



Universidad
Nacional
de Loja

Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables

Carrera de Ingeniería en Electrónica y Telecomunicaciones

**Diseño e implementación de un prototipo de sistema de
seguridad inteligente, para el centro I2TEC de la UNL.**

Trabajo de Titulación previo a optar
por el Título de Ingeniero en
Electrónica y Telecomunicaciones

AUTOR:

Darwin Augusto Palacios Yunga

DIRECTOR:

Ing. Rodolfo Pabel Merino Vivanco, Mg. Sc.

Loja – Ecuador

2023

Certificación

Loja, 12 de junio del 2023

Ing. Rodolfo Pabel Merino Vivanco, Mg. Sc.

DIRECTOR DEL TRABAJO DE TITULACIÓN

CERTIFICO:

Que he revisado y orientado todo proceso de la elaboración del Trabajo de Titulación denominado: **Diseño e implementación de un prototipo de sistema de seguridad inteligente, para el centro I2TEC de la UNL.**, previo a la obtención del título de Ingeniero en **Electrónica y Telecomunicaciones**, de la autoría del estudiante: Darwin Augusto Palacios Yunga, **con cédula de identidad Nro.1150634788**, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja para el efecto, autorizo la presentación para la respectiva sustentación y defensa.

Ing. Rodolfo Pabel Merino Vivanco, Mg. Sc.

DIRECTOR DEL TRABAJO DE TITULACIÓN

Autoría

Yo, **Darwin Augusto Palacios Yunga**, declaro ser autor del presente Trabajo de Titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales por el contenido del mismo. Adicionalmente, acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi Trabajo de Titulación en el Repositorio Digital Institucional – Biblioteca Virtual.

Firma:

Cédula de Identidad: 1150634788

Fecha: 02/08/2023

Correo electrónico: darwin.a.palacios@unl.edu.ec

Teléfono: 0980649546

Carta de autorización del Trabajo de Titulación por parte del autor para la consulta de producción parcial o total, y/o publicación electrónica de texto completo.

Yo, **Darwin Augusto Palacios Yunga**, declaro ser autor del Trabajo de Titulación denominado: **Diseño e implementación de un prototipo de sistema de seguridad inteligente, para el centro I2TEC de la UNL.**, como requisito para optar al grado de: **Ingeniero en Electrónica y Telecomunicaciones**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Digital, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Titulación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los dos días del mes de agosto del dos mil veintitrés.

Firma:

Autor: Darwin Augusto Palacios Yunga

Cédula: 1150634788

Dirección: Loja

Correo Electrónico: darwin.a.palacios@unl.edu.ec

Celular: 0980649546

DATOS COMPLEMENTARIOS:

Director del Trabajo de Titulación: Ing. Rodolfo Pabel Merino Vivanco, Mg. Sc.

Dedicatoria

El presente Trabajo de Titulación lo dedico a Dios por guiarme, bendecirme y brindarme fortaleza para poder sobrellevar las diferentes adversidades en cada una de las etapas de mi vida.

A mis padres Milton Palacios y Rosa Yunga, quienes han confiado en mí y me han apoyado de manera incondicional para poder cumplir cada una de las metas que me he propuesto. Ustedes han sido mi constante fuente de inspiración, impulsándome a enfrentar cada desafío con valentía y determinación. Cada logro que alcanzo lleva su amor y dedicación grabados en mi corazón.

A mis hermanos Cristina, José y César, por todo su apoyo y ejemplo de perseverancia.

A mi abuelita, ya que ahora finalizo este largo camino que comenzamos juntos, y aunque la vida nos separó físicamente a mitad de esta carrera, sé que siempre estuviste conmigo en espíritu y corazón. Cada logro alcanzado, cada obstáculo superado, ha sido en honor a ti y al legado de amor, sabiduría y fuerza que dejaste en mi vida. Lamento profundamente que no puedas estar presente en este momento tan importante, pero sé que desde donde estés, sigues guiando mis pasos con tu inmenso amor y protección.

Darwin Augusto Palacios Yunga

Agradecimiento

Agradezco profundamente a mis padres, quienes desde mi infancia me han inculcado los valores más importantes de la vida. Su amor incondicional, motivación, paciencia y esfuerzo han sido fundamentales para mi desarrollo personal y académico. Este Trabajo de Titulación es un testimonio de su sacrificio y su influencia en mi vida, y dedico cada logro a su nombre con todo mi corazón.

A mi novia por su constante motivación y por sus palabras de aliento cuando más lo necesitaba.

A mis amigos con los cuales conformamos un gran equipo desde el inicio y pudimos sobrellevar la carrera de una mejor manera.

A la Universidad Nacional de Loja y a la SENESCYT por haberme brindado la oportunidad de estudiar la carrera que me apasiona desde mi niñez.

Al equipo del centro I2TEC, quiero expresar mis más sinceros agradecimientos por su compromiso con la innovación, el cual me permitió desarrollar y llevar a cabo la implementación del prototipo en su espacio físico.

De igual manera quiero agradecer a toda la planta docente de la carrera de Ingeniería en Electrónica y Telecomunicaciones, y de manera muy especial al Ingeniero Rodolfo Pabel Merino por su apoyo y asesoría en cada una de las etapas del desarrollo del presente trabajo de titulación.

Con profunda gratitud y respeto.

Darwin Augusto Palacios Yunga

Índice de contenidos

Certificación	ii
Autoría	iii
Carta de autorización	iv
Dedicatoria	v
Agradecimiento	vi
Índice de contenidos	vii
Índice de Tablas:	x
Índice de Figuras:	x
Índice de Anexos:	xiii
1. Título	1
2. Resumen	2
2.1 Abstract	3
3. Introducción	4
4. Marco teórico	7
4.1 Seguridad Ciudadana	7
4.1.1 Entidades Gubernamentales Encargadas de la Seguridad	7
4.2 Sistema de Seguridad.....	8
4.2.1 Sistema de Antirrobo e Intrusión.....	9
4.2.1.1 Dispositivos Electrónicos Capaces de Detectar Intrusiones.	10
4.2.1.2 Grados de Seguridad de los Sistemas.....	13
4.2.1.3 Falsas Alarmas.	13
4.2.2 Circuito Cerrado de Televisión.....	14
4.2.2.1 Sistema de CCTV Sobre IP.....	15
4.2.2.2 Evolución de los Sistemas de Videovigilancia.	16
4.3 Sistemas Embebidos	17
4.3.1 Beneficios de los Sistemas Embebidos.....	18
4.4 Fundamentos de una Imagen Digital.....	18
4.4.1 El Peso en una Imagen	20
4.4.2 Frecuencia de Imagen (frame rate)	20
4.5 Visión por Computador	21
4.5.1 Etapas en un Proceso de Visión Artificial	22
4.5.2 Componentes de un Sistema de Visión Artificial.....	24
4.5.2.1 Iluminación.....	24
4.5.2.2 Lentes.	24
4.5.2.3 Sensor de Imagen.	25

4.5.2.4	Procesamiento de Visión.....	25
4.5.2.5	Comunicaciones.....	26
4.5.3	OpenCV.....	26
4.6	Raspberry Pi (RPI).....	27
4.6.1	Partes Fundamentales de Raspberry Pi.....	28
4.6.2	Ventajas.....	30
4.7	Aplicaciones Web.....	30
4.7.1	Los protocolos de Internet en el desarrollo web.....	32
4.7.2	Arquitecturas web de contenido estático o dinámico.....	32
4.7.3	Bases de datos.....	34
5.	Metodología.....	35
5.1	Área de Estudio.....	35
5.2	Materiales.....	36
5.2.1	Hardware.....	36
5.2.1.1	Microordenador.....	36
5.2.1.2	Cámara.....	37
5.2.1.3	Módulo Sensor de Movimiento.....	38
5.2.2	Software.....	39
5.2.2.1	Sistema Operativo del Microordenador.....	39
5.2.2.2	Lenguaje de Programación.....	39
5.2.2.3	Biblioteca de Visión Artificial.....	40
5.2.2.4	Plataforma en la nube para lanzar un servidor.....	41
5.2.2.5	Software necesario para crear la aplicación web.....	42
5.2.2.6	Lenguajes de programación y de estilo para la aplicación web.....	42
5.2.2.7	Plataforma necesaria para el almacenamiento en la nube.....	43
5.2.2.8	Proveedor de correo electrónico.....	44
5.2.2.9	Software para conexión remota al servidor en la nube y/o Raspberry.....	44
5.3	Método.....	45
5.3.1	Técnica de recolección de datos.....	45
5.3.2	Técnicas de análisis y procesamiento de la información.....	46
5.4	Procedimiento.....	47
5.5.	Diseño.....	48
5.5.1	Dimensionamiento del sistema de seguridad.....	48
5.5.2	Elección del hardware.....	50
5.5.2.1	Microordenador.....	50

5.5.2.2	Cámara	52
5.5.2.3	Módulo Sensor de Movimiento	54
5.5.3	Elección del software	54
5.5.3.1	Sistema operativo del microordenador	54
5.5.3.2	Biblioteca de Visión Artificial.	56
5.5.3.3	Lenguaje de Programación	57
5.5.3.4	Plataforma en la nube para lanzar un servidor	58
5.5.3.5	Software necesario para crear la aplicación web.	60
5.5.3.6	Lenguajes de programación y de estilo para la aplicación web.	61
5.5.3.7	Plataforma necesaria para el almacenamiento en la nube.	62
5.5.3.8	Proveedor de correo electrónico.	63
5.5.3.9	Software para la conexión remota al servidor en la nube y/o Raspberry.....	63
5.5.4	Diagrama de conexión	64
5.5.5	Proceso para la construcción del prototipo.....	65
5.5.5.1	Instalación del sistema operativo de Raspberry “Raspbian”	65
5.5.5.2	Conexión remota a la Raspberry Pi.	68
5.5.5.3	Habilitación de la cámara de la Raspberry Pi.....	70
5.5.5.4	Instalación de la biblioteca de visión artificial y de las dependencias necesarias.....	71
5.5.5.5	Lanzamiento de la instancia EC2 en AWS	72
5.5.5.6	Instalación del software necesario para crear la aplicación web	75
5.5.5.7	Configuración de Gmail para poder utilizarlo desde Python.	80
5.5.5.8	Configuración de Firebase storage para utilizarlo desde Python.....	80
5.5.5.9	Desarrollo del script en Python	83
5.5.5.10	Presentación de los datos en la aplicación web.....	87
5.5.5.11	Diseño del case del prototipo.....	93
5.5.5.12	Consideraciones de seguridad informática del prototipo.....	94
6.	Resultados.....	96
6.1	Descripción general del sistema de seguridad inteligente.....	96
6.2	Resultados estadísticos de la encuesta	97
6.3	Pruebas de funcionamiento del prototipo	103
6.4	Presupuesto del prototipo y comparación con otros sistemas de seguridad .	111
7.	Discusión.....	113
8.	Conclusiones	115
9.	Recomendaciones	116

10. Bibliografía	117
11. Anexos	121

Índice de Tablas:

Tabla 1. Relación entre objetivos estratégicos y aplicaciones de visión artificial. ..22	
Tabla 2. Lista de materiales mínimos para poder desarrollar el sistema de seguridad.36	
Tabla 3. Comparación entre diferentes versiones de RPi.52	
Tabla 4. Comparación entre cámara AVMP y el módulo RaspiCam V2.53	
Tabla 5. Comparación entre diferentes herramientas de visión artificial.....57	
Tabla 6. Comparación entre diferentes lenguajes de programación.....58	
Tabla 7. Comparación entre diferentes plataformas.....59	
Tabla 8. Comparación entre lenguaje.62	
Tabla 9. Resultados de pruebas de funcionamiento del prototipo.108	
Tabla 10. Presupuesto aproximado del proyecto.111	
Tabla 11. Comparación de sistemas de seguridad comerciales con el sistema propuesto.....112	

Índice de Figuras:

Figura 1. Sensor magnético.....11	
Figura 2. Detector volumétrico PIR11	
Figura 3. Emisión del haz de una barrera microondas.12	
Figura 4. Sensor ultrasónico.....12	
Figura 5. Relación inversa entre el FAR y la seguridad instalación.....14	
Figura 6. Instalación completa de cámara CCTV con DVR.....15	
Figura 7. Esquema básico de un CCTV sobre IP.16	
Figura 8. Diferentes versiones de una imagen.19	
Figura 9. Etapas de un sistema de visión artificial.23	
Figura 10. Diferentes modelos de Raspberry Pi (RPI).....28	
Figura 11. Ubicación de los conectores y pines de una RPI.29	
Figura 12. Tecnologías empleadas en el cliente y en el servidor web.31	
Figura 13. Ubicación del centro I2EC.....35	
Figura 14. Raspberry Pi 4 Modelo B37	
Figura 15. Cámara full HD AVMP.....38	
Figura 16. Sensor PIR HC-SR501.....38	

Figura 17. Escritorio de Raspberry Pi OS Full	39
Figura 18. Python.....	40
Figura 19. OpenCV	41
Figura 20. AWS.....	41
Figura 21. Conjunto de software libre para crear aplicaciones web.	42
Figura 22. Lenguajes para crear aplicaciones web.....	43
Figura 23. Plataforma para el almacenamiento en la nube: Firebase.....	44
Figura 24. Proveedor de correo electrónico: Gmail.	44
Figura 25. Software para conexión remota: PuTTY, WinSCP, TeamViewer.....	45
Figura 26. Identificación de los puntos más vulnerables.	48
Figura 27. Diagrama de funcionamiento del sistema.....	49
Figura 28. Diagrama de conexión del prototipo.	65
Figura 29. Identificación de la SD que se tendrá que formatear.	65
Figura 30. Elección de los parámetros óptimos para formatear la SD.	66
Figura 31. Software Raspberry Pi Imager.	67
Figura 32. Elección del sistema Operativo.....	67
Figura 33. Elección de la tarjeta SD y de otras opciones avanzadas.	68
Figura 34. Herramientas de configuración de la Raspberry Pi.....	70
Figura 35. Selección de la cámara.	71
Figura 36. Selección del sistema operativo de la máquina virtual.....	72
Figura 37. Selección el tipo de instancia.	72
Figura 38. Crear el par de claves para administrar el servidor de manera remota....	73
Figura 39. Configuración del almacenamiento.....	74
Figura 40. Configuración de la IP elástica.....	75
Figura 41. Acceso al servidor remoto de AWS.	75
Figura 42. Carga de la llave privada ppk.....	76
Figura 43. Configuraciones de Apache.	77
Figura 44. Configuraciones adicionales de phpMyAdmin.....	79
Figura 45. Configuraciones adicionales de phpMyAdmin.....	79
Figura 46. Configuraciones adicionales de phpMyAdmin.....	79
Figura 47. Crear un nuevo proyecto de Firebase storage.	81
Figura 48. Configuraciones de seguridad.	81
Figura 49. Configuración de la región.	82
Figura 50. Configuración del proyecto.....	82
Figura 51. Diagrama de flujo del funcionamiento del script.....	86

Figura 52. Diseño del mecanismo de autenticación.	87
Figura 53. Diseño de la página principal.	88
Figura 54. Diseño de la página de imágenes capturadas.....	88
Figura 55. Diseño de la página de información de usuario.....	89
Figura 56. Diseño de la página de soporte técnico.....	89
Figura 57. Estructura del directorio de la aplicación web.	90
Figura 58. Estructura del dominio de la aplicación web.....	91
Figura 59. Configuración de los registros en AWS.	91
Figura 60. Verificar la validez de certificado SSL.....	93
Figura 61. Diseño de case para sensor.....	94
Figura 62. Diseño de case para la Raspberry Pi.	94
Figura 63. Etapas de funcionamiento del prototipo.....	96
Figura 64. Resultado de la pregunta 1.	98
Figura 65. Resultado de la pregunta 2.	98
Figura 66. Resultado de la pregunta 3.	99
Figura 67. Resultado de la pregunta 4.	99
Figura 68. Resultado de la pregunta 5.	100
Figura 69. Resultado de la pregunta 6.	100
Figura 70. Resultado de la pregunta 7.	101
Figura 71. Resultado de la pregunta 8.....	101
Figura 72. Resultado de la pregunta 9.	102
Figura 73. Resultado de la pregunta 10.	102
Figura 74. Plano del centro I2TEC.	103
Figura 75. Prototipo instalado.....	104
Figura 76. Configuración del horario de activación.....	104
Figura 77. Prueba de la aplicación web.	105
Figura 78. Inicio exitoso a la aplicación web.	105
Figura 79. Imagen cargada a la aplicación web.....	106
Figura 80. Mensaje de alerta por correo electrónico.....	106
Figura 81. Respaldo de las imágenes en Firebase.....	107

Índice de Anexos:

Anexo 1. Cifras de robos proporcionadas por la FGE	121
Anexo 2. Presupuestos de sistema de seguridad, CCTV y cámara con IA.	123
Anexo 3. Preguntas realizadas en la encuesta	126
Anexo 4. Función <i>Video_Stream</i>	128
Anexo 5. Código Fuente del sistema de seguridad.	129
Anexo 6. Manual de usuario y de mantenimiento.	133
Anexo 7. Certificado de traducción.....	146

1. Título

**Diseño e implementación de un prototipo de sistema de seguridad inteligente,
para el centro I2TEC de la UNL.**

2. Resumen

El presente trabajo de titulación explica exhaustivamente cada una de las fases necesarias para la implementación de un sistema de seguridad inteligente y activo, que emplea técnicas de visión artificial y de procesamiento de imágenes para detectar la presencia de posibles intrusos en una determinada zona de interés. Para ello, se emplea la biblioteca de visión artificial denominada OpenCV, la cual permite una integración eficiente y efectiva del sistema. Con el objetivo de recopilar información sobre las necesidades y preferencias de las personas, se llevó a cabo una encuesta para evaluar su conocimiento en relación a los sistemas de seguridad e identificar sus preferencias. De esta forma, se logró obtener información valiosa para el diseño del prototipo. En el desarrollo del prototipo se hace énfasis en mantener una relación costo-efectividad para garantizar que el sistema esté al alcance de las personas que no disponen de ningún tipo de sistema de seguridad o para aquellas personas que requieren alternativas con tecnología superior a CCTV, cercas eléctricas, etc. Para ello se da inicio con la revisión de los conceptos teóricos que sirven como base en la construcción del prototipo, se identificaron los puntos más vulnerables del lugar de la implementación, a partir de ello se investigaron y se ofrecen múltiples alternativas de software y/o hardware. Los lenguajes de programación que se utilizaron son Python, HTML, PHP y CSS. En el código fuente se aplican múltiples condiciones para la activación, el control de la iluminación y la toma de decisiones. En caso de que se cumplan las condiciones preestablecidas, se desencadena una alerta inmediata mediante correo electrónico, paralelamente se cargan las imágenes en un servidor y los datos de fecha y hora se cargan en una base de datos, esto permite el monitoreo de las incidencias desde una aplicación web, además se activa una alarma sonora y las imágenes se almacenan en la nube de Firebase como un respaldo adicional.

Palabras clave: *OpenCV, Sistema de seguridad activo, Visión artificial, Procesamiento de imágenes, Control de iluminación, Aplicación web, Bases de datos.*

2.1 Abstract

This degree work comprehensively explains each of the necessary phases for embedding an intelligent and active security system, which uses artificial vision and image processing techniques to detect the presence of possible intruders in a predetermined area of interest. For this purpose, we used the Computer Vision library called OpenCV, which allows to integrate the system in an efficient and effective way. To gather information about people's needs and preferences, we conducted a survey to assess their knowledge about security systems and identify their choices. In this way, we obtained valuable information for the design of the prototype. In the development of the prototype, we placed emphasis on maintaining a cost-effectiveness ratio to ensure that the system is accessible to people who do not have any other type of security system or for those who require alternatives with technology superior to CCTV, electric fences, among others, to do so, we started with the review of the theoretical concepts that serve as a basis in the construction of the prototype, we identified the most vulnerable points of the implementation site, from this we investigated and offered multiple alternatives of software (and/or hardware) the programming languages used are Python, HTML, PHP and CSS. In the source code we applied multiple conditions for activation, lighting control and decision making. If we comply the pre-established criteria, we trigger an immediate alert via email; simultaneously, we upload the images to a server and load the date time data to a database; this allows the monitoring of incidents from a web application. Furthermore, we activated an audible alarm. And we save the images in the Firebase cloud as an additional backup.

Keywords: OpenCV, Active security system, Artificial vision, Image processing, Lighting control, Web application, Databases

3. Introducción

La constante evolución tecnológica se hace presente en actividades cotidianas del ser humano, la tecnología viene siendo un aliado en varios sectores como: la salud, industria, agricultura, ambiente, movilidad, turismo, comercio, seguridad, entre otras actividades. De igual manera, las necesidades de contar con tecnología van en aumento debido a que es común que se requieran optimizar procesos y transformar el entorno, de modo que se adecuen a los nuevos requerimientos de los diversos sectores.

La investigación es fundamental para poder contribuir con soluciones a actividades del diario vivir, una de las necesidades más apremiantes y de carácter social es brindar tranquilidad y seguridad a las personas, así como también a sus bienes. Y la mejor manera de solventar este inconveniente es poder apoyarse de la tecnología disponible en la actualidad; para de esa manera crear soluciones eficientes, que generen confianza y calma a las personas que confían en la tecnología.

Los inconvenientes relacionados con temas de seguridad en la ciudad y país son preocupantes debido a que se observa un incremento de delitos de todos los tipos de robo en el periodo comprendido entre los meses de enero a noviembre del 2022, con respecto al mismo periodo del año 2021. Por ejemplo, los robos a entornos privados en el 2022 incrementaron en un 28.34% con respecto al año anterior; es por ello que es indispensable la contribución de la tecnología como apoyo a los diversos sistemas de seguridad.

Actualmente, por medio de diferentes tecnologías, software y hardware se brindan varias soluciones en el sector de la seguridad, dichas soluciones son de gran aporte para todas las personas que les interesa salvaguardar de la mejor manera sus bienes más preciados. El Ministerio del interior (2019) argumenta que la seguridad ciudadana son aquellas condiciones en que las personas pueden disfrutar libremente de cualquier actividad, sin temor a los múltiples tipos de actos delictivos que infringen las obligaciones de un estado de proteger los derechos humanos.

Los sistemas de seguridad tradicionales han evolucionado, de tal manera que pueden permitir almacenar los videos de vigilancia en servidores públicos, privados o haciendo uso de internet, y de esta manera facilitar el acceso a la información requerida. Puede que el uso de estos sistemas presente ventajas importantes, y de manera general mayor flexibilidad en cuanto a la transferencia de información. Así mismo, puede haber algunas limitaciones en lo que respecta a seguridad y a la rapidez con la que se pueden acceder a los datos.

Aquellas personas que cuentan con locales comerciales, pequeñas y medianas empresas o con cualquier espacio físico que necesiten resguardar, sostienen que los sistemas de seguridad habituales tienen limitaciones. Por ejemplo, si ocurre cualquier hecho delictivo y más aún si se da en la noche, que es donde estos actos ocurren con mayor frecuencia según las estadísticas proporcionadas por la Fiscalía General del Estado (FGE). En estas situaciones la tecnología de videovigilancia o CCTV captará lo sucedido y lo almacenará, luego cuando se pueda conocer de lo sucedido quizá han pasado algunas horas y en estas circunstancias es muy difícil el poder encontrar al o los culpables de los actos delictivos tales como robos, intrusiones o sustracción de información.

Una de las razones por la cual las personas no optan por un sistema de seguridad de antirrobo e intrusión es por los costos, los sistemas más básicos tienen valores que están por encima de 432.00 dólares y lo que hacen es únicamente grabar y almacenar lo sucedido, lo que no garantiza de ninguna manera la protección de los bienes. Si bien es cierto, existen alternativas con características superiores como: cámaras que incluyen visión artificial o sistemas completos de seguridad, pero de igual forma tienen valores muy altos, por lo tanto, muchas de las veces en los hogares e inclusive en los locales comerciales se les hace un gasto que está fuera del alcance de su economía.

Previo al planteamiento de la investigación, el centro de investigación, innovación, desarrollo de prototipos tecnológicos y pruebas electroenergéticas I2TEC de la Universidad Nacional de Loja no contaba con un sistema de seguridad inteligente y activo, en el mismo solo existía un sensor de movimiento que se encontraba anclado al sistema de alarma contra incendios del edificio principal. Además, en un contexto más amplio, es relevante destacar que una considerable cantidad de residencias y empresas de pequeño y mediano tamaño en nuestra localidad y país carecen de sistemas de seguridad activos, lo cual se traduce en la exposición a situaciones de actos delictivos. Esta ausencia de medidas preventivas representa una vulnerabilidad significativa para estos entornos, y puede ocasionar pérdidas considerables.

Es por ello que esta investigación cobra mayor relevancia tratando de disminuir los costos en estos sistemas, utilizando tecnología moderna, que es más funcional, flexible y que cuenta con beneficios similares a los que ofrecen otras soluciones comerciales, pero evidentemente a un costo menor; para que resulten más accesibles a aquellas personas que buscan prevenir robos, intrusiones o mantener un control del aforo con ayuda de técnicas de visión artificial. De esta manera se reduciría la brecha digital en cuanto al acceso a tecnologías modernas y con grandes capacidades.

La visión artificial y las bibliotecas de visión artificial de código abierto como Open Source Computer Vision (OpenCV) en la actualidad se usan con mucha frecuencia. Esto debido a que proporcionan técnicas que permiten la adquisición, el procesamiento, el análisis y la comprensión de las imágenes, de modo que la información pueda ser extraída y procesada por un ordenador (Hashemi, 2019).

OpenCV está disponible de manera gratuita, ya sean para fines académicos o incluso para fines comerciales. Uno de los usos más importantes de dicha biblioteca de visión artificial es la detección de rostros y objetos, sobre todo en áreas como la seguridad, el marketing, la fotografía, etc. Además, cuenta con una buena eficiencia computacional y con un fuerte enfoque en aplicaciones en tiempo real, que es precisamente para lo que será utilizado.

En ese contexto, se concibió como objetivo principal del presente trabajo de titulación el diseñar e implementar un prototipo de un sistema de seguridad activo para el centro de investigación, innovación, desarrollo de prototipos tecnológicos y prueba electroenergéticas I2TEC de la Universidad Nacional de Loja.

Para el cumplimiento del objetivo general se establecieron los siguientes objetivos específicos:

- Dimensionar un sistema de seguridad activo e inteligente para la detección, captura y posteriormente la transferencia de imágenes.
- Emplear herramientas de software y/o hardware Open Source y una aplicación web donde se puedan visualizar los eventos inusuales captados en el centro I2TEC.
- Implementar el prototipo con sus manuales de uso y mantenimiento.

4. Marco teórico

4.1 Seguridad Ciudadana

La seguridad ciudadana es un tema que afecta a todas las clases sociales, cuyos matices determinan el bienestar de los ciudadanos, por lo que es indispensable la participación de todos los habitantes del país, para que de esa manera se puedan encontrar soluciones efectivas. Situaciones como la pobreza, el hambre, la falta de oportunidades, el desempleo, la violencia, la represión política, la delincuencia y el consumo de drogas representan serias amenazas para la seguridad de los ciudadanos (Fuentes y Castellanos, 2019).

Desde otro punto de vista se puede argumentar que la seguridad ciudadana representa el hecho de no tener miedo a ser víctima de algún ataque violento, ni temer por la integridad física; sino más bien que se pueda disfrutar libremente de varias actividades dentro o fuera del hogar, sin sentir temor a ser asaltado o a que los bienes sean sustraídos por personas con conductas de antisociales.

En Ecuador se han trazado ciertas estrategias de seguridad ciudadana de manera nacional, pero también existen estrategias locales para una ciudad y/o provincia, las cuales en su mayoría son establecidas por los gobiernos autónomos descentralizados (GAD). En cambio, el plan nacional de seguridad es establecido por el gobierno de turno para la ejecución y el cumplimiento en todo el país. El Ministerio del Interior (2018) propone el actual plan que se encuentra en vigencia denominado Plan Nacional de Seguridad Ciudadana y Convivencia Social Pacífica 2019-2030, el cual contiene nueve objetivos estratégicos que se alinean con la Agenda 2030 de Desarrollo Sostenible (propuesta por la Organización de las Naciones Unidas).

Basándose en las investigaciones realizadas se puede argumentar que; aunque existan estrategias de seguridad ciudadana locales o nacionales y planes establecidos por organismos internacionales, no son del todo efectivas. Esto se puede ratificar con los datos que proporciona la FGE, en donde se analiza desde el año 2019 hasta el 2021 y se puede observar que en el último año existió un incremento en todos los tipos de robo (véase Anexo 1).

4.1.1 Entidades Gubernamentales Encargadas de la Seguridad

Según una investigación de Armas (2021) en los años 80 la policía permanecía en los denominados retenes policiales, luego en los años 90 se dieron a conocer los puestos de

auxilio inmediato que fueron ubicados de manera estratégica en las ciudades. En los años 2000 se crearon las Unidades de Policía Comunitaria (UPC), esto dio tranquilidad a los ciudadanos, ya que aseguraban que las respuestas a diferentes actos delictivos serían de manera inmediata. Sin embargo, con el tiempo se presentaron problemas debido a que personas influyentes hacían todo lo necesario para que se construyan UPC cerca de sus viviendas para poder tener protección personal, lo cual perjudicó a otros sectores que realmente necesitaban contar con esta infraestructura. Pero con el tiempo se planificó de mejor forma y se reestructuró la ubicación de las UPC de una manera técnica para que los resultados sean más visibles.

En el año 2011, el presidente de la República por medio del Decreto Ejecutivo N.º 988 estableció la implementación del Servicio Integrado de Seguridad ECU 911 como una herramienta tecnológica integradora de los servicios de emergencia. Este es un servicio de respuesta inmediata ante emergencias en el territorio ecuatoriano (Servicio Integrado de Seguridad ECU 911, 2021). Las instituciones que han unido esfuerzos para brindar una mejor atención a los ciudadanos son:

- Policía Nacional
- Cuerpo de Bomberos
- Fuerzas Armadas
- Comisión Nacional de Tránsito
- Instituto Ecuatoriano de Seguridad Social
- Servicio Nacional de Gestión de Riesgos y Emergencias
- Ministerio de Salud Pública
- Cruz Roja Ecuatoriana
- Otros organismos locales encargados de la atención de emergencias

Todas estas instituciones son las encargadas de atender emergencias que surgen en el día a día en el territorio nacional; aquellas que han sido reportadas a través del número de atención único 911 o las que se generan por medio de monitoreo de alarmas y videovigilancia.

4.2 Sistema de Seguridad

Son varias las definiciones que hacen referencia a los sistemas de seguridad debido a que el concepto se encuentra en constante desarrollo, ya que cada vez aparecen nuevas tecnologías que prometen mayor alcance y efectividad. Sin embargo, dichas definiciones tienen como idea primordial el brindar protección a los bienes públicos o privados dentro de un área en específico.

Según Rodríguez (2018) afirma que “un sistema de seguridad puede ser definido como el conjunto de equipos y componentes necesarios para que se pueda garantizar a las personas y los bienes materiales existentes en un determinado lugar, la protección necesaria frente a agresiones externas” (pág.2).

Por lo general, todos los equipos que conforman un sistema de seguridad se encuentran conectados a una única central de alarmas; que actúa en función de la situación y del riesgo que exista en el entorno. Usualmente, estos sistemas activan mecanismos de disuasión, mecanismos de captura de imágenes o vídeos, entre otros. Esto podría servir para alertar a las fuerzas del orden público o a los propietarios para que puedan interferir.

Lo que hacen los diferentes sistemas de seguridad es poder detectar una situación de riesgo, identificarla y luego dar inicio con las medidas correspondientes que están encaminadas a minimizar, o en el mejor de los casos eliminar los efectos de una situación que representa peligro. La seguridad es un tema muy importante, como muestra de ello podemos palpar los avances tecnológicos, en donde se han implementado varias medidas para mejorar los sistemas existentes. Es por esto que la seguridad es fundamental para hogares, empresas pequeñas o para empresas de grandes proporciones (Rodríguez, 2018).

Los sistemas electrónicos de seguridad más comunes en la actualidad son:

- Sistema de seguridad contra incendios
- Circuito cerrado de televisión (CCTV)
- Sistema de control de acceso
- Sistema de detección de gas
- Sistema antirrobo e intrusión

Cada uno de estos sistemas se pueden encontrar en cualquier tipo de infraestructura, ya sea pequeña, mediana o grande. Pero es más común que los instalen en aeropuertos, colegios, hospitales, bancos, universidades, entre otros.

4.2.1 Sistema de Antirrobo e Intrusión

Desde el punto de vista de Aranda (2013) “los Sistemas de Intrusión tienen el objetivo de la seguridad contra actos antisociales, con la aplicación de medios y métodos para evitar, reducir o controlar, las acciones delictivas provocadas por actividades antisociales” (p.11).

El objeto de estos sistemas es proteger al sujeto paciente frente a un riesgo contra:

- La salud

- La integridad física
- Sus bienes y patrimonio
- La intimidad
- Las comunicaciones
- La integridad moral
- El medio ambiente
- Robo y hurto
- Atraco
- Fraude y estafa
- Vandalismo
- Amenazas
- Sabotaje y manipulación
- Espionaje industrial, comercial o financiero.

Para prevenir estos riesgos se requieren de elementos y equipos que estén en la capacidad de poder gestionar las funciones de intrusión, atraco o robo, control de accesos, control de presencia, etc.

4.2.1.1 Dispositivos Electrónicos Capaces de Detectar Intrusiones.

En la actualidad, existen diversos sensores o dispositivos electrónicos que son bastante utilizados a la hora de crear un sistema de seguridad de anti intrusión debido a su precisión y sobre todo por su bajo costo. A continuación, se mencionan los más comunes en el mercado de los dispositivos electrónicos.

- Detectores magnéticos: son aquellos dispositivos que se encargan de controlar el ingreso a cualquier espacio físico, por ejemplo: puede verificar la apertura de puertas o ventanas. Como se muestra en la Figura 1, este dispositivo es de dos piezas que internamente contienen imanes, una vez que se abre una puerta o ventana los imanes se separan, lo que producirá una activación de un interruptor que se encuentra en el interior (Jiménez, 2022).

Figura 1.

Sensor magnético



Nota. En la Figura se muestra las dos piezas del sensor. **Fuente:** Getterson (2020).

- Detectores volumétricos infrarrojos: son aquellos dispositivos capaces de captar la radiación térmica que pudiese emitir un intruso en una zona controlada. Se puede observar en la Figura 2 que es de pequeñas dimensiones y si capta cualquier movimiento no autorizado estará en la capacidad de activar alguna alarma que se encuentre vinculada.

Figura 2.

Detector volumétrico PIR



Nota. En la Figura se muestra al sensor volumétrico. **Fuente:** Onate (2017).

- Barrera microondas: este dispositivo emite un haz electromagnético desde un emisor hasta un receptor por medio de microondas de alta frecuencia, de esa manera crea un muro de protección, esto se detalla en la Figura 3.

Figura 3.

Emisión del haz de una barrera microondas.

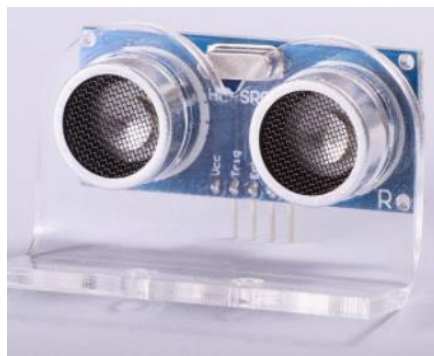


Nota. En la Figura se presenta como se realiza la emisión del haz de una barrera microondas. **Fuente:** Bunker Seguridad Electrónica (2018).

- Sensor de distancia por ultrasonido: aunque este dispositivo tenga más uso en robots, de igual manera podría emplearse para medir la distancia a la que se pudiese encontrar algún intruso. En la Figura 4 se muestra el sensor ultrasónico, este mide distancias en función de la reflexión de ultrasonidos (Solectro, 2021).

Figura 4.

Sensor ultrasónico.



Nota. En la Figura se muestra al sensor ultrasónico. **Fuente:** Solectro (2021).

El uso de los dispositivos descritos anteriormente es muy común en proyectos básicos. Sin embargo, pudiesen usarse en sistemas de seguridad de antirrobo e intrusión más complejos, siempre y cuando actúen en combinación con otros elementos que aseguren una robustez de todo el sistema, de manera que puedan garantizar un óptimo desempeño.

A pesar de que los dispositivos que se han descrito se utilizan con frecuencia, para un mayor funcionamiento y solidez del sistema se deberían combinar con otros elementos.

4.2.1.2 Grados de Seguridad de los Sistemas.

En una orden ministerial del Gobierno Español INT/316/2011 en su artículo 2 explica la definición de los cuatro grados de los sistemas de seguridad de alarma, en función de diferentes parámetros. A continuación, se describen los grados definidos por Rodríguez (2018).

El grado 1 representa un riesgo bajo, se considera muy poco probable que un intruso intente eludir este tipo de instalaciones, es por ello que el sistema de alarma no se encuentra conectado a una central.

El grado 2 representa un riesgo bajo-medio, se considera poco probable que un intruso intente eludir estas instalaciones, está dedicado para viviendas y para pequeñas infraestructuras que se conectan a una central de alarmas.

El grado 3 representa un riesgo medio-alto en donde se considera probable que un intruso intente eludir las instalaciones, está destinado para establecimientos con gran actividad, aquellos tienen la obligación de disponer de medidas de seguridad, por ende, el contar con una central es imprescindible.

El grado 4 representa un riesgo alto en donde es muy probable que un intruso intente sabotear las instalaciones, está predestinado para las infraestructuras críticas como, por ejemplo: empresas de seguridad, instalaciones militares, empresas que manejan grandes cantidades de dinero, etc. Estas cuentan con una central de alarmas y adicionalmente con centros de control.

4.2.1.3 Falsas Alarmas.

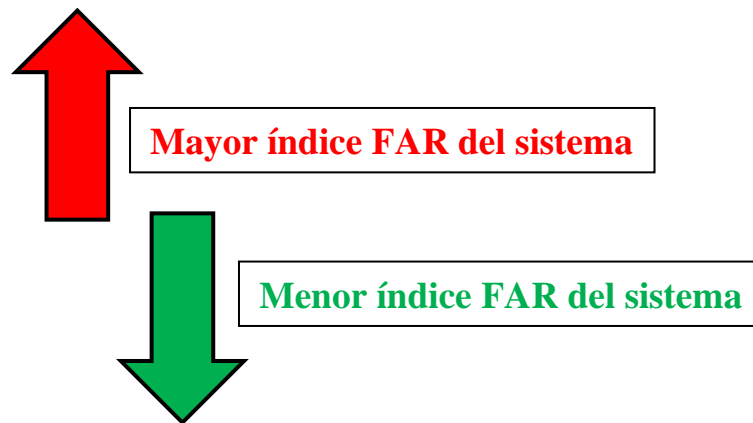
Una falsa alarma se denomina como un falso disparo, esto se produce cuando un sistema de seguridad detecta algún evento que activa un disparo de detección sin ninguna causa que sea real. Entre las causas más usuales de las falsas alarmas están; posibles problemas de mantenimiento, baja calidad de los equipos, error de usuario, mala ingeniería de instalación, hacer uso erróneo del manual de usuario (EPS Security, 2021).

