraposición a una basada en partes)”

Acotando a la idea del autor, debemos recalcar que este método es de los más utilizados, debido a su forma de procesar la información que, al comparar las imágenes almacenadas, se crea una maya y se miden la distancia euclidiana entre el vector de características de la imagen de entrada y los vectores de características para determinar la similitud.

## DeepFace:

Conforme a lo expuesto por (Marta Lahuerta, 2014) “el sistema Deepface utiliza una técnica de modelado 3D para detectar las caras y recortar y deformar para que se enfrentan a frente, en un método conocido como frontalización.”

DeepFace utiliza una arquitectura de red neuronal convolucional para extraer características de la imagen de entrada y una red neuronal completamente conectada para comparar las características extraídas con las características almacenadas en una base de datos. Este algoritmo ha demostrado tener un alto rendimiento en diversas pruebas de reconocimiento facial.

## Local Binary Patterns (LBP):

Según (Jesús Martínez, 2022) “[Patrones Binarios Locales (LBP, por sus siglas en](https://es.xcv.wiki/wiki/Local_binary_patterns) [inglés)](https://es.xcv.wiki/wiki/Local_binary_patterns), el cual se apoya en histogramas de patrones binarios para extraer features o vectores descriptivos de cada imagen, que luego son usados para entrenar un clasificador de machine learning.”

Este algoritmo se basa en la extracción de patrones locales de la imagen de entrada y la comparación de estos patrones con los patrones almacenados en una base de datos para determinar la similitud. Para entrenar el algoritmo, se utiliza un conjunto de imágenes etiquetadas para extraer los patrones locales de cada imagen. Los patrones se representan como histogramas de frecuencia y se almacenan en una base de datos. Para reconocer una imagen desconocida, el algoritmo extrae los patrones locales de la imagen y los compara con los patrones almacenados en la base de datos utilizando medidas de similitud como la distancia euclidiana o la correlación de Pearson.

## Tasa de éxito del reconocimiento facial.

Cuando hablamos de tasa de éxito en el reconocimiento facial, hablamos de cuan preciso es, porque se requiere la mayor precisión posible en cada uso, pero como lo explica (AWS, s.f.) “Los algoritmos de reconocimiento facial tienen una precisión casi perfecta en condiciones ideales. Existe una mayor tasa de éxito en entornos controlados, pero generalmente una tasa de rendimiento inferior en el mundo real. Es difícil predecir con exactitud la tasa de éxito de esta tecnología, ya que ninguna medida única proporciona un panorama completo”.

Esto se debe a que, en un ambiente controlado, está a disposición del investigador todos los recursos necesarios, y un banco enorme de imágenes, las cuales se pueden procesar para hallar la coincidencia con el rostro con el que se esté comparando, además con los siguientes aspectos:

* Posicionamiento e iluminación coherentes
* Rasgos faciales claros y libres de obstrucciones
* Colores y fondos controlados
* Calidad de la cámara y resolución de la imagen

En la realidad, existen varios inconvenientes al momento de analizar el rostro de las personas, como en el caso de:

Las mascarillas han supuesto un problema para los sistemas de reconocimiento facial. Al fin y al cabo, estos algoritmos se valen de la posición de los ojos, la nariz y la boca para identificar a los usuarios, algo que en pleno 2020, en plena pandemia, es complicado debido a la obligación de llevar mascarillas que se ha impuesto en muchos países. (Garcia, 2020)

Todo esto supuso un reto para el reconocimiento facial, ya que fallaba un cincuenta por ciento de las ocasiones, pero con el estudio necesario, se logró adiestrar a la inteligencia artificial para poder disminuir este porcentaje.

## La inteligencia artificial en la videovigilancia

Como ya se ha mencionado, la inteligencia artificial está cubriendo cada uno de los ámbitos laborales, sociales, domésticos, etc. En términos de seguridad, la inteligencia artificial, desempeña un rol importante al facilitar la detección de intrusos debido al reconocimiento facial, como también a detectar posibles delincuentes con la detección de objetos o reconocimiento de emociones.