Desde el punto de vista de Rodríguez (2018), otras causas por las que se producen las falsas alarmas son; deterioro de los componentes, factores ambientales como, por ejemplo: la luz, la temperatura, modificaciones del entorno, subidas de tensión eléctrica, presencia de mascotas, etc. Lo que se espera es que en cualquier sistema de seguridad

exista la menor cantidad de falsas alarmas para que el grado de fiabilidad sea elevado. En la Figura 5 se muestra la relación para poder indicar el grado de fiabilidad (pág.9).

Figura 5.

Relación inversa entre el FAR y la seguridad instalación.



Nota. FAR significa índice de falsas alarmas. **Fuente:** Rodríguez (2018).

En resumen, cualquier sistema de seguridad de cualquier tipo tiene por objetivo primordial cumplir con su función, pero además deberá estar en la capacidad de ser inmune a las falsas alarmas. Para ello se debe seguir un debido proceso de diseño, instalación, pruebas y mantenimiento.

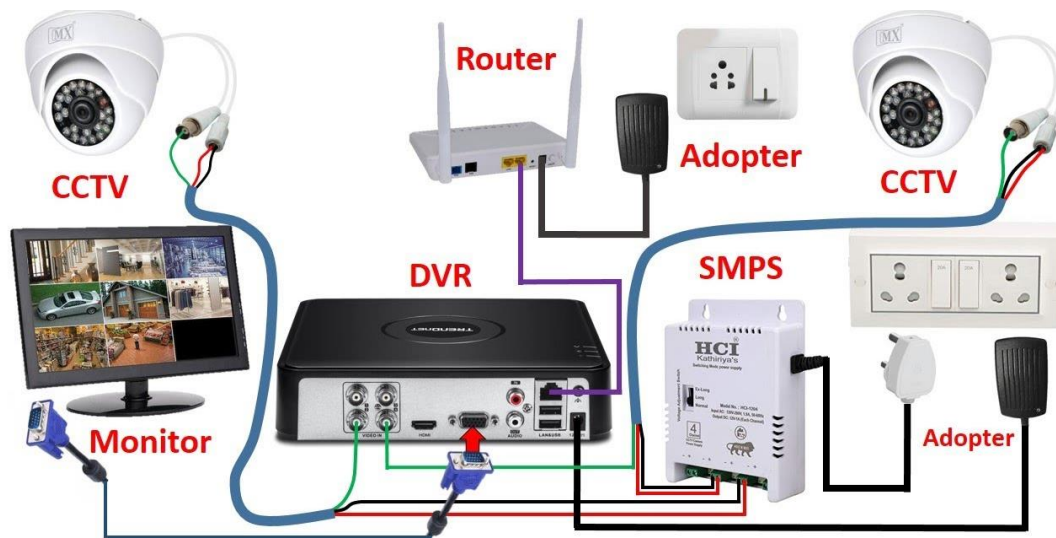
4.2.2 Circuito Cerrado de Televisión

El concepto de circuito cerrado de televisión (CCTV) data de los años 1942, cuando por primera vez se documentó el uso de CCTV por parte del ejército alemán. De acuerdo con García Mata (2010) el circuito cerrado de televisión tiene como objetivo principal el supervisar, controlar y registrar la actividad dentro de un espacio o ambiente en general. El sistema está compuesto por una o varias cámaras de vigilancia que se encuentran conectadas por lo menos a un monitor, los cuales muestran los videos capturados. Se denomina circuito cerrado de televisión porque el acceso a las imágenes o vídeos es permitido solo a ciertos usuarios que cuentan con la respectiva autorización.

Entre los componentes que conforman un sistema CCTV están: cámaras, lentes, monitores, grabadoras, matriz de video, líneas de transmisión, dispositivos de acoplamiento y conectores. En la Figura 6 se puede observar el diagrama de una instalación típica.

Figura 6.

Instalación completa de cámara CCTV con DVR.



Nota. En la figura se muestra cada uno de los elementos que hacen posible que un sistema CCTV funcione. **Fuente:** Electrical Technician (2022).

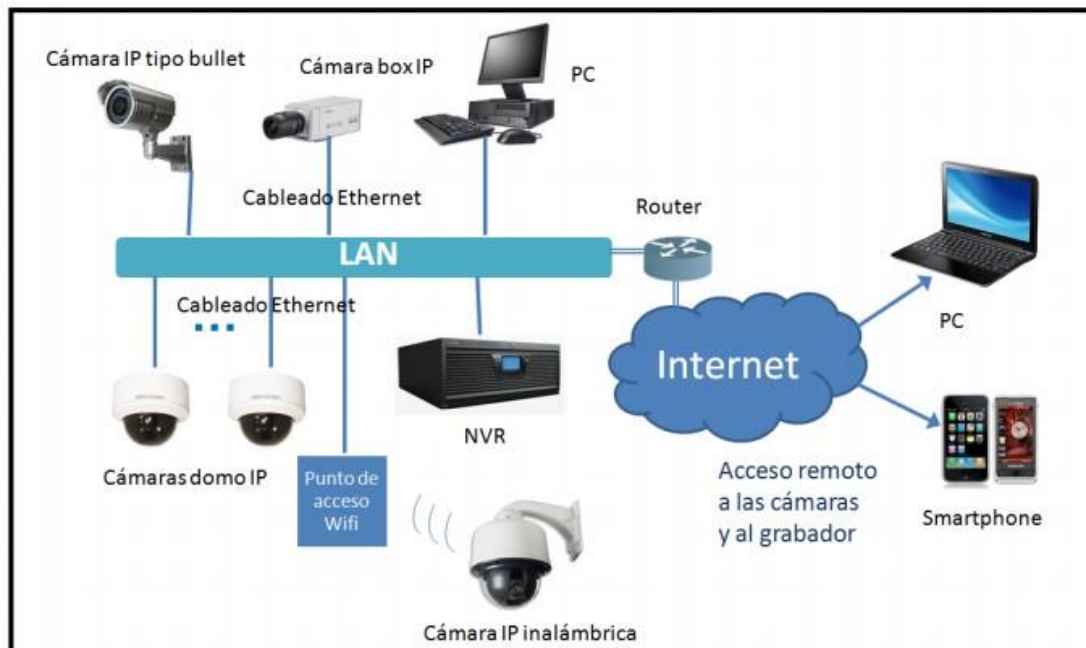
4.2.2.1 Sistema de CCTV Sobre IP.

Los sistemas de CCTV que utilizan video IP se efectúan por medio de redes que pudieran ser cableadas o inalámbricas. Este sistema proporciona ventajas con respecto al tradicional sistema analógico de CCTV; principalmente por dos razones. La primera razón es la facilidad del despliegue que tienen estos sistemas, esto produce incluso que los costos de instalación se reduzcan, puesto que puede aprovechar la infraestructura de internet para la red de videovigilancia. La segunda razón es debido a que permite el monitoreo del contenido de manera local o de manera remota, pero manteniendo una alta calidad de imagen.

Los elementos que conforman este tipo de sistema son: cámaras IP, cable Ethernet, NVR, router, switch, PC y un dispositivo inteligente por si se necesita acceder de manera remota. En la Figura 7 podemos observar el esquema básico de un CCTV sobre IP.

Figura 7.

Esquema básico de un CCTV sobre IP.



Nota. En la figura se muestra cada uno de los elementos que hacen posible que un sistema CCTV sobre IP funcione. **Fuente:** Electrical Technician (2022).

4.2.2.2 Evolución de los Sistemas de Videovigilancia.

Existen dos sistemas de videovigilancia más usados para llevar a cabo el control de entornos videovigilados; los sistemas de CCTV tradicional (de los cuales ya se ha hablado) y otra basada en técnicas de visión artificial, que fue la que se hizo más común en la última década. La principal diferencia es el uso de sistemas dotados de inteligencia y de autonomía, estos están en la capacidad de analizar los videos capturados en tiempo real, frente a los sistemas tradicionales que necesitan de una persona que analice y pueda detectar ciertas anomalías (García Mata, 2010, p.47).

Los sistemas que cuentan con inteligencia tienen una función que va más allá de simplemente grabar y almacenar fotos o videos, están en la capacidad de extraer en tiempo real y de forma automática cierta información de interés. Esto permite que se facilite la labor, o en el mejor de los casos que se deje de contar con personas encargadas del monitoreo.

Estos sistemas automáticos realizan multitud de tareas que incluyen: detección, interpretación, comprensión, registro y creación de alarmas basadas en el análisis. Estudios recientes han logrado un mejor rendimiento de monitoreo para evitar posibles fallas humanas por manipulación de diferentes características de estos sistemas. Algunas de las tareas de

estos sistemas inteligentes podrían ser; seguimiento de objetos, detección de movimiento, detección de objetos, gestión de multitudes, etc. Pero existen muchas más tareas que se pudiesen integrar para obtener un buen desempeño. En este campo, y especialmente cuando se vigila una zona concurrida, podemos extraer mucha información que puede ser útil para la seguridad de las personas, pero esta extracción puede ser difícil cuando la escena es compleja. Además, el reconocimiento y el seguimiento de objetos representa un problema sobre todo en el entorno con escenas complejas y esta es la principal dificultad en la visión por computador (Elharrouss et al., 2021).

Con el pasar de los años, con la explotación de la visión por computador y con la constante innovación de la tecnología, seguramente se darán a conocer nuevas formas para poder crear sistemas de videovigilancia y otras aplicaciones importantes (por ejemplo, la robótica, la medicina, la gestión vehicular).

4.3 Sistemas Embebidos

Luchetti (2021) describe a un sistema embebido como aquel sistema de computación que está diseñado para realizar funciones específicas, cuyos componentes se encuentran integrados en una placa base. Estos sistemas generalmente están diseñados para proyectos que requieren de una computación en tiempo real, y para ello destacan tarjetas como Raspberry Pi o Arduino, que se usan comúnmente para el diseño y desarrollo de prototipos con sistemas embebidos, pero haciendo uso de entornos gráficos.

Algunos sistemas embebidos se ocupan de tareas relativamente simples, sin embargo, cada vez se utilizan para tareas más complejas; por ejemplo, ofrecer capacidades que van más allá de lo que un humano podría llevar a cabo. Muchas de las tareas que se desempeñan empleando sistemas embebidos están pensadas para suplantar a las personas en actividades cotidianas que se podrían automatizar o realizar a menor tiempo.

Para Baldwin (2022), un sistema embebido tiene tres componentes principales:

- Un sistema operativo que permite supervisar las aplicaciones, además de proveer los mecanismos para la ejecución de procesos.
- Un software primario o aplicación principal. Este software o aplicación lleva a cabo una tarea en específico, o en algunas ocasiones una serie de tareas.
- El Hardware que está constituido por los componentes físicos, estos componentes permiten realizar un conjunto de tareas al ejecutar programas.

4.3.1 Beneficios de los Sistemas Embebidos

Los sistemas embebidos se aplican en casi todos los ámbitos profesionales. Entre ellos está la industria de la automatización, sector militar, la salud, la seguridad, la electrónica, de defensa, las telecomunicaciones y también en la industria. A continuación, se pueden apreciar los beneficios más relevantes en cuanto a estos sistemas (Oasys, 2022).

- Conectividad y adaptabilidad: esto resulta ser muy útil para poder monitorizar diversas actividades.
- Reducción de costes: debido a que estos están conformados por módulos electrónicos, se facilita el mantenimiento y resulta económico poder el sustituir los componentes que están integrados en el sistema.
- Control total: estos sistemas permiten una personalización casi completa según sean las necesidades.
- Diseño modular: los dispositivos integrados son fáciles de transportar e instalar y se pueden desarmar y reorganizar fácilmente. Esto les permite integrarse en cualquier lugar y en cualquier otro sistema electrónico
- Accesibilidad: estos sistemas en los últimos años se han popularizado y cualquier persona puede conformar un sistema embebido para cualquier actividad o tarea que se desee. Algunas soluciones para sistemas embebidos como Arduino o Raspberry Pi permiten crear sistemas de control lumínico, sensores de apertura automática de puertas o incluso videoconsolas. Todo ello fácilmente y a costos extremadamente bajos.
- Corto tiempo de respuesta: suelen operar en tiempo real. Necesitan tomar medidas dentro de un plazo inmediato, por lo que su tiempo de respuesta es corto.

4.4 Fundamentos de una Imagen Digital

Quintana (2021) sostiene que “una imagen digital es una representación bidimensional de una imagen utilizando bits (unos y ceros). Dependiendo de si la resolución de la imagen es estática o dinámica puede tratarse de un gráfico rasterizado o de un gráfico vectorial”.

Una imagen rasterizada, también llamada imagen matricial o mapa de bits es una estructura de datos o un archivo que representa una cuadrícula rectangular de píxeles (si una imagen contiene más píxeles, tendrá mayor calidad, y viceversa.) o puntos de color, se los conoce como raster y pueden observar en un monitor de un computador, en una pantalla celular, en papel o en otro medio visuales. Las imágenes rasterizadas suelen caracterizarse por su altura y anchura (en píxeles) y también por su profundidad de color (en bits por píxel)

que determina la cantidad de colores distintos que se pueden almacenar en cada píxel, esto determina en gran medida la calidad de color de la imagen (Machuca, 2022).

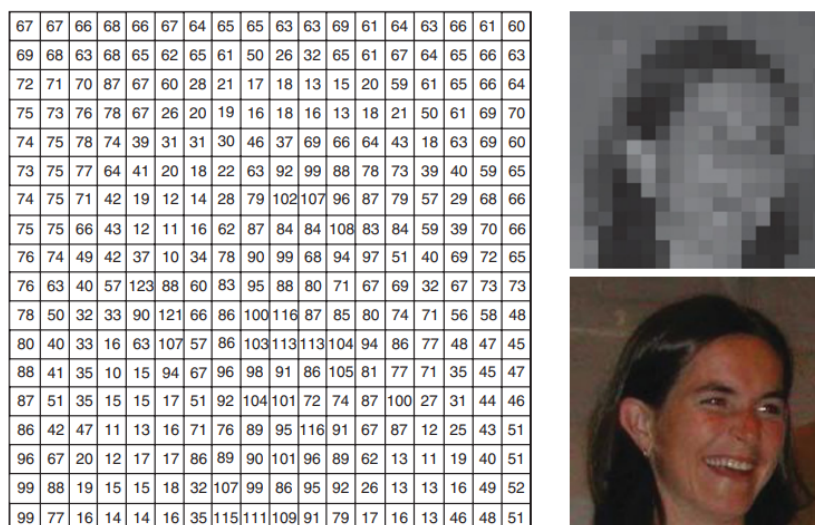
Las dimensiones de una imagen equivalen al tamaño de la cuadrícula, donde el ancho representa el número de columnas y la altura el número de filas. Por ende, el número de celdas de la cuadrícula es equivalente al ancho x el alto. Cada celda de la cuadrícula es un píxel de color. Para imágenes en escala de grises, un píxel es un número que representa la intensidad del tono gris. Si se usa un byte de datos para representar cada píxel, la escala de grises estará dentro del rango de 0 a 255 (Chung, 2017).

Una característica fundamental para poder trabajar con una imagen digital, es precisamente tener buena calidad en las imágenes; para el uso de imágenes en aplicaciones de visión artificial se debe asegurar que se puedan extraer las características necesarias. Uno de los factores que pueden contribuir en mejorar la calidad de las imágenes es la iluminación, si se toma en cuenta las consideraciones descritas seguramente los resultados sean mejores en cualquier aplicación que implique la visión por computador.

La Figura 8 representa tres versiones diferentes de la misma imagen; a la izquierda se presenta una matriz de números con 18 columnas y 18 filas, en la parte superior derecha se muestra una imagen de un rostro en escala de grises con baja resolución y en la parte inferior derecha se puede visualizar la misma imagen de un rostro con mayor resolución.

Figura 8.

Diferentes versiones de una imagen.



Nota. En la imagen se puede visualizar tres distintas representaciones de una imagen.

Fuente: Dawson-Howe (2014).

Para una imagen a color, un píxel es un grupo de números que representan la intensidad de los canales de color individuales. Las representaciones más comunes de una

imagen son: RGB (rojo, verde, azul), HSV (tono, saturación, brillo), escala de grises (puede tomar valores entre 0 y 255). Por ejemplo, un objeto que es totalmente de color azul estará representado por (0, 0, 255), o en notación hexadecimal sería # 0000FF.

En resumen, se utiliza la anchura y la altura para describir la dimensión de una imagen digital, el canal para describir el número de elementos de color en cada píxel y la profundidad para describir cuántos bits de datos representan cada color.

4.4.1 El Peso en una Imagen

En la investigación de López (2021) se menciona que:

Para calcular el peso (en bytes) de una imagen, es necesario contar el número de píxeles que contiene esa imagen, que equivale a calcular el número de celdas de la tabla, es decir, la altura de la tabla multiplicada por el ancho. Entonces el peso de la imagen equivale al número de píxeles multiplicado por la altura de cada uno de esos elementos.

A continuación, se indica un ejemplo de cómo calcular el peso de una imagen de color verdadero (24 bits) de 640 x 480.

- La cantidad de píxeles sería: $640 \times 480 = 307200$
- El peso de cada píxel es: $24 \text{ bits} / 8 = 3 \text{ bytes}$
- Entonces el peso de la imagen es igual a: $307200 \times 3 = 921600 \text{ bytes}$
- Finalmente, para calcular el tamaño en KB, basta con dividirlo por 1024: $921600 / 1024 = 900 \text{ KB}$

4.4.2 Frecuencia de Imagen (frame rate)

La frecuencia de imagen hace referencia al número de imágenes por segundo. Es la medida de la frecuencia a la que un reproductor de imágenes muestra diferentes fotogramas (frames). En informática estos fotogramas están constituidos por un número determinado de píxeles que se distribuyen a lo largo de una red de texturas. La frecuencia de los fotogramas es proporcional al número de píxeles que se han de generar y que inciden en el rendimiento del ordenador que los reproduce. La frecuencia de actualización de las imágenes oscila en el entorno digital entre los 15 y los 60 FPS (frames por segundo). Sin embargo, el rango entre 25 y 30 FPS es el más común (García, 2020).

Por ejemplo, si se necesita extraer datos y analizar objetos que se desplazan a grandes velocidades (autos, deportistas, aves, helicópteros, drones, etc.) se necesitaría un

sistema de captación de video con grandes capacidades, con una frecuencia de imagen muy alta, es decir, más fotogramas por segundo.

4.5 Visión por Computador

Según la investigación de Cicolani (2021) la visión por computador o visión artificial es un conjunto de algoritmos que permiten a un computador analizar una imagen y extraer información útil. Se utiliza en muchas aplicaciones, por muchas empresas y se está convirtiendo rápidamente en una parte de la vida cotidiana. Todo empieza con una imagen, el ordenador analiza una imagen para identificar líneas, esquinas y una amplia zona de color. Este proceso se denomina extracción de características y es el primer paso en prácticamente para todos los algoritmos de visión por ordenador. Una vez extraídas las características, el ordenador puede utilizar esta información para muchas tareas diferentes.

La detección de objetos en movimiento tiene una gran variedad de usos, ya sea para aplicaciones sencillas o para tareas más complejas. Por ello, es primordial hallar una técnica que pueda ser usada fácilmente en dispositivos de bajas características; para qué inclusive se pueda analizar vídeo en tiempo real, por lo general una aplicación habitual es el seguimiento del movimiento. Para detectar el movimiento el ordenador compara fotogramas individuales de una cámara fija. Si no hay movimiento, las características no cambiarán entre los fotogramas. Por tanto, si el ordenador identifica diferencias entre los fotogramas, lo más probable es que haya movimiento. El seguimiento del movimiento basado en la visión por ordenador es más fiable que los sensores IR, como el sensor PIR, pero si se combinan seguramente tendrán un resultado eficiente (Rath, 2021).

Si bien es cierto la visión humana es mejor para interpretar cualitativamente una escena compleja y desestructurada, la visión artificial sobresale en la medición cuantitativa de una escena estructurada debido a su velocidad, precisión y repetibilidad. El sistema de visión artificial gira en torno a la resolución correcta de la cámara y también a la óptica que le permite inspeccionar e identificar fácilmente detalles de un objeto (Cognex, 2016).

En la Tabla 1 se pueden observar ciertos objetivos estratégicos en relación con las aplicaciones de la visión artificial.

Tabla 1.

Relación entre objetivos estratégicos y aplicaciones de visión artificial.

Objetivo estratégico	Aplicaciones de visión artificial
Mayor productividad	Las tareas repetitivas que se hacían antes manualmente se realizan ahora con el sistema de visión artificial
Calidad superior	Inspección, medición, calibración y verificación de montaje
Flexibilidad de producción	Medición y calibración / Guiado de robots / Verificación previa a la operación
Menos tiempo de inactividad de las máquinas y reducción del tiempo de configuración	Cambios programados de antemano
Información más completa y control de procesos más estrictos	Las tareas manuales pueden ahora ofrecer retroalimentación de datos por ordenador
Reducción de gastos de bienes de capital	La adición de visión a una máquina mejora su rendimiento y evita la obsolescencia
Menos costes de producción	Un sistema de visión vs. muchas personas. Detección de tareas en una etapa temprana del proceso
Reducción de la tasa de deshechos	Inspección, medición y calibración
Espacio reducido	Sistema de visión vs. Operador
Control de inventarios	Reconocimiento óptico de caracteres e identificación

Fuente: (Cognex, 2016).

4.5.1 Etapas en un Proceso de Visión Artificial

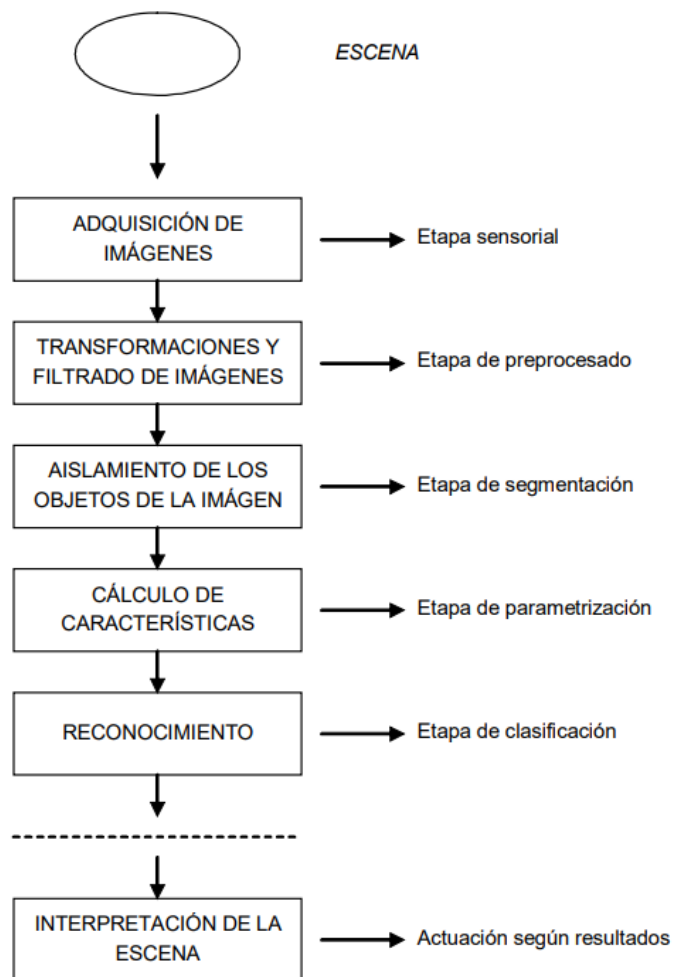
Para llevar a cabo alguna aplicación empleando visión artificial, es necesario seguir ciertos pasos que son fundamentales.

En investigaciones de González et al. (2006), el proceso de visión artificial implica el desarrollo de 5 etapas. Para el cumplimiento del debido proceso se da inicio con la adquisición de la imagen, una vez que la imagen ha sido obtenida, el siguiente paso consiste en el procesamiento de dicha imagen; el objetivo de este paso es mejorar la imagen para que se tengan mejores resultados en etapas siguientes. El paso siguiente es la segmentación, que tiene como objetivo dividir la imagen en las partes que la constituyen o los objetos que

conforman la imagen; la salida es una imagen de datos que contiene una frontera de la región o los puntos de ella, pero lo importante es especificar un método que pueda extraer los datos de interés. En la parametrización se extraen los rasgos que son básicos para poder diferenciar una clase de objetos de otra. Finalmente, se encuentra el reconocimiento y la interpretación; el reconocimiento es el proceso de designar una etiqueta a un objeto basada en la información que es proporcionada en la etapa de clasificación. Todo esto se ve representado en el diagrama de bloques de la Figura 9.

Figura 9.

Etapas de un sistema de visión artificial.



Nota. En la figura se muestra el diagrama de bloques de las fases de un sistema de visión artificial, nótese que existen dos fases que también intervienen que son; la escena y la actuación según los resultados, esta última es la que permitirá activar algún mecanismo de acción. **Fuente:** González et al. (2006).

4.5.2 Componentes de un Sistema de Visión Artificial

Varios autores coinciden en que los principales componentes que intervienen en la visión artificial son:

4.5.2.1 Iluminación

La iluminación es uno de los factores más relevantes de las aplicaciones de visión artificial. Si un objetivo no se ilumina adecuadamente, se puede perder información y productividad. Los sistemas de visión artificial producen imágenes al analizar la luz reflejada por un objeto, no al analizar el objeto en sí. Una de las técnicas de iluminación implica el posicionamiento de una fuente de luz con relación a la pieza y a la cámara. Si se aplica una cierta técnica de iluminación a una zona, esta puede mejorar una imagen, de manera que suprima algunas características y resalte otras. Algunas de las técnicas empleadas son:

- Retroiluminación
- Luz estructurada
- Iluminación difusa axial
- Iluminación de campo oscuro
- Iluminación de campo brillante
- Iluminación cenital difusa
- Iluminación estroboscópica (Cognex, 2020).

En definitiva, la iluminación es un parámetro elemental para la adquisición de las imágenes o videos, en un entorno controlado se obtendrán muy buenos resultados, pero no está demás tomar en cuenta la posición de la cámara, las características de la cámara y otros factores que pueden influir.

4.5.2.2 Lentes.

Todas y cada una de las aplicaciones de visión artificial implican la necesidad de recurrir a una lente que debe ser óptima para el sensor utilizado, principalmente por su tamaño y por el tamaño de los píxeles.

El lente debe adaptarse al sensor de imagen montado en el dispositivo. El componente transparente cuenta con lados curvos que se encargan de dispersar los rayos de luz. Se puede emplear de forma individual o se puede combinar con otras lentes. Lo que la convierte en especial es que se considera el componente de captación de luz del sistema de visión. Todas estas piezas son imprescindibles por igual para que el sistema de visión brinde la

máxima funcionalidad a todos sus usuarios. La omisión de uno de los componentes hace que todo el sistema carezca de eficacia (Bestell, 2019).

4.5.2.3 Sensor de Imagen.

De acuerdo a las investigaciones de Grupo bncvision (2021) la función del sensor en una cámara de visión artificial es convertir la luz captada por la óptica en una imagen digital (que será enviada al procesador para luego ser analizada). Los sensores generalmente usan un dispositivo de carga acoplada (CCD) o un semiconductor complementario de óxido metálico (CMOS) para convertir la luz (fotones) en señales eléctricas (electrones). Prácticamente, el trabajo del sensor de imagen es capturar la luz y convertirla en un ruido de imagen digital, sensibilidad y rango dinámico. La imagen es un grupo de píxeles. La luz baja origina píxeles oscuros, mientras que la luz brillante produce píxeles más brillantes.

Es fundamental asegurarse que la cámara tenga la resolución de sensor correcta para la aplicación en donde se vaya a emplear. Cuanto más elevada sea la resolución, más detalles tendrá la imagen y más exactas serán las lecturas. El tamaño de la pieza, las tolerancias de inspección y demás factores determinarán la resolución adecuada.

4.5.2.4 Procesamiento de Visión.

Desde el punto de vista de Viera (2017) el procesamiento digital de imágenes es el conjunto de prácticas que modifican imágenes digitales para mejorar la visibilidad de ciertas características de los objetos o formas presentes en la imagen, para su posterior análisis o simplemente para mejorar la visualización de la imagen. Es importante mencionar que el procesamiento no aumenta la información que se puede extraer de las imágenes, solo realiza ciertas características de la imagen. Para procesar la imagen efectivamente se debe considerar el proceso de formación y las características de interés de la imagen. Cuando se da la formación de la imagen digital, es común el ingreso de ruido o la degradación de la imagen, por ello se deben considerar técnicas para mejorar la imagen. Algunas de estas técnicas de mejora consisten en disminuir el ruido, mejorar el contraste de la imagen, ajustar el brillo, suavizar bordes, mejorar el enfoque, resaltar contornos, entre otras cosas.

Algunos algoritmos que frecuentemente se aplican a las imágenes son:

- Transformación a escala de grises
- Binarización por umbral
- Sustracción de fondo
- Filtro de Kalman para el seguimiento de objetos

- Diferencia de frames
- Los algoritmos de aprendizaje automático como Support Vector Machine (SVM), K-nearest neighbors (KNN), Naive Bayes, etc.
- Umbral adaptativo
- SIFT y SURF para extracción de puntos característicos
- Algoritmo de cambio medio para seguimiento rápido de objetos
- Algoritmo de Viola-Jones usado para la detección de objetos en tiempo real
- Algoritmo de Lucas-Kanade para el cálculo del flujo óptico
- Correlación y FFT
- Otras operaciones morfológicas como: erosión, dilatación, gradiente, apertura y cierre (Tutor de Programación, 2017).

4.5.2.5 Comunicaciones.

Dado que los sistemas de visión suelen utilizar diversos componentes comerciales, estos elementos deben coordinarse y conectarse rápida y fácilmente con los demás elementos de la máquina. Por lo general, la comunicación se realiza a través de una señal de E/S discreta o los datos se transmiten a través de una conexión en serie a un dispositivo que registra o usa la información. Los puntos discretos de E/S pueden conectarse a un controlador lógico programable (PLC), que utilizará esa información para controlar un indicador, como una lámpara, o directamente a un solenoide que podría utilizarse para activar un mecanismo de rechazo. La comunicación de datos a través de una conexión en serie puede ser una salida en serie, RS-232 convencional o Ethernet. Ciertos sistemas utilizan un protocolo industrial de nivel superior como Ethernet/IP, que puede conectarse a un dispositivo como un monitor u otra interfaz de operador específica de la aplicación para poder controlar y monitorizar convenientemente el proceso (Cognex, 2020).

4.5.3 OpenCV

OpenCV es una de las bibliotecas de visión artificial y aprendizaje automático más empleadas, y de código abierto, que comenzó como una iniciativa de investigación por parte de Intel en el año de 1999. La biblioteca está escrita en C y C++, fue diseñada para la eficiencia computacional y con un fuerte enfoque en las aplicaciones en tiempo real y funciona en Windows, Linux y Mac OS. Hay un desarrollo activo de interfaces para Python, Ruby, Matlab y otros lenguajes. Uno de los objetivos de OpenCV es facilitar una infraestructura de visión por ordenador fácil de usar que ayude a los usuarios a crear rápidamente aplicaciones de visión bastante avanzadas. La biblioteca contiene más de 2500 algoritmos optimizados que abarcan muchos ámbitos de la visión, como la inspección de productos en fábricas,

aprendizaje automático, la seguridad, las imágenes médicas, la calibración de cámaras, la interfaz de usuario, la visión estereoscópica y la robótica. Puesto que la visión por ordenador y el aprendizaje automático suelen ir de la mano (Bradski y Kaehler, 2008).

Entre las características más relevantes de la biblioteca de OpenCV resaltan las siguientes:

- Ofrece una facilidad para capturar y almacenar videos
- Crea reconocimiento de características
- En OpenCV se puede leer y escribir en las imágenes
- Facilita el procesamiento de imágenes como transformación, filtro, cambio de elemento, etc.
- Es una biblioteca que ofrece un enfoque para analizar el video, medir el movimiento del vídeo, identificar el fondo y reconocer los objetos (Ginni, 2021).

4.6 Raspberry Pi (RPI)

Actualmente, existen diversas alternativas en cuanto a hardware, con las que se pueden elaborar diversos proyectos tanto básicos como avanzados para aportar soluciones a la sociedad, mediante el uso de la tecnología. Entre las placas más populares están Arduino, Raspberry Pi y FPGA, en ellas se puede programar una serie de instrucciones con un lenguaje de programación determinado.

La Raspberry Pi fue desarrollada en Inglaterra por la Fundación Raspberry Pi, que es una organización sin fines de lucro con la intención de fomentar la enseñanza de la informática en las escuelas u otros sectores educativos. La iniciativa de crear este ordenador surgió en 2006, ya que buscaban desarrollar un ordenador de bajo presupuesto, pero con capacidades de programación. Es así que en 2011 salió el primer modelo de Raspberry Pi, producido en Inglaterra. A partir de ese año se siguieron desarrollando más placas con mejores características y capacidades, en la actualidad se encuentra en el mercado la más reciente, que es la Raspberry Pi 4 B de 8 GB de RAM.

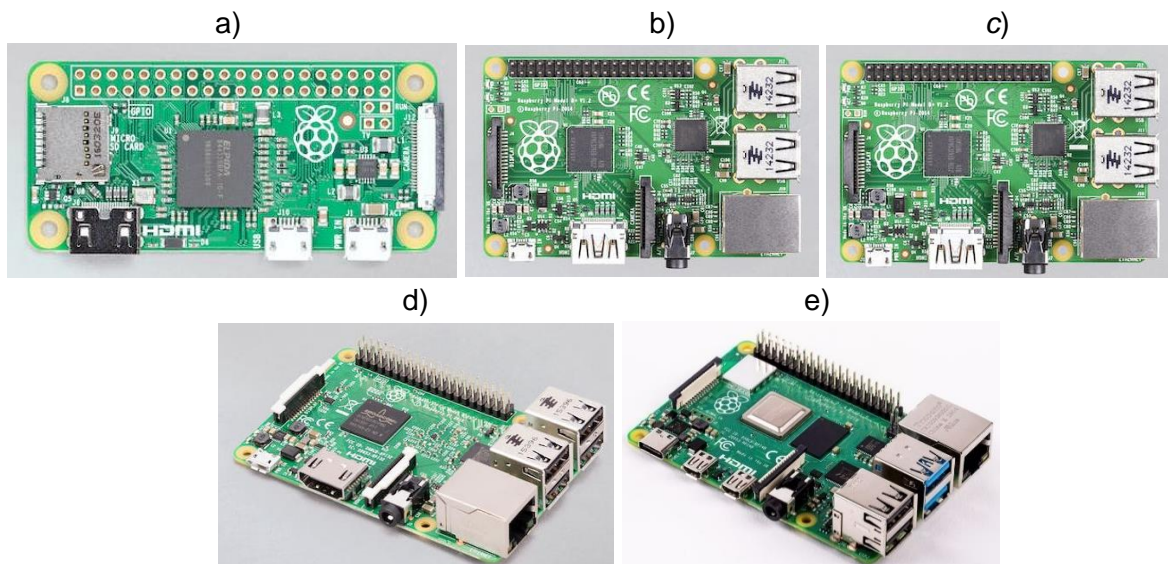
La RPI es un ordenador barato y compacto que puede estar conectado a un televisor o a un monitor de ordenador y que también puede utilizarse con un teclado y un ratón. Este ordenador opera con el sistema operativo Linux, permite a personas de todas las edades explorar la informática y el aprendizaje de lenguajes de programación como Scratch, Java, Python, HTML, etc. Es capaz de desarrollar la mayor parte de las tareas comunes de un ordenador de escritorio, como navegar por Internet, manipular documentos de oficina,

reproducir vídeos de alta resolución, aplicaciones de reconocimiento visual, para abrir puertas o ventanas, automatización, robótica, jugar, entre otras cosas (Raspberry Pi, 2021).

En las siguientes imágenes se puede observar algunos de los modelos de RPI con todos sus elementos y puertos.

Figura 10.

Diferentes modelos de Raspberry Pi (RPI)



Nota. a) Raspberry Pi Zero, b) Raspberry Pi 1 Modelo B+, c) Raspberry Pi 2 Modelo B, d) Raspberry Pi 3 Modelo B, e) Raspberry Pi 4. **Fuente:** Raspberry Pi (2019).

4.6.1 Partes Fundamentales de Raspberry Pi

Sus principales componentes se detallan a continuación:

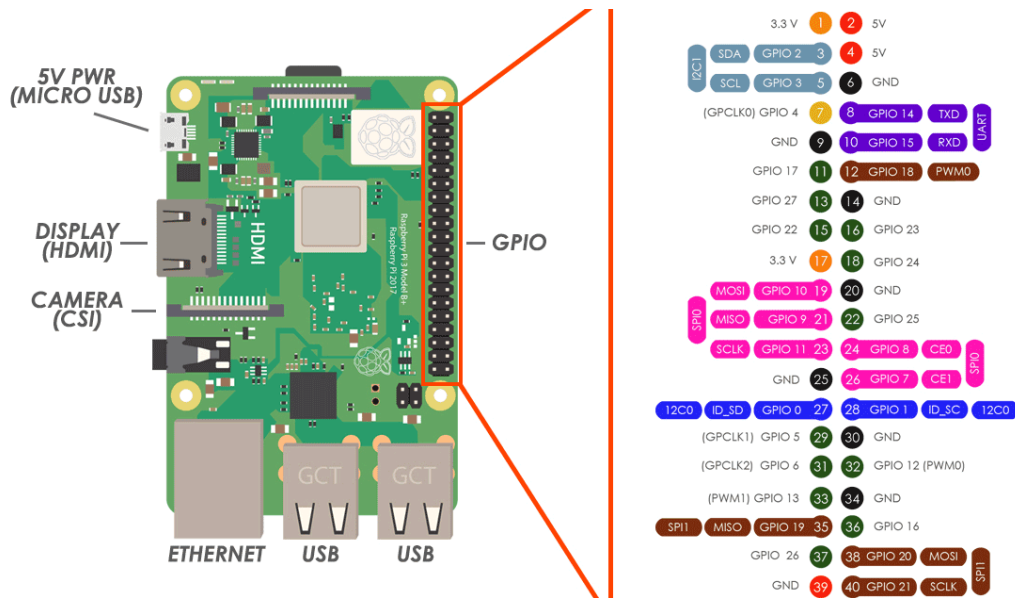
- Procesador
- Puerto Ethernet
- Memoria RAM
- 40 pines para GPIO
- 4 puertos para USB
- Salida de audio
- Puerto de video compuesto
- Puerto para HDMI o Micro HDMI
- Puerto de cámara CSI (Interfaz en Serie de Cámara)
- Puerto DSI para pantalla táctil Raspberry Pi
- Indicadores Led
- Puerto micro SD para cargar su sistema operativo y almacenar datos

- Puerto para alimentación micro USB

En la Figura 11 se muestra la ubicación de algunos de los componentes que se mencionaron en la lista anterior.

Figura 11.

Ubicación de los conectores y pines de una RPI.



Nota. Conectores y pines que contienen las placas Raspberry Pi (puede diferir según el modelo de la Raspberry). **Fuente:** YoungWonks (2020).

De acuerdo con Viera (2017) existen otros elementos que por lo general no vienen incluidos cuando se adquiere una Raspberry Pi, pero son fundamentales para que pueda funcionar de manera óptima. Entre estos elementos están:

- Fuente de alimentación
- Cable Ethernet
- Ventilador
- Disipadores de calor
- Monitor, teclado y ratón
- Cable HDMI-HDMI / Micro HDMI-HDMI (dependiendo el modelo de la Raspberry Pi)
- Lector de Tarjeta SD
- Tarjeta SD

4.6.2 Ventajas

Luchetti (2021), describe algunas de las ventajas del uso de Raspberry:

- Ordenador de pequeñas dimensiones
- Es económico
- Consume poca energía
- Capacidad para poder navegar a grandes velocidades
- Sencillo de utilizar
- Se le puede instalar un sistema operativo Open Source.

4.7 Aplicaciones Web

Hoy por hoy, las aplicaciones web son muy populares y su uso es de gran contribución en ámbitos académicos, científicos, políticos, culturales, empresariales, comerciales, entre otros, y esto es por las ventajas que el usuario final tiene. Una de las grandes ventajas es el poder acceder de manera remota desde cualquier parte del mundo con cualquier dispositivo (independientemente del sistema operativo) siempre y cuando se tenga una conexión a internet.

Las aplicaciones Web son una parte fundamental de la era digital y están diseñadas para ser utilizadas en línea a través de una conexión a Internet o Intranet mediante un navegador. En este sentido, las aplicaciones Web se han convertido en una herramienta ofimática muy versátil, que permite realizar tareas como la creación de documentos, hojas de cálculo, presentaciones, entre otras, sin necesidad de tener un software específico instalado en el dispositivo. Además, en muchos casos, se puede optar por usar el ordenador solo como un medio para procesar la aplicación en línea, lo que significa que los datos y la información se almacenan en la nube y se pueden acceder desde cualquier lugar y en cualquier momento con una conexión a Internet (Traverso et al., 2013).

Según Ramos A. y Ramos M. (2014) una aplicación web es una aplicación cliente/servidor: un ordenador solicita servicios (cliente) y otro está a la espera de recibir solicitudes y las responde (servidor). Los tres componentes que intervienen son; el cliente, el servidor y el protocolo de comunicación (como HTTP) estos están debidamente estandarizados.

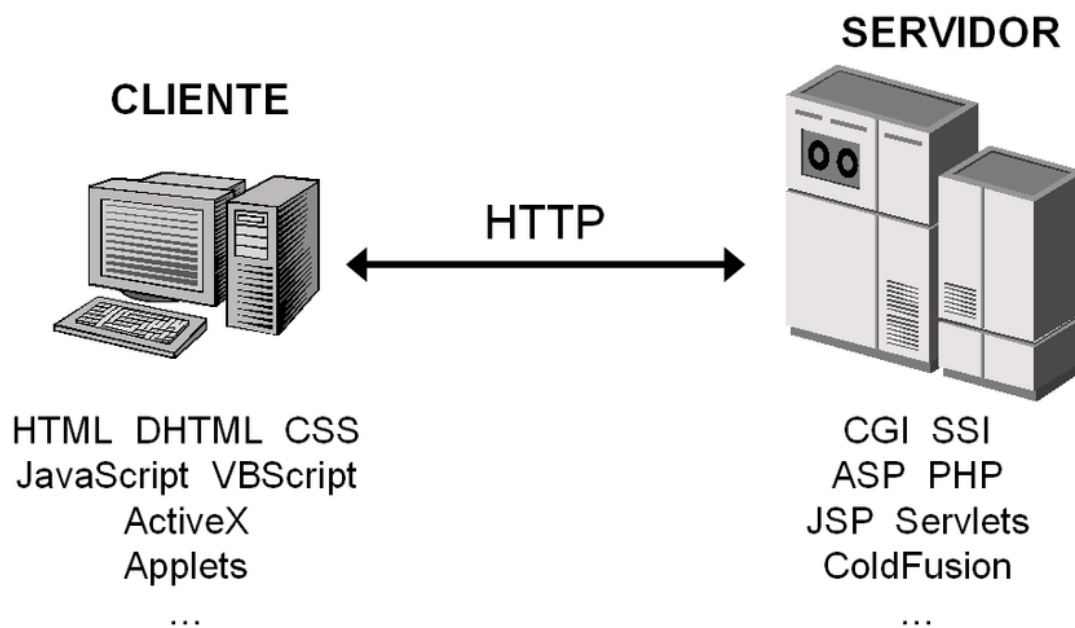
Existen dos términos muy comunes en el desarrollo de aplicaciones web, el "*front end*" y el "*back end*", en realidad son dos mundos diferentes pero que se complementan entre sí.

En el lado del cliente se emplea el término “*front end*” y se refiere a aquellos lenguajes que operan del lado del cliente para que sean interpretados por el navegador, entre ellos se encuentran: HTML, JavaScript, CSS, DHTML, VBScript, ActiveX, Applets, siendo los primeros tres lenguajes los que se emplean con mayor frecuencia en la actualidad, los demás ya han sido reemplazados por lenguajes que se adoptan a las necesidades actuales del desarrollo web.

Del lado del servidor se emplea el término de “*back end*” y se refiere a la programación del lado del servidor, en donde se pueden usar lenguajes como: PHP, Python, Java, CGI, SSI, Ruby, Node.js, Servlets, ColdFusion, ASP.NET. En la Figura 12 se muestra el modelo cliente/servidor con algunos de los lenguajes que se emplean en cada instancia.

Figura 12.

Tecnologías empleadas en el cliente y en el servidor web.



Fuente: Mora (2002).

En resumen, existe gran variedad de frameworks, arquitecturas, herramientas y lenguajes que son útiles a la hora de desarrollar sitios web, e incluso hay varias técnicas para la administración, la gestión de datos, la escalabilidad y la monitorización del sitio. Además, existen plataformas gratuitas o de pago para el alojamiento web que ofrecen servicios de alojamiento y gestión para sitios web, y herramientas muy útiles de monitorización para supervisar el rendimiento y garantizar la disponibilidad del sitio.

4.7.1 Los protocolos de Internet en el desarrollo web.

Los protocolos de Internet son conjuntos de normas para compartir datos, archivos o cualquier tipo de información entre dispositivos. Dentro de los protocolos más conocidos están los siguientes:

- Protocolo SSH: está enfocado en brindar una opción segura para acceder a un ordenador remoto por medio de un canal. Esto lo hace cifrando los datos de las diversas computadoras o dispositivos que se conectan a internet.
- Protocolo FTP: el protocolo de transferencia de archivos, es utilizado para transferir archivos mediante redes que se encuentran conectadas al protocolo de control de transmisión (TCP). Es así que el usuario puede conectarse a un servidor para descargar archivos, basado en la estructura cliente/servidor.
- Protocolo DNS: se trata de un sistema que asigna y asocia nombres de dominios a las diferentes direcciones IP. El DNS se encarga de identificar el nombre de una URL utilizada por un usuario, mediante su dirección IP.
- Protocolo TCP/IP: este está enfocado a la comunicación en redes. Se encarga de describir cómo la información debe ser transmitida y luego receptada de un equipo emisor a otro receptor. Esto con el objetivo de lograr una comunicación más simple, para la cual han sido necesarios varios procedimientos por separado por parte del software.
- Protocolo HTTP: se trata de las transmisiones de información o mensajes que se dan por las etiquetas HTML u otro lenguaje de marcado en la “WWW” o World Wide web.
- Protocolo HTTPS: es una versión segura de HTTP, la cual utiliza un certificado SSL/TLS para proteger la información transmitida.
- Protocolo SMTP: este protocolo se utiliza para enviar correos electrónicos (Olivares, 2021).

4.7.2 Arquitecturas web de contenido estático o dinámico

El contenido que se puede visualizar en una página web determinada o en un sitio web es contenido estático siempre y cuando el usuario no pueda interactuar de ninguna manera, por el contrario, una aplicación web que proporciona un contenido dinámico es aquella que invita al visitante a interactuar a través de diferentes elementos como botones, formularios, mapas, etc.

Según IngenieroVirtual (2018), existen cuatro diferentes tipos de arquitecturas web de contenido:

- Cliente estático y servidor estático: en este modelo el navegador hace una petición al servidor mediante el protocolo http, luego el servidor transforma la URL a ruta de disco y devuelve el fichero al navegador que lo dibuja o renderiza mostrando la estructura de la página en HTML y su contenido como archivos, fotos y vídeos, también la estética de su diseño gracias a los estilos CSS. En este caso no existe ningún tipo de interacción utilizando JavaScript, el servidor devuelve siempre los mismos recursos, así que desde este punto de vista la web es estática.
- Cliente estático y servidor dinámico: este modelo se compone de 3 capas, ya que intervienen por un lado el navegador y el servidor web, pero también una base de datos asociada a este último. Cuando el servidor recibe una petición, devuelve contenido del disco o ejecuta código para generar el recurso dinámicamente, este código normalmente realiza consultas a la base de datos para recuperar la información, generando la página HTML y contenidos de forma dinámica. Generalmente se emplea un sistema de gestión de bases de datos relacionales como Mysql.
- Cliente dinámico y servidor estático: El contenido está alojado en el disco duro del servidor de forma estática, pero el cliente es dinámico porque las páginas incluyen código JavaScript que se ejecuta en el navegador. Este código JavaScript puede realizar acciones y efectos gráficos, mostrar y ocultar información, desplegar elementos interactivos, adaptar los contenidos, etc.
- Cliente dinámico y servidor dinámico: Se combinan los conceptos de los dos casos anteriores, utilizando JavaScript para efectos gráficos y comportamientos interactivos, pero también para realizar peticiones en segundo plano (AJAX) y aplicaciones de página única con API REST. JavaScript se puede utilizar para no tener que recargar completamente la página al ingresar a un enlace, realizando peticiones al servidor web en segundo plano (ocultas al usuario). Cuando llega al navegador el resultado de la petición, el código JavaScript actualiza solo las partes necesarias de la página. A esta técnica se la conoce como AJAX (Asynchronous JavaScript And XML) y mejora mucho la experiencia de usuario ya que al realizar las peticiones el servidor puede devolver fragmentos de HTML generados dinámicamente, recursos estáticos en disco como PDF, imágenes, mostrar

errores, cambiar colores, información estructurada en XML o JSON, y realizar muchas más acciones.

4.7.3 Bases de datos

Una base de datos, puede ser definida, de manera simple, como:

El conjunto de datos relacionados que se encuentran agrupados o estructurados y almacenados con acceso directo a partir de un sistema de gestión de bases de datos, tipo de software muy específico para servir de interfaz entre la base de datos y el usuario (López, et al., 2017, p.144).

En otras palabras, las bases de datos son una colección de información y datos sistemáticamente estructurados y almacenados que se pueden buscar, acceder y modificar de una manera fácil.

Las bases de datos relacionales son las que comúnmente se emplean para el desarrollo de aplicaciones web. Dentro de esta clasificación existen bases de datos relacionales de software libre como Derby, SQLite, MySQL, Oracle, MariaDB, MS SQL Server, MongoDB, PostgreSQL o también existen bases de datos que son comerciales.

Actualmente, el sistema gestor de bases de datos de software libre que se usa con mayor frecuencia es MySQL, esto debido a que es multiplataforma y está desarrollado en C, consta de una herramienta interactiva para hacer consultas y crear bases de datos. En definitiva, por todas las imponentes ventajas que posee se ha hecho muy popular en el desarrollo web.

5. Metodología

En esta sección se detallan los materiales y métodos que se han empleado para poder ejecutar el presente Trabajo de Titulación, además de otros criterios que se han tomado en cuenta con el fin de que se pueda cumplir satisfactoriamente todas las actividades planificadas.

5.1 Área de Estudio

El presente proyecto se desarrolló en la Universidad Nacional de Loja, en la Facultad de Energía, las Industrias y los Recursos Naturales no Renovables, en la carrera de Ingeniería en Electrónica y Telecomunicaciones.

El prototipo se implementó en el Centro de Investigación, Innovación, Desarrollo de Prototipos Tecnológicos y Pruebas Electroenergéticas I2TEC de la Universidad Nacional de Loja. Este centro está ubicado en la facultad de Energía, las Industrias y los Recursos Naturales no Renovables, en el bloque 2, correspondiente a los laboratorios de la F.E.I.R.N.N.R., en el piso N° 3, mismo que se encuentra en las coordenadas:

LATITUD: 4° 01' 48.1"S

LONGITUD: 79° 11' 58.4"W

Figura 13.

Ubicación del centro I2EC



Fuente: Google Maps (2022).

Para diseñar, desarrollar e implementar el proyecto en el centro I2TEC de la UNL, se consideraron las necesidades existentes en dicho centro.

5.2 Materiales

El proyecto de diseño e implementación de un prototipo de sistema de seguridad requiere de los elementos que se muestran en la Tabla 2.

Tabla 2.

Lista de materiales mínimos para poder desarrollar el sistema de seguridad.

Materiales	Cantidad
Microordenador	1
Teclado	1
Mouse	1
Cámara	1
Modulo sensor de movimiento	1
Sirena	1
Tarjeta SD	1
Relé	1

Fuente: Elaboración propia.

De todos los materiales que se han enlistado, en donde se debe poner mayor énfasis es en el microordenador, en la cámara y en el módulo sensor de movimiento. Los demás materiales pueden ser de libre elección en cuanto a marcas o modelos.

5.2.1 Hardware

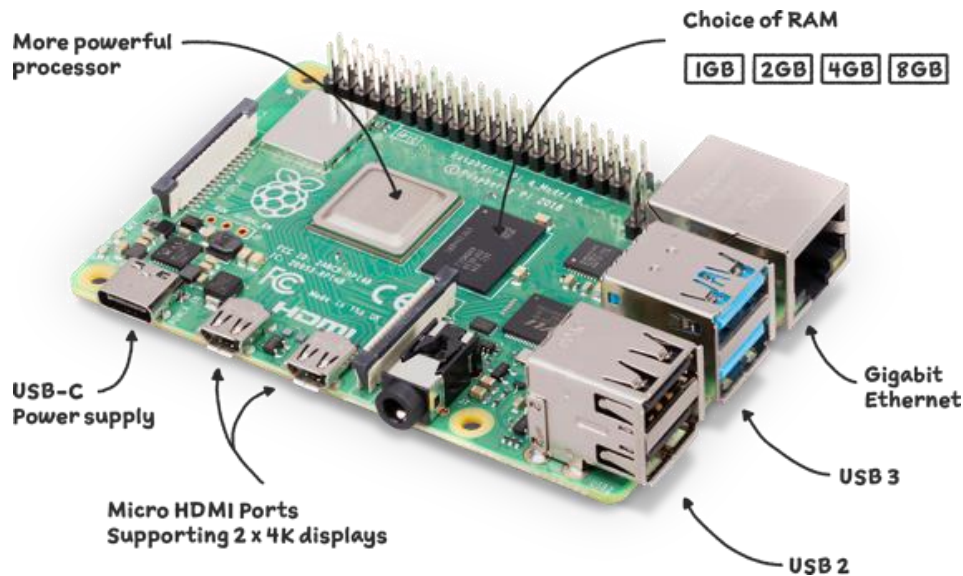
5.2.1.1 Microordenador.

El microordenador es el componente más importante en el desarrollo del prototipo, ya que debe estar en la capacidad de conectar diferentes dispositivos externos como; cámara, sensores, actuadores, pantallas y otros componentes electrónicos. Además, debe ser lo suficientemente capaz de ejecutar scripts de visión artificial.

La Raspberry Pi 4 modelo B (Figura 14), es el microordenador que se optó por utilizar.

Figura 14.

Raspberry Pi 4 Modelo B



Fuente: Raspberry Pi (2018).

Los criterios técnicos que influyeron en la elección de la Raspberry Pi 4 modelo B por sobre otros microordenadores o microcontroladores se pueden observar en el siguiente apartado denominado diseño (sección 5.5.2.1).

5.2.1.2 Cámara.

Este componente es esencial en sistemas de visión artificial, ya que proporciona la entrada de datos necesarios para el procesamiento y análisis. La calidad y características de la cámara son cruciales para el funcionamiento eficiente y preciso del sistema.

Una cámara de baja calidad puede producir imágenes con poca información, borrosas o con poco contraste, lo que dificulta el procesamiento y análisis de las imágenes, por otro lado, una cámara de alta calidad puede proporcionar imágenes nítidas y con un alto contraste, lo que facilita el procesamiento y análisis de las imágenes. Sin embargo, el precio de cámaras de alta calidad puede resultar significativamente más elevado que el de las cámaras de baja calidad.

La cámara que se seleccionó fue la cámara AVMP (Figura 15), cuyas características se dan a conocer en la sección de diseño.

Figura 15.

Cámara full HD AVMP.



Fuente: Joom (2023).

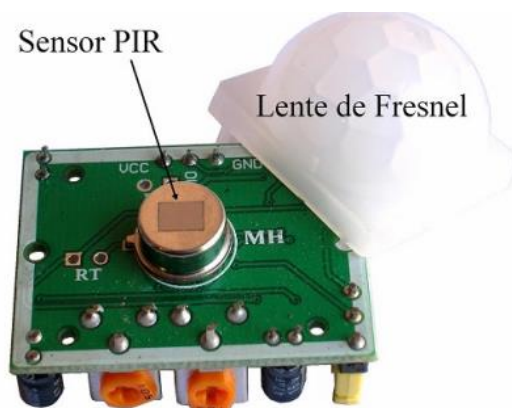
5.2.1.3 Módulo Sensor de Movimiento.

El módulo sensor de movimiento es un dispositivo que se emplea en muchos sistemas de seguridad, ya que detecta movimientos de calor emitidos por los seres vivos.

Se optó por elegir el sensor infrarrojo de movimiento PIR HC-SR501 (Figura 16). Este sensor está diseñado para detectar movimientos de seres humanos en un rango de detección de movimiento de hasta 7 metros (se puede ajustar según sean los requerimientos), lo que lo hace adecuado para proyectos de seguridad, automatización del hogar, y proyectos relacionados con la detección de presencia humana.

Figura 16.

Sensor PIR HC-SR501



Fuente: Punto Flotante (2017).

5.2.2 Software

5.2.2.1 Sistema Operativo del Microordenador.

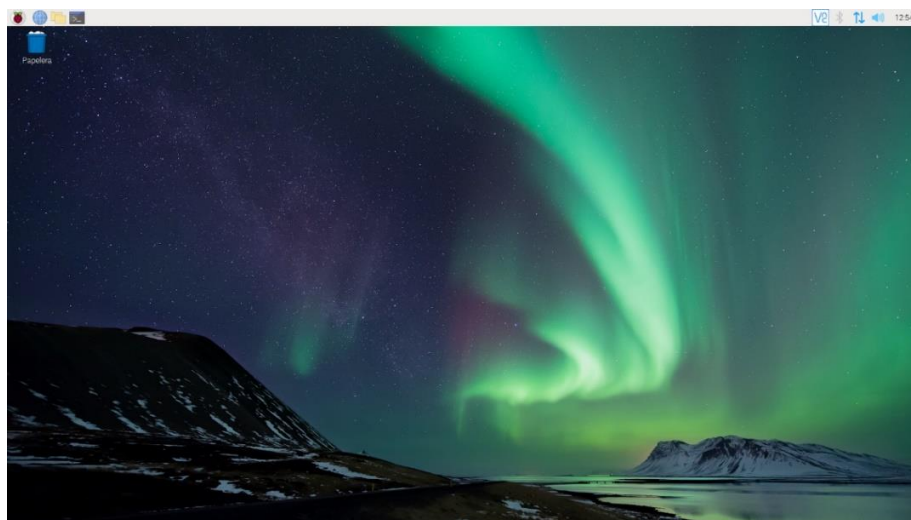
El sistema operativo es la parte esencial para que el microordenador pueda ejecutar instrucciones. El microordenador y el sistema operativo deben ser compatibles al 100% para que puedan trabajar conjuntamente.

El sistema operativo que se instaló en la Raspberry Pi 4 es Raspberry Pi OS Full (32-bit), ya que es completamente Open source, no comercial y totalmente gratuito para cualquier uso, esto quiere decir que los usuarios tienen la libertad de copiar, ejecutar, estudiar, distribuir, modificar y mejorar el software (Free Software Foundation, 2022).

La versión de escritorio (Figura 17) tiene un tamaño aproximado de 1.8 GB, cuenta con varias herramientas de programación. Además, mantiene una alta estabilidad del sistema, lo que permite que se trabaje de manera eficiente.

Figura 17.

Escritorio de Raspberry Pi OS Full



Fuente: Elaboración propia.

5.2.2.2 Lenguaje de Programación.

El lenguaje de programación por el que se optó es Python (Figura 18). Este lenguaje de alto nivel, es un lenguaje interpretado, cuenta con varios entornos de desarrollo integrado (IDLE), cuenta con alrededor de 137.000 bibliotecas para múltiples aplicaciones (sin contar las que se encuentran en desarrollo). Así mismo se utiliza con mucha frecuencia en el desarrollo de proyectos de gran complejidad, en aplicaciones web, machine learning, inteligencia artificial, robótica, desarrollo de juegos, etc.

Figura 18.

Python



Fuente: Python Software Foundation (2020).

En la investigación de García Monsálvez (2017) se destacan las principales características que se debería considerar para usar Python:

- Tiene sintaxis simple
- Es de alta legibilidad
- Abstracciones de más alto nivel
- Entorno amigable
- Lenguaje de propósito general
- Multi-paradigma
- Software libre
- Multiplataforma

5.2.2.3 Biblioteca de Visión Artificial.

Para iniciar con el tratamiento digital de imágenes y con visión artificial es necesario contar con una librería que proporcione la documentación suficiente para poder guiarse en ella.

La librería que se empleo es OpenCV (Figura 19), esta es la más utilizada por sus características, por la gran información que se puede encontrar en su página oficial o en los foros online, porque es completamente open source y de manera general porque es una herramienta muy potente que se encuentra disponible para trabajar en el lenguaje de programación Python.

Figura 19.

OpenCV



Fuente: OpenCV (2020).

5.2.2.4 Plataforma en la nube para lanzar un servidor

Una plataforma de administración en la nube contribuye en la optimización de los recursos, la administración de los servicios de la nube, la virtualización de los servidores, entre otras características esenciales.

Amazon Web Services (AWS) es uno de los proveedores de nube más populares del mundo y es utilizado por una amplia variedad de empresas y organizaciones, por ello y en virtud de la amplia gama de servicios en línea que proporciona para desarrollar, implementar y escalar servicios en línea o aplicaciones dentro de la capa gratuita se escogió AWS (Figura 20). Esta plataforma permite lanzar una instancia llamada EC2, misma que proporciona una combinación de recursos informáticos, memoria y red; opciones que son convenientes para aplicaciones web.

Figura 20.

AWS



Fuente: Amazon Web Services (2022).

5.2.2.5 Software necesario para crear la aplicación web

Se hizo uso de varias herramientas de desarrollo de software libre y de código abierto para poder alojar una aplicación web en un servidor en la nube, en donde se muestran la hora, fecha, imágenes de los posibles eventos inusuales suscitados dentro del centro I2TEC.

El sistema operativo para la máquina virtual es Ubuntu server 18.04. Además, se empleó un conjunto de software de código abierto y gratuito, que incluye Apache como servidor web, MySQL como sistema de gestión de bases de datos y PHPMyAdmin como herramienta de administración de bases de datos, los cuales en combinación permiten crear como producto final una aplicación web atractiva y funcional capaz de mostrar contenido dinámico.

Figura 21.

Conjunto de software libre para crear aplicaciones web.



Fuente: Hutomo (2022).

5.2.2.6 Lenguajes de programación y de estilo para la aplicación web

Se usó HTML para crear la estructura y el contenido de una página web. Este lenguaje es muy útil a la hora de definir los elementos de una página o aplicación web, como títulos, párrafos, enlaces, imágenes, formularios, entre otros.

Para que el contenido de la aplicación sea dinámico se empleó PHP, este es un lenguaje de programación del lado del servidor. Es muy popular en la creación de aplicaciones web y se utiliza para interactuar con bases de datos, para procesar formularios, realizar operaciones aritméticas y lógicas, entre otras cosas más. En el desarrollo de la aplicación web PHP permitió conectarse con la base de datos para validar las credenciales de acceso a

la página principal, así como también para invocar y mostrar el contenido de la base de datos de la fecha y hora de los sucesos.

El lenguaje de estilo que sirvió de nexa para definir el diseño de la aplicación web es CSS, este es una parte importante del desarrollo web, ya que es esencial para crear sitios web modernos, atractivos y permite definir el aspecto visual de una página web. Desde el tamaño y la posición de los elementos hasta el uso de fuentes y colores, en conjunto con lenguajes de programación como HTML y PHP, CSS permite la creación de sitios web y aplicaciones web interactivos y visualmente atractivos que brindan una excelente experiencia de usuario.

Figura 22.

Lenguajes para crear aplicaciones web.



Fuente: Web Monkey (2022).

5.2.2.7 Plataforma necesaria para el almacenamiento en la nube

En lugar de almacenar las imágenes en la memoria local de la Raspberry Pi, lo que limita su capacidad de almacenamiento, se seleccionó una solución de respaldo seguro y con un entorno gráfico. Para ello, se tomó en cuenta a uno de los servicios que ofrece Firebase (Figura 23), el cual se denomina Firebase storage como plataforma de almacenamiento en la nube.

El uso de esta plataforma permite acceder a las imágenes capturadas de los eventos suscitados desde cualquier lugar del mundo y desde cualquier dispositivo con conexión a Internet. De esta manera, se asegura la protección y accesibilidad de los archivos de imagen, sin importar la ubicación física.

Figura 23.

Plataforma para el almacenamiento en la nube: Firebase.



Fuente: Firebase (2021).

5.2.2.8 Proveedor de correo electrónico

Un proveedor de correo electrónico es un servicio que ofrece la capacidad de enviar, recibir y almacenar correos electrónicos a través de internet. Se usó Gmail debido a que ofrece una gran capacidad de almacenamiento y una potente organización de correos electrónicos. Además, cuenta con medidas de seguridad para proteger la cuenta del usuario.

Figura 24.

Proveedor de correo electrónico: Gmail.



Fuente: Gmail (2021).

5.2.2.9 Software para conexión remota al servidor en la nube y/o Raspberry

Para el acceso de manera remota se emplearon dos opciones que son muy útiles y que además están disponibles de manera gratuita para varios sistemas operativos. El software denominado PuTTY permitió conectarse de manera segura al servidor en la nube y a la Raspberry mediante el protocolo cifrado SSH, es importante mencionar que con PuTTY únicamente se podrá usar la terminal y ejecutar comandos desde ella.

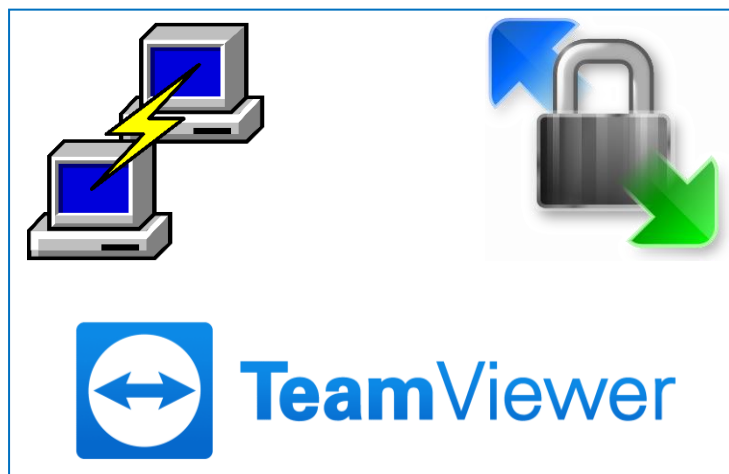
La transferencia de archivos se realizó con ayuda de WinSCP, que es una herramienta muy versátil para la transferencia de archivos que se utiliza comúnmente en entornos de red y servidores, sin embargo, también provee funcionalidades adicionales, como la capacidad de editar archivos remotos y la capacidad de ejecutar comandos remotos. A diferencia de PuTTY, WinSCP admite transferencias de archivos encriptadas a través de SSH y SFTP, lo

que lo hace más seguro para transferir archivos sensibles y tiene una interfaz gráfica de usuario amigable.

Por otro lado, para facilitar el soporte remoto, se utilizó TeamViewer, que tiene la posibilidad de usarlo de manera gratuita. Esto permitió conectarse a la Raspberry Pi de manera rápida, segura y sin importar su ubicación geográfica, para tener una mayor eficiencia y productividad.

Figura 25.

Software para conexión remota: PuTTY, WinSCP, TeamViewer.



Fuente: Elaboración propia.

5.3 Método

El proyecto de titulación es una investigación aplicada que puede ser usada de manera práctica para resolver una problemática real y de interés social, con ayuda de las bases teóricas necesarias. Debido a la naturaleza de la investigación aplicada, se usó el método científico.

Las principales características que se tomaron en cuenta del método científico son; la fiabilidad y la reproductividad, la primera característica se refiere a lo confiable que pueden ser los resultados obtenidos, sin embargo, con el tiempo pueden surgir otros prototipos con tecnología más reciente; entonces el presente prototipo puede quedar desactualizado. La segunda característica describe que el prototipo que se diseñó e implementó puede ser replicado por otra persona y se obtendrá el mismo resultado, de modo que se puedan llegar a conclusiones similares a las que se obtuvo en la presente investigación.

5.3.1 Técnica de recolección de datos

Se utilizaron dos técnicas principales de recolección de datos; la técnica del análisis de documentos y la encuesta.

Para el análisis de los documentos se llevó a cabo una revisión sistemática de los documentos, en la que se recopiló, evaluó y se sintetizó la información relevante para esta investigación y se desechó la información que se encontraba obsoleta o aquella que no aporta significativamente.

Por otro lado, se utilizó la técnica de la encuesta para poder recopilar información acerca del conocimiento que tienen las personas sobre; los actuales sistemas de seguridad, la contribución de la visión artificial en el desarrollo de sistemas de seguridades inteligentes, las preferencias de las personas que actualmente usan sistemas de seguridad y de aquellas que estarían dispuestas a usarlos, así como también la opinión de las personas en cuanto a los precios que estarían dispuestos a pagar por un sistema de seguridad inteligente que integra visión artificial. Se realizaron un total de 10 preguntas, en el Anexo 3 se adjuntan las preguntas que se aplicaron.

Se tomó una muestra de un total de 171 personas que habitan en el área urbana y rural del cantón Loja (el cálculo de la muestra se puede observar en la sección 6.2), la muestra para esta encuesta se seleccionó de manera totalmente aleatoria, considerando solo a las personas con edades de entre 25 y 59 años; que son las que probablemente utilizan o están pensando en utilizar sistemas de seguridad. La selección aleatoria de los participantes dentro de la población de interés, ayudó a garantizar que cada persona dentro del rango de edad tenga la misma probabilidad de ser incluida en la muestra y que los resultados obtenidos fueran representativos de la población en general.

5.3.2 Técnicas de análisis y procesamiento de la información

Se requirió de un enfoque metodológico cuantitativo para:

- Análisis de diferentes documentos técnicos para la elección del software y hardware.
- Análisis de la solución que permite la implementación del prototipo manteniendo la relación eficiencia-costo.
- Análisis de los resultados de las pruebas de funcionamiento del prototipo.

La técnica de tabulación de datos se empleó para resumir y agrupar los datos de la encuesta de manera sistemática en tablas y gráficos. A través de esta técnica, se organizaron los datos en una forma que permita la identificación de patrones y tendencias en los resultados de la encuesta. Esto permitió evaluar el conocimiento de las personas respecto a

los sistemas de seguridad que emplean tecnología moderna, la usabilidad y las preferencias del usuario para analizar el comportamiento del usuario.

5.4 Procedimiento

Para el cumplimiento de cada uno de los objetivos planteados que dieron como resultado final la implementación del prototipo, se realizaron diversas actividades, el procedimiento se detalla a continuación:

- Se dio inicio por una revisión bibliográfica, se recolectó aquellos aportes teóricos de distintos temas que son trascendentales para el desarrollo del prototipo. Para ello se tomaron en cuenta libros, informes técnicos, publicaciones en revistas científicas, tesis y también se consideró la búsqueda de información específica mediante sitios web o foros de ayuda. Además, se recogieron opiniones mediante la técnica de la encuesta.
- Para el dimensionamiento, del sistema de seguridad se identificó los requerimientos de seguridad en el centro I2TEC, se realizó una evaluación del centro para identificar los puntos vulnerables por los cuales podría haber una intrusión de personas no autorizadas y se determinó los componentes que se deberán usar.
- Para la selección de las herramientas de software y hardware se realizó un estudio y comparación de varios dispositivos electrónicos y softwares necesarios para desarrollar el prototipo. Se tomó mucho en cuenta el costo final del prototipo y si las herramientas seleccionadas eran de código abierto (open source) o no. También se evaluaron las herramientas para mostrar los datos en la aplicación web, enviar el reporte por correo electrónico y respaldar la información en la nube, para garantizar que todas las funcionalidades estén cubiertas de manera eficiente y eficaz.
- La construcción del prototipo requirió de aprender a programar en los diferentes lenguajes de programación que se emplean (PYTHON, HTML, PHP, CSS), de igual manera, se debió aprender a utilizar la plataforma de Amazon Web Services, Firebase, phpMyAdmin, Fritzling, GoGetSSL y los comandos del sistema operativo Linux.
- Para la implementación del prototipo se evaluaron diversas zonas del centro para comprobar el lugar en que se debía ubicar la cámara y el sensor, con el fin de que se cubran correctamente los puntos más vulnerables.
- En los manuales de uso y de mantenimiento se especifican sus características, especificaciones técnicas, funciones y usos. Posteriormente, se incluyeron las instrucciones de uso paso a paso, para garantizar el correcto manejo del prototipo. Además, se proporcionaron instrucciones detalladas sobre el mantenimiento para garantizar su correcto funcionamiento a lo largo del tiempo

5.5. Diseño

5.5.1 Dimensionamiento del sistema de seguridad

Se realizó una evaluación exhaustiva del lugar para identificar los puntos más vulnerables por los cuales podría haber una intrusión de personas no autorizadas. Durante esta evaluación, se revisaron cuidadosamente las características del entorno, la disposición de las puertas, ventanas, y se identificaron las posibles vías de acceso no autorizadas. También se analizó la ubicación de los sistemas de CCTV existentes cerca del centro I2TEC (ya que en la parte interna actualmente no existe ningún sistema de seguridad de este tipo).

Como resultado de esta evaluación, se identificaron los lugares específicos del centro que necesitan una mayor atención en cuanto a la seguridad y se propusieron medidas de seguridad adicionales para proteger el área contra las intrusiones no autorizadas, como por ejemplo, el uso de un sensor PIR para que el sistema ofrezca un grado mayor de confiabilidad, además del control de iluminación en horas de la noche.

Figura 26.

Identificación de los puntos más vulnerables.

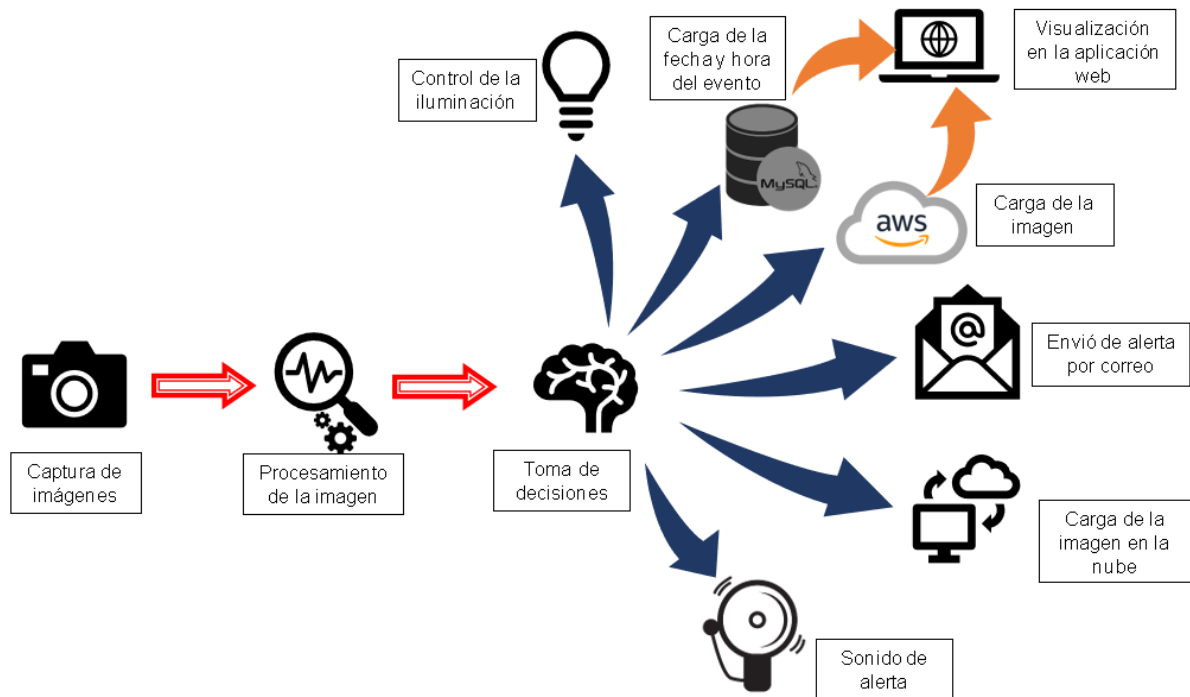


Fuente: Elaboración propia.

A partir de la identificación de los puntos vulnerables, se procedió a definir los requerimientos de seguridad que se deben cumplir para la detección de posibles intrusos y posteriormente la captura de la imagen y efectuar la transferencia de dicha imagen. En la Figura 27 se muestra un diagrama en el que intervienen cada una de las etapas que permiten el funcionamiento del sistema.

Figura 27.

Diagrama de funcionamiento del sistema.



Fuente: Elaboración propia.