La inteligencia artificial destaca, según (ARGÜELLO, 2022) debido a que “mientras vemos objetos, la máquina ve los detalles más finitos disponibles, es decir, todos y cada uno de los píxeles. Dentro del píxel, la máquina puede ver aún más detalles, que son el tono de los colores de esa imagen”.

## ¿Qué es el diseño de una red?

Las infraestructuras tecnológicas tienen como base el diseño de una red, la cual está conectada a una red interna o externa de la institución. Sobre el diseño de una red, podemos apoyarnos a lo que se explica en el foro de (UNIVERSITY, 2022) “el diseño de red es una categoría del desarrollo de sistemas que permite determinar la estructura física de una red de computadoras. Se refiere a la planificación de la implementación de una infraestructura de red informática”.

Al diseñar una red se debe analizar y determinar la cobertura que dicha red tendrá, para así determinar la estructura del cableado, la cantidad de equipos a necesitar, los servidores y los demás procesos que el diseño conlleva.

## Modelo OSI

El modelo OSI es un protocolo que usa la red, que está divido en siete capas y lo podemos definir basándonos en lo que (Etecé, 2021) expones, es un “un modelo de referencia para los protocolos de comunicación de las redes informáticas o redes de computadores” y sus siete capas son:

1. Física
2. Datos
3. Red
4. Transporte
5. Sesión
6. Presentación
7. Aplicación

Dentro de las capas de red, cuatro son esenciales en el diseño de una red, las cuales son:

1. Física
2. Datos
3. Red
4. Transporte

# METODOLOGÍA

## Tipo y diseño de investigación

### Tipo de investigación

El tipo de investigación es descriptiva, debido a que se describirán los riesgos de seguridad a los que se enfrentan los estudiantes, docentes y personal administrativo de la FACIAG, y para identificar las necesidades específicas de seguridad de la institución. También se utilizará el tipo de investigación debido a que se recabará información de antecedentes en el área que se ha analizará durante el trayecto de este trabajo de investigación.

### Metodología

La metodología de la investigación será de tipo mixta debido a que se combinan elementos cuantitativos y cualitativos. En cuanto a la recolección de datos cuantitativos, se aplicará una encuesta a los estudiantes, en la que se puedan medir de manera cuantitativa sus opiniones y actitudes en relación con el tema.

Por otro lado, con la recolección de datos cualitativos se realizará a través de entrevista al decano y personal administrativo de sistemas con el fin de profundizar en sus opiniones, experiencias y percepciones con relación a la seguridad en la FACIAG.

## Operacionalización de variables

### Tabla 1

*1Operacionalización de las variables de pendiente e independiente*

|  |  |  |  |
| --- | --- | --- | --- |
| **VARIABLE****S** | **CONCEPTUALIZACI****ON** | **DIMENSIONES** | **INDICADORES** |
| **Dependien** | Uso de | Aeronave no | Precisión | Frecuencia de |
| **te** | drones con | tripulada con un | Tiempo | uso, precisión del |
|  | reconocimi | sistema de |  | reconocimiento |
|  | ento facial. | detecciones de |  | facial. |
|  |  | rostro. |  | Tiempo de vuelo, |
|  |  |  |  | área de cobertura. |

## Independi ente

Seguridad La seguridad se

refiere a la protección de un individuo, un organización o una comunidad contra peligros o amenazas potenciales. En términos generales, ser refiere a la ausencia de riesgos o la minimización de los mismos.

* + - * Tasa de inciden tes reporta dos
			* Cantidad de casos reportados

.

## Población y muestra de investigación

### Población

Debido a que no se pudo obtener los datos sobre una población exacta debido a protocolos, se ha optado por tomar una población aleatoria estratificada, teniendo en cuenta un dato ambiguo que la población es mayor a tres mil quinientos estudiantes:

*2 Tabla de población*

4000

**Estudiantes**

1

**Administrador de Sistemas**

**1**

**Decano de la FACIAG**

### Muestra

Para la determinación de la muestra de estudiantes se aplicó la formula n = N / (1 + N \* e^2) que estableció un valor de n= 363.

n = 4000 / (1 + 4000 \* 0.05^2)

n = 4000 / (1 + 4000 \* 0.0025)

n = 4000 / (1 + 10)

n = 363

## Técnicas e instrumentos de medición

### Técnicas

Las técnicas a utilizar son:

* La entrevista al director del departamento de sistemas.
* La entrevista al decano de la FACIAG
* La encuesta dirigida a los estudiantes.