En base al diagrama, se determinó que las herramientas de hardware y software necesarias para que el prototipo funcione correctamente son:

- Cámara
- Microordenador
- Modulo sensor de movimiento
- Sirena
- Relé
- Tarjeta SD
- Plataforma para el almacenamiento en la nube
- Plataforma para lanzar un servidor
- Plataforma de correo electrónico
- Entornos de programación
- Biblioteca de visión artificial
- Servidor web
- Sistema de administración de base de datos

Todos los elementos enlistados contribuyen para garantizar la eficacia del sistema de seguridad inteligente. Este se clasifica como un sistema de seguridad activo ya que, en caso de una intrusión, la alerta se emite de manera inmediata, a diferencia de CCTV que solo proporciona evidencias después de que el hecho haya sucedido. De esta manera, se logra reducir o, en el mejor de los casos, prevenir cualquier suceso no deseado dentro del centro I2TEC.

5.5.2 Elección del hardware

Aquí se describen los criterios que se tomaron en cuenta para optar por el respectivo hardware que permitió cumplir con cada uno de los objetivos planteados.

5.5.2.1 Microordenador

Al comparar varios de los microcontroladores o microordenadores más populares, los cuales son:

- Banana Pi
- PocketBeagle
- Arduino
- UDOO
- ASUS Tinker Board
- Libre Computer Board AML-S905X-CC (Le Potato)
- Orange Pi
- Raspberry Pi
- ODROID-XU4
- ROCK64
- ROCK Pi
- Nvidia Jetson nano

Se llegó a concluir que Raspberry Pi es la mejor opción, dado de que cuenta con puertos para periféricos, transferencia rápida de datos, conexión a internet por Wi-Fi o Ethernet, pines para la conexión de cámara, 40 pines GPIO para incluir sensores u otros dispositivos, sistema operativo optimizado, versiones con diferentes tamaños de memoria RAM, facilidad de adquisición, la información disponible es abundante, y además cualquier duda se puede consultar en las comunidades disponibles de manera online. Otras características que resaltan son las siguientes:

- El hardware de Raspberry Pi es de código abierto, lo que significa que el diseño y la documentación técnica están disponibles públicamente en su página oficial para que cualquiera los revise, modifique y distribuya.
- Versatilidad: la Raspberry Pi 4 puede ser utilizada para una variedad de proyectos, incluyendo el emulador de consolas, desarrollo de juegos, programación de sensores, media center, sistemas de seguridad, servidor web, y más.
- Fácil de usar: Raspberry Pi 4 puede operar con algunas distribuciones de Linux, el sistema operativo que se usa con mayor frecuencia es el Raspbian, el cual contiene una gran variedad de herramientas de programación y desarrollo disponibles.
- Tamaño compacto.
- Bajo costo.

A pesar de que en el mercado existen microcomputadores que tienen características muy similares o superiores a la Raspberry Pi (como es el caso de Nvidia Jetson nano), estos tienen un costo más elevado que la opción que se eligió, lo cual no contribuye a mantener la relación calidad-precio del prototipo. Es por ello que se eligió la Raspberry Pi 4 (Figura 14) de 2 GB de memoria RAM y con una tarjeta micro SD de 32 GB, con la finalidad de poder cumplir con los objetivos propuestos.

Para la selección de la Raspberry Pi 4 modelo B, se analizaron varios factores de cuatro versiones distintas de esta placa, cuyas características se muestran en la Tabla 3, todos estos dispositivos que se comparan son del modelo B. Se eligió el modelo B sobre todo por las características de la CPU.

Tabla 3.*Comparación entre diferentes versiones de RPi.*

Modelo	RPI 2B	RPI 3B	RPI 3B +	RPI 4B
Tipo de SOC	Broadcom BCM2836	Broadcom BCM2837	Broadcom BCM2837B0	Broadcom BCM2711
Reloj de la CPU	4xArm Cortex- A7, 900 MHz	4 xArm Cortex- A53, 1.2 GHz	4 xArm Cortex-A53, 1.4 GHz	4 xArm Cortex- A72, 1.5 GHz
RAM	1 GB	1 GB	1 GB	1 GB/2 GB/4 GB
GPU	Broadcom VideoCore IV	Broadcom VideoCore IV	Broadcom VideoCore IV	Broadcom VideoCore VI
Ethernet	100 Mbit/s base Ethernet	100 Mbit/s base Ethernet	Gigabit Ethernet (max. 300 Mbps)	Gigabit Ethernet (no limit)
Puertos USB	4	4	4	4 (2 xUSB 3.0 + 2 xUSB 2.0)
Power over Ethernet	No	No	Sí (requiere un HAT PoE)	Sí (requiere un HAT PoE)
WiFi	No	WiFi 802.11n	WiFi 802.11ac doble banda	WiFi 802.11ac doble banda
Bluetooth	No	4.1	4.2	5.0
Salida de vídeo	HDMI/3.5 mm Comp./DSI	HDMI/3.5 mm Comp./DSI	HDMI/3.5 mm Comp./DSI	micro-HDMI/3.5 mm Comp./DSI
Entrada de cámara	15 Pin CSI	15 Pin CSI	15 Pin CSI	15 Pin CSI
Pines GPIO	40	40	40	40
Memoria	MicroSD	MicroSD	MicroSD	MicroSD

Fuente: (Lemus et al., 2019)

El contar con un teclado USB y un mouse USB de cualquier modelo o marca es fundamental para trabajar con mayor facilidad (útiles únicamente para el proceso de desarrollo). Además, es recomendable usar una tarjeta microSD de clase 10 o superior, de al menos 16 GB de almacenamiento, ya que en ella se cargará el sistema operativo, y será el lugar donde se guardarán los scripts y otros archivos que se generen en la RPi.

5.5.2.2 Cámara

Para la elección de la cámara se analizaron características como: tamaño, resolución fija, modos de vídeo, tipo de sensor, resolución de sensores, campo de visión, precio, compatibilidad con la RPi, entre otras. Las marcas y modelos que se tomaron en cuenta para la comparación son: Tp-link Tapo C100, Cámara AVMP FULL HD, Nexxt AHIMPF14U2, EC80-

V13, Yamla 1080p, Strom Loki Ac01, Ezviz C8c Lite P/N EZC8C1F24, Insta360 Link, EMEET S600, EMEET C990, Spedal FF931, y los módulos RaspiCam.

Luego de analizar las características de las diferentes opciones de cámaras, se determinó analizar detalladamente la cámara AVMP y el módulo de cámara v2.

Tabla 4.

Comparación entre cámara AVMP y el módulo de cámara RaspiCam V2.

Parámetro	Cámara AVMP	Módulo de cámara v2
Tamaño	76 x 48 x 56 mm	25 x 24 x 9 mm
Peso	8g	3g
Resolución fija	8 megapíxeles	8 megapíxeles
Modos de vídeo	MP4/AVI	1080p47, 1640 x 1232p41 y 640 x 480p206
Sensor	CMOS/GC4653	Sony IMX219
Resolución de sensores	3840x2160 píxeles	3280 x 2464 píxeles
Área de imagen del sensor	2.40 x 2.40 mm	3.68 x 2.76 mm (4.60 mm en diagonal)
Tamaño óptico	1/3"	1/4"
Campo de visión horizontal	86.00 grados	62.20 grados
Campo de visión vertical	56.00 grados	48.80 grados
Velocidad de cuadro	30FPS/25FPS/10FPS	30FPS
Formato de foto	BMP, JPG, PNG	JEPG, RAW

Fuente: Elaboración propia.

Las características más importantes por las cuales se eligió la cámara AVMP es por el tipo de sensor, por el campo de visión horizontal, vertical y por su resolución ya que cuenta con resolución UHD 3840 * 2160 de ultra alta definición y vídeo de alta definición a 30 FPS, que brinda imágenes de alta calidad y vídeos fluidos. Además, el balance de blancos automático y la corrección de exposición automática combinados con la luz integrada pueden ajustar la imagen para producir la mejor imagen posible incluso en áreas con poca luz o con poca luz de fondo

5.5.2.3 Módulo Sensor de Movimiento

Las características por las cuales se eligió al sensor de movimiento, son las siguientes:

- Incorpora la tecnología más reciente en sensores de movimiento, el controlador es el BISS0001.
- Ajuste de parámetros: cuenta con dos potenciómetros, con los cuales el usuario puede modificar o regular la distancia de detección y la sensibilidad del PIR.
- Salida de alarma de movimiento con ajuste de tiempo entre 3 segundos a 5 minutos.
- Tiempo de salida inactiva: cada vez que la salida pase de activa a inactiva, permanecerá en ese estado los siguientes 3s. Cualquier evento que ocurra durante ese lapso es ignorado.
- Rango de distancia de 3 a 7 metros ajustable, y con aperturas de 90° a 110°.
- La instalación del PIR puede realizarse según convenga la aplicación.
- Consumo promedio: menor a 1mA.
- Voltaje de alimentación: de 5 a 12 VDC.
- Temperatura de operación: entre -15° a +70° C.
- Dimensiones: (3.2 x 2.4 x 1.8) cm.
- Tiempo de inicialización: después de alimentar el módulo HC-SR05, debe transcurrir 1 minuto antes de que inicie su operación normal (Punto Flotante, 2017).

5.5.3 Elección del software

5.5.3.1 Sistema operativo del microordenador

Se debe prestar la atención necesaria para elegir la mejor opción entre la multitud de sistemas operativos que se pudiesen instalar y ejecutar en la Raspberry Pi. La elección está directamente relacionada con los requerimientos, características y aplicaciones que se desean utilizar.

Los sistemas operativos que se podrían instalar en la Raspberry para el desarrollo del prototipo son los siguientes:

- Raspberry Pi OS (32-bit): es la versión estándar y oficial del sistema operativo Raspbian, diseñada para funcionar en procesadores de 32 bits. Viene con una variedad de herramientas y programas preinstalados, incluido el entorno de escritorio de GNOME.

- Raspberry Pi OS (64-bit): es una versión reciente del sistema operativo Raspbian diseñada para funcionar en procesadores de 64 bits, es recomendada para aquellos que buscan un rendimiento mejorado y mayor capacidad de manejo de memoria.
- Raspberry Pi OS Lite (32-bit): es una versión liviana del sistema operativo oficial de Raspberry Pi, no incluye un entorno de escritorio, está diseñado para usarse en servidores sin cabeza o para situaciones en las que no se necesita la interfaz gráfica.
- Raspberry Pi OS Full (32-bit): es una versión completa que incluye la interfaz gráfica y todo el software incluido en Raspberry Pi OS Lite, esta versión está destinada a usuarios que desean usar Raspberry Pi para uso regular de escritorio.
- Raspberry Pi OS Lite (64-bit): es una versión del sistema operativo oficial de Raspberry Pi, no incluye un entorno de escritorio y es compatible con procesador de 64 bits.
- Ubuntu: es un sistema operativo gratuito y de código abierto basado en Linux. No está desarrollado oficialmente para Raspberry Pi, pero se puede instalar en el dispositivo a través de un proceso llamado "instalación portátil". Ubuntu es ampliamente utilizado en servidores, computadoras de escritorio y portátiles.
- Manjaro ARM Linux: es una distribución de Linux desarrollada de forma independiente que se basa en Arch Linux y está específicamente optimizada para procesadores ARM, no está desarrollada oficialmente por la Fundación Raspberry Pi, pero se puede instalar en el dispositivo.
- Apertis: es un sistema operativo de código abierto desarrollado por la fundación Linux y se utiliza en dispositivos integrados y dispositivos de Internet de las cosas (IoT). No está desarrollado oficialmente para Raspberry Pi y está destinado a ser utilizado en los dispositivos integrados.

En resumen, Raspberry Pi OS (32-bit) y Raspberry Pi OS Lite (32-bit) son las versiones más recientes y estables del sistema operativo Raspbian, con las que se podría trabajar dependiendo de la versión de la Raspberry que se use. En ese contexto, cómo se está optando por la versión del microordenador más reciente, se podría usar cualquiera de las dos versiones.

5.5.3.2 Biblioteca de Visión Artificial.

Algunas de las bibliotecas más populares que están disponibles en el lenguaje de programación de Python son:

- SimpleCv
- OpenCV
- TensorFlow
- Scikit-image
- Keras
- Dlib
- PyTorch

Una de las razones por las que se seleccionó a OpenCV es debido a que es una biblioteca de código abierto, lo que significa que es gratuita y está disponible para cualquier persona que desee utilizarla o modificarla, otra razón es debido a que proporciona una gran cantidad de funciones para el procesamiento de imágenes y videos, como el filtrado, la transformación, el seguimiento de objetos y la detección de rostros. Así como también, cuenta con una amplia documentación y con una comunidad activa que está lista para poder contestar preguntas o compartir conocimiento.

Finalmente, la selección de una biblioteca de Python dependerá del uso específico que se le dará, pero OpenCV es una elección muy común debido a su amplia gama de funciones y porque es una biblioteca multiplataforma, lo que significa que puede ser utilizada en diferentes sistemas operativos.

En la Tabla 5 se muestra la tabla comparativa entre las diferentes bibliotecas de visión artificial, en donde se describen parámetros como: los lenguajes compatibles principales que se emplean en cada biblioteca, la cantidad/calidad de la documentación disponible en línea, si la biblioteca sigue en desarrollo o recibe actualizaciones y el nivel de complejidad que presenta cada biblioteca para aprenderla y utilizarla.

Tabla 5.*Comparación entre diferentes herramientas de visión artificial.*

Herramienta de visión artificial	Lenguajes principales	Documentación	Desarrollo activo	Nivel de complejidad
SimpleCV	Python	Limitada	No activo	Bajo
OpenCV	C++, Python, Java	Amplia	Activo	Moderado
TensorFlow	Python	Amplia	Activo	Alto
Scikit-image	Python	Amplia	Activo	Moderado
Keras	Python	Amplia	Activo	Bajo
Dlib	C++, Python	Amplia	Activo	Alto
PyTorch	Python	Amplia	Activo	Moderado

Fuente: Elaboración propia.

5.5.3.3 Lenguaje de Programación

De los diferentes lenguajes de programación que se emplean con mayor frecuencia en el campo de la visión artificial destacan los siguientes:

- Java
- Matlab
- Python
- C++

Luego de comparar los lenguajes enlistados (Tabla 6), se seleccionó a Python por su amplia variedad de bibliotecas y frameworks como, TensorFlow, OpenCV y PyTorch. Además, es el lenguaje de programación más utilizado en el campo de la visión artificial debido a su gran comunidad y la disponibilidad de una amplia variedad de bibliotecas y frameworks.

Python es fácil de aprender, ya que tiene una sintaxis clara y sencilla, se puede integrar fácilmente con otros lenguajes, lo que permite desarrollar proyectos más robustos y con varias funcionalidades. Finalmente, existe gran cantidad de documentación disponible de manera online.

Tabla 6.

Comparación entre diferentes lenguajes de programación.

Lenguaje	Área de aplicación	Tipo de lenguaje	Nivel de complejidad	Documentación	Comunidad
Java	Desarrollo de software, aplicaciones empresariales	Compilado	Alto	Amplia	Activa
MATLAB	Procesamiento de señales, cálculo numérico	Interactivo	Moderado	Amplia	Activa
Python	Ciencia de datos, aprendizaje automático, desarrollo web, etc.	Interactivo, interpretado	Bajo a moderado	Amplia	Activa
C++	Desarrollo de software, sistemas operativos, juegos	Compilado	Alto	Amplia	Activa

Fuente: Stuart McGarrity (2023).

5.5.3.4 Plataforma en la nube para lanzar un servidor

Al comparar algunas de las plataformas más populares como:

- Microsoft Azure
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Heroku

Se llegó a determinar que Amazon Web Services es la mejor opción, dado que ofrece una gran cantidad de servicios, que incluyen almacenamiento, máquinas virtuales, bases de datos, análisis, redes, seguridad, aprendizaje automático y mucho más. Esto permite que los usuarios puedan construir soluciones completas en la nube sin tener que preocuparse por la integración de diferentes proveedores o servicios. Cada una de estas características pueden ser beneficiosas para el uso personal pero también para empresas de todos los tamaños.

La plataforma de AWS es altamente escalable, flexible, segura, tiene buena relación de costo-efectividad y cuenta con una amplia comunidad de usuarios y documentación en línea. Estos factores hacen que AWS sea una buena opción para desplegar un servicio que se encuentre alojado en la nube.

Para la selección AWS como plataforma para desplegar una instancia EC2, se analizaron varios factores de cinco diferentes plataformas que ofrecen servicios similares. A continuación, en la Tabla 5 se muestran las características más relevantes que se tomaron en cuenta.

Tabla 7.

Comparación entre diferentes plataformas.

Servicio	Microsoft Azure	Amazon Web Services	Google Cloud Platform	Heroku
Máquina virtual	Máquina virtual de Azure	EC2 (cómputo elástico)	Motor de cómputo de Google	Heroku Private Spaces
PaaS	Servicio de aplicaciones	Beanstalk elástico de AWS	Motor de aplicaciones de Google	Servicio de Heroku
Contenedor	Servicio Azure Kubernetes	Servicio AWS Elastic Container/Kubernetes	Motor Kubernetes de Google	Dynos
Funciones sin servidor	Azure Function	AWS Lambda	Funciones de la nube de Google	Heroku Functions
Número de servicios	Más de 200	Más de 200	Más de 100	Aproximadamente 24
Nivel gratuito	12 meses, junto con un crédito de \$200	12 meses	Crédito de \$300 durante 12 meses	No
Documentación	Amplia	Amplia	Amplia	Básica
Soporte al Cliente	Si	Si	Si	Si
Relación con código abierto	No tiene una relación tan buena con la comunidad de código abierto	Es amigable con el modelo de código abierto	Ofrece servicios administrados de código abierto	Buena relación con el código abierto.
Adopción mundial en 2022	21%	34%	11%	3%

Fuente: Wickramasinghe (2021).

5.5.3.5 Software necesario para crear la aplicación web.

La creación de la aplicación web requiere de varias herramientas para el servidor web, para la gestión y administración de bases de datos.

Para el servidor web se tomaron en cuenta a:

- Nginx
- Apache
- LiteSpeed
- Lighttpd

Al evaluar cada uno de estos servidores se llegó a determinar que el mejor software para implementar un servidor web es sin duda Apache. Es el paquete de software libre que se emplea en un gran porcentaje de servidores GNU/Linux. Una de las características más importantes de Apache es la flexibilidad y escalabilidad. Además, es compatible con la amplia gama de tecnologías y lenguajes de programación. Finalmente, pero no menos importante es la seguridad, Apache cuenta con una buena reputación en cuanto a seguridad ya que ha demostrado ser resistente a varios tipos de ataques que existen.

A pesar de las grandes ventajas que nos ofrece apache, es importante mencionar que los otros servidores web enlistados también tienen sus ventajas y desventajas, y pueden ser una mejor opción en ciertos casos, por ejemplo, Nginx es conocido por su alta eficiencia en el manejo de conexiones concurrentes y LiteSpeed es conocido por su alta velocidad y capacidad de procesamiento de solicitudes. Por lo tanto, se debe evaluar cuidadosamente las necesidades y los recursos informáticos o económicos disponibles.

Para crear la base de datos que contiene usuario, contraseña y eventos suscitados, se consideraron a las siguientes herramientas:

- Oracle
- PostgreSQL
- MariaDB
- HeidiSQL
- MySQL

Oracle es de propósito general y bastante escalable que se utiliza principalmente en empresas y organizaciones que generan grandes volúmenes de datos y necesitan alta

escalabilidad, disponibilidad y seguridad. La desventaja es que es un software de pago y de código cerrado, pero ofrece una amplia gama de funcionalidades.

PostgreSQL es de código abierto y gratuito que se enfoca en ofrecer características avanzadas de SQL, es ampliamente utilizado en entornos empresariales y de investigación. Es ampliamente utilizado en entornos de investigación y empresariales.

MariaDB es de código abierto y gratuito, es una bifurcación de MySQL que fue creado para ser una alternativa más abierta y comunitaria de MySQL, tiene características adicionales, como almacenamiento en caché de columna, almacenamiento de datos en la nube y soporte mejorado para clústeres.

HeidiSQL es una herramienta de software libre y gratuito que se utiliza para conectarse y administrar servidores de bases de datos MySQL, Microsoft SQL Server, MariaDB y PostgreSQL, que además ofrece una interfaz de usuario intuitiva y fácil de usar.

MySQL es un software de código abierto y gratuito que se utiliza en una amplia variedad de aplicaciones, desde sitios web hasta aplicaciones empresariales. Es popular por su rendimiento, escalabilidad y flexibilidad. MySQL tiene características como soporte de transacciones de Atomicidad, Consistencia, Aislamiento y Durabilidad (ACID), claves foráneas, vistas, índices avanzados y procedimientos almacenados. Por estas razones, por la seguridad, por la facilidad de administración de manera remota a través de phpmyadmin y además por la integración con lenguajes de programación como PHP, C++, Java, Python; se eligió a MySQL.

5.5.3.6 Lenguajes de programación y de estilo para la aplicación web.

Para la aplicación web se compararon los siguientes lenguajes:

- HTML
- XHTML
- Markdown

En la Tabla 8 se presentan las principales características de cada uno de los lenguajes mencionados.

Tabla 8.*Comparación entre lenguaje.*

Característica	HTML	XHTML	Markdown
Sintaxis	Basado en HTML, con una estructura menos estricta	Basado en XML, con una estructura más estricta	Más sencillo y fácil de leer que HTML y XHTML
Facilidad de programación	Requiere conocimiento medio de programación	Requiere un conocimiento profundo de las reglas y sintaxis de XML	Fácil de aprender y escribir, no requiere conocimientos de programación
Uso	Ampliamente utilizado para crear páginas web	Menos utilizado que HTML	Muy utilizado para la creación de contenido enriquecido en blogs, notas y documentación
Compatibilidad con navegadores	Compatible con la mayoría de los navegadores web	Compatible con los navegadores web, pero los documentos deben seguir una sintaxis más estricta	No es necesario la compatibilidad con navegadores, ya que no está destinado para crear páginas web complejas

Fuente: Comunidad.dev (2020).

Al analizar cada uno de los parámetros pareciera que Markdown es el lenguaje ideal, sin embargo, con este lenguaje no se puede desplegar aplicaciones web complejas, es por ello que HTML resulta ser la mejor opción. Además, para que la aplicación web escrita en HTML pueda interactuar con bases de datos y mostrar contenido dinámico se consideró usar PHP, estos dos lenguajes en combinación con un lenguaje de marcado que es CSS, el cual permite diseñar y dar un estilo profesional, se complementaron para crear la aplicación fácil de usar y visualmente atractiva.

5.5.3.7 Plataforma necesaria para el almacenamiento en la nube.

Existe una gran variedad de plataformas en la nube que permiten almacenar contenido, para objetos de comparación se tomó en cuenta a las más conocidas y con mayores beneficios como Amazon S3, Microsoft Azure Blob Storage, Google Cloud Storage, Firebase storage, Google Cloud Storage, Backblaze B2. Algunas de estas plataformas ya se analizaron anteriormente por el hecho de que estas brindan muchos servicios.

Se determinó que Firebase storage es una excelente opción para cargar, almacenar y compartir archivos, como videos, imágenes, archivos de audio, documentos y otros tipos de archivos, son 5GB de almacenamiento que se puede utilizar de manera gratuita en esta plataforma. Otra de las razones predominantes que incidió en esta decisión es el hecho de que a través de la API RESTful es posible cargar de manera rápida las imágenes utilizando el lenguaje de Python.

5.5.3.8 Proveedor de correo electrónico.

Al elegir un proveedor de correo electrónico, se deben tener en cuenta varios factores importantes, entre ellos la seguridad, fiabilidad, espacio de almacenamiento, etc. Existe gran variedad de proveedores de correo electrónico como Hotmail, Yahoo, Gmail, Outlook, sin embargo, las características por las cuales se eligió a Gmail son:

- Almacenamiento: Gmail ofrece una gran cantidad de espacio de almacenamiento gratuito para sus usuarios de 15 GB.
- Filtros y organización: Gmail tiene una función de poder filtrar y organizar los correos electrónicos de acuerdo con diferentes categorías.
- Integración: Gmail es parte de la suite de productos de Google, lo que significa que se integra perfectamente con otras aplicaciones.
- Seguridad: Gmail utiliza cifrado SSL/TLS para proteger todos los correos electrónicos mientras están en tránsito. También cuenta con protección de phishing y spam. Además, se puede activar la verificación en dos pasos para evitar posibles hackeos o accesos no autorizados
- Fiabilidad: Gmail es conocido por ser uno de los proveedores de correo electrónico más confiables de todos.
- Integración: es fácil el integrar Gmail con Python utilizando la API de Gmail de Google, o mediante el protocolo SMTP.

5.5.3.9 Software para conexión remota al servidor en la nube y/o Raspberry.

Se usó PuTTY dado que es un software libre y gratuito que se utiliza como cliente de terminal para conectarse a servidores remotos a través de protocolos de red como Telnet, SSH, SUPDUP, Rlogin, y otros. Es una herramienta muy útil para acceder a servidores remotos para realizar tareas de desarrollo, configuración y mantenimiento. Es por ello que se usa principalmente para la administración, mantenimiento o soporte técnico a la aplicación web que se encuentra alojada en el servidor en la nube.

Se usó WinSCP, este es un cliente de transferencia de archivos de código abierto y gratuito que está disponible para Windows. Con este software se puede realizar la transferencia segura de archivos entre un equipo local y un servidor remoto a través de protocolos como SCP, FTP, SFTP y FTPS.

TeamViewer se usó para el acceso remoto y control remoto que permite a los usuarios conectarse a una computadora u otro dispositivo desde cualquier lugar del mundo a través de Internet. Hay varias razones por las cuales se podría usar TeamViewer, incluyendo soporte remoto, trabajo remoto, acceso a archivos, colaboración, etc. Por medio de este software se podrá dar soporte técnico en caso de alguna falla en el script alojado en la Raspberry Pi.

Estas tres herramientas de conexión se pueden usar de manera segura, rápida y gratuita. Aunque se pueden usar fácilmente otras alternativas para acceder a la Raspberry o al servidor en la nube como:

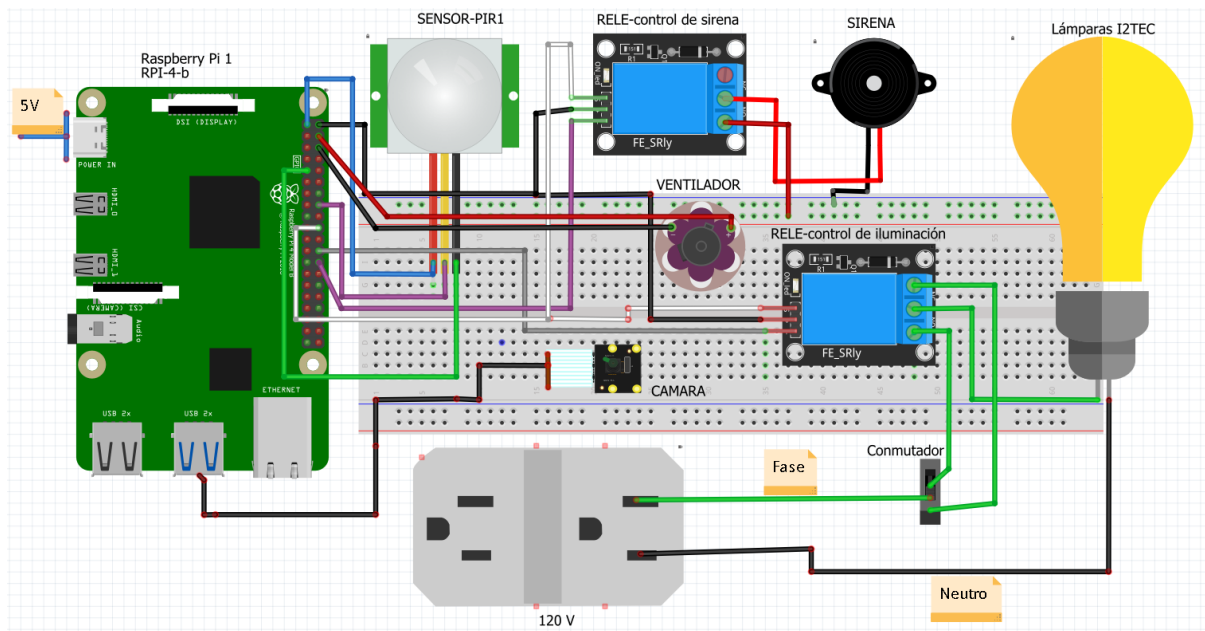
- MobaXterm
- OpenSSH
- FileZilla
- VNC Connect
- AnyDesk
- SecureCRT
- Termius

5.5.4 Diagrama de conexión

La Figura 28 muestra un diagrama elaborado con el software de código abierto denominado Fritzing. En este diagrama se pueden apreciar los componentes necesarios para construir y poner en funcionamiento el prototipo, así como sus conexiones a los pines GPIO. Es importante destacar que los pines GPIO pueden identificarse utilizando dos tipos de notaciones distintas: el modo BCM (Broadcom SOC channel) y el modo board. Esta distinción es relevante tanto para su identificación física como para su denominación en la programación. En el caso de este prototipo, se ha optado por utilizar la notación BCM.

Figura 28.

Diagrama de conexión del prototipo.



Fuente: Elaboración propia.

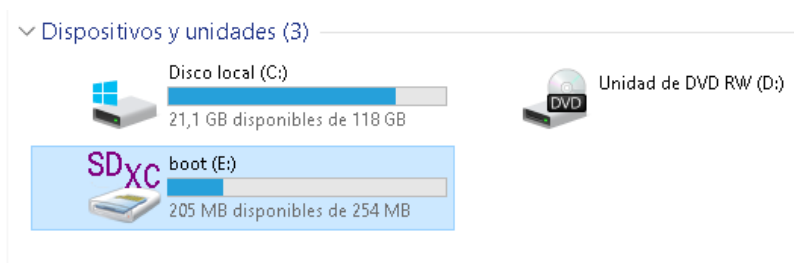
5.5.5 Proceso para la construcción del prototipo.

5.5.5.1 Instalación del sistema operativo de Raspberry “Raspbian”

En primer lugar, se debe introducir la tarjeta SD en una computadora para formatearla y cargar el Sistema Operativo con el cual se va a trabajar.

Figura 29.

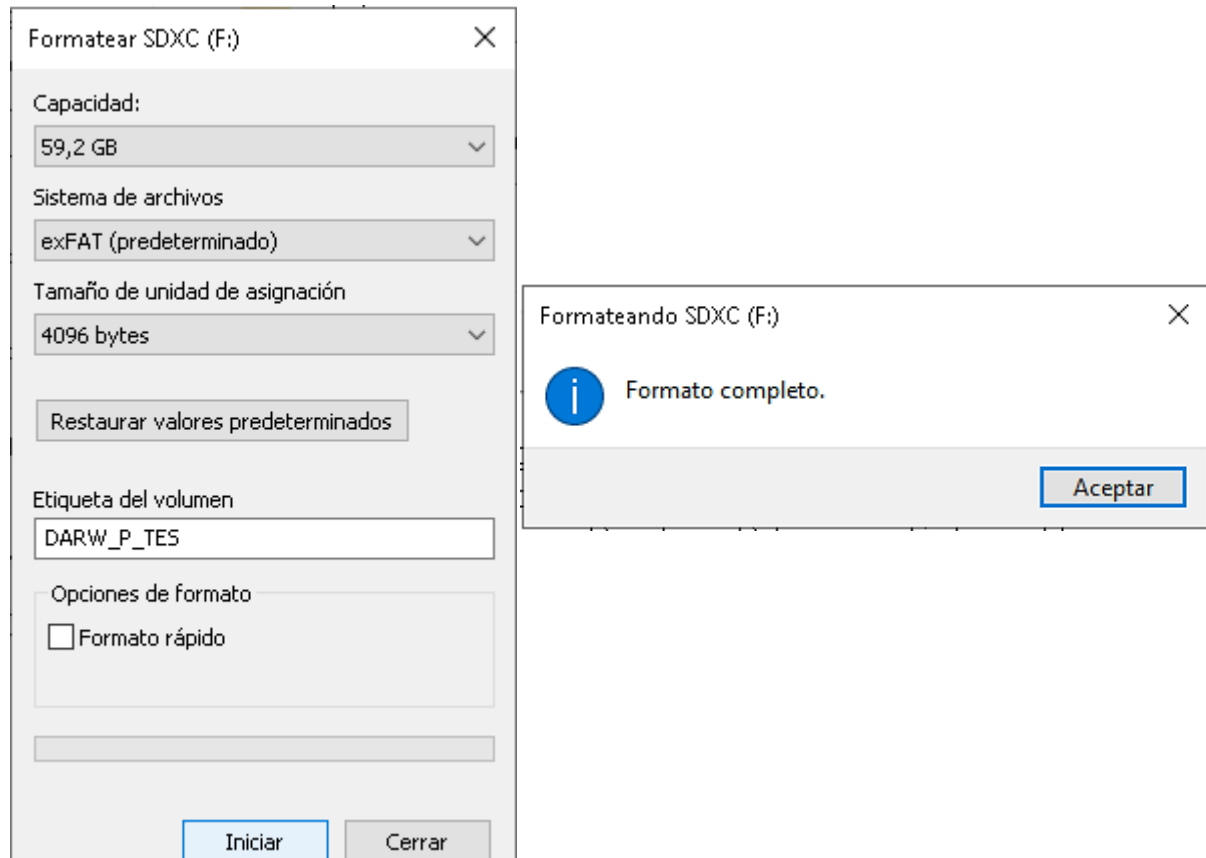
Identificación de la SD que se tendrá que formatear.



Fuente: Elaboración propia.

Figura 30.

Elección de los parámetros óptimos para formatear la SD.



Fuente: Elaboración propia.

Para la instalación del Sistema Operativo hace falta descargar e instalar Raspberry Pi Imager (el cual se puede descargar desde el siguiente enlace: <https://www.raspberrypi.com/software/>) en el computador donde se insertó y formateo la SD.

La instalación de Raspberry Pi Imager es muy fácil e intuitiva, además está disponible para varios sistemas operativos como Windows, MAC, UBUNTU, etc. Por lo que ofrece flexibilidad para ser utilizada en diferentes dispositivos, facilita el proceso de instalación en comparación con otras alternativas, y de manera general es una herramienta oficial desarrollada por la Fundación Raspberry Pi que cuenta con una interfaz gráfica fácil de usar.

Una vez que se haya instalado el software para poder cargar el sistema operativo en la tarjeta micro SD, se procede a abrir el software, tal como se muestra en la Figura 31. Lo importante a tener en cuenta es que la computadora en la que se va a instalar Raspberry Pi Imager debe contar con el lector de tarjetas SD y adicionalmente se debe contar con el adaptador externo micro SD a SD.

Figura 31.

Software Raspberry Pi Imager.

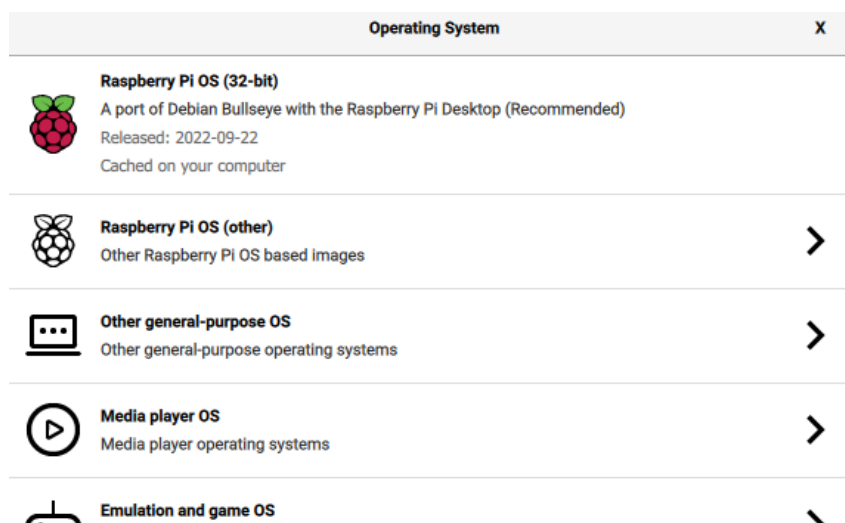


Fuente: Elaboración propia.

Se deberá dar clic en “CHOSEE OS” para la elección del sistema operativo (Figura 32) que se va a cargar en la SD.

Figura 32.

Elección del sistema Operativo.



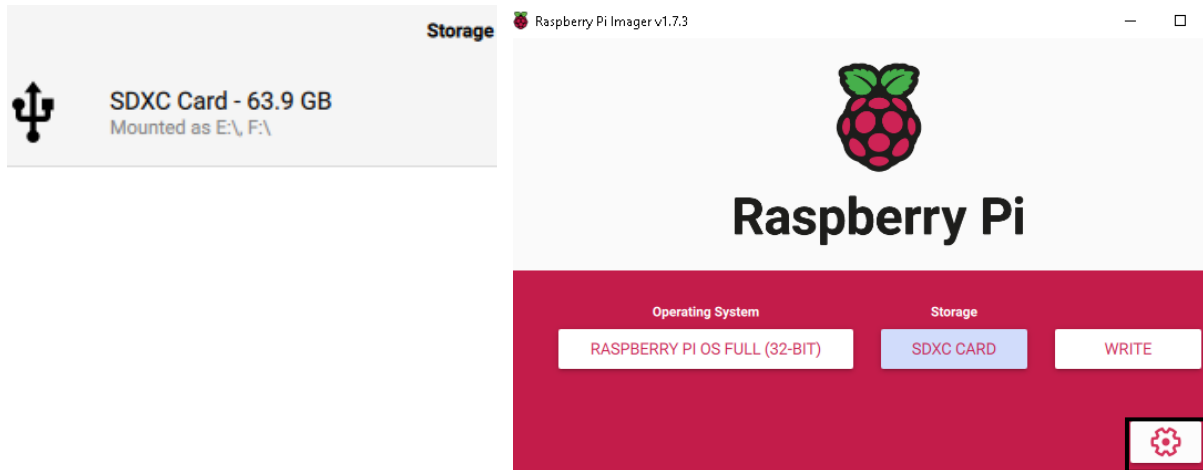
Fuente: Elaboración propia.

Luego de la elección del Sistema Operativo, se deberá realizar la selección de la tarjeta SD Figura 33 (lado izquierdo). A continuación, se mostrará la ventana que se observa

en la Figura 33 (lado derecho), en donde se podrá dirigir a las opciones avanzadas y ahí se colocará un username, password, tipo de teclado, zona horaria, red LAN/WLAN, entre otros parámetros que sean necesarios.

Figura 33.

Elección de la tarjeta SD y de otras opciones avanzadas.



Fuente: Elaboración propia.

Finalmente, se deberá dar clic en “WRITE” y continuar para que se proceda con la carga del Sistema Operativo.