### Instrumentos

Como instrumentos se tiene:

* Cuestionario para encuesta.
* Preguntas para entrevista.

## Procesamiento de datos

El estudio de esta investigación se comenzó con un análisis cuantitativo de los datos recopilados de la encuesta presentado mediante gráficos estadísticos. Además, el análisis de la entrevista que se realizó al director del departamento de sistemas.

## Aspectos éticos

El uso de drones con reconocimiento facial para la vigilancia tiene aspectos positivos como: incrementar la seguridad en el área que se aplique, grabar y almacenar los datos que recopile, hacer análisis de datos, etc. Siendo esto bueno respecto a la integridad de las personas, es cierto que, presentan interrogantes respecto a la privacidad de las personas.

La implementación de un sistema de vigilancia en la FACIAG de la Universidad Técnica de Babahoyo podría generar dilemas éticos relacionados con la privacidad y el monitoreo masivo. Es fundamental evaluar si es necesario y proporcional establecer tal vigilancia, además de definir políticas claras sobre el uso y protección de datos, con el fin de asegurar el respeto a los derechos fundamentales de las personas, a pesar de que se realizará una encuesta a los estudiantes.

# PRESUPUESTO

El presupuesto, a continuación, será presentado con varias opciones para analizar, por lo que teniendo en cuenta eso, se pueda tomar las decisiones pertinentes.

Para hacer este presupuesto, se asumió que el departamento de sistemas, además de estar sustentado con la entrevista del director de este departamento de la UTB, cuenta con los medios necesarios para enviar la señal hasta la FACIAG y crear la conexiones en caso de necesitarse, pero el presupuesto está orientado a lo que se necesitaría para complementar esta infraestructura.

## Presupuesto de los cursos de drones:

|  |  |  |
| --- | --- | --- |
| Empresa | Curso | Precio |
| Drone Pilot U | Comprehensive Training | $499 |
| Drone Pilot Academy | Professional Drone Training | $999 |

**Presupuesto de los equipos:**

|  |  |  |  |
| --- | --- | --- | --- |
| Producto | Modelo | Precio (USD) | Cantidad |
| Antena | LAVA HD8008 | 89.95 | 3 |
| Repetidor de señal | TP-Link RE650 | 99.99 | 6 |

|  |  |  |  |
| --- | --- | --- | --- |
| Servidor de video | Western Digital My Cloud EX2 | 259.99 | 1 |
| Software de transmisión de video en tiempo real | QGroundControl | gratis | 1 |

**Para el presupuesto de los drones hay que tener en cuenta el área a cubrir:**



*Captura de pantalla de Google Earth. Recuperado de:*

[*https://earth.google.com/web/@-1.79755208,-79.48387204,8.84693239a,461.86739292d,35y,0h,0t,0r*](https://earth.google.com/web/%40-1.79755208%2C-79.48387204%2C8.84693239a%2C461.86739292d%2C35y%2C0h%2C0t%2C0r)

Para determinar la cantidad de drones necesarios para cubrir un perímetro de 4141,69 metros, es importante tener en cuenta varios factores. Uno de los principales es la capacidad de vuelo de cada dron y la distancia que puede cubrir en un solo vuelo.

Supongamos que un dron tiene una velocidad de vuelo de 20 metros por segundo y una autonomía de 30 minutos, lo que significa que puede volar durante 30 minutos a una velocidad de 20 metros por segundo, lo que equivale a recorrer una

distancia total de 36 kilómetros (20 metros/segundo \* 60 segundos/minuto \* 30 minutos).

Si dividimos la distancia total que se desea cubrir (4141,69 metros) entre la distancia que puede cubrir cada dron en un solo vuelo (36 kilómetros), obtenemos el número aproximado de drones necesarios para cubrir el perímetro.

Entonces, para cubrir un perímetro de, 4141,69 metros con drones con una capacidad de vuelo de 30 minutos y velocidad de 20 metros por segundo, necesitaríamos aproximadamente 9 drones en total

Asimismo, cabe señalar, que el diseño de una infraestructura no suele ser económica y estos precios son muestras para complementar la investigación.

# RESULTADOS Y DISCUSIÓN

* 1. Resultados

## Encuesta

* + - 1. **¿Ha oído usted hablar de los drones con inteligencia artificial?**



La primera pregunta de la encuesta dio como resultado un 75% de respuestas positivas y un 25% de respuestas negativas, lo que demuestra el grado de conocimiento de los encuestados respecto a los drones con inteligencia artificial.

## ¿Conoce usted acerca de la tecnología de reconocimiento facial utilizada por los drones?



La segunda pregunta de la encuesta dio como resultado un 70% de respuestas positivas y un 30% de respuestas negativas, lo que demuestra el grado de conocimiento de los encuestados respecto a la tecnología de reconocimiento facial, en parte porque es una tecnología usada ampliamente en los dispositivos móviles por lo que tienen cierta familiaridad con el tema.

## ¿Cree usted que el uso de drones con reconocimiento facial mejoría la seguridad en el campus universitario?

La tercera pregunta de la encuesta dio como resultado un 95% de respuestas positivas y un 5% de respuestas negativas, respecto a su opinión sobre si creen que el uso de drones con reconocimiento facial mejoraría la seguridad en la facultad.

## ¿Considera usted que el uso de drones con reconocimiento facial invade la privacidad de las personas?



La cuarta pregunta de la encuesta dio como resultado un 68% de respuestas positivas y un 32% de respuestas negativas, respecto a su opinión sobre si creen que el uso de drones con reconocimiento facial invadiría la privacidad de las personas, por lo que hay que tener en cuenta al determinar las políticas a seguir.

## ¿Se sentiría usted más seguro (a) al saber que drones con reconocimiento facial se utilizarían en la FACIAG?

La quinta pregunta de la encuesta dio como resultado un 96% de respuestas positivas y un 4% de respuestas negativas, respecto a su opinión sobre la perspectiva de seguridad que tendrían si se aplicaría un sistema de vigilancia con drones con inteligencia artificial en la facultad, a pesar de que evidentemente esto significaría plantear políticas sobre su uso dentro de la facultad.

## ¿Considera sted que la FACIAG debería implementar más medidas de seguridad además del uso de drones con reconocimiento facial?



La sexta pregunta de la encuesta dio como resultado un 91% de respuestas positivas y un 9% de respuestas negativas, respecto a su opinión sobre si se deberían implementar otras medidas además de los drones con reconocimiento facial, como lo podrían ser cámaras estáticas, sensores u otros dispositivos que están orientados a la seguridad.

## Decano de la FACIAG

1. **¿Cómo estima usted la seguridad de bienes y personas en la facultad?**

Creo que hemos sabido llevarla de una manera eficaz el aspecto de la seguridad institucional, es un trabajo constante donde tenemos que estar unidos para ayudarnos a controlar y evitar desmanes, afortunadamente tenemos personal responsable y capaz que ha sabido proteger a nuestra facultad.

## ¿Se han registrado eventos delincuenciales que pongan en riesgos los bienes y personas de la FACIAG?

Dentro de nuestra institución no hemos tenido situaciones de riesgo, lastimosamente por la situación que atraviesa nuestro país, donde la delincuencia ha incrementado, si hemos tenido conocimiento de compañeros y estudiantes que han sido víctimas de la delincuencia, con pérdidas materiales, cabe indicar que estos episodios no han sido en la institución.

## ¿Qué tipos de eventos delincuenciales se han registrado que representen riesgos para los bienes y personas de la FACIAG?

Fuera de los predios universitarios se han presentado asaltos.

## ¿De qué manera enfrentan ustedes los riesgos por delincuencia para bienes y personas en la facultad?

Contamos con personal capacitado, además se ha puesto a disposición del personal Universitario y estudiantes un bus institucional para que se los traslade hasta los predios de la FACIAG para evitar que sean víctimas del hampa, además se ha pedido que haya resguardo policial fuera de las instalaciones de la facultad.