Al encender por primera vez la Raspberry se deberá configurar la red, asignar un nombre de usuario, una contraseña y otras configuraciones importantes (en caso de que no se haya realizado a la hora de cargar el sistema operativo). Luego se tendrá que abrir la terminal y proceder a descargar y actualizar todos los repositorios o paquetes disponibles con los siguientes comandos:

```
- sudo apt update  
- sudo apt upgrade
```

El comando "sudo apt update" actualiza la lista de paquetes disponibles en los repositorios, mientras que "sudo apt upgrade" instala las actualizaciones disponibles para todos los paquetes instalados. Es recomendable ejecutar estos comandos para mantener todo el sistema operativo y las aplicaciones instaladas actualizadas y seguras.

5.5.5.2 Conexión remota a la Raspberry Pi.

Si se está tratando de trabajar con la Raspberry Pi sin monitor, lo primero que se debe hacer es conectarse por el protocolo SSH mediante PuTTY, para ello se debe conocer la

dirección IP de la Raspberry, esto se lo puede realizar con ayuda del software *Advanced IP Scanner* o si se tiene activo el antivirus *ESET Smart Security*, dirigirse a la sección de inspector de red y buscar Raspberry en el nombre del dispositivo o el proveedor y copiar la IP.

Luego abrir PuTTY y en la sección denominada *Host name (or IP address)* colocar la dirección IP, en *connection type* seleccionar ssh, presionar enter y colocar el username y el password que se configuró previamente en la instalación del sistema operativo, una vez realizado cada uno de estos pasos ya se puede trabajar en la Raspberry por medio de líneas de comando.

Si por comodidad se necesita hacer uso del escritorio y del entorno gráfico de la Raspberry, se necesitará instalar TeamViewer, esto requiere ejecutar las siguientes líneas de código en la terminal, en la sesión que se creó en PuTTY:

```
- wget https://download.teamviewer.com/download/linux/teamviewer-host_armhf.deb  
- sudo dpkg -i teamviewer-host_armhf.deb  
- sudo apt --fix-broken install
```

Con estos comandos Teamviewer se instalará satisfactoriamente. Posteriormente, será necesario realizar algunas configuraciones para poder utilizarlo. Para ello, se deberá ejecutar el siguiente comando:

```
sudo teamviewer setup
```

Se tendrá que aceptar los términos y condiciones, ahora hay que colocarle una clave a Teamviewer para poder ingresar de manera segura, esto se puede realizar con el siguiente comando, sustituir PASSWORD por la clave que se crea conveniente.

```
sudo teamviewer passwd PASSWORD
```

Finalmente, para obtener el ID que permitirá establecer una conexión de manera remota desde otro dispositivo a la Raspberry, ejecutar el siguiente comando:

```
sudo teamviewer info
```

Recordar la ID y la clave que se colocó anteriormente, ya que la conexión únicamente se efectuará validando estos dos datos.

5.5.5.3 Habilitación de la cámara de la Raspberry Pi.

Para el desarrollo de proyectos de visión artificial o cualquier otro proyecto que implique el uso de algún módulo externo de cámara se tendrá que habilitar el uso de la misma, ya que por defecto suele estar deshabilitada.

Lo primero será conectar la cámara a la Raspberry Pi. Para verificar que la cámara está conectada correctamente se emplea el siguiente comando en la terminal.

```
vcgencmd get_camera
```

Si como resultado de ejecutar el comando anterior se muestra "supported=1 detected=1" significa que la cámara está conectada correctamente.

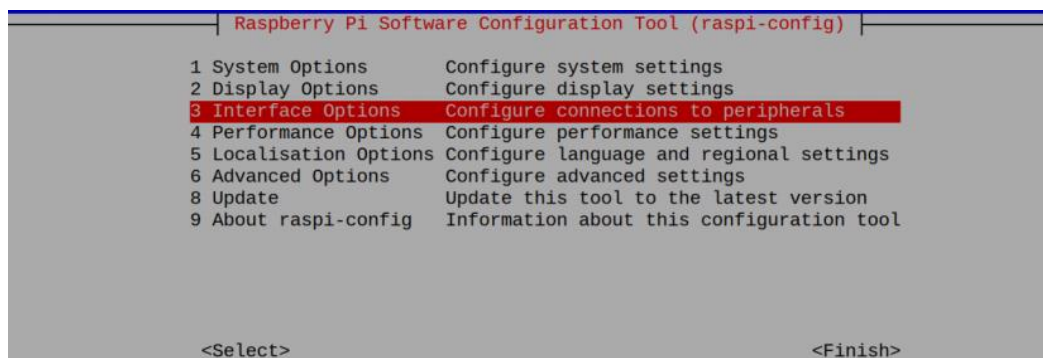
La habilitación del uso de la cámara en el sistema operativo requiere el ir al archivo de configuración, para ello se emplea el siguiente comando:

```
sudo raspi-config
```

Al ejecutar el comando se muestra la ventana de la Figura 34, se necesitará dirigirse hasta la opción de *Interface Options* para presionar Enter y luego aparecerá la ventana de la Figura 35.

Figura 34.

Herramientas de configuración de la Raspberry Pi

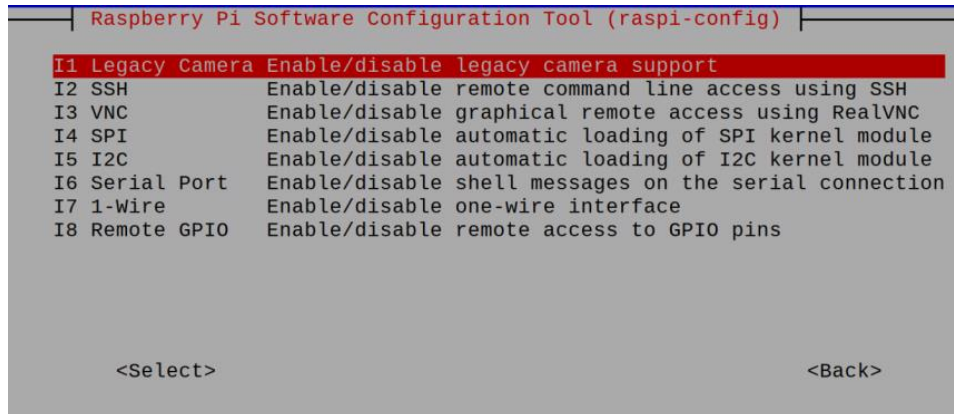


Fuente: Elaboración propia.

En esta ventana se deberá seleccionar la opción *Legacy Camera* y aparecerá la ventana de la Figura 35, en donde simplemente se tendrá que presionar Enter en la opción *Si* y finalmente *Aceptar*. Una vez realizado estos pasos se habilitará y se podrá hacer uso de la cámara en la Raspberry Pi.

Figura 35.

Selección de la cámara.



Fuente: Elaboración propia.

5.5.5.4 Instalación de la biblioteca de visión artificial y de las dependencias necesarias

La librería de visión artificial requiere de paquetes complementarios que son indispensables para que OpenCV pueda ejecutarse de manera satisfactoria, las dependencias necesarias se instalarán abriendo una terminal y ejecutando los siguientes comandos:

```
- sudo apt-get install build-essential cmake pkg-config python3-dev libgtk2.0-dev libgtk2.0-zlib1g-dev libpng-dev libjpeg-dev libtiff-dev libjasper-dev libavcodec-dev swig unzip vim  
- sudo apt-get install python3-numpy python3-opencv  
- sudo apt-get install python3-pip  
- sudo apt-get install python3-dev  
- sudo pip install picamera  
- sudo pip install rpio  
- sudo apt-get install v4l2ucp v4l-utils libv4l-dev
```

A continuación, se deberá descargar e instalar OpenCV con los comandos:

```
- wget http://downloads.sourceforge.net/project/opencvlibrary/opencv-unix/2.4.9/opencv-2.4.9.zip  
- unzip opencv-2.4.9.zip  
- cd opencv-2.4.9  
- cmake -DCMAKE_BUILD_TYPE=RELEASE -DCMAKE_INSTALL_PREFIX=/usr/local -DBUILD_PERF_TESTS=OFF -DBUILD_opencv_gpu=OFF -DBUILD_opencv_ocl=OFF  
- make  
- sudo make install
```

5.5.5.5 Lanzamiento de la instancia EC2 en AWS

Se lanzará un servidor en la nube para poder desplegar la aplicación web y poder visualizar los datos desde allí. Lo primero es registrarse en AWS. Una vez que se haya creado una nueva cuenta en AWS, se debe dirigir a crear una solución y seleccionar *Lance una máquina virtual con EC2*.

Luego de ello se deberá colocar un nombre a la instancia y seleccionar el sistema operativo de la máquina, en este caso se eligió a Ubuntu server 18.04 LTS con una arquitectura de 64 bits (disponible en la capa gratuita).

Figura 36.

Selección del sistema operativo de la máquina virtual.

Amazon Machine Image (AMI)

Ubuntu Server 18.04 LTS (HVM), SSD Volume Type Apto para la capa gratuita

ami-0263e4deb427da90e (64 bits (x86)) / ami-0e5599794d252b611 (64 bits (Arm))

Virtualización: hvm Habilitado para ENA: true Tipo de dispositivo raíz: ebs

Descripción

Canonical, Ubuntu, 18.04 LTS, amd64 bionic image build on 2023-01-31

Arquitectura ID de AMI

64 bits (x86) ami-0263e4deb427da90e Proveedor verificado

Fuente: Elaboración propia.

Figura 37.

Selección el tipo de instancia.

▼ **Tipo de instancia** [Información](#)

Tipo de instancia

t2.micro Apto para la capa gratuita

Fuente: Elaboración propia.


Figura 38.


Crear el par de claves para poder administrar el servidor de manera remota.

▼ **Par de claves (inicio de sesión)** [Información](#)

Puede utilizar un par de claves para conectarse de forma segura a la instancia. Asegúrese de que tiene acceso al par de claves seleccionado antes de lanzar la instancia.

Nombre del par de claves - *obligatorio*



 [Crear un nuevo par de claves](#)

Tipo de par de claves

RSA
Par de claves pública y privada cifradas mediante RSA

ED25519
Par de claves pública y privada cifradas con ED25519 (no es compatible con instancias Windows)

Formato de archivo de clave privada

.pem
Para usar con OpenSSH

.ppk
Para usar con PuTTY

Fuente: Elaboración propia.

Cuando se haya colocado el nombre del par de claves, se selecciona el tipo y el formato; .pem es para usarla con OpenSSH y .ppk para usarla con PuTTY, finalmente seleccionar *Create key pair* y se descargara el archivo correspondiente, el cual se deberá guardar en un lugar seguro ya que se lo requerirá cada vez que se requiera acceder al servidor .

A continuación, se debe crear el grupo de reglas de seguridad, en donde es necesario permitir el tráfico SSH, HTTPS, HTTP, MYSQL/Aurora.

En la Figura 39 se muestra la configuración del almacenamiento, en donde está permitido ubicar hasta 30 GB de almacenamiento para la capa gratuita.

Figura 39.

Configuración del almacenamiento.

The screenshot shows the 'Configurar almacenamiento' (Configure storage) section in the AWS console. It features a header with 'Configurar almacenamiento' and 'Información' on the left, and 'Avanzado' on the right. Below the header, there is a configuration row: '1x' followed by a text input field containing '25', 'GiB' followed by a dropdown menu showing 'gp2', and the text 'Volumen raíz (Sin cifrar)'. Below this row is a light blue information box with an information icon, the text 'Los clientes que cumplan los requisitos de la capa gratuita pueden obtener hasta 30 GB de almacenamiento magnético o de uso general (SSD) de EBS', and a close icon. At the bottom of the configuration area is a button labeled 'Agregar un nuevo volumen'.

Fuente: Elaboración propia.

Una vez que se concluye con las configuraciones previas, se debe presionar en *Lanzar instancia*.

Lo que falta por realizar es una buena práctica para mantener una dirección IP que sea constante y fija incluso si el servidor se reinicia, esto requiere la asignación de la llamada *IP elástica* a la instancia creada. Para realizar esto es necesario ingresar al panel de administración de EC2, seleccionar la opción *Direcciones IP Elásticas*, después *Asignar la dirección IP elástica* con la opción por defecto *Grupo de direcciones IPv4 de Amazon*

Cuando ya haya sido asignada la dirección, la asociación de la IP elástica se realiza al seleccionar la misma y dirigirse a *Acciones*, luego escoger la opción *Asociar dirección IP elástica*, seleccionar la instancia y finalmente *Asociar*. En la Figura 40 se visualizan los parámetros de configuración para dar por concluida la asociación de la instancia con la dirección IP elástica.

Figura 40.

Configuración de la IP elástica.

The screenshot shows the 'Asociar la dirección IP elástica' (Associate Elastic IP address) dialog box in the AWS Management Console. At the top, it says 'Elegir la instancia o la interfaz de red que se desea asociar a esta dirección IP elástica' (Choose the instance or network interface that you want to associate with this Elastic IP address). Below this is a dropdown menu. The main section is titled 'Dirección IP elástica:' (Elastic IP address:). Underneath, there's a section for 'Tipo de recurso' (Resource type) with two radio buttons: 'Instancia' (Instance) which is selected, and 'Interfaz de red' (Network interface). A warning message states: 'Si asocia una dirección IP elástica a una instancia que ya tiene asociada una dirección de este tipo, esa dirección IP elástica anterior se desasociará, pero aun así se asignará a su cuenta. Más Información' (If you associate an Elastic IP address with an instance that already has an Elastic IP address of this type associated with it, the previous Elastic IP address will be disassociated, but it will still be assigned to your account. More Information). Below the warning, there's a note: 'If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.' There are two input fields: 'Instancia' (Instance) containing 'i-0057f535b89c7e9b4' and 'Dirección IP privada' (Private IP address) containing '172.31.59.12'. At the bottom, there's a checkbox for 'Nueva asociación' (New association) with the label 'Permitir que se vuelva a asociar esta dirección IP elástica' (Allow this Elastic IP address to be associated again). The dialog has 'Cancelar' (Cancel) and 'Asociar' (Associate) buttons.

Fuente: Elaboración propia.

5.5.5.6 Instalación del software necesario para crear la aplicación web

La instalación de Apache, MySQL y phpMyAdmin requiere conectarse remotamente al servidor desplegado en la instancia EC2 de AWS, esto requiere del software PuTTY:

Figura 41.

Acceso al servidor remoto de AWS.

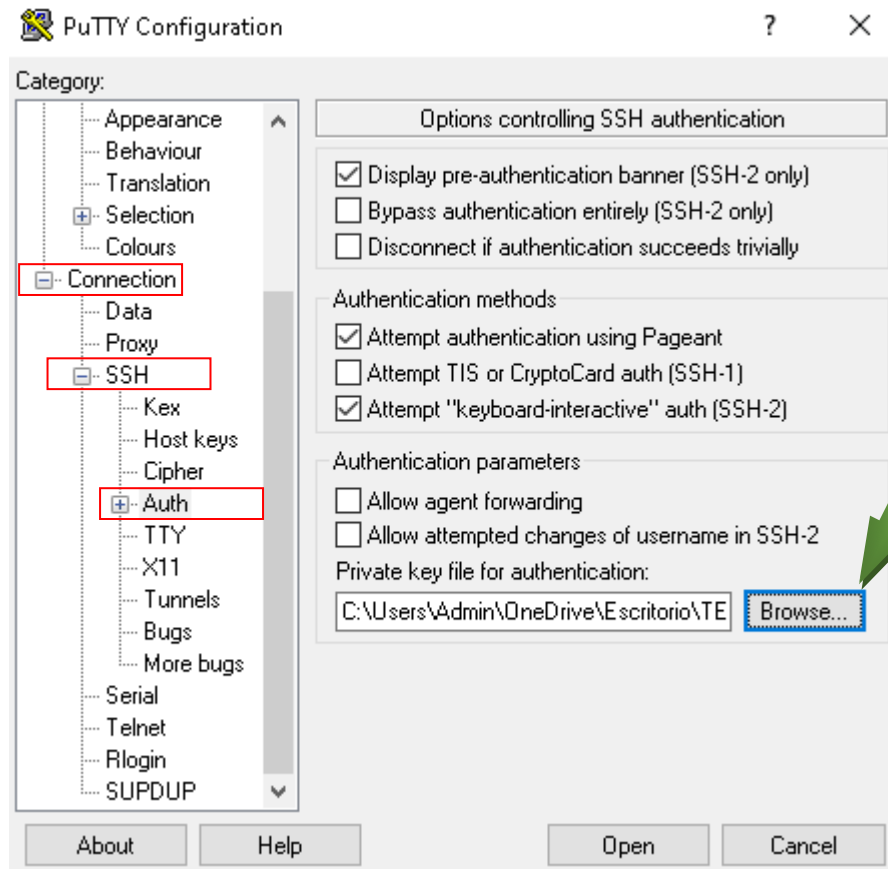
The screenshot shows the 'PuTTY Configuration' dialog box. On the left is a tree view with categories: 'Session', 'Terminal', and 'Window'. The 'Session' category is expanded, showing sub-items: 'Logging', 'Keyboard', 'Bell', 'Features', 'Appearance', 'Behaviour', and 'Translation'. The main area is titled 'Basic options for your PuTTY session'. It contains a section 'Specify the destination you want to connect to' with a 'Host Name (or IP address)' field and a 'Port' field set to '22'. Below this is the 'Connection type:' section with three radio buttons: 'SSH' (selected), 'Serial', and 'Other:'. The 'Other:' dropdown menu is set to 'Telnet'. At the bottom, there's a section for 'Load, save or delete a stored session' with a 'Saved Sessions' list.

Fuente: Elaboración propia.

En donde se solicita el *Host Name*, se debe colocar la dirección IP del servidor. A continuación, se tendrá que dirigir a la sección de Connection-SSH-Auth y se deberá cargar el archivo en formato ppk que se obtuvo al lanzar el servidor, este archivo contiene la llave privada que permite la autenticación para admitir el acceso remoto al servidor.

Figura 42.

Carga de la llave privada ppk.



Fuente: Elaboración propia.

Después de completar esta acción, se presentará el terminal del servidor, en donde se podrá ejecutar los comandos necesarios, en primera instancia se actualizan los paquetes disponibles con los comandos:

```
- sudo apt update  
- sudo apt upgrade
```

Para la instalación de Apache se ejecuta el comando:

```
sudo apt install apache2
```

Una acción importante es comprobar el estado del firewall, habilitar el tráfico de red entrante para el servicio de *Apache full*, que incluye HTTP y HTTPS, para ello se ejecuta los siguientes comandos:

```
- sudo ufw status
- sudo ufw app list
- sudo ufw allow in "Apache Full"
- sudo ufw enable
```

Cada vez que se realice cualquier cambio es conveniente reiniciar el servicio:

```
sudo systemctl restart apache2
```

Una vez instalado apache es necesario realizar ciertas configuraciones, para ello dirigirse al directorio de Apache2, ejecutar el comando:

```
sudo nano apache2.conf
```

Buscar *AllowOverride None* y reemplazar *None* por *All*, tal y como se muestra en la Figura 43.

Figura 43.

Configuraciones de Apache.



```
<Directory /var/www/>
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
```

```
<Directory /var/www/html>
Options Indexes FollowSymLinks
AllowOverride All
Require all granted
</Directory>
```

Fuente: Elaboración propia.

Ejecutar el siguiente comando para reescribir URL's y redireccionar solicitudes de la aplicación web, luego de ello se debe reiniciar el servicio de apache.

```
sudo a2enmod rewrite
```

Para instalar MySQL se utiliza el siguiente comando:

```
sudo apt install mysql-server
```

Luego se deberá iniciar el proceso de configuración de seguridad de MySQL, en donde pedirá que se cree una contraseña para root.

```
sudo mysql_secure_installation
```

Una buena práctica de seguridad es entrar a las configuraciones de mysql y colocar los siguientes comandos, con la finalidad de que cada vez que se ingrese a mysql solicite una contraseña.

```
- sudo mysql
  - ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password
    BY'*****';
  - FLUSH PRIVILEGES
  - exit
```

Reemplazar ***** por la contraseña de su elección para ingresar a mysql de manera segura. A partir de realizar estas acciones cada vez que se intente ingresar a mysql deberá hacerlo con `mysql -u root -p`, mismo que solicitará que se ubique la contraseña para permitir el acceso.

Es importante crear un nuevo usuario y otorgarle permisos necesarios para acceso de manera remota:

```
- CREATE USER 'xxx'@'%' IDENTIFIED BY '****';
- GRANT ALL PRIVILEGES ON *.* TO 'xxx'@'%' WITH GRANT OPTION;
- exit
```

Reemplazar xxx por un nombre de usuario para acceso remoto, reemplazar % con la dirección IP a la que se otorgará el acceso; caso contrario, si se deja con % podrá acceder cualquier dirección IP y en **** ubicar la contraseña para ese usuario con privilegios distintos.

Para instalar los paquetes necesarios y poder ejecutar aplicaciones PHP en un servidor web Apache, se ejecuta el comando:

```
sudo apt install php libapache2-mod-php php-mysql
```

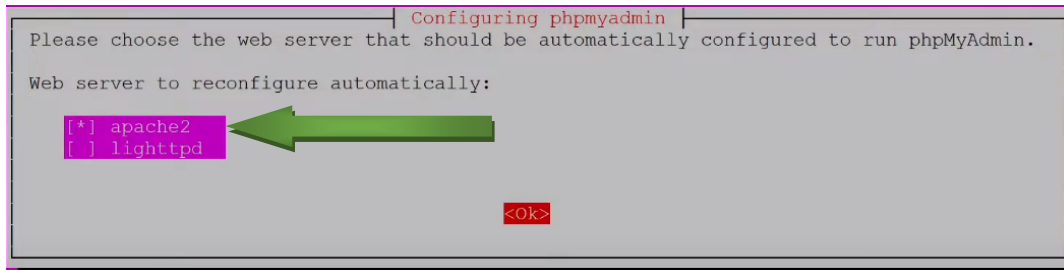
Para ejecutar la herramienta de administración de bases de datos MySQL llamada PhpMyAdmin, se utiliza el comando:

```
sudo apt install phpmyadmin php-mbstring php-gettext
```

Al ejecutar este comando aparecerá la ventana de la Figura 44, en donde se pide que se elija el servidor que se va a configurar automáticamente para ejecutar con phpMyAdmin, aquí se debe seleccionar Apache2 (que fue el servidor web que se instaló anteriormente), es muy importante realizar esta acción para que el servidor pueda funcionar correctamente.

Figura 44.

Configuraciones adicionales de phpMyAdmin.

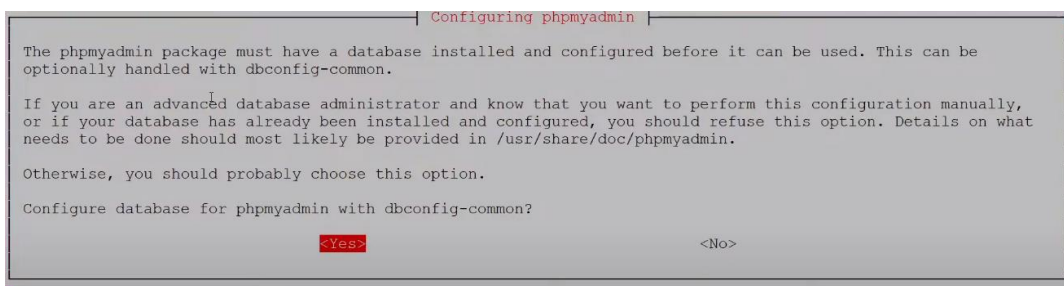


Fuente: Elaboración propia.

En la siguiente ventana que aparece seleccionar “Yes” (Figura 45), luego solicitará crear una contraseña para phpMyAdmin (Figura 46), con ello se habrá finalizado la parte de las configuraciones de phpMyAdmin.

Figura 45.

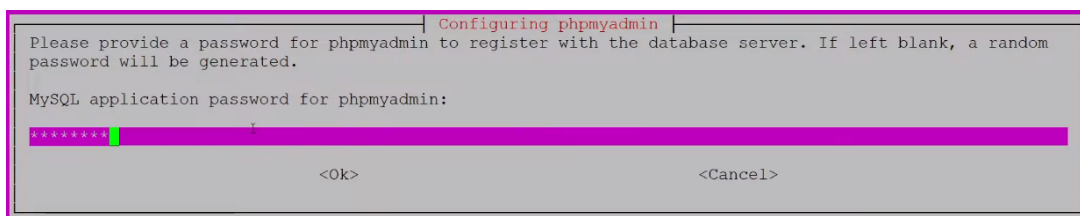
Configuraciones adicionales de phpMyAdmin.



Fuente: Elaboración propia.

Figura 46.

Configuraciones adicionales de phpMyAdmin.



Fuente: Elaboración propia.

Finalmente, ejecutar el comando que permite habilitar las funciones de cadena multibyte para que estén disponibles en PHP.

```
sudo phpenmod mbstring
```

5.5.5.7 Configuración de Gmail para poder utilizarlo desde Python.

Es muy importante realizar las respectivas configuraciones que se indican a continuación, ya que en mayo de 2022 se actualizaron las políticas de seguridad. Pero también debido a los cambios en la forma en que Google maneja los permisos de las aplicaciones, esta sección se actualizó para reflejar el nuevo método que utiliza contraseñas de aplicaciones específicas.

Para poder realizar esto dirigirse a Gmail y crear una nueva cuenta de correo electrónico desde donde se enviará el mensaje y adicionalmente es recomendable crear una nueva cuenta para que sea la receptora.

Para permitir que Python o cualquier aplicación utilice la cuenta de Gmail de manera segura, se deberá tener habilitada la verificación en dos pasos. Esto se puede hacer a través de la cuenta de Google en la pestaña denominada *Seguridad* o a través del siguiente enlace: <https://myaccount.google.com/security>.

Una vez que se habilita la autenticación en dos pasos, hay que dirigirse a la sección de *Contraseñas de aplicaciones*, para crear una contraseña de aplicación específica para el dispositivo desde donde se enviarán los correos electrónicos que es la Raspberry Pi. Esto garantiza que la contraseña de la cuenta de Gmail no necesite almacenarse en el script, sino que se tendrá una contraseña específica para el dispositivo. En la ventana Contraseñas de la aplicación, hacer clic en el menú desplegable *Seleccionar app* y seleccionar *Otro*.

En el cuadro de texto que aparece, asignar un nombre a su dispositivo. Este nombre es únicamente de referencia, así que se puede colocar lo que se crea conveniente, de preferencia se recomienda que se coloque algún nombre que haga referencia a la Raspberry Pi. Una vez hecho esto, presione clic en "Generar" para crear la contraseña de la aplicación.

5.5.5.8 Configuración de Firebase storage para poder utilizarlo desde Python.

El poder ingresar a la consola de administración de Firebase requiere de iniciar sesión con un correo de Gmail. En la consola se deberá *Agregar proyecto*, colocar un nombre y seguir con las demás configuraciones que se solicitan.

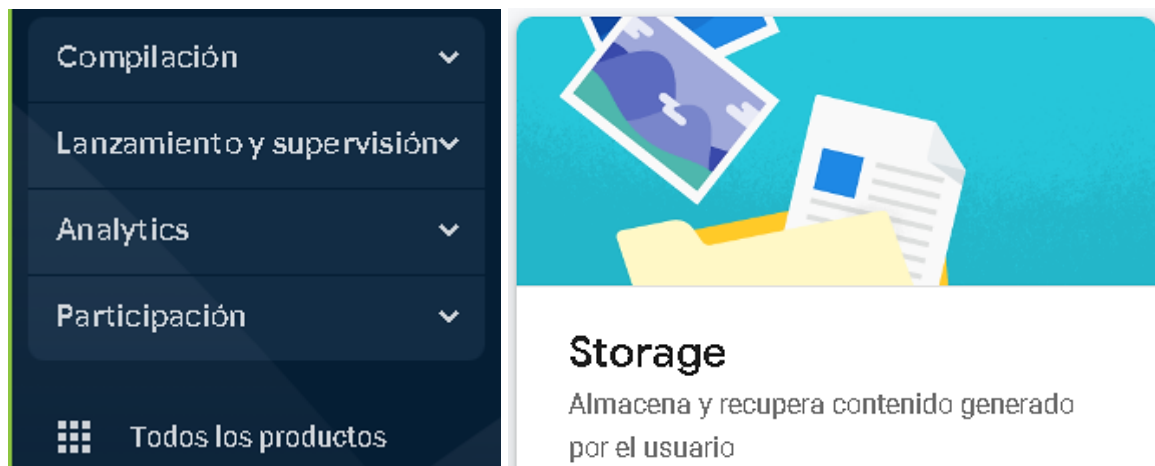
Cuando haya concluido este proceso, en la parte izquierda aparecen varias opciones, seleccionar *Todos los productos*, buscar Storage y comenzar a configurar las reglas de seguridad.

En la Figura 48, se muestran las configuraciones de las reglas de seguridad para poder utilizar Firebase storage.

En la Figura 49, se muestra la configuración de la región, allí se puede ubicar cualquier ubicación y se da por terminada la sección de las configuraciones previas.

Figura 47.

Crear un nuevo proyecto de Firebase storage.



Fuente: Elaboración propia.

Figura 48.

Configuraciones de seguridad.

Configura Cloud Storage

1 Reglas de seguridad para Cloud Storage

2 Configura la ubicación de Cloud Storage

Después de definir la estructura de tus datos, **debes crear reglas para protegerlos.**
[Más información](#)

Iniciar en modo de producción

Tus datos son privados de forma predeterminada. El acceso de lectura/escritura de los clientes solo se otorgará como se indica en tus reglas de seguridad.

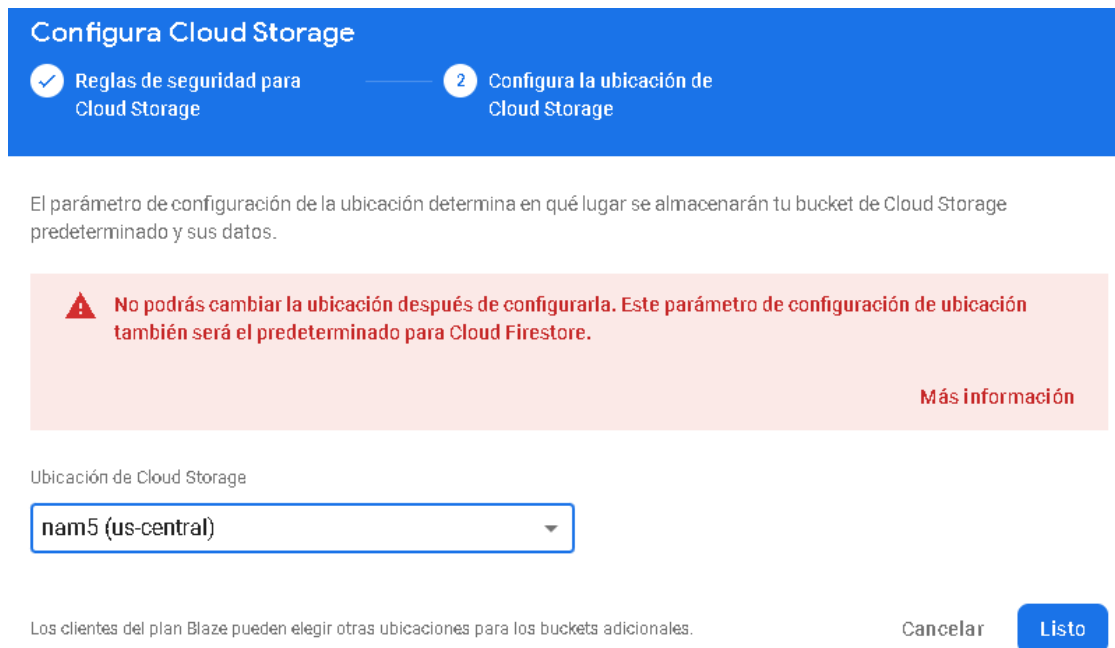
Comenzar en modo de prueba

```
rules_version = '2';
service firebase.storage {
  match /b/{bucket}/o {
    match /{allPaths=**} {
      allow read, write: if false;
    }
  }
}
```

Fuente: Elaboración propia.

Figura 49.

Configuración de la región.

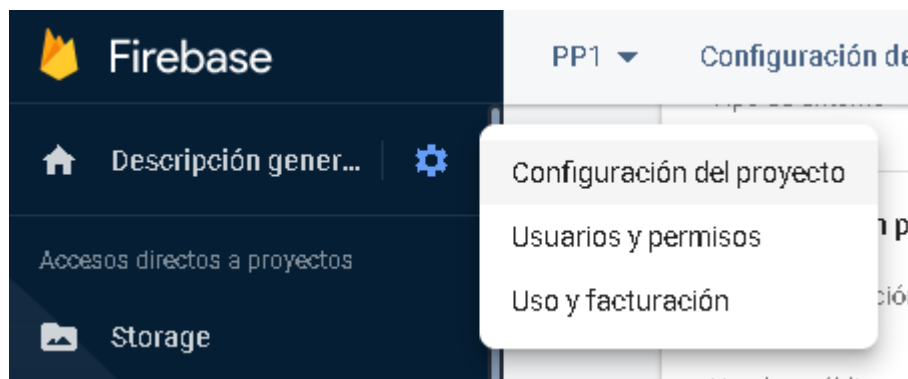


Fuente: Elaboración propia.

A continuación, dirigirse a la configuración del proyecto (Figura 50), buscar la *configuración del SDK*, marcar en *config* y copiar *todo* el bloque de código que se presenta para que sea integrado en Python y se puedan almacenar las imágenes en la nube.

Figura 50.

Configuración del proyecto.



Fuente: Elaboración propia.

5.5.5.9 Desarrollo del script en Python

Para el desarrollo del script se empleó la versión 3.9 de Python, en primer lugar, se desarrolló una función denominada *Video_Stream* (Anexo 4) con la finalidad de poder utilizar diferentes tipos de cámaras sin tener que modificar el código, ya sea que se utilice el módulo de cámara que está propiamente desarrollado para la Raspberry o incluso cámaras web, cámaras IP, etc.

La técnica empleada para la detección de movimiento es una combinación entre la diferencia de fotogramas y de la detección de contornos. Estas dos técnicas se complementan perfectamente ya que además de comparar el frame actual con el frame anterior, se buscan los píxeles que están conectados para posteriormente calcular el área de ese conjunto de píxeles y detectar si los cambios en la imagen son significativos como para considerarse una persona.

El script desarrollado da inicio con la instalación de librerías necesarias para luego poderlas importar al script, las librerías necesarias son:

- OpenCV → librería de visión artificial
- Tkinter → librería necesaria para desarrollar una interfaz gráfica
- Threading → librería que permite que distintos procesos se ejecuten de manera simultánea
- Time → librería para hora y fecha
- SMTP → librería para el envío de correo electrónico
- GPIO → librería para usar los pines GPIO de la Raspberry
- Argparse → librería para analizar argumentos
- Imutils → librería para el procesamiento de imágenes
- Pyrebase → librería que permite la sincronización con la plataforma firebase
- Os → librería para que permite acceder y/o manipular los recursos del sistema operativo de la Raspberry como archivos, directorios, etc.
- Unidecode → librería utilizada para procesar texto en diferentes idiomas, especialmente en aquellos que utilizan acentos o caracteres especiales.
- Pymysql → librería que permite conectarse a la base de datos creada en MySQL y poder realizar operaciones en ella utilizando código Python.

Luego de importar cada una de las librerías se procede a definir variables y a realizar las configuraciones necesarias, dando inicio por configurar los pines GPIO en modo BCM, establecer los pines que se van a utilizar como entrada o como salida.

Especificar el servidor de correo electrónico, el puerto, el correo electrónico desde el cual se hace el envío de la alerta y la clave de seguridad creada para aplicaciones externas de Gmail.

Se deberá también establecer la conexión con la base de datos, en donde se tendrá que especificar la dirección IP del servidor virtual de la instancia EC2 desplegada en AWS, el usuario habilitado para la conexión remota, la contraseña y el nombre de la base de datos.

De igual manera se deberá cargar el SDK para poder utilizar Firebase, para ello dirigirse a la consola de administración de Firebase, ubicarse en la configuración del proyecto y buscar la sección de *Configuración del SDK* de allí se podrá copiar el SDK.

A continuación, se tendrá que inicializar el video, establecer dimensiones, dar un formato al video y crear la interfaz de configuración del sistema. Luego, se crea una clase que contiene toda la estructura y la información para el envío de correo electrónico en donde se coloca el asunto, se adjunta la imagen capturada y un texto.

Una vez que se definió las variables y las especificaciones previas, se continúa con la creación de las diferentes funciones importantes para utilizarlas posteriormente, una de las funciones creadas contiene un proceso iterativo con ayuda del bucle *While*, el cual estará capturando frames en tiempo real, para luego realizar un procesamiento de imágenes que implica:

- El cálculo de la diferencia absoluta de los frames capturados
- Conversión de la imagen a escala de grises para que el procesamiento sea mucho más rápido
- Aplicar un filtro de suavizado Gaussiano para reducir la cantidad de ruido y suavizar los píxeles
- Aplicar un umbral a la imagen suavizada para transformar a una imagen binaria, en donde los píxeles que estén por encima de un umbral se convertirán a color blanco y los que están por debajo a color negro
- Operación de dilatación a la imagen binaria para incrementar los objetos que contienen mayor información y eliminar los que contengan muy poca información
- Encontrar los contornos de cada uno de los objetos dilatados en la imagen y almacenarlos en una variable. Los contornos o también llamados blobs son un conjunto de píxeles que están conectados entre sí.

Luego de aplicar el procesamiento se da inicio con un bucle *for*, el cual permite iterar cada uno de los contornos que se almacenaron en la etapa de procesamiento, luego se incluye una línea de código fundamental que devuelve los parámetros *x*, *y*, *w* y *h* que describen un rectángulo delimitador, de esta manera se va a encerrar completamente el contorno proporcionado como entrada.

```
for contour in contours:  
    (x, y, w, h) = cv2.boundingRect(contour)
```

A continuación, se da inicio con la sentencia condicional *if*, la cual permite filtrar los contornos que son demasiado pequeños para ser considerados como posibles personas en la imagen que se está analizando.

```
if cv2.contourArea(contour) < 9000:
```

La función `cv2.contourArea(contour)` calcula el área del contorno especificado. Si el área del contorno es menor que 9000 píxeles, se considera que el contorno es demasiado pequeño para ser una persona y, por lo tanto, se desecha. Esto ayuda a mejorar la precisión del detector de personas.