## ¿Qué opina del uso de drones con reconocimiento facial puede mejorar la seguridad en la FACIAG?

Pienso que todos los mecanismos y herramientas que contribuyan al mejoramiento y seguridad de la institución deben ser probados y si cumplen con los estándares de calidad adoptados para el fortalecimiento institucional.

## ¿Cuáles son los aspectos negativos que presentaría el uso de drones con reconocimiento facial para la seguridad en la FACIAG?

Que es un equipo de costo elevado y puede ser derribado por los delincuentes y llevárselo.

## ¿Apoyaría usted un sistema de vigilancia con drones y reconocimiento facial?

Creo que se lo podría poner a prueba para verificar su utilidad.

## Director del departamento de sistemas.

1. **¿Podría describir el equipamiento tecnológico actual del departamento de sistemas de la FACIAG y la central?**

El departamento de sistemas de FACIAG, el departamento actualmente se encuentra en la central, pero en FACIAG lo que hay son varios switches, equipos de UPC por la energía, fibra óptica, equipos de rayos láser, en este caso simplemente es un nodo, un nodo el cual, con fibra óptica a través de cedia y se reparte a través de fibra a todas las oficinas, no hay como tal un departamento de sistemas en agronomía, todo se encuentra en la FACIAG.

## ¿Cómo cree que el uso de drones con reconocimiento facial podría mejorar la seguridad en la FACIAG?

Respecto a la segunda pregunta, la FACIAG es un área grande, tiene muchas hectáreas, bueno, tenemos una cantidad de compañeros, guardias que vigilan allá, pero ha habido situaciones de robo y cosas así, porque la zona es grande. Bueno lo que tú me estás indicando en el asunto de los drones, sería interesante tener un equipo especializado que con drones vigilen todo el campo de la FACIAG debido a su área amplia en el que se tenga la zona de control y se haga una revisión con estos equipos modernos y viene bien para los tiempos que estamos.

## ¿Cuáles son las principales preocupaciones o desafíos que ve en la implementación de un sistema de drones con reconocimiento facial en la FACIAG?

El primer desafío sería la parte cultural, siempre cuando se implemente un cambio, las personas tienden a la resistencia y, si el cambio es beneficioso, se tiene la pauta de sus buenos beneficios. Además, como segundo punto, tenemos la parte económica que no sé de cuantos drones se necesitarían para vigilar toda la facultad y cambiar la cultura de las personas para usar estos aparatos y capacitar la gente para hacer el trabajo de vigilancia.

## ¿Cuál es su opinión sobre la integración de un sistema de vigilancia con drones y reconocimiento facial con la infraestructura tecnológica actual de la UTB?

Los drones se utilizan hoy en día para los sembríos, líquidos, plagas, fertilizante y en la parte de vigilancia y con reconocimiento facial sería interesante y novedoso, ya que no se ha hecho ni he visto en el país, lo que sería un buen caso para tesis para que se implemente en una ubicación que se tiene una extensión bien fuerte de terreno y donde hay bastantes usuarios que estén yendo a la facultad por servicios o los estudiantes mismos.

Respecto a la infraestructura actual, como ya mencioné, en la FACIAG lo que hay es un nodo conectado con CEDIA, en caso de querer hacer el proyecto, podrías hacerlo tranquilamente en la central de agronomía porque ancho de banda y espacio hay suficiente, en caso de ser en toda la universidad, los costos serían elevados, pero al ser solo en la facultad de agronomía, ya que el nodo principal llega a la biblioteca y se reparte con fibra óptica a todos los departamentos.

## Discusión

Una vez finalizado el análisis de las preguntas de encuestas hacia los estudiantes y al director del departamento de sistemas, queda claro de que, además de una necesidad en la FACIAG, es algo asequible, no olvidando que toda implementación a una infraestructura independientemente del área, tiene sus costes. Otro punto a favor que se obtuvo fue la percepción que lograría en la comunidad universitaria, como también cumplir con ese derecho a la seguridad que todas las ciudadanas y ciudadanos tenemos.