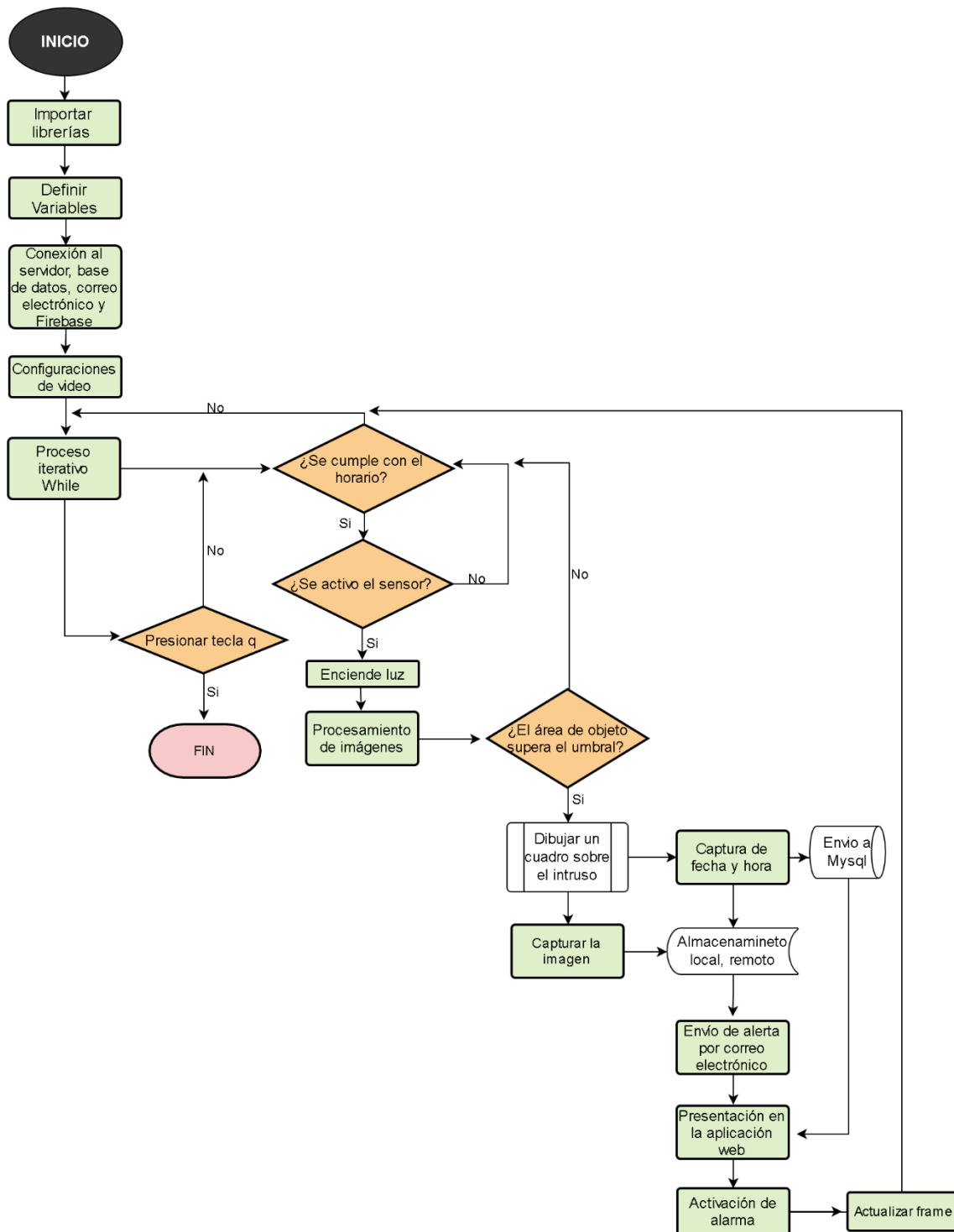
Por el contrario, si el área del contorno es superior a 9000 píxeles se determina que se trata de una persona y por lo tanto se procede con la toma de decisión que implica la carga de la hora y fecha del evento en la base de datos de MySQL, se carga la imagen en el servidor en la nube; estas dos acciones se combinan para poder visualizar los datos en la aplicación web. Al mismo tiempo se hace él envió de una alerta por correo electrónico, en donde se incluye un asunto, un mensaje de alerta, la hora, la fecha y se adjuntan dos imágenes del evento suscitado. Para poder incrementar la confianza como backup se cargan las imágenes en la nube empleando Firebase storage.

Finalmente, como medida de disuasión se activa una alarma sonora y se emplea un sensor PIR, este sensor tiene como objetivo principal aumentar el nivel de precisión y hacer que el sistema sea menos propenso a falsas alarmas debido a cambios de luz o a otros factores. El código completo, el cual se encuentra debidamente estructurado por medio de funciones se encuentra adjunto en el Anexo 5.

En la Figura 51 se muestra un diagrama de flujo que ilustra todo el proceso que se lleva a cabo para el funcionamiento del sistema de seguridad inteligente y activo.

Figura 51.

Diagrama de flujo del funcionamiento del script.



Fuente: Elaboración propia.

5.5.5.10 Presentación de los datos en la aplicación web.

El primer paso a seguir para dar inicio con la aplicación web, es delimitar todo el contenido que se va a mostrar, las páginas o secciones y la información que contendrán cada una de las secciones. Lo que se planea mostrar es:

- Mecanismo de autenticación
- Ventana principal
- Ventana de imágenes capturadas
- Ventana de información de usuario
- Ventana de soporte técnico
- Ventana para cerrar sesión

Luego de ello, se realizó el diseño de la estructura de la aplicación web, incorporando detalles visuales, para que se aprecie estéticamente y se puedan elegir imágenes, colores, letras y luego todo eso se pueda plasmar mediante programación en HTML y CSS.

En la Figura 52 se muestra el diseño del mecanismo de autenticación, el cual permite garantizar la seguridad y privacidad de la información que se almacenará en la aplicación web. En esta ventana se solicitará que se ingrese un nombre de usuario y una contraseña, estos datos verifican la identidad del usuario; si las credenciales ingresadas coinciden con las que se encuentran almacenadas en la base de datos, se permitirá el acceso al sistema caso contrario se solicitará que se intente nuevamente.

Figura 52.

Diseño del mecanismo de autenticación.

El diseño de la ventana de acceso (login) se muestra en un recuadro rectangular. En la parte superior, el título "Acceso" está centrado. Debajo del título, hay dos campos de entrada de texto. El primer campo está precedido por un ícono de un usuario (una silueta humana) y el segundo campo está precedido por un ícono de un candado cerrado. En la parte inferior del recuadro, hay un botón rectangular de color azul oscuro con el texto "Acceder" en blanco, centrado.

Fuente: Elaboración propia.

En la Figura 53 se muestra el diseño de la página principal, misma que aparecerá luego de que se haya verificado satisfactoriamente las credenciales ingresadas.

Figura 53.

Diseño de la página principal.



Fuente: Elaboración propia.

En la Figura 54 se muestra el diseño de la ventana de las imágenes capturadas.

Figura 54.

Diseño de la página de imágenes capturadas.



Fuente: Elaboración propia.

En la Figura 55 se muestra el diseño de la ventana de información de usuario.

Figura 55.

Diseño de la página de información de usuario.

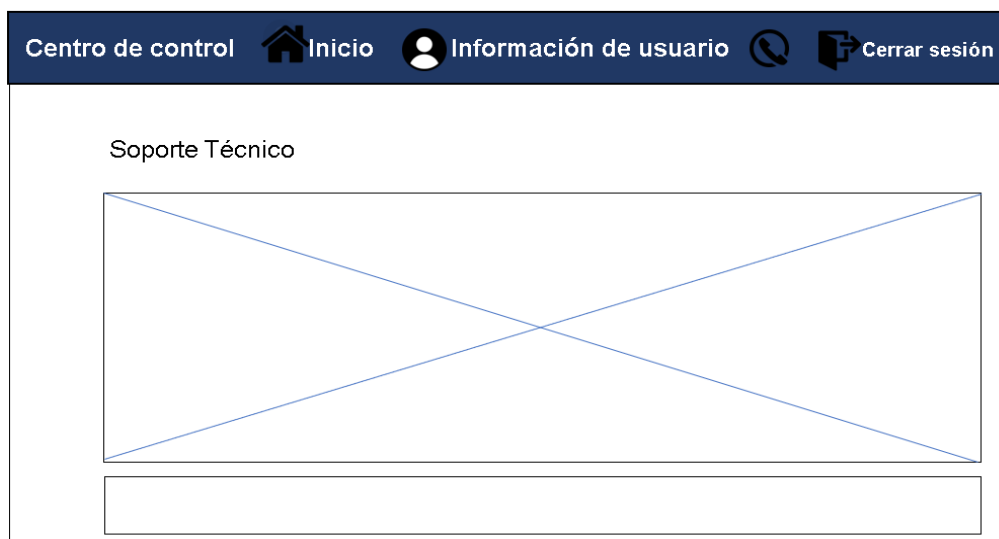


Fuente: Elaboración propia.

En la Figura 56 se muestra el diseño de la ventana de soporte técnico.

Figura 56.

Diseño de la página de soporte técnico.

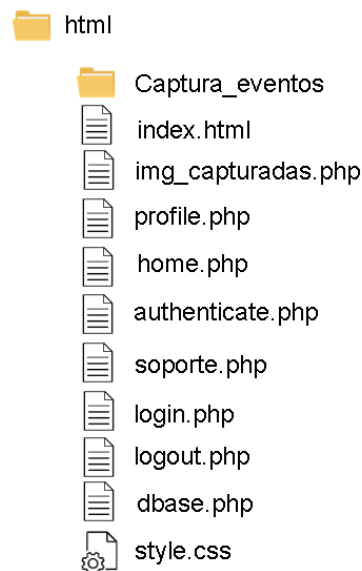


Fuente: Elaboración propia.

Una vez finalizado el proceso de diseño se inicia con el desarrollo Front-end y Back-end. La estructura del directorio que contiene la aplicación es la siguiente:

Figura 57.

Estructura del directorio de la aplicación web.



Fuente: Elaboración propia.

Para crear cada uno de estos archivos se puede ejecutar en la terminal el siguiente comando:

```
sudo nano /var/www/html/index.html
```

Se abrirá un editor de texto en donde se podrá programar el Front-end y Back-end con HTML, PHP y CSS. Para crear los demás archivos se reemplaza *index.html* con los demás nombres de los archivos que se muestran en la Figura 57.

Los archivos enlistados son fundamentales para poner en marcha a una aplicación web que brinda acceso remoto a las incidencias dentro del centro I2TEC y que está en comunicación con el script principal de Python. Esta aplicación web establece una conexión con una base de datos para garantizar la seguridad y la autenticidad de las credenciales de los usuarios. Además, la aplicación web proporciona información actualizada sobre los eventos y situaciones que se han producido en el centro I2TEC, lo que permite tomar decisiones más informadas y oportunas.

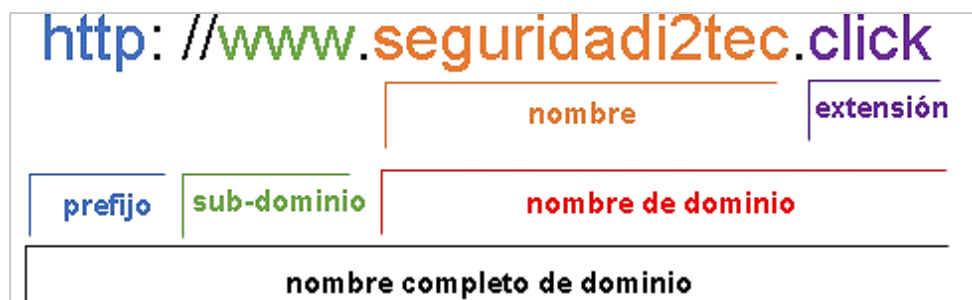
Una vez que se haya finalizado la programación de la aplicación web, se podrá acceder a ella simplemente abriendo en cualquier dispositivo con conexión a internet un navegador e ingresando la dirección IP elástica que se ha configurado en la instancia de

AWS. En este caso es, <http://54.145.71.122/>, el hecho de recordar la dirección IP para poder ingresar resulta ser un poco complicado o confuso, solucionar este inconveniente es necesario y requiere redireccionar la dirección IP a un dominio (DNS).

Para ello, se deberá adquirir un dominio con algún proveedor de servicios de registro de dominios, en este caso se optó por conseguirlo directamente desde *Amazon Route 53* (<https://us-east-1.console.aws.amazon.com/route53/v2/home#Dashboard>). En primer lugar, se comprueba la disponibilidad del nombre de dominio que se intenta registrar y se elige una extensión como por ejemplo el “.com”, “.ec”, “.org”, “.net”, “.click”, “.io”, “.info”, “.me” etc. La estructura de un dominio que se eligió se puede observar en la Figura 58.

Figura 58.

Estructura del dominio de la aplicación web.



Fuente: Elaboración propia.

Ahora bien, se debe crear un registro en AWS para especificar que el tráfico de la IP elástica se redirija al dominio que se contrató, debe quedar de la siguiente manera:

Figura 59.

Configuración de los registros en AWS.

Nombre del registro ▼	Tipo ▼	Polí... ▼	Di... ▼	Valor/Dirigir el tráfico
www.seguridadi2tec.click	A	Simple	-	54.145.71.122
seguridadi2tec.click	A	Simple	-	54.145.71.122
seguridadi2tec.click	NS	Simple	-	ns-173.awsdns-21.com ns-748.awsdns-29.net ns-1807.awsdns-33.co ns-1439.awsdns-51.or
seguridadi2tec.click	SOA	Simple	-	ns-1439.awsdns-51.or
_782e5bf2978a67c01...	CNAME	Simple	-	A3076E84114A647E9

Fuente: Elaboración propia.

Realizado esto, se puede acceder a la página web ingresando a la siguiente URL:

```
http://www.seguridadi2tec.click/
```

Una particularidad de esta URL es que la comunicación se efectúa por medio del protocolo HTTP, esta no es una forma segura de enviar y recibir datos a través de Internet ya que la información no se encuentra cifrada, en este caso los datos que se transmiten como las claves y nombres de usuarios pueden ser interceptados o leídos por personas no autorizadas. Por lo que se requiere instalar un certificado SSL.

La instalación del certificado se realizó por medio de GogetSSL. Para ello se debe generar una solicitud de firma de certificado (CSR), luego enviar la solicitud de CSR a GoGetSS, se generará un archivo de certificado, el cual se debe descargar y guardar en el servidor web (agregar un nuevo registro en AWS). A continuación, ingresar al servidor, en el directorio denominado *sites-available* que es en donde se encuentran los archivos de configuración de los sitios web, el comando es el siguiente:

```
cd /etc/apache2/sites-available/
```

Después, ejecutar los comandos:

```
> /etc/apache2/cerificate/seguridadi2tec.key  
nano /etc/apache2/cerificate/seguridadi2tec.key
```

El primero sirve para borrar el contenido que se encuentra en el archivo *seguridadi2tec.key*, el segundo comando permite abrir el archivo con el editor de texto nano, en este editor se deberá pegar la llave privada que previamente se obtuvo en GogetSSL.

```
>/etc/apache2/cerificate/AAA_Certificate_Services_seguridadi2tec.crt  
nano /etc/apache2/cerificate/seguridadi2tec.crt
```

En el editor de texto, se coloca el archivo que se descargó en GogetSSL denominado *seguridadi2tec_click.crt*.




```
nano /etc/apache2/cerificate/AAA_Certificate_Services_seguridadi2tec.crt
```

En este último editor de texto de deberá pegar el contenido de los archivos denominados *USERTrust_RSA_Certification_Authority.crt* y *GoGetSSL_RSA_DV_CA.crt*, reiniciar apache y con eso estará instalado el certificado SSL en el sitio web.

Para comprobar que el certificado instalado sea válido ingresar a la URL: <https://ssltools.godaddy.com/views/certChecker> y pegar el dominio completo, el cual es: <https://www.seguridadi2tec.click/>.

Figura 60.

Verificar la validez de certificado SSL.

IP Address (IPv4)	54.145.71.122
Server Type	Apache/2.4.29(Ubuntu)
Certificate Names	 Hostname matches  Primary Domain: seguridadi2tec.click Subject Alternative Domains: seguridadi2tec.click, www.seguridadi2tec.click
Certificate Signature Algorithm	 Sha256 With RSA Encryption

Fuente: Elaboración propia.

Finalmente, es recomendable probar el funcionamiento de cada una de las ventanas creadas, el mecanismo de autenticación se deberá probar con diferentes nombres de usuarios y contraseñas a fin de asegurarse de que el proceso de inicio de sesión funciona correctamente y de que se impiden los accesos no autorizados. También es recomendable probar la aplicación en diferentes navegadores web y dispositivos para garantizar la compatibilidad y el correcto funcionamiento en cada uno de ellos.

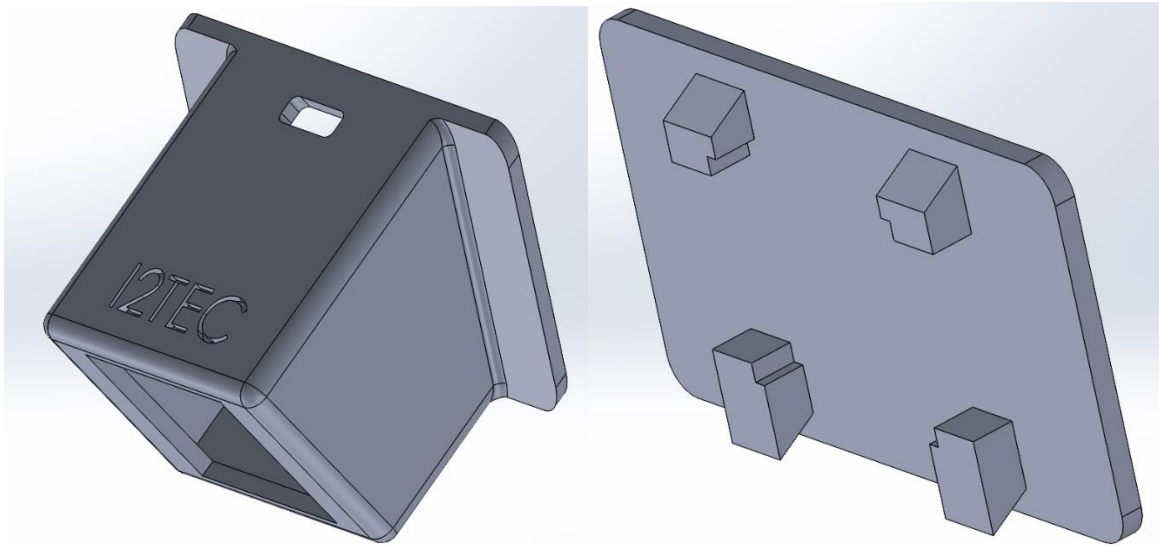
5.5.5.11 Diseño del case del prototipo.

En este proyecto se llevó a cabo el diseño de dos cases, uno para un sensor y otro para una Raspberry Pi 4. El proceso de diseño se realizó utilizando el software de diseño CAD, denominado SolidWorks, el cual permitió modelar las piezas con las medidas precisas y de manera detallada. Se tuvieron en cuenta consideraciones ergonómicas y funcionales, como la disposición de los puertos, la ventilación y la accesibilidad a los componentes.

Una vez finalizado el proceso de diseño, se procedió a imprimir los cases en una impresora 3D, lo que permitió obtener las piezas personalizadas con un acabado profesional y de alta calidad.

Figura 61.

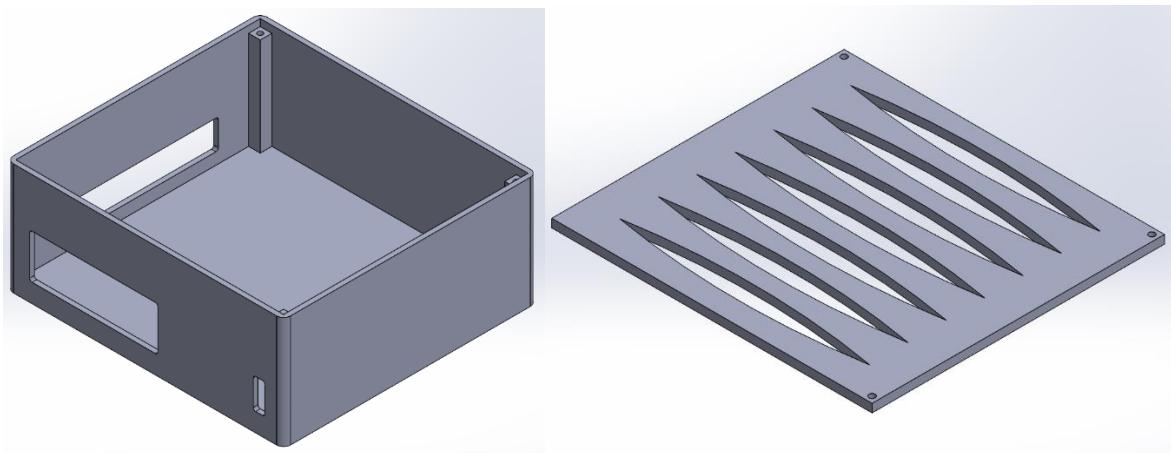
Diseño de case para sensor.



Fuente: Elaboración propia.

Figura 62.

Diseño de case para la Raspberry Pi.



Fuente: Elaboración propia.

5.5.5.12 Consideraciones de seguridad informática del prototipo.

Aquí se describen las medidas que se tomaron en cuenta para proteger la seguridad informática del prototipo.

- **Contraseñas seguras:** es importante utilizar contraseñas seguras tanto en la Raspberry Pi como en los demás servidores que se utilizan. Las contraseñas deben ser complejas, se puede utilizar una combinación de letras mayúsculas

y minúsculas, números y caracteres especiales para evitar que se descifren mediante técnicas de fuerza bruta u otras técnicas de hacking. Se recomienda utilizar una herramienta disponible en línea, como *Kaspersky Password Checker* (<https://password.kaspersky.com/es/>), para verificar el nivel de seguridad de las contraseñas.

- Actualizaciones de software: es importante mantener el software actualizado, ya que las actualizaciones muchas de las veces contienen parches de seguridad que corrigen vulnerabilidades ya conocidas.
- Navegación segura: el hecho de no descargar archivos de fuentes desconocidas o sospechosas es una medida importante para evitar la propagación de malware.
- Crear copias de seguridad: es fundamental crear copias de seguridad para protegerse contra la pérdida de datos causada por errores involuntarios o ataques cibernéticos. Realizar regularmente copias de seguridad asegura que, en caso de una eventualidad, se pueda recuperar la información. Esto es especialmente importante para los datos sensibles o críticos, como los scripts de Python, código fuente de la aplicación web o las contraseñas. La creación de copias de seguridad también garantiza que se pueda restaurar el sistema en caso de una falla del hardware o software.
- Usar la autenticación de dos factores: se utilizó este método para que sea difícil para los hackers acceder a la plataforma de correo electrónico y a la plataforma en la nube para lanzar el servidor (AWS).
- Acceso restringido: para acceder a las Raspberry se configuró un Id y una contraseña, para acceder al servidor en la nube se requiere de la llave única en formato ppk (la cual no se deberá compartir para evitar que terceros puedan modificar las configuraciones) y para ingresar a la aplicación web se requiere de las credenciales que fueron creadas y almacenadas en Mysql.
- Encriptación de datos: en la aplicación web se instaló un certificado SSL para habilitar la encriptación de las credenciales que se transfieren entre el servidor y el navegador del usuario.
- Uso de Fail2Ban: se empleó esta herramienta de seguridad para la prevención de ataques de fuerza bruta, ya que bloquea automáticamente la dirección IP del posible atacante.
- Uso de la función `bind_param()` en PHP para prevenir la inyección SQL en la aplicación web.

6. Resultados

6.1 Descripción general del sistema de seguridad inteligente

La propuesta consistió en desarrollar un prototipo que permita analizar y detectar la presencia de posibles intrusos en las instalaciones del centro de investigación, innovación, desarrollo de prototipos tecnológicos y pruebas electroenergéticas I2TEC de la UNIVERSIDAD NACIONAL DE LOJA. A partir de ello, se podrá capturar una imagen del posible suceso en donde se desarrollen intrusiones, para posteriormente transferir esa imagen desde la Raspberry Pi hacia una cuenta de correo electrónico de la persona encargada del laboratorio. O a su vez, se registre la hora y fecha del posible evento suscitado y se cargue esta información a una base de datos, de igual manera la captura de la imagen se suba a un servidor en la nube y conjuntamente se puedan mostrar estos datos en una aplicación web que estará limitada su acceso únicamente con las credenciales válidas.

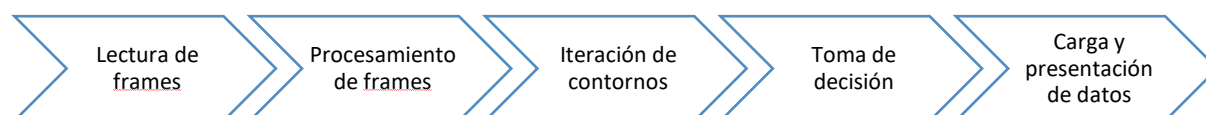
Es importante mencionar que el prototipo podría configurarse para que entre en funcionamiento a partir de un horario específico, en el que las cifras de los robos se producen con mayor frecuencia, o a su vez se pueda configurar la hora de activación que se crea conveniente mediante una interfaz gráfica. Además, se agregó un sensor de movimiento para mayor solidez del sistema y una sirena que actúa como medida disuasiva en el caso de que se susciten actos delictivos.

La visión artificial se aplicó en el procesamiento, tratamiento y análisis de imágenes a través de algoritmos escritos en Python. Las técnicas que se utilizaron para la detección de movimiento no consumen demasiados recursos, esto es beneficioso para que no ocurra ningún problema al ejecutar el script desde la Raspberry Pi, además las técnicas son rápidas, pero pueden ser susceptibles a errores cuando hay cambios bruscos de iluminación o cuando el objeto en movimiento es muy pequeño; pero para solventar este inconveniente se ubicó un sensor PIR estratégicamente, lo cual aumentó significativamente la eficiencia del sistema de seguridad.

El funcionamiento del prototipo se dividió en cinco etapas, las cuales se muestran en la siguiente figura:

Figura 63.

Etapas de funcionamiento del prototipo.



Fuente: Elaboración propia.

6.2 Resultados estadísticos de la encuesta

Para el cálculo del tamaño de la muestra se utilizó la siguiente ecuación:

$$n = \frac{N * z^2 * p * q}{(N-1)e^2 + z^2 * p * q} \quad (1)$$

Donde:

n = tamaño de la muestra

N = población

z = porcentaje de certeza

p = probabilidad de éxito

q = probabilidad de fracaso

e = error de estimación máximo aceptado

- Para determinar la población se consideró un total de 214855 habitantes del cantón Loja según el censo del 2010, de ese total de habitantes únicamente se consideró a aquellas personas que estén entre 25 y 59 años, el cual representa aproximadamente el 37%; dando un resultado de 79496 personas.
- El valor recomendado para el porcentaje de certeza o nivel de confianza es del 95% que representa un valor $z=1.96$.
- Dado que se desconoce la probabilidad de que ocurra o no el evento estudiado, se asigna un 50% a p y un 50% a q .
- El error de estimación máximo aceptado (e) representa el límite aceptable de error muestral, el valor estándar va de entre 1 a 10%, para este caso se seleccionó 7.5% (0.075).

$$n = \frac{79496 * 1.96^2 * 0.5 * 0.5}{(79496 - 1)0.075^2 + 1.96^2 * 0.5 * 0.5}$$

$$n = 170,3739; \quad \boxed{n \approx 171}$$

Al aplicar la ecuación se obtuvo que el tamaño de la muestra debe ser de 171 personas encuestadas.

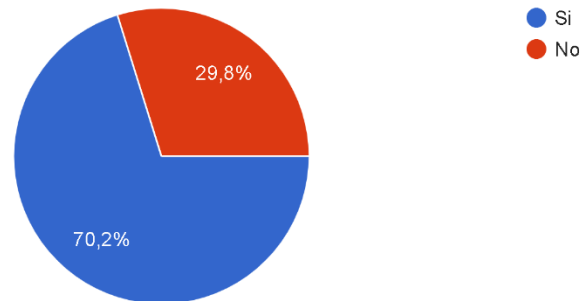
Los resultados se presentan en gráficos que muestran la distribución de las respuestas a cada una de las preguntas de la encuesta.

Figura 64.

Resultado de la pregunta 1.

1. ¿Conoce usted lo que es un sistema de seguridad contra robos e intrusiones?

171 respuestas



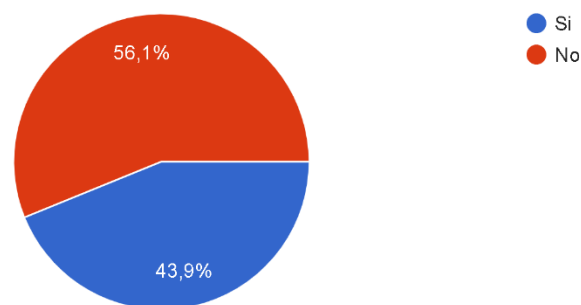
Fuente: Elaboración propia.

Figura 65.

Resultado de la pregunta 2.

2. ¿Entiende usted las diferencias entre un sistema de seguridad pasivo y un sistema de seguridad activo?

171 respuestas



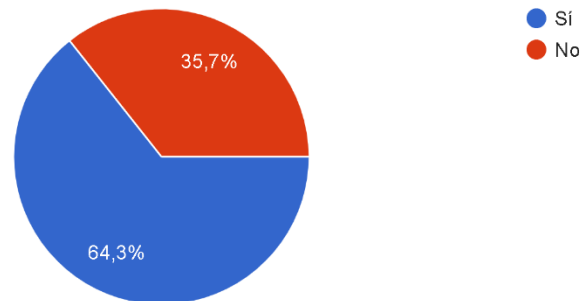
Fuente: Elaboración propia.

Figura 66.

Resultado de la pregunta 3.

3. ¿Está consciente de los beneficios que ofrecen los sistemas de seguridad activos en la prevención de robos o intrusiones?

171 respuestas



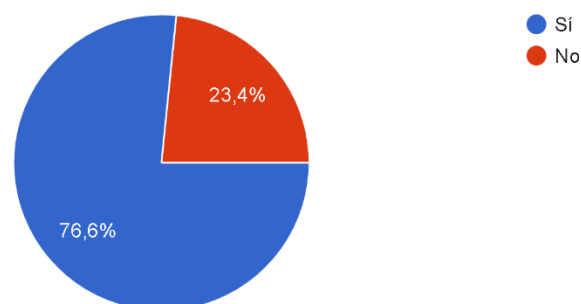
Fuente: Elaboración propia.

Figura 67.

Resultado de la pregunta 4.

4. ¿Ha oído hablar de múltiples dispositivos como sensores, cámaras, actuadores que se pudiesen utilizar en distintos sistemas de seguridad?

171 respuestas



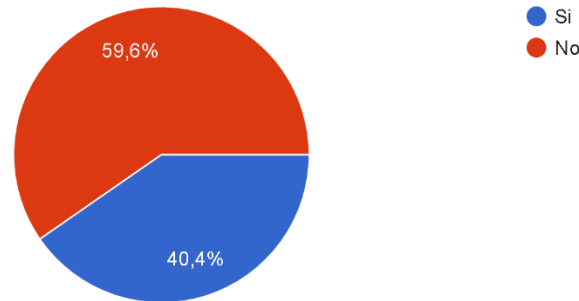
Fuente: Elaboración propia.

Figura 68.

Resultado de la pregunta 5.

5. ¿Ha oído hablar de la visión artificial y su contribución en el desarrollo de sistemas de seguridad inteligentes?

171 respuestas



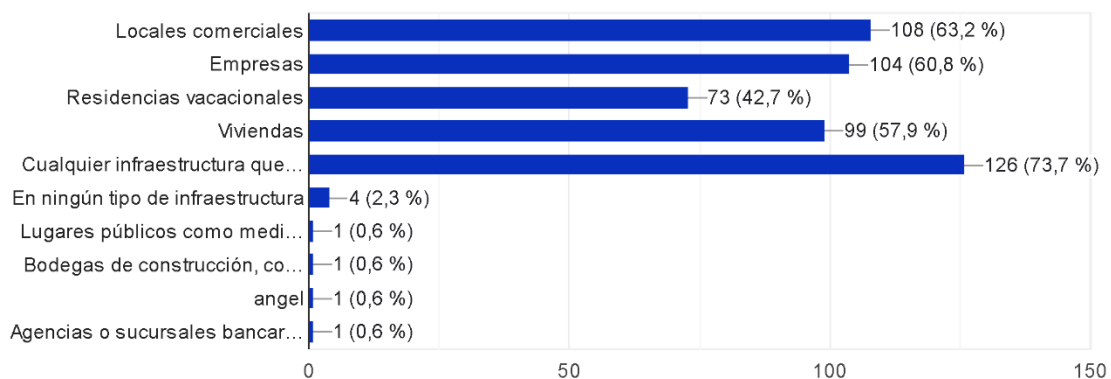
Fuente: Elaboración propia.

Figura 69.

Resultado de la pregunta 6.

6. Seleccione una o varias respuestas. ¿En qué tipo de infraestructuras cree usted que es necesario instalar un sistema de seguridad?

171 respuestas



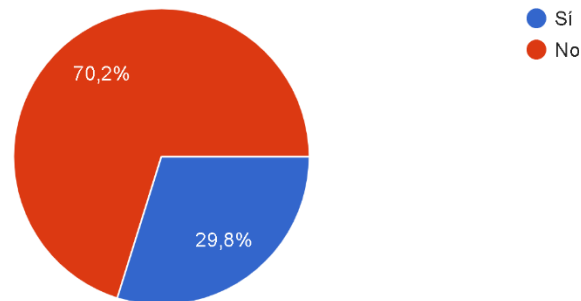
Fuente: Elaboración propia.

Figura 70.

Resultado de la pregunta 7.

7. ¿Cuenta con algún sistema de seguridad para prevenir robos o intrusiones en cualquier tipo de infraestructura?

171 respuestas



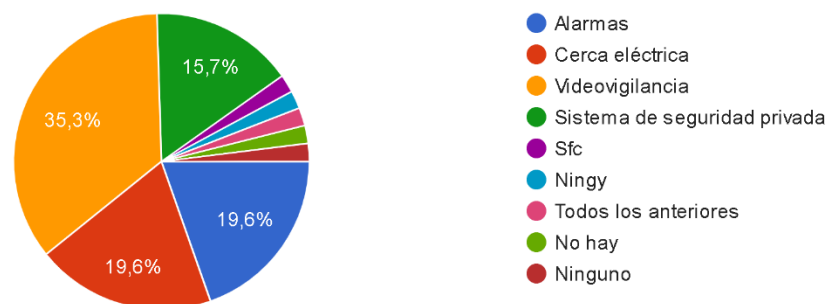
Fuente: Elaboración propia.

Figura 71.

Resultado de la pregunta 8.

8. **Si su respuesta anterior fue sí.** Indique: ¿Con cuál de los siguientes sistemas de seguridad cuenta?

51 respuestas



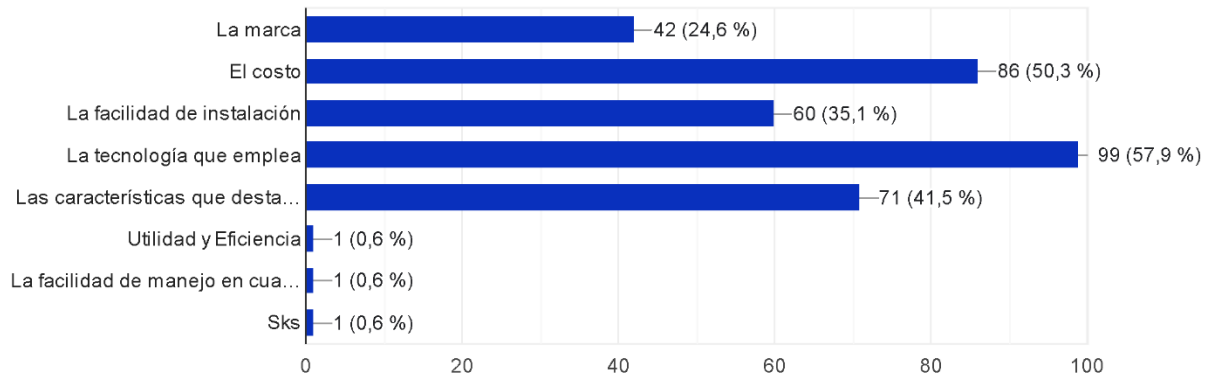
Fuente: Elaboración propia.

Figura 72.

Resultado de la pregunta 9.

9. Seleccione una o varias respuestas. ¿Al momento de adquirir un sistema de seguridad, que es lo primero que tiene en cuenta?

171 respuestas



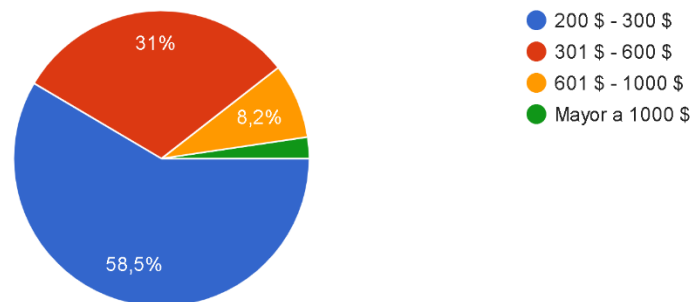
Fuente: Elaboración propia.

Figura 73.

Resultado de la pregunta 10.

10. ¿Cuál es el rango de precios que usted estaría dispuesto a pagar por un sistema de seguridad activo, con tecnología moderna y de altas prestaciones?

171 respuestas



Fuente: Elaboración propia.

El análisis de los resultados reveló que la mayoría de las personas conocen lo que es un sistema de seguridad, sin embargo, el 70.2% de las personas encuestadas no cuentan con un sistema de seguridad de ningún tipo. La encuesta también reveló que existe desconocimiento acerca de la visión artificial en apoyo a los sistemas de seguridad. Además, lo que los consumidores tienen o tendrían en cuenta al momento de adquirir un sistema de seguridad es: la tecnología que se emplea, el costo y las características que destacan del sistema.

Finalmente, la encuesta dio a conocer que la gran mayoría de las personas toman mucho en cuenta el factor económico, debido a que el 58.5% estaría dispuesta a pagar entre 200 a 300 dólares por un sistema de seguridad activo, con tecnología moderna y de altas prestaciones.

6.3 Pruebas de funcionamiento del prototipo

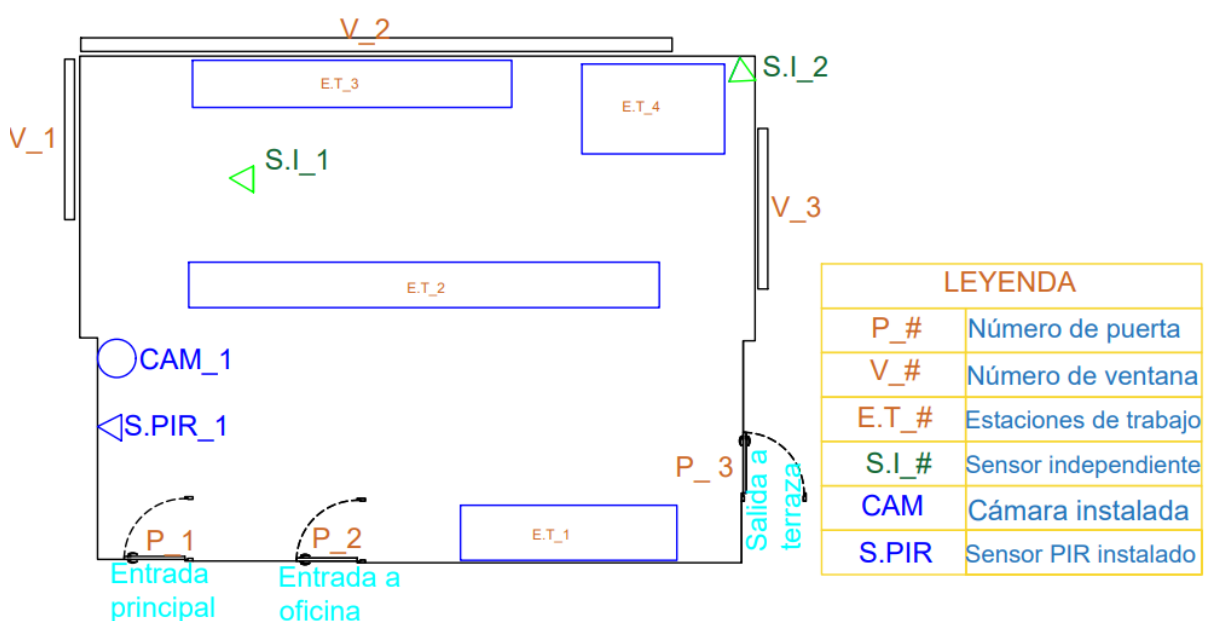
Los aspectos que se deben tener en cuenta en la instalación del prototipo son:

- Se necesita de una conexión eléctrica para conectar el dispositivo.
- La Raspberry Pi 4 B tiene que estar conectada a internet, la conexión puede ser mediante WiFi o Ethernet.
- Se necesita de cable AWG 22 para la conexión al sensor y al relé.
- Para la instalación de la cámara, sensor y Raspberry Pi, se requiere de case con orificios para poder fijarlos en la pared.
- Las configuraciones iniciales requieren de una computadora/smartphone con Teamviewer instalado.

En la Figura 74 se puede apreciar el plano del centro I2TEC, en donde se muestra la disposición de puertas, ventanas y demás elementos relevantes que se encuentran en el centro. Además, se detalla la ubicación de los dispositivos que se han instalado. Sin embargo, por razones de seguridad, no se revela la ubicación exacta del microordenador, ya que es de vital importancia mantenerlo resguardado en un lugar seguro.

Figura 74.

Plano del centro I2TEC.



Fuente: Elaboración propia.

Figura 75.

Prototipo instalado.



Fuente: Elaboración propia.

En las imágenes posteriores se podrá evidenciar la configuración inicial del sistema, el ingreso a la aplicación web con las credenciales únicas, el contenido de la aplicación web, los mensajes de alerta que se envían por correo electrónico y el respaldo de todos los eventos capturados.

Figura 76.

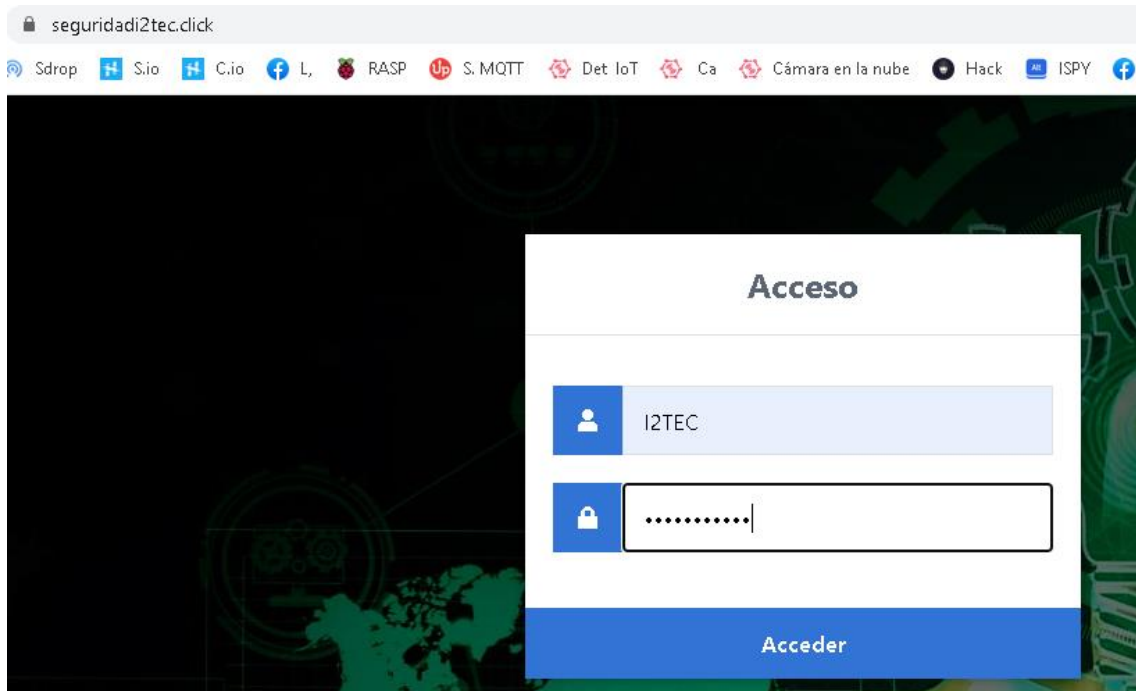
Configuración del horario de activación.



Fuente: Elaboración propia.

Figura 77.

Prueba de la aplicación web.



Fuente: Elaboración propia.

Figura 78.

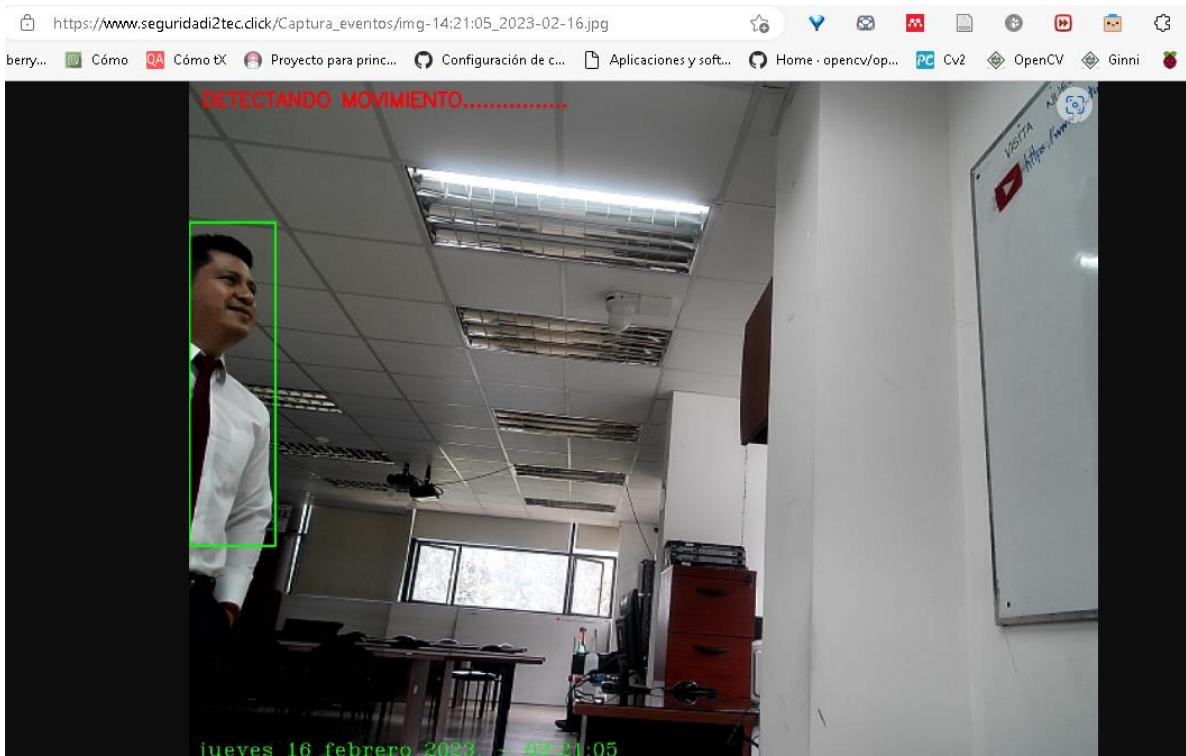
Ingreso exitoso a la aplicación web.



Fuente: Elaboración propia.

Figura 79.

Imagen cargada a la aplicación web.



Fuente: Elaboración propia.

Figura 80.

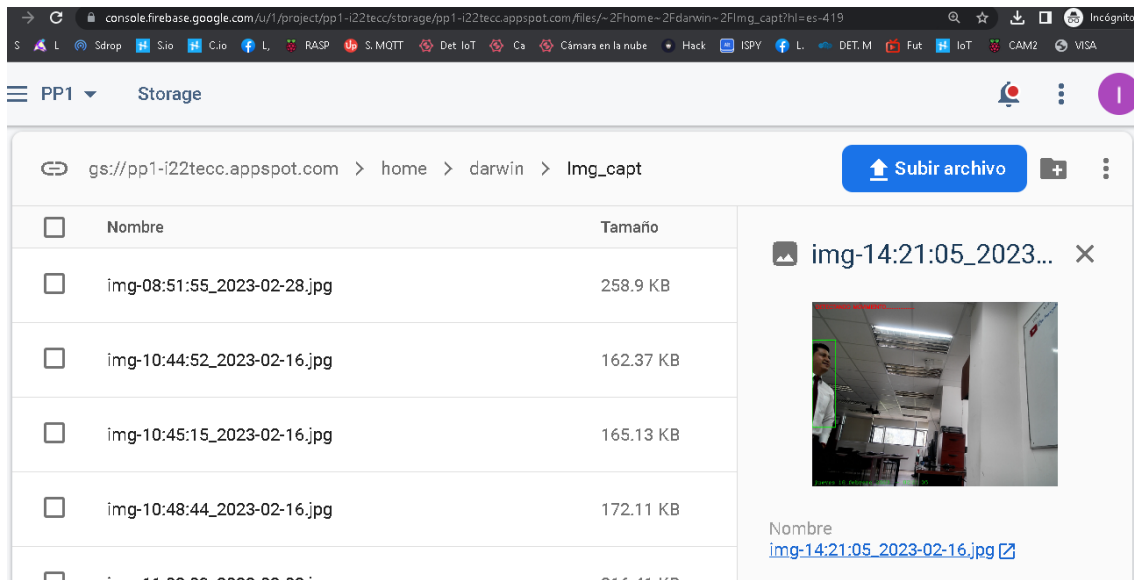
Mensaje de alerta por correo electrónico.



Fuente: Elaboración propia.

Figura 81.

Respaldo de las imágenes en Firebase.



Fuente: Elaboración propia.

En la Tabla 9 se resumen cada una de las pruebas realizadas en días, horarios, escenarios y condiciones diferentes; con el fin de poder evaluar la actuación y el funcionamiento del prototipo basándose en la cantidad total de pruebas efectuadas, la cantidad de detecciones realizadas correctamente y a los fallos que se registraron.

Tabla 9.

Resultados de pruebas de funcionamiento del prototipo.

N°	Fecha	Hora	¿Ocurrió intrusión?	¿Se activo la iluminación?	¿Se registro la intrusión?
001	16-02-2023	13:59:11	Si	Si	Si
002	16-02-2023	14:21:05	Si	Si	Si
003	16-02-2023	14:21:41	Si	Si	Si
004	16-02-2023	14:22:16	Si	Si	Si
005	16-02-2023	15:28:39	Si	Si	Si
006	16-02-2023	15:28:58	Si	Si	Si
007	16-02-2023	15:29:23	Si	Si	Si
008	16-02-2023	15:30:09	Si	Si	Si
009	16-02-2023	15:30:39	Si	Si	Si
010	16-02-2023	15:31:19	No	No	Si
011	16-02-2023	15:31:31	Si	Si	Si
012	16-02-2023	15:32:01	Si	Si	Si
013	16-02-2023	15:32:14	Si	Si	Si
014	16-02-2023	15:34:15	Si	Si	Si
015	16-02-2023	15:34:28	Si	Si	Si
016	16-02-2023	15:35:10	Si	Si	Si
017	16-02-2023	15:35:52	Si	Si	Si
018	16-02-2023	15:36:30	Si	Si	Si
019	16-02-2023	15:36:47	Si	Si	Si
020	16-02-2023	15:36:59	Si	Si	Si
021	16-02-2023	15:37:12	Si	Si	Si
022	16-02-2023	15:37:25	Si	Si	Si
023	16-02-2023	15:37:40	Si	Si	Si
024	16-02-2023	15:37:53	Si	Si	Si
025	16-02-2023	15:38:09	Si	Si	Si
026	16-02-2023	15:38:23	Si	Si	Si
027	16-02-2023	15:40:01	Si	Si	Si
028	16-02-2023	15:40:27	Si	Si	Si
029	16-02-2023	15:42:13	Si	Si	Si
030	16-02-2023	15:43:28	Si	Si	Si
031	16-02-2023	15:47:15	Si	Si	Si
032	16-02-2023	15:53:16	Si	Si	Si
033	16-02-2023	15:56:47	Si	Si	Si
034	16-02-2023	15:57:00	Si	Si	Si
035	16-02-2023	15:58:07	Si	Si	Si
036	16-02-2023	16:03:53	Si	Si	Si
037	16-02-2023	16:15:11	No	No	No
038	16-02-2023	16:43:30	Si	Si	Si
039	16-02-2023	16:51:36	Si	Si	Si
040	16-02-2023	16:57:02	Si	Si	Si
041	22-02-2023	14:50:44	Si	Si	Si
042	22-02-2023	15:07:50	Si	Si	Si
043	22-02-2023	15:08:13	Si	Si	Si
044	22-02-2023	15:11:05	Si	Si	Si
045	22-02-2023	15:12:21	Si	Si	Si
046	22-02-2023	15:36:44	Si	Si	Si
047	22-02-2023	15:40:09	Si	Si	Si
048	22-02-2023	15:44:42	Si	Si	Si
049	22-02-2023	15:46:46	Si	Si	Si
050	22-02-2023	15:47:00	Si	Si	Si
051	22-02-2023	15:50:02	Si	Si	Si
052	22-02-2023	15:50:29	Si	Si	Si

053	22-02-2023	15:52:07	Si	Si	Si
054	22-02-2023	15:52:35	Si	Si	Si
055	22-02-2023	15:53:23	Si	Si	Si
056	22-02-2023	15:54:32	Si	Si	Si
057	22-02-2023	15:54:57	Si	Si	Si
058	22-02-2023	15:55:18	Si	Si	Si
059	22-02-2023	15:56:02	Si	Si	Si
060	23-02-2023	09:05:06	No	No	No
061	23-02-2023	12:56:04	No	No	No
062	23-02-2023	14:40:24	Si	Si	Si
063	23-02-2023	15:50:15	Si	Si	Si
064	28-02-2023	08:52:05	Si	Si	Si
065	28-02-2023	16:28:38	Si	Si	Si
066	28-02-2023	16:29:03	Si	Si	Si
067	28-02-2023	16:29:25	Si	Si	Si
068	28-02-2023	16:30:03	Si	Si	Si
069	28-02-2023	16:30:35	Si	Si	Si
070	28-02-2023	16:30:50	Si	Si	Si
071	28-02-2023	16:31:04	Si	Si	Si
072	28-02-2023	16:47:16	Si	Si	Si
073	28-02-2023	16:49:32	Si	Si	Si
074	28-02-2023	16:50:08	Si	Si	Si
075	28-02-2023	16:54:40	Si	Si	Si
076	28-02-2023	20:03:40	No	No	Si
077	02-03-2023	11:02:18	Si	Si	Si
078	02-03-2023	11:02:55	Si	Si	Si
079	02-03-2023	11:03:09	Si	Si	Si
080	02-03-2023	11:04:51	Si	Si	Si
081	02-03-2023	11:05:16	Si	Si	Si
082	09-03-2023	11:05:28	Si	Si	Si
083	09-03-2023	17:54:16	Si	Si	Si
084	09-03-2023	17:55:23	Si	Si	Si
085	09-03-2023	17:56:21	Si	Si	Si
086	09-03-2023	17:57:05	Si	Si	Si
087	09-03-2023	18:00:07	Si	Si	Si
088	09-03-2023	18:01:21	Si	Si	Si
089	09-03-2023	18:06:22	Si	Si	Si
090	09-03-2023	18:07:10	Si	Si	Si
091	09-03-2023	18:08:24	Si	Si	Si
092	09-03-2023	18:09:11	Si	Si	Si
093	09-03-2023	18:09:56	Si	Si	Si
094	09-03-2023	18:10:23	Si	Si	Si
095	09-03-2023	18:10:42	Si	Si	Si
096	09-03-2023	18:11:06	Si	Si	Si
097	09-03-2023	18:11:24	Si	Si	Si
098	09-03-2023	21:15:23	No	No	No
099	14-03-2023	17:13:08	Si	Si	Si
100	14-03-2023	17:13:42	Si	Si	Si
101	14-03-2023	17:14:11	Si	Si	Si
102	14-03-2023	17:14:29	Si	Si	Si
103	14-03-2023	17:14:58	Si	Si	Si
104	14-03-2023	17:15:13	Si	Si	Si
105	14-03-2023	17:15:41	Si	Si	Si
106	14-03-2023	17:15:56	Si	Si	Si
107	14-03-2023	17:16:33	Si	Si	Si
108	14-03-2023	17:17:18	Si	Si	Si
109	14-03-2023	17:17:33	Si	Si	Si

110	14-03-2023	17:18:22	Si	Si	Si
111	14-03-2023	17:18:51	Si	Si	Si
112	14-03-2023	17:34:51	Si	Si	Si
113	14-03-2023	17:49:51	Si	Si	Si
114	14-03-2023	17:50:47	Si	Si	Si
115	14-03-2023	17:53:31	Si	Si	Si
116	14-03-2023	17:54:22	Si	Si	Si
117	14-03-2023	17:55:18	Si	Si	Si
118	14-03-2023	17:56:15	Si	Si	Si
119	14-03-2023	17:57:46	Si	Si	Si
120	14-03-2023	17:58:18	Si	Si	Si
121	14-03-2023	17:59:13	Si	Si	Si
122	14-03-2023	18:00:09	Si	Si	Si
123	14-03-2023	18:01:43	Si	Si	Si
124	14-03-2023	18:02:10	Si	Si	Si
125	22-03-2023	08:30:45	No	No	No
126	22-03-2023	12:20:16	No	No	No
127	22-03-2023	22:34:11	No	No	No
128	05-04-2021	17:16:40	Si	Si	Si
129	05-04-2021	17:18:55	Si	Si	Si
130	05-04-2021	17:19:44	Si	Si	Si
131	05-04-2021	17:21:40	Si	Si	Si
132	05-04-2021	19:04:43	Si	Si	No
133	05-04-2021	20:56:32	No	No	No
134	13-04-2023	21:29:01	No	No	No
135	13-04-2023	21:35:10	No	No	No
136	24-04-2023	08:04:36	Si	Si	Si
137	24-04-2023	08:05:55	Si	Si	Si
138	03-05-2023	15:26:06	Si	Si	Si
139	03-05-2023	15:27:35	Si	Si	Si
140	03-05-2023	15:28:23	Si	Si	Si
141	08-05-2023	05:23:13	No	No	No
142	11-05-2023	16:38:51	Si	Si	Si
143	11-05-2023	16:40:52	Si	Si	Si
144	11-05-2023	16:42:12	Si	Si	Si
145	16-05-2023	14:11:44	Si	Si	Si
146	16-05-2023	14:15:05	Si	Si	Si
147	16-05-2023	14:16:27	Si	Si	Si
148	16-05-2023	14:18:36	Si	Si	Si
149	16-05-2023	14:19:14	Si	Si	Si
150	16-05-2023	14:20:19	Si	Si	Si
151	16-05-2023	14:21:23	Si	Si	Si
152	16-05-2023	14:22:07	Si	Si	Si
153	16-05-2023	14:23:08	Si	Si	Si
154	16-05-2023	14:24:24	Si	Si	Si
155	16-05-2023	14:24:51	Si	Si	Si
156	16-05-2023	15:25:06	Si	Si	Si
157	16-05-2023	15:25:14	Si	Si	Si
158	16-05-2023	15:25:21	Si	Si	Si
159	19-05-2023	05:46:24	No	No	No
160	19-05-2023	06:02:23	No	No	No
161	19-05-2023	06:08:02	No	No	No
162	19-05-2023	06:12:06	No	No	No
163	19-05-2023	06:16:49	No	No	No
164	19-05-2023	06:16:58	No	No	No

Fuente: Elaboración propia.

Los datos recopilados en la Tabla 9 proporcionan una visión clara y cuantitativa del desempeño del prototipo en diversos escenarios y condiciones. Los resultados son fundamentales para evaluar la eficacia y confiabilidad del sistema, así como para identificar posibles mejoras. Los cálculos realizados a partir de las pruebas efectuadas revelan que el sistema cuenta con una efectividad del 98.17%. Este porcentaje demuestra que el sistema cuenta con una alta efectividad en detecciones.

6.4 Presupuesto del prototipo y comparación con otros sistemas de seguridad

En la Tabla 10 se detalla el valor de cada uno de los rubros necesarios para el despliegue del sistema de seguridad inteligente, esto con la finalidad de comparar con valores que se han cotizado (Anexo 2) de los sistemas de seguridad más comerciales y más solicitados. Lo cual ayuda para tener una visión clara de la factibilidad de la implementación, tomando en cuenta que según la encuesta realizada el 58.5% de las personas encuestadas estarían dispuestas a invertir entre 200 a 300 dólares en un sistema de seguridad.

Tabla 10.

Presupuesto aproximado del proyecto.

DENOMINACIÓN DEL RUBRO	Unidades	Cantidad	Precio unitario (\$)	Precio Total (\$)
-Kit Raspberry Pi 4 2GB Modelo B+	U	1	120.00	120.00
-Cámara AVMP	U	1	42.00	42.00
-Modulo Sensor De Movimiento	U	1	4.40	4.40
-Alarma de 110dB	U	1	16.50	16.50
-Case - sensor PIR	U	1	3.00	3.00
-Case - Raspberry	U	1	7.00	7.00
-Relé 5V- 2 canales	U	1	4.00	4.00
-Jumpers para Raspberry	U	7	0.10	0.70
-Tornillo de pared + taco Fisher	U	4	0.05	0.20
-Tornillo + tuerca	U	8	0.05	0.40
-Cinta termoretráctil	m	1	0.40	0.40
-Imprevistos	U	1	10.00	10.00
-Costos importación	U	1	14.50	14.50
-Costo de DNS	U	1	5.00	5.00
			Total	228.10

Fuente: Elaboración propia.

Tabla 11.

Comparación de sistemas de seguridad comerciales con el sistema propuesto.

Sistema de seguridad	Características principales	Ventajas	Desventajas	Rango de costos \$
Sistemas de seguridad con CCTV	Incluye cámaras de videovigilancia, grabación de videos	Proporciona revisión de las grabaciones y monitoreo	Requiere de NVR para poder funcionar, instalación complicada	432-480 (varía según el número de cámaras)
Sistema de alarma tradicional	Incluye panel de control, sensores de puertas y ventanas, alarmas	Fácil de instalar, ampliamente utilizado	Genera varias falsas alarmas, no dispone de monitoreo ni de grabaciones	130 -250 (varía según la marca y número de zonas)
Sistema de seguridad con control de acceso	Incluye lectores biométricos o cerraduras electrónicas	Restringe el acceso no autorizado, registra la entrada y salida de personas	Requiere constante configuración de credenciales o tarjetas, no dispone de monitoreo ni de grabaciones	150-290 (varía según la marca)
Sistemas de seguridad con cercas eléctricas	Incluye cercas electrificadas que generan descargas eléctricas al ser tocadas	Disuade a los intrusos, crea una barrera física de seguridad	No protege las entradas principales, costos de mantenimiento elevados, se debe vigilar que niños o animales no se acerquen a ellas	200-350 (varía según la cantidad)
Sistemas de seguridad con visión artificial	Incluye cámaras con capacidades de reconocimiento facial, detección de objetos	Mayor precisión en la detección de intrusos	Para tener mayor precisión requiere entrenamiento, y configuración para un correcto funcionamiento	680-2000 (varía según la marca y sus capacidades)
Sistema de seguridad inteligente planteado en esta investigación	Incluye un microcomputador de bajo costo que realiza todo el proceso de visión artificial	Mayor precisión en la detección de intrusos, cuenta con control de iluminación para capturar imágenes en las horas de la noche y permite la visualización de las incidencias en una aplicación web	Requiere de una buena conexión a internet para asegurar que las imágenes y las alertas se den de manera inmediata	218.10 (valor de todos los rubros necesarios para la implementación)

Fuente: Elaboración propia

7. Discusión

La implementación del sistema de seguridad inteligente y activo en el centro I2TEC de la UNL representa una solución tecnológica innovadora que permitirá garantizar la protección de las instalaciones y equipos. Con la implementación de este sistema, se podrán detectar rápidamente y en el mejor de los casos prevenir incidentes de manera eficiente, por el hecho de que, a diferencia de CCTV, este sistema está en la capacidad de detectar la presencia de personas no autorizadas en un área de interés mediante las técnicas de visión artificial y alertar de manera inmediata.

El prototipo de sistema de seguridad inteligente se configura de manera sencilla e intuitiva. Este sistema se integra con una aplicación web que brinda a los usuarios acceso desde cualquier dispositivo a las imágenes capturadas y permite monitorear eventos anómalos en tiempo real. Asimismo, se ha establecido una conexión con una base de datos para almacenar los datos y generar informes de los eventos registrados. Esta integración y funcionalidad proporcionan una experiencia completa y eficiente para el monitoreo y la gestión de la seguridad.

Durante las exhaustivas pruebas de funcionamiento, se determinó que el sistema exhibe un impresionante nivel de efectividad del 98.17%. Esto se traduce en que, del total de pruebas realizadas en diversas ocasiones, condiciones y horarios, se obtuvieron tres resultados incorrectos. Estos resultados pueden ser contrastados con investigaciones previas, como es el caso del estudio realizado por Masgo (2020) donde se observó una efectividad del sistema de seguridad del 92%. Estos resultados validan la robustez y confiabilidad del sistema diseñado e implementado en esta investigación, respaldando la capacidad para cumplir con precisión su objetivo de detección y respuesta inmediata.

Una particularidad que se abordó desde esta investigación es la posibilidad de permitir la interoperabilidad de cámaras en sistemas de visión por computador, es decir que el mismo script puede funcionar tanto como para los distintos módulos de cámaras propiamente contruidos para Raspberry Pi como para cámaras web o incluso con cámaras Ip. Esto simplifica significativamente el proceso de configuración y puesta en marcha del sistema de seguridad, permitiendo a los usuarios aprovechar al máximo la funcionalidad del script sin preocuparse por la compatibilidad de la cámara. En las diferentes investigaciones que se han revisado como es el caso de Espinoza (2022) y Valiente (2019), se evidenció que el código principal únicamente funciona para un solo tipo de cámaras, de manera que si se intenta implementar el sistema con una cámara diferente el sistema no funcionará.

A diferencia de otras investigaciones relacionadas con el tema planteado, en la presente se consideró importante añadir aspectos de seguridad informática como restricción del acceso con un login, encriptación de datos con el protocolo SSL, uso de fail2ban para la detección y prevención de ataques de fuerza bruta hacia el dispositivo central, uso de contraseñas robustas, creación de copias de seguridad y prevención de inyección SQL. Todas las acciones que se tomaron en cuenta se enfocan en salvaguardar la confidencialidad, integridad y disponibilidad de la información, de manera que se pueda prevenir cualquier intento de manipulación del sistema o acceso no autorizado.

Cada uno de los componentes que se emplean han sido seleccionados convenientemente con el objetivo de lograr un sistema robusto, confiable y que ofrezca ventajas significativas en comparación con otros sistemas implementados. En investigaciones previas realizadas por Rodríguez (2019), se emplearon únicamente sensores de movimiento, alarmas sonoras y una central de control. Si bien estos elementos contribuyen a mejorar la seguridad de un lugar, no se obtienen resultados tan precisos como con un sistema de seguridad que incluye cámaras, control de iluminación para mejorar las imágenes capturadas y técnicas de visión artificial para la actuación del sistema.

Uno de los aspectos de alta relevancia para la implementación del sistema es el aspecto económico, el cual es bastante favorable en comparación con sistemas comerciales que se han cotizado. En la investigación de Ortega (2022) se evidenció que el costo de los respectivos rubros para la implementación de un sistema de detección y reconocimiento de intrusos aplicado a sistemas de video vigilancia alcanzó un valor final de 913.87 dólares sin considerar los costos que implican la mano de obra, valor que según las encuestas realizadas solo el 8.2% de las personas estarían dispuestas a pagar. Esta diferencia significativa en los costos se debe principalmente a la utilización de software y/o hardware de open source, al lograr un equilibrio entre el costo y el rendimiento, se abre la posibilidad de implementar sistemas de seguridad con visión artificial en una variedad de entornos y aplicaciones.

La implementación de este prototipo de sistema de seguridad inteligente representa un importante avance en la mejora de la seguridad en el centro I2TEC de la UNL, ya que es el único sistema de seguridad que se encuentra funcionando en dicho centro, así mismo, se dan a conocer las bases para el desarrollo e implementación de futuros sistemas de seguridad inteligentes en cualquier tipo de infraestructura.

8. Conclusiones

- En el presente trabajo de titulación se logró el diseño e implementación exitosa de un prototipo de sistema de seguridad inteligente y activo, basado en técnicas de visión artificial, para fortalecer la seguridad de los bienes que se encuentran en el centro I2TEC.
- Como resultado de la evaluación exhaustiva realizada en el centro I2TEC, se pudo identificar cuidadosamente las características del entorno, la disposición de las puertas, ventanas, las zonas más vulnerables y las posibles vías de acceso no autorizadas. En base a los hallazgos, se propusieron medidas rigurosas como utilización de sensores para proteger de mejor manera el área contra las intrusiones.
- La implementación del sistema de seguridad propuesto destaca por su aspecto económico altamente favorable en comparación con sistemas comerciales y demás sistemas propuestos en investigaciones. La investigación y el uso de las respectivas herramientas de software y hardware open source contribuyeron a que se redujeran los costos finales, de manera que las posibilidades para que las personas puedan optar por este sistema aumentan considerablemente.
- La configuración del sistema destaca por su facilidad de uso y su simplicidad. La integración de la aplicación web y de un sistema de alerta inmediata mediante el protocolo SMTP permite a los usuarios tener un control de las incidencias ocurridas de manera rápida y segura. Además, el monitoreo en tiempo real permite supervisar de forma continua los eventos capturados por la cámara. Esta combinación de integración y funcionalidad proporciona una mayor capacidad de respuesta ante situaciones de seguridad y se logra una solución efectiva para garantizar la respuesta rápida ante situaciones de riesgo.
- Los resultados de las pruebas preliminares indicaron que el factor de iluminación juega un rol importante a la hora de capturar imágenes en horas de la noche, para abordar esta situación se incluyó un sistema de control de iluminación que permite activar la iluminación del centro al detectar la presencia de un intruso. Esta solución permitió mejorar las imágenes en condiciones de baja luminosidad y según las pruebas finales se obtuvo una efectividad del 98.17%.
- La elaboración minuciosamente de los manuales de uso y de mantenimiento del sistema de seguridad inteligente han permitido garantizar la correcta operatividad y utilización de los usuarios. Estos manuales brindan instrucciones detalladas e ilustrativas sobre cómo debe ser configuración, la operación y el mantenimiento.

9. Recomendaciones

- Para mejorar las detecciones, se recomienda usar una combinación de técnicas de visión artificial en donde se pueda diferenciar los fotogramas y se pueda detectar los contornos de un posible individuo.
- Evaluar cuidadosamente cada una de las zonas del centro es un aspecto fundamental a tomar en cuenta para que no quede ninguna área desprotegida. Esto garantizará una cobertura completa y efectiva del sistema de seguridad.
- Considerar la iluminación de manera que sea adecuada sobre todo en el área de interés, esto permitirá que las imágenes sean lo más claras posibles.
- Comprimir la imagen para agilizar la transferencia de la imagen, es importante encontrar un equilibrio calidad-compresión de imagen para obtener los mejores resultados. Al aplicar cualquier técnica de compresión de imágenes de manera adecuada, se optimiza el consumo de ancho de banda y de igual forma se reduce el tiempo de carga, lo que resultará una mejora en la experiencia del usuario.
- Se debe garantizar que la conexión a internet (por cable o de manera inalámbrica) sea estable y confiable para que el funcionamiento sea óptimo. De ser posible usar una conexión cableada para así minimizar posibles interferencias de la señal.
- Se recomienda tener en cuenta la escalabilidad como factor clave al momento de diseñar e implementar un sistema de seguridad basado en Raspberry Pi. La Raspberry Pi ofrece varios puertos GPIO en los que se podría colocar diferentes dispositivos, detectores de humo, sensor de gas, sensor de inundación, entre otros.
- Como posible mejora al presente trabajo de titulación se podría considerar tomar en cuenta la gestión de datos para el ingreso a la aplicación web, para ello se requiere de la implementación de un botón en el mecanismo de autenticación, para que permita añadir un nuevo usuario y se pueda almacenar en la base de datos.