Por parte de quién está a cargo de la FACIAG, se dio una disposición a usar la tecnología o cualquier otro pedio para precautelar la integridad de los que a esta asisten, aunque teniendo en cuenta que esto podría generar gastos (que es un factor determinante)

En los antecedentes se mencionó sobre el uso de estos aparatos por parte del gobierno de china para la disminución de robos, para el control de las personas durante la pandemia del COVID-19, sin tener en cuenta los aspectos de derechos humanos o los de libertad social, esta herramienta es altamente recomendada. Varios drones con altavoces patrullan las calles de las zonas rurales de China. Los alcaldes han recurrido a ellos para llamar la atención a aquellos ciudadanos que pasean por la calle sin mascarilla en estos días de plena batalla contra el coronavirus. (NIUS,2020).

Siguiendo la idea del párrafo anterior, China, a pesar de ser el que más está explotando el potencial de los drones, otras potencias como Estados Unidos están usando a los drones para rescate, apoyo policial, entretenimiento, delivery, etc.

Recalcando una vez más el potencial uso que tienen los drones.

# CONCLUSIONES Y RECOMENDACIONES

## Conclusiones

Basándonos en lo estudiado se concluye que:

* Los drones con reconocimiento facial y en general los drones; han demostrado ser herramientas útiles en diferentes ámbitos de la vida y sociedad, además este uso solo se ha visto ampliado y seguirá en expansión.
* Éticamente, se deben definir políticas para evitar el abuso de esta herramienta por parte de los operarios o como también por parte de los dirigentes de la facultad.
* La infraestructura actual de la UTB puede soportar la implementación de este tipo de sistemas, debido a que se cuenta con la infraestructura necesaria, como: Switches, cableado, fibra óptica, rayos-láser, etc.
* El uso de drones con reconocimiento facial, es una herramienta tecnológica relativamente nueva, por lo que es pertinente continuar con la investigación para el desarrollo de nuevas tecnologías relacionadas con este tema.

## Recomendaciones

Basándose en lo estudiado se recomienda:

* Realizar más estudios referentes al tema, porque la tecnología se actualiza constantemente, por lo que hoy es novedoso, mañana podría ser obsoleto.
* Incentivar a la comunidad de la FAFI en la carrera de Sistemas de Información, conjuntamente con los profesores, a crear nuestros propios diseños de drones con inteligencia artificial de reconocimiento facial.
* Definir políticas claras del uso de estos aparatos para evitar daños a la comunidad estudiantil en la FACIAG.
* Integrar otras tecnologías para tener un sistema de vigilancia más robusto, ya que una limitante de los drones es su autonomía de vuelo, que está alrededor de los treinta minutos.

# BIBLIOGRAFÍA

Jesús Martínez. (2022, Febrero 23). *Cómo Crear un Reconocedor Facial con Patrones Binarios Locales (LBP) con OpenCV*. DataSmarts. https://datasmarts.net/es/como-crear-un-reconocedor-facial-con-patrones-binarios-locales-lbps-c on-opencv/

JPL. (1991, Julio 14). *Eigenface*. Eigenface. https://proyectoidis.org/eigenface/

Marta Lahuerta. (2014, Marzo 18). *DeepFace, software de reconocimiento facial de Facebook*.

Computerhoy.

[https://computerhoy.com/noticias/software/deepface-software-reconocimiento-facial-facebook-1](https://computerhoy.com/noticias/software/deepface-software-reconocimiento-facial-facebook-10405) [0405](https://computerhoy.com/noticias/software/deepface-software-reconocimiento-facial-facebook-10405)

ARGÜELLO, F. (10 de Julio de 2022). *infoteknico*. Obtenido de infoteknico: https://[www.infoteknico.com/inteligencia-artificial-ia-video-vigilancia/](http://www.infoteknico.com/inteligencia-artificial-ia-video-vigilancia/)

Benito, A. (13 de Febrero de 2023). *roams*. Obtenido de roams: https://alarmas.roams.es/seguridad/videovigilancia/

Daley, S. (18 de Agosto de 2022). *builtin*. Obtenido de builtin: https://builtin.com/drones ecu911. (25 de Junio de 2020). *ecu911*. Obtenido de ecu911:

https://[www.ecu911.gob.ec/con-un-moderno-software-camaras-del-ecu-911-miden-el-distanciam](http://www.ecu911.gob.ec/con-un-moderno-software-camaras-del-ecu-911-miden-el-distanciam) iento-fisico-y-generan-alertas/

Estapé, J. A. (02 de Diciembre de 2022). *computerhoy*. Obtenido de computerhoy:

https://computerhoy.com/reportajes/tecnologia/inteligencia-artificial-469917#%C2%BFQu%C3

%A9-es-la-inteligencia-artificial?-1669974186473

Etecé, E. (05 de Agosto de 2021). *concepto*. Obtenido de concepto: https://concepto.de/modelo-osi/

IBM Cloud Education. (03 de Junio de 2020). *IBM*. Obtenido de IBM: https://[www.ibm.com/mx-es/cloud/learn/what-is-artificial-intelligence](http://www.ibm.com/mx-es/cloud/learn/what-is-artificial-intelligence)

Kellett, S. (23 de Febrero de 2023). *avast*. Obtenido de avast: https://[www.avast.com/c-facial-recognition](http://www.avast.com/c-facial-recognition)

Pérez, M. G. (25 de Mayo de 2021). *DerechosEcuador*. Obtenido de DerechosEcuador: https://derechoecuador.com/seguridad-ciudadana/

UNIVERSITY, S. L. (06 de Octubre de 2022). *SAINT LEO UNIVERSITY*. Obtenido de SAINT LEO UNIVERSITY:

https://worldcampus.saintleo.edu/noticias/que-es-el-diseno-de-red-diseno-de-red-de-computador as#:~:text=El%20dise%C3%B1o%20de%20red%20es%20una%20categor%C3%ADa%20del,de%20la% 20red%20que%20se%20va%20a%20implementar.

# ANEXOS

## Preguntas al Director del departamento de sistemas.

1. ¿Podría describir el equipamiento tecnológico actual del departamento de sistemas de la FACIAG y la central?
2. ¿Cómo cree que el uso de drones con reconocimiento facial podría mejorar la seguridad en la FACIAG?
3. ¿Cuáles son las principales preocupaciones o desafíos que ve en la implementación de un sistema de drones con reconocimiento facial en la FACIAG?
4. ¿Cuál es su opinión sobre la integración de un sistema de vigilancia con drones y reconocimiento facial con la infraestructura tecnológica actual de la UTB?

## Preguntas al Decano de la FACIAG

1. ¿Cómo estima usted la seguridad de bienes y personas en la facultad?
2. ¿Se han registrado eventos delincuenciales que pongan en riesgos los bienes y personas de la FACIAG?
3. ¿Qué tipos de eventos delincuenciales se han registrado que representen riesgos para los bienes y personas de la FACIAG?
4. ¿De qué manera enfrentan ustedes los riesgos por delincuencia para bienes y personas en la facultad?
5. ¿Qué opina del uso de drones con reconocimiento facial puede mejorar la seguridad en la FACIAG?
6. ¿Cuáles son los aspectos negativos que presentaría el uso de drones con reconocimiento facial para la seguridad en la FACIAG?
7. ¿Apoyaría usted un sistema de vigilancia con drones y reconocimiento facial?

## Preguntas de Encuesta

* 1. ¿Ha oído usted hablar de los drones con inteligencia artificial?
	2. ¿Conoce usted acerca de la tecnología de reconocimiento facial utilizada por los drones?
	3. ¿Cree usted que el uso de drones con reconocimiento facial mejoría la seguridad en el campus universitario?
	4. ¿Considera usted que el uso de drones con reconocimiento facial invade la privacidad de las personas?
	5. ¿Se sentiría usted más seguro (a) al saber que drones con reconocimiento facial se utilizarían en la FACIAG?
	6. ¿Considera usted que la FACIAG debería implementar más medidas de seguridad además del uso de drones con reconocimiento facial?