10. Bibliografía

- Aranda, R. (2013). *Estudio de sistemas de seguridad basado en la detección de intrusos física y tecnológica*. <https://bit.ly/3AbpDpt>
- Armas, G. (2021). *Seguridad ciudadana. Derecho Ecuador* -. <https://derechoecuador.com/seguridad-ciudadana/>
- Baldwin, B. (2022, 6 junio). *What are the components of embedded system? Meaning-Once*. <https://meaning-once.com/qa/what-are-the-components-of-embedded-system.html>
- Bestell. (2019). *What Are The Components of A Machine Vision System*. <https://www.bestell.com.sg/what-are-the-components-of-a-machine-vision-system/>
- Bradski, G. & Kaehler, A. (2008). *Learning Opencv: Computer Vision with the Opencv Library (Illustrated)*. O'Reilly Media.
- BUNKER SEGURIDAD. (2018). *Barreras de microondas: Una solución eficaz para la detección perimetral de la mano de la empresa italiana CIAS*. <https://www.bunkerseguridad.es/ES/barreras-de-microondas-una-solucion-eficaz-para-la-deteccion-perimetral-de-la-mano-de-la>
- Cicolani, J. (2021). *Beginning Robotics with Raspberry Pi and Arduino: Using Python and OpenCV (English Edition) (2.ª ed.)*. Apress.
- Cognex. (2020). *Machine Vision Lighting*. <https://www.cognex.com/what-is/machine-vision/components/lighting>
- Chung, B. W. C. (2017). *Pro Processing for Images and Computer Vision with OpenCV: Solutions for Media Artists and Creative Coders*. Apress.
- Dawson-Howe, K. (2014). *A Practical Introduction to Computer Vision with OpenCV*. Wiley.
- Electrical Technician. (2022). *CCTV Camera Complete Installation with DVR* [Video]. YouTube. <https://www.youtube.com/watch?v=0P8wR3Npkw0>
- Elharrouss, O., Almaadeed, N. & Maadeed, S. (2021). *A review of video surveillance systems*. ScienceDirect. <https://3dvar.com/Elharrouss2021A.pdf>
- EPS Security. (2021). *What causes security system false alarms—and how to prevent them*. <https://www.epssecurity.com/news/business-security/what-causes-security-system-false-alarms-and-how-to-prevent-them/>
- Espinoza, V. (2022). *Desarrollo de un prototipo de sistema de prevención de intrusos en residencias, basado en una plataforma raspberry pi mediante procesamiento de imágenes*. Escuela Politécnica Nacional. Repositorio institucional EPN. <http://bibdigital.epn.edu.ec/handle/15000/22651>
- Free Software Foundation. (2022). *¿Qué es el Software Libre? GNU*. <https://www.gnu.org/philosophy/free-sw.es.html>

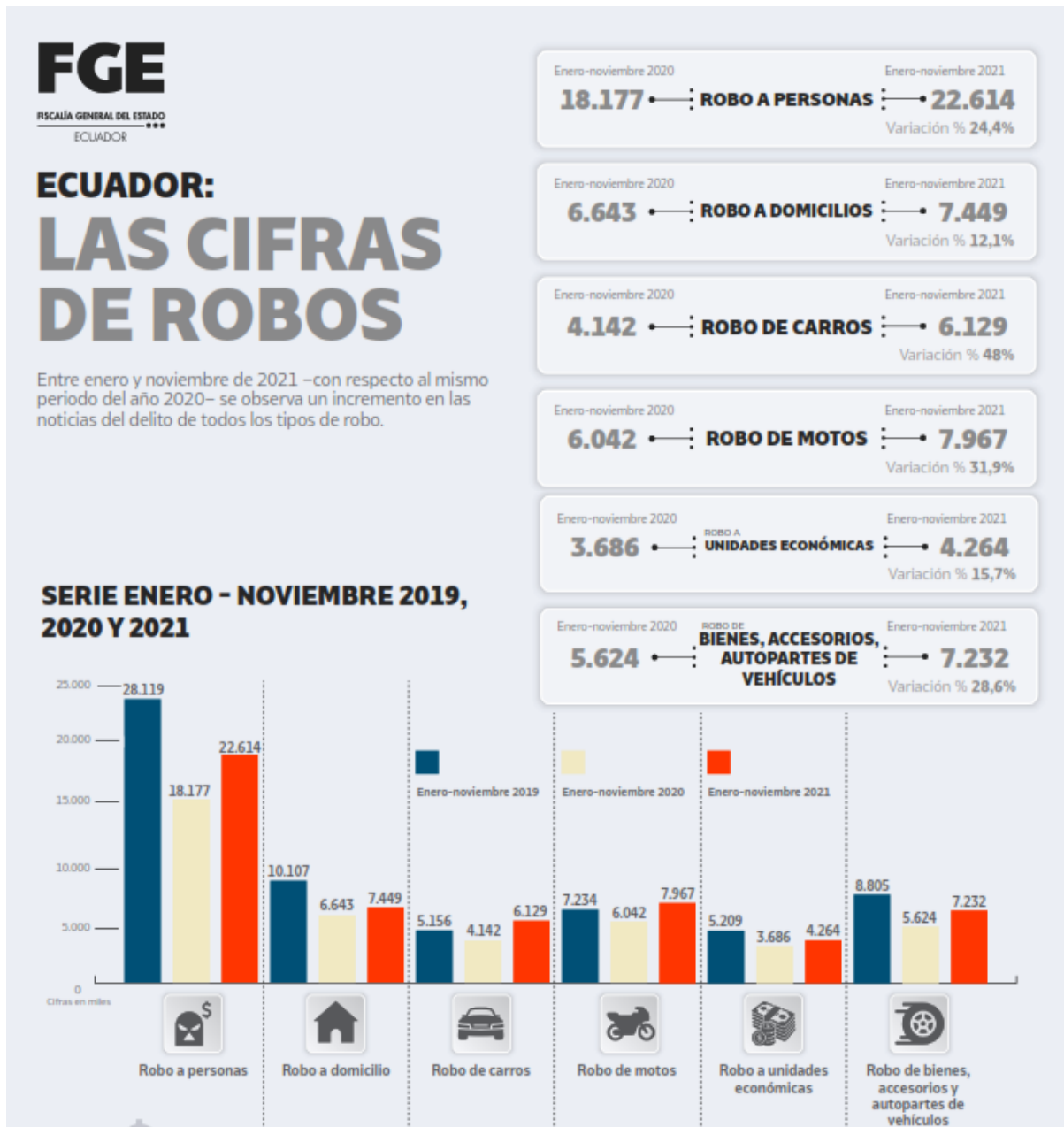
- Fuentes, M. & Castellanos, P. (2019). *La responsabilidad del estado con la seguridad ciudadana*. Revista metropolitana de ciencias aplicadas. <http://remca.umet.edu.ec/index.php/REMCA>
- García, E. (2020). *Visión artificial*. *Exabyte Informática*. [https://www.exabyteinformatica.com/uoc/Informatica/Diseno_de_interaccion/Diseno_de_interaccion_\(Modulo_5\).pdf](https://www.exabyteinformatica.com/uoc/Informatica/Diseno_de_interaccion/Diseno_de_interaccion_(Modulo_5).pdf)
- García Mata, F. (2010). *Videovigilancia: CCTV usando vídeos IP*. Publicaciones Vértice SL
- García Monsálvez, J. C. (2017). Python como primer lenguaje de programación textual en la Enseñanza Secundaria. *Education in the Knowledge Society (EKS)*, 18(2), 147-162. <https://doi.org/10.14201/eks2017182147162>
- Getterson. (2020). *Magnético precableado para montaje en superficie*. <http://www.getterson.com.ar/Category/96>
- Ginni. (2021). *What is OpenCV?*. <https://www.tutorialspoint.com/what-is-opencv>
- González, A., Martínez, F., Pernía, A., Alba, F., Castejón, M., Ordieres, J. & Vergara, E. (2006). Técnicas y algoritmos básicos de visión artificial. Universidad de la RDioja. <https://publicaciones.unirioja.es/catalogo/online/VisionArtificial.pdf>
- Grupo bncvision. (2017). *Componentes de la visión artificial para aplicaciones industriales*. <https://www.bcnvision.es/blog-vision-artificial/componentes-vision-artificial/>
- Hashemi, M. (2019). *Enlarging smaller images before inputting into convolutional neural network: zero-padding vs. interpolation*. *J Big Data* 6, 98 (2019). <https://doi.org/10.1186/s40537-019-0263-7>
- IngenieroVirtual. (2018). Conceptos básicos sobre tecnologías de desarrollo web. [ingeniovirtual.com. https://www.ingeniovirtual.com/conceptos-basicos-sobre-tecnologias-de-desarrollo-web/](https://www.ingeniovirtual.com/conceptos-basicos-sobre-tecnologias-de-desarrollo-web/)
- Jiménez, J. (2022). *Detecta si se abre una puerta o ventana con este aparato de 20 euros*. *RedesZone*. <https://www.redeszone.net/noticias/hogar/detectar-ventana-puerta-abierta-panamalar-20e/>
- Lemus, F., Pérez, M. & García, J. (2019). Analysis of Energy Consumption and Optimization Techniques for Writing Energy-Efficient Code. *Electronics*, 8(10), 1192. <https://doi.org/10.3390/electronics8101192>
- López de la Teja, M., Sarría, D. Ángela, & Fernández, D. (2017). *La formación de conceptos en el proceso de enseñanza-aprendizaje de los sistemas de gestión de bases de datos*. *Revista Conrado*, 13(57), 139-145. Recuperado a partir de <https://conrado.ucf.edu.cu/index.php/conrado/article/view/451>
- López, C. (2021). *¿Qué es una imagen digital y cómo se calcula su peso?* CCM. <https://es.ccm.net/contents/710-infografia>

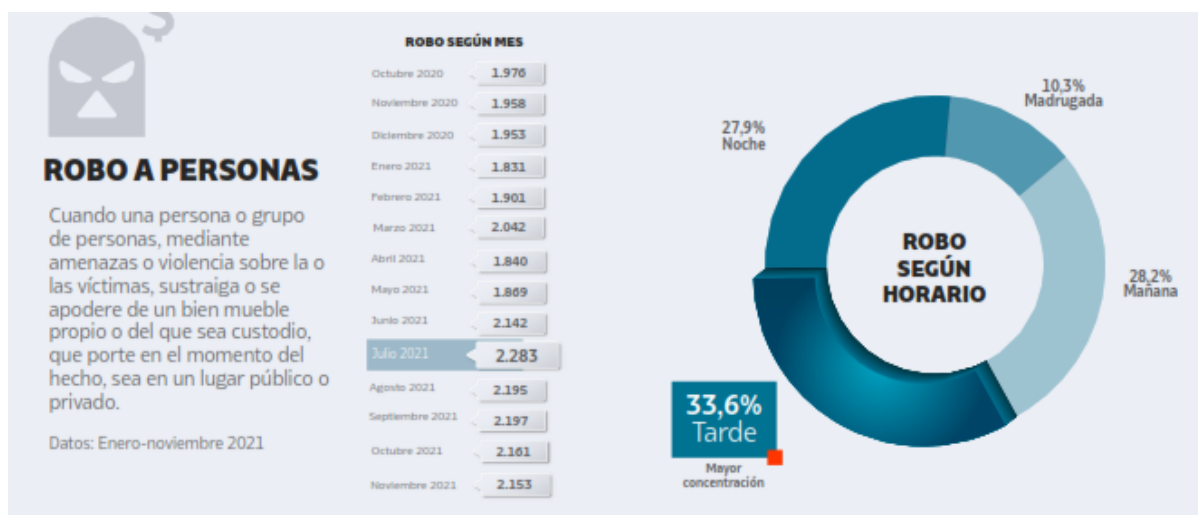
- Luchetti, S. (2021). *Sistema embebido y sus características | Conceptos fundamentales*. Tribalyte Technologies. <https://tech.tribalyte.eu/blog-sistema-embebido-caracteristicas>
- Luchetti, S. (2021). *Arduino vs Raspberry Pi | ¿Cómo elegir? ¿Para qué sirven? 10 Tips*. Tribalyte Technologies. <https://tech.tribalyte.eu/blog-arduino-vs-raspberry-pi>
- Machuca, F. (2022). *Aprende qué es un mapa de bits y haz que tus trabajos resalten por su calidad*. Crehana. <https://www.crehana.com/blog/estilo-vida/que-es-mapa-bits/>
- Masgo, D. (2020). *Implementación de un sistema web basado en visión artificial y geolocalización, y su influencia en la vigilancia del distrito de Lince*. <https://hdl.handle.net/11537/26350>
- Ministerio del Interior. (2018). *Plan nacional de seguridad ciudadana y convivencia social pacífica para la república del Ecuador 2019 – 2030*. Ministerio de gobierno. <https://bit.ly/3UGPBjy>.
- Oasys. (2022). *Sistemas embebidos y su aportación a la industria*. <https://oasys-sw.com/sistemas-embebidos-industria/>
- Olivares, A. (2021). *Protocolos de seguridad web: ¡Descubre cómo se protege la información que insertas en la red!* Crehana. <https://www.crehana.com/blog/transformacion-digital/protocolos-de-seguridad-web/>
- Onate, I. (2017). *Detectores volumétricos de movimiento*. Editorial técnica online NTDoy, S.L. <https://www.seguridadprofesionalhoy.com/detectores-volumetricos-movimiento/>
- Ortega, J. (2022). *Sistema de detección y reconocimiento de intrusos de bajo costo basado en visión artificial, aplicado a sistemas de videovigilancia*. https://dspace.unl.edu.ec/jspui/bitstream/123456789/25093/1/JorgeEnrique_OrtegaJaramillo.pdf
- Punto Flotante. (2017). *Sensor infrarrojo de movimiento PIR HC-SR501*. Punto Flotante S.A. <https://puntoflotante.net/MANUAL-DEL-USUARIO-SENSOR-DE-MOVIMIENTO-PIR-HC-SR501.pdf>
- Quintana, A. (2021). *Asignatura 6: Codificación de caracteres*. <https://abrahamquintana.blogspot.com/2021/11/asignatura-6-codificacion-de-caracteres.html>
- Ramos, M., & Ramos, M. (2014). *Aplicaciones Web 2.a edición (2.a ed.)*. Paraninfo.
- Raspberry Pi Foundation. (2015). *What is a Raspberry Pi?* Raspberry Pi. <https://www.raspberrypi.org/help/what-is-a-raspberry-pi/>
- Rath, S. (2021). *Moving Object Detection using Frame Differencing with OpenCV*. DebuggerCafe. <https://debuggercafe.com/moving-object-detection-using-frame-differencing-with-opencv/>
- Rodríguez, J. (2018). *Circuito cerrado de televisión y seguridad electrónica 2.^a*. Paraninfo.

- Rodriguez, R. (2019). *Sistema de alarma controlado por sensores de movimiento y su contribución en la seguridad institucional del laboratorio de telecomunicaciones de la carrera de ingeniería en computación y redes*. [UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ]. <http://repositorio.unesum.edu.ec/bitstream/53000/1594/1/UNESUM-ECU-REDES-2019-40.pdf>
- Servicio Integrado de Seguridad ECU 911, (2021). *Servicio Integrado de Seguridad ECU 911*. <https://www.ecu911.gob.ec/servicio-integrado-de-seguridad-ecu-911/>
- Solectro. (2021). *¿Cómo funciona el sensor de ultrasonidos medidor de distancia?* <https://solectroshop.com/es/blog/como-funciona-el-sensor-de-ultrasonidos-medidor-de-distancia--n99>
- Traverso, H., Prato, L., Villoria, L., Gómez, G., Priegue, M., Caivano, R., & Fissore, M. (2013). *Herramientas de la Web 2.0 aplicadas a la educación*. <http://sedici.unlp.edu.ar/handle/10915/27532>
- Tutor de Programación. (2017). *OpenCV Operaciones Morfológicas*. <https://acodigo.blogspot.com/2017/04/opencv-operaciones-morfologicas.html>
- Valiente, A. (2019). *Alarma para el hogar basada en Raspberry Pi*. Universidad Politécnica de Valencia.
- Viera, G. (2017). *Procesamiento de imágenes usando OpenCV aplicado en Raspberry Pi para la clasificación del cacao*. <https://pirhua.udep.edu.pe/handle/11042/29>

11. Anexos


Anexo 1. Cifras de robos proporcionadas por la FGE





TIPO DE ROBO	2019	2020	2021	2022	Total
Robo a domicilio	187	204	254	326	971
Robo a personas	275	189	208	365	1.037
Robo de bienes, accesorios y autopartes	62	69	87	102	320
Robo de carros	27	9	12	34	82
Robo de motos	15	19	17	60	111
Robo de unidades económicas	43	27	50	88	208
Total	609	517	628	975	2.729

Anexo 2. Presupuestos de sistema de seguridad, CCTV y cámara con IA.

	MORESEG CIA LTDA BEETHOVEN E1-183 Y PABLO CASALS RUC: 0691701832001		PROFORMA N° 2022-009
	ATENCIÓN:	RUC:	
	CLIENTE: DARWIN PALACIOS	FECHA: 18/1/2022	
	DIRECCIÓN: S/N	ASESOR: ALBA ALTAMIRANO	
TELÉFONO: S/N			
CAN.	DETALLE	P. UNIT	P. TOTAL
1	DVR DAHUA 4 CANALES	\$70.00	\$70.00
1	DISCO DURO DE 1TB	\$85.00	\$85.00
3	CAMARA TUBO 720 DAHUA	\$22.00	\$66.00
3	BALUN DE VIDEO	\$6.00	\$18.00
3	FUENTE DE CORRIENTE PARA CAMARA	\$7.00	\$21.00
1	INSTALACION	\$66.00	\$66.00
1	MATERIALES	\$60.00	\$60.00
		SUBTOTAL	\$386.00
		IVA	\$46.32
		TOTAL	\$432,.52
CONDICIONES:		Proforma válida por 30 días. Equipos incluyen garantía por un año. Proforma considerada con cable visto	

Asesor Comercial

Móvil: 099-758-5034 **MORESEG CIA. LTDA.**

Beethoven E1-183 y Pablo Casals (Quito – Ecuador)

Teléfonos: PBX 02- 241-8884 / 240-1275 ext. 32

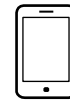
E-mail: ventas2@moreseg.com

Web: www.moreseg.com



SEGURIDAD PRIVADA CON MONITOREO ELECTRÓNICO, ALARMAS Y CERCAS ELÉCTRICAS
Porque tu seguridad no es un gasto, es una inversión

Av. Urdoñez Lasso frente a Industrias Kamaleon
diag. Cooperativa Jep



07 418 5088
099 454 3368
098 644 3480

PROFORMA N° 009368

CLIENTE: DARWIN PALACIOS

Cuenca, 18 de enero del 2022

RUC: 1900373745001

DIRECCION:CUENCA

TELEFONO: 0994543368

De acuerdo a las especificaciones requeridas, le presento la información solicitada:

CANT	DESCRIPCION	IMAGEN	PRECIO
1	COMBO BASICO DE 4 CAMARAS TODO INSTALADO 1 GRABADOR DIGITAL 4CH HD-TVI 1HDD 1080P ACUSENSE CON AUDIO 1 DISCO DURO 1TB ESPECIAL DVR WD PURPLE 4 DOMO DIA NOCHE 4 EN 1 1080P IR L FIJO 4 FUENTE PARA CAMARA 110VAC/12VDC 1 AMP 4 PAREJA DE BALUMS HD-TVI HIKVISION 1 REGLETA DE 6 TOMAS + Instalación, Transporte	480.00	480.00

PRECIO NO INCLUYE EL IVA

Garantía: 1 año por defectos de Fabricación

Validez de Oferta: 5 días Laborables

Forma de Pago: Contado

Entrega: Inmediata

Atentamente

Ing. Wilson Lupercio

GERENTE DE NOVATECH

RUC: 1900373745001



Sale

Panasonic

[Panasonic](#)



Panasonic WV-S1136 1080p Full HD Indoor Box IP Camera

Add to Cart to for Sale Price!

\$679.37

SKU:	WV-S1136
Condition:	New
Availability:	Usually Ships Same Business Day
Shipping:	Calculated at Checkout
Warranty:	3 Year

Quantity:

ADD TO CART

ADD TO QUOTE

DESCRIPTION

Note: Panasonic WV-S1136 does not come with a lens. It requires a CS Mount lens (not included).

Panasonic WV-S1136 is an IP camera for indoor surveillance — with an advanced AI engine. Part of the Panasonic i-PRO line, WV-S1136 provides 1080p Full HD video — professional detail. It uses the AI engine to optimize image quality and video compression — plus Intelligent Auto and Color Night Vision technology. Super Dynamic 144dB technology adapts to high contrast lighting — limits loss of detail.

WV-S1136 has pre-installed analytics capabilities — including detection of humans vs vehicles. Audio support can be used to detect sounds like gunshots, breaking glass and more — additional layer of protection. Panasonic WV-S1136 is ONVIF Profile G, Profile S and Profile T compliant — interoperable with third party systems.

© 2021 IP Phone Warehouse. All rights reserved, including the right to reproduce this product description or portions thereof in any form whatsoever.

Panasonic WV-S1136 Network Security Camera Package Contents:

- WV-S1136 Camera
- Installation Guide
- Warranty Card
- Important Safety Instructions
- Code Label

Panasonic WV-S1136 Documentation:

- [Panasonic WV-S1136 Datasheet](#)
- [Panasonic WV-S1136 Basic Information](#)
- [Panasonic WV-S1136 Installation Guide](#)

Anexo 3. Preguntas realizadas en la encuesta

1. ¿Conoce usted lo que es un sistema de seguridad contra robos e intrusiones?
 - Si
 - No
2. ¿Entiende usted las diferencias entre un sistema de seguridad pasivo y un sistema de seguridad activo?
 - Si
 - No
3. ¿Está consciente de los beneficios que ofrecen los sistemas de seguridad activos en la prevención de robos o intrusiones?
 - Si
 - No
4. ¿Ha oído hablar de múltiples dispositivos como sensores, cámaras, actuadores que se pudiesen utilizar en distintos sistemas de seguridad?
 - Si
 - No
5. ¿Ha oído hablar de la visión artificial y su contribución en el desarrollo de sistemas de seguridad inteligentes?
 - Si
 - No
6. Seleccione una o varias respuestas. ¿En qué tipo de infraestructuras cree usted que es necesario instalar un sistema de seguridad?
 - Locales comerciales
 - Empresas
 - Residencias vacacionales
 - Viviendas
 - Cualquier infraestructura que cuente con bienes que se requieran salvaguardar
 - En ningún tipo de infraestructura
7. ¿Cuenta con algún sistema de seguridad para prevenir robos o intrusiones en cualquier tipo de infraestructura?
 - Si
 - No
8. **Si la respuesta anterior fue sí, indique** ¿Con cuál de los siguientes sistemas de seguridad cuenta?

- Alarmas
- Cerca eléctrica
- Videovigilancia
- Sistema de seguridad privada
- Otra

9. Seleccione una o varias respuestas. ¿Al momento de adquirir un sistema de seguridad, que es lo primero que tiene en cuenta?

- La marca
- El costo
- La facilidad de instalación
- La tecnología que emplea
- Las características que destacan
- Otra

10. ¿Cuál es el rango de precios que usted estaría dispuesto a pagar por un sistema de seguridad activo, con tecnología moderna y de altas prestaciones?

- Menor a 200 \$
- 200 \$ - 300 \$
- 301 \$ - 600 \$
- 601 \$ - 1000 \$

Anexo 4. Función `Video_Stream`.

```
from streamvideowebcam import WebcamVideoStream
class VideoStream:
    def __init__(self, src=0, usePiCamera=False, resolution=(320, 240),#320, 240  ##1280, 720
    framerate=32):#32-40
        # comprobar si se debe utilizar el módulo picamera
        if usePiCamera:
            from pvideostream import PiVideoStream
            # inicializar el flujo de picamera y permitir que la cámara se caliente
            self.stream = PiVideoStream(resolution=resolution,
            framerate=framerate)
        # de lo contrario, estamos usando OpenCV así que inicializa el flujo de la webcam u otra cámara
        else:
            self.stream = WebcamVideoStream(src=src)
    def start(self):
        # iniciar el flujo de vídeo
        return self.stream.start()
    def update(self):
        # toma el siguiente fotograma del flujo
        self.stream.update()
    def read(self):
        # devuelve el fotograma actual
        return self.stream.read()
    def stop(self):
        # detener la ejecución y se liberan los recursos
        self.stream.stop()
```

```
from streamvideo import WebcamVideoStream
class VideoStream:
    def __init__(self, src=0, usePiCamera=False, resolution=(1280, 720),#320, 240  ##1280, 720
    framerate=40):#32
        # comprueba si se debe utilizar el módulo picamera
        if usePiCamera:
            from pvideostream import PiVideoStream

            self.stream = PiVideoStream(resolution=resolution,
            framerate=framerate)
        else:
            self.stream = WebcamVideoStream(src=src)
    def start(self):
        # iniciar el flujo de vídeo
        return self.stream.start()
    def update(self):
        # toma el siguiente fotograma del flujo
        self.stream.update()
    def read(self):
        # devuelve el fotograma actual
        return self.stream.read()
    def stop(self):
        # detener la ejecución y se liberan los recursos
        self.stream.stop()
```

Anexo 5. Código Fuente del sistema de seguridad.

```
1 import cv2
2 import tkinter as tk
3 from tkinter import ttk
4 from PIL import ImageTk, Image
5 import threading
6 import imutils
7 from datetime import datetime, time
8 from tkinter import messagebox
9 import datetime
10 import argparse
11 import imutils
12 import time
13 import VideoStream
14 from time import sleep
15 from datetime import datetime
16 ##
17 import pyrebase
18 #Librerias para enviar correo electronico
19 import smtplib
20 from email.mime.multipart import MIMEMultipart
21 from email.mime.text import MIMEText
22 from email.mime.image import MIMEImage
23 ##
24 import os
25 import threading
26 import locale
27 locale.setlocale(locale.LC_ALL, '')
28 from unidecode import unidecode
29 #
30 ##libreria para habilitar los pines GPIO
31 import RPi.GPIO as GPIO
32 ##
33 import pymysql
34 ##Configuracion de los pines GPIO
35 GPIO.setwarnings(False) ##evitar mensaje de alerta
36 GPIO.setmode(GPIO.BCM) ##configuracion de modo BCM
37 #GPIO.setup(23, GPIO.IN) ##definir el pin 23 como entrada
38 GPIO.setup(7, GPIO.OUT) ##definir el pin 7 como salida
39 GPIO.setup(8, GPIO.OUT)
40 GPIO.setup(23, GPIO.IN)
41
42 #Variables para el uso del correo
43 SMTP_SERVER = 'smtp.gmail.com' #Servidor de correo electronico(protocolo smtp)
44 SMTP_PORT = 587 #puerto de SMTP
45 EMAIL_USERNAME = 'seguridad.i2tec@gmail.com'#Correo electronico emisor
46 EMAIL_PASSWORD = ' ' Clave de seguridad especifica para una aplicacion externa
47
48 # Establecer conexión con la base de datos
49 conn = pymysql.connect(
50     host=' ',
51     user=' ',
52     password=' ',
53     database='php_login_database'
54 )
55 ###
56 firebaseConfig = {
57     'apiKey': " ",
58     'authDomain': "pp1-i22tecc.firebaseio.com",
59     'databaseURL': " ",
60     'projectId': "pp1-i22tecc",
61     'storageBucket': "pp1-i22tecc.appspot.com",
62     'messagingSenderId': "982929006678",
63     'appId': "1:982929006678:web:7dbd2d69ed02e217039bf7",
64     'measurementId': "G-EFDJTW7FBL"
65 }
66
67 }
68
69 firebase = pyrebase.initialize_app(firebaseConfig)
70
```

```

71 storage = firebase.storage()
72 # Crear un cursor para la base de datos
73 cursor = conn.cursor()
74
75 class Emailer:
76     def sendmail(self, recipient, subject, content, image):
77
78         #Creacion de encabezados
79         emailData = MIME multipart()
80         emailData['Subject'] = subject
81         emailData['To'] = recipient
82         emailData['From'] = GMAIL_USERNAME
83
84         #Adjuntar texto
85         emailData.attach(MIMEText(content))
86
87         #Crear datos de la imagen a enviar
88         imageData = MIMEImage(open(image, 'rb').read(), 'jpg')
89         imageData.add_header('Content-Disposition', 'attachment; filename="image.jpg"')
90         emailData.attach(imageData)
91
92         #Conectando con el servidor de Gmail
93         session = smtplib.SMTP(SMTP_SERVER, SMTP_PORT)
94         session.ehlo()
95         session.starttls()
96         session.ehlo()
97
98         #Iniciando sesion de Gmail
99         session.login(GMAIL_USERNAME, GMAIL_PASSWORD)
100
101         #Enviar correo electronico & Salir
102         session.sendmail(GMAIL_USERNAME, recipient, emailData.as_string())
103         session.quit
104
105 sender = Emailer()
106
107 class Webcam:
108     def __init__(self):
109         self.cap = None
110         self.frame = None
111         self.paused = False
112         self.thread = None
113         self.root = tk.Tk()
114         self.root.title("Configuracion de horario")
115         self.root.geometry("550x450+20+30")#510x400+20+30
116         self.root.configure(background="#f2f2f2")
117         self.img_1 = Image.open("new_1.png")
118         self.logo = ImageTk.PhotoImage(self.img_1)
119         self.label = ttk.Label(self.root, image=self.logo)
120         self.label.pack()
121
122         self.estilo_botones = ttk.Style()
123         self.estilo_botones.configure("TButton",background="#4CAF50",
124                                     foreground="ffffff", font=("Helvetica", 12, "bold"),relief="flat")
125         self.estilo_etiquetas = ttk.Style()
126         self.estilo_etiquetas.configure("TLabel", background="#f2f2f2",
127                                       foreground="#333333", font=("Helvetica", 14))
128
129         self.etiqueta_instrucciones = ttk.Label(self.root, text="Configuración para activación del sistema de seguridad:",
130                                               style="TLabel", font=("Arial", 14, "bold"))
131         self.etiqueta_instrucciones.pack(pady=10, padx=10)
132
133         self.create_widgets()
134         self.root.mainloop()
135
136     def create_widgets(self):
137         # Entradas de texto para la hora de inicio y fin
138         self.start_time_label = tk.Label(self.root, text="Hora de inicio (formato 24 horas-HH:MM):",
139                                       font=("Arial",14), fg="black", padx=10, pady=7, bg="#AED6F1")
140         self.start_time_label.pack(padx=50, pady=5, ipadx=10, ipady=5, fill="x")
141         self.start_time_entry = tk.Entry(self.root, font=("Arial", 14))
142         self.start_time_entry.pack(pady=5, padx=50, ipadx=10, ipady=5, fill="x")
143
144         self.end_time_label = tk.Label(self.root, text="Hora de fin (formato 24 horas-HH:MM):",
145                                       font=("Arial",14), fg="black", padx=10, pady=7, bg="#ABB2B9")
146         self.end_time_label.pack(pady=5, padx=50, ipadx=10, ipady=5, fill="x")
147         self.end_time_entry = tk.Entry(self.root, font=("Arial", 14))
148         self.end_time_entry.pack(pady=5, padx=50, ipadx=10, ipady=5, fill="x")
149
150         # Botón de iniciar la cámara
151         self.start_button = tk.Button(self.root, text="Iniciar", command=self.start_camera)
152         self.start_button.pack(side=tk.LEFT, padx=10, pady=10)

```

```

153
154     # Botón de pausar la cámara
155     self.pause_button = tk.Button(self.root, text="Pausar", command=self.pause_camera)
156     self.pause_button.pack(side=tk.LEFT, padx=10, pady=10)
157     self.pause_button.config(state="disabled")
158
159     # Botón de reanudar la cámara
160     self.resume_button = tk.Button(self.root, text="Reanudar", command=self.resume_camera)
161     self.resume_button.pack(side=tk.LEFT, padx=10, pady=10)
162     self.resume_button.config(state="disabled")
163
164 # Función para activar el relé
165 def activar_rele():
166     #GPIO.output(8, GPIO.HIGH)
167     GPIO.output(8, True)
168     time.sleep(40)
169     GPIO.output(8, False)
170 # Función para desactivar el relé
171 def desactivar_rele():
172     #GPIO.output(8, GPIO.LOW)
173     GPIO.output(8, False)
174 # Loop infinito para verificar la hora actual y activar/desactivar el relé
175 def start_camera(self):
176     # Convertir las cadenas de texto en objetos time
177     start_time_str = self.start_time_entry.get()
178     end_time_str = self.end_time_entry.get()
179     try:
180         start_time = datetime.strptime(start_time_str, "%H:%M").time()
181         end_time = datetime.strptime(end_time_str, "%H:%M").time()
182     except ValueError:
183         # Mostrar un mensaje de error si las cadenas no tienen el formato correcto
184         tk.messagebox.showerror("Error",
185                                 "Las horas deben estar en formato de 24 horas, por ejemplo:8:15, 14:30, etc.")
186         return
187
188     # Iniciar la cámara y el hilo
189     self.cap = cv2.VideoCapture(0)
190     self.cap.set(cv2.CAP_PROP_FRAME_WIDTH, 1920)
191     self.cap.set(cv2.CAP_PROP_FRAME_HEIGHT, 1080)
192
193
194     self.fourcc = cv2.VideoWriter_fourcc('X', 'V', 'I', 'D')
195
196     self.out = cv2.VideoWriter("output.avi", self.fourcc, 5.0, (3840, 2160))#1280, 720 #1920, 1080
197     self.thread = threading.Thread(target=self.update_frame, args=(start_time, end_time))
198     self.thread.start()
199     self.start_button.config(state="disabled")
200     self.pause_button.config(state="normal")
201     self.resume_button.config(state="disabled")
202
203 def pause_camera(self):
204     self.paused = True
205     self.start_button.config(state="disabled")
206     self.pause_button.config(state="disabled")
207     self.resume_button.config(state="normal")
208
209 def resume_camera(self):
210     self.paused = False
211     self.start_button.config(state="disabled")
212     self.pause_button.config(state="normal")
213     self.resume_button.config(state="disabled")
214
215 def update_frame(self, start_time, end_time):
216     while True:
217         # Obtener la hora actual y verificar si está dentro del intervalo de tiempo permitido
218         now = datetime.now().time()
219         if start_time <= now or now <= end_time:
220             if GPIO.input(23):
221                 activar_rele()
222                 ret, self.frame = self.cap.read()
223                 self.frame = imutils.rotate(self.frame, 180)
224                 self.frame = imutils.resize(self.frame, width=1200)
225
226                 ret, self.frame2 = self.cap.read()
227                 self.frame2 = imutils.rotate(self.frame2, 180)
228                 self.frame2 = imutils.resize(self.frame2, width=1200)
229                 diff = cv2.absdiff(self.frame, self.frame2)
230                 gray = cv2.cvtColor(diff, cv2.COLOR_BGR2GRAY)
231                 blur = cv2.GaussianBlur(gray, (5, 5), 0)
232                 _, thresh = cv2.threshold(blur, 20, 255, cv2.THRESH_BINARY)
233                 dilated = cv2.dilate(thresh, None, iterations=3)
234                 contours, _ = cv2.findContours(dilated, cv2.RETR_TREE, cv2.CHAIN_APPROX_SIMPLE)
235                 contador = 0

```



```

236     for contour in contours:
237         (x, y, w, h) = cv2.boundingRect(contour)
238
239         if cv2.contourArea(contour) < 7000: #9000 valor con el que se hizo pruebas
240             continue
241
242         cv2.rectangle(self.frame, (x, y), (x+w, y+h), (0, 255, 0), 2)
243         cv2.putText(self.frame, "DETECTANDO {}".format('PRESENCIA.....'), (15, 30), cv2.FONT_HERSHEY_SIMPLEX,
244             0.8, (5, 0, 255), 2)
245         timestamp = datetime.now()
246         ts = timestamp.strftime("%A %d %B %Y. - %I:%M:%S%p")
247         ts = unicode(ts)
248         cv2.putText(self.frame, ts, (10, self.frame.shape[0] - 10), cv2.FONT_HERSHEY_COMPLEX_SMALL, 1.2, (0, 255, 0), 1)
249
250         tife=time.strftime('%H:%M:%S_%Y-%m-%d')
251         prefijo="img-"
252         path="/home/darwin/Img_capt"
253         n_local=path+"/"+prefijo+tife+".jpg"
254
255
256         cv2.imwrite(n_local, self.frame)
257         print("Tratando de cargar a AWS ")
258
259         os.system('sudo scp -r -i /home/darwin/K_imp@@Da_Pa_2023@unl.lab-I2TEC.pem "%s"
260             ubuntu@ :%n_local)
261         storage.child(n_local).put(n_local)
262         print("Cargado en firebase")
263
264     ##
265     # Obtener la fecha y hora actual
266     now = datetime.now()
267     current_date = now.strftime("%Y-%m-%d")
268     current_time = now.strftime("%H:%M:%S")
269     # Insertar datos en la tabla
270     sql = "INSERT INTO Eventos_suscitados (Fecha, Hora) VALUES (%s, %s)"
271     cursor.execute(sql, (current_date, current_time))
272
273     # Guardar los cambios en la base de datos
274     conn.commit()
275     ###
276     sendTo = 'receptor.i2tec.seg@gmail.com'
277     emailSubject = 'ALERTA DE SEGURIDAD'
278     emailContent = 'Se ha detectado movimiento en el area establecida a la hora: ' + time.ctime()
279     sender.sendmail(sendTo, emailSubject, emailContent, n_local)
280     print("Se ha tomado la captura de la imagen")
281
282     ##
283     GPIO.output(7, True)
284     time.sleep(5)
285     GPIO.output(7, False)
286
287     time.sleep(1)
288     contador += 1
289     if contador >= 2:
290         break
291
292     if self.paused:
293         continue
294     #cv2.imshow("webcam", self.frame)
295     image = cv2.resize(self.frame, (1280, 720))
296     self.out.write(image)
297     # mostrar el marco
298     timestamp = datetime.now()
299     ts1 = timestamp.strftime("%A %d %B %Y. - %I:%M:%S%p")
300     ts1 = unicode(ts1)
301     cv2.putText(self.frame, ts1, (10, self.frame.shape[0] - 10),
302         cv2.FONT_HERSHEY_COMPLEX_SMALL, 1.2, (0, 255, 0), 1)
303     cv2.imshow("Frame", self.frame)
304     self.frame = self.frame2
305     ret, self.frame2 = self.cap.read()
306     if cv2.waitKey(1) == ord("q"):
307         break
308     else:
309         continue
310     # Mostrar un mensaje si la hora actual está fuera del intervalo de tiempo permitido
311     cv2.putText(self.frame, "Camara desactivada - fuera del horario permitido", (50, 50),
312         cv2.FONT_HERSHEY_SIMPLEX, 0.7, (0, 0, 255), 2)
313     cv2.imshow("Webcam", self.frame)
314     if cv2.waitKey(1) == ord("q"):
315         break
316     self.cap.release()
317     cv2.destroyAllWindows()
318 if __name__ == "__main__":
319     Webcam()

```



unl

Universidad
Nacional
de Loja



CIT

MANUAL DE USUARIO

SISTEMA DE SEGURIDAD ACTIVO E INTELIGENTE



Autor: Darwin Augusto Palacios Yunga

Índice de contenidos

Introducción	143
¿Qué es visión artificial?	143
¿Qué es un sistema de seguridad de antirrobo e intrusión que incorpora visión artificial?	143
Descripción del sistema	144
Vida útil	144
Medidas del dispositivo	144
Requerimientos	145
Instalación	145
Uso del sistema de seguridad.....	146
Mantenimiento	149
Información de contacto.....	149

Introducción

El objetivo principal de este texto es dar a conocer el manual de usuario del sistema de seguridad inteligente y activo. Este sistema ha sido diseñado para proporcionar una solución de seguridad avanzada y eficiente para su hogar, negocio o cualquier infraestructura que necesite ser resguarda. Con ayuda de la tecnología de visión artificial, el sistema puede detectar automáticamente la presencia de un posible intruso y generar diversas alertas de manera inmediata, lo que garantiza una protección completa en todo momento.

Este manual de usuario ha sido creado para proporcionar instrucciones detalladas sobre cómo instalar, configurar y utilizar el sistema de seguridad. A través de este manual, aprenderá a configurar el sistema, a realizar tareas comunes, como el monitoreo en la aplicación web y a solucionar problemas comunes.

Se espera que este manual ayude a aprovechar al máximo el sistema de seguridad, para que de esa manera se sienta tranquilo y seguro al saber que su hogar o negocio está protegido en todo momento. Si tiene alguna pregunta o problema, no dude en ponerse en contacto con el equipo de soporte técnico.

¿Qué es visión artificial?

La visión artificial es una rama de la inteligencia artificial, la cual se centra en desarrollar algoritmos y técnicas para que las computadoras puedan procesar, ver y comprender el entorno mediante el análisis de imágenes y videos como si lo estuviera haciendo una persona. Con la visión artificial se pueden automatizar muchos procesos que requieren de la interpretación de información visual.

En resumen, la visión artificial es una tecnología con un gran potencial para transformar muchos aspectos de nuestra vida diaria, desde la producción industrial hasta la atención médica y la seguridad pública, entre otros campos que son importantes.

¿Qué es un sistema de seguridad de antirrobo e intrusión que incorpora visión artificial?

Un sistema de seguridad de antirrobo e intrusión que incorpora visión artificial es una solución de seguridad avanzada que utiliza tecnología de visión artificial para detectar la presencia de intrusos en un área determinada. Este tipo de sistema utiliza cámaras y algoritmos de visión artificial para monitorear y analizar la actividad en un área específica, y puede detectar la presencia de personas y objetos no autorizados en tiempo real.

Cuando se detecta una intrusión, el sistema puede activar alarmas y enviar notificaciones a los propietarios o a las autoridades correspondientes. Estos sistemas de seguridad son cada vez más populares en hogares, negocios y otras aplicaciones, ya que ofrecen una protección avanzada y efectiva contra robos e intrusiones, y permiten a los usuarios monitorear su propiedad y mantenerla segura en todo momento.

Descripción del sistema

El microordenador es un componente fundamental en este sistema, ya que es el encargado de ejecutar el código fuente y procesar la información recopilada por el sensor y la cámara del sistema. A través del microordenador, se pueden analizar los datos en tiempo real y tomar decisiones basadas en los resultados obtenidos. De esta forma, el microordenador se convierte en un elemento crítico para el correcto funcionamiento y la eficacia del sistema de seguridad.

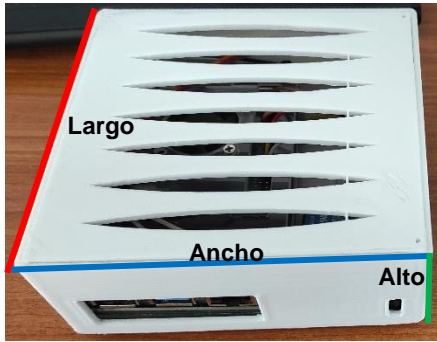
En la implementación del sistema de seguridad también se hizo uso de un relé de dos canales. Este componente fue utilizado para activar la alarma sonora en caso de detección de una intrusión, y también para encender la iluminación en el área monitoreada. De esta forma, se garantiza una respuesta rápida y oportuna ante posibles situaciones de intrusión o robo, y se mejoró la capacidad de monitoreo y protección del área.

Vida útil

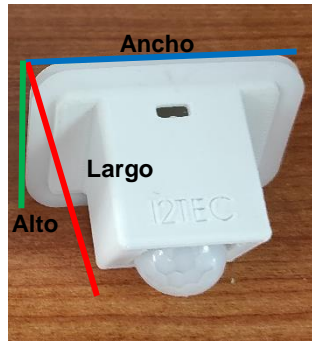
La vida útil del sistema de seguridad depende de factores como, el cuidado, el uso, el mantenimiento, la temperatura de funcionamiento y de la calidad de los demás componentes utilizados. De manera general se estima que tenga una vida útil de al menos 6 años, siempre y cuando se utilice correctamente y se mantenga en buenas condiciones. Además, el rendimiento del sistema puede disminuir con el tiempo debido a factores como la acumulación de polvo y la degradación de los componentes, por ello es indispensable realizar un mantenimiento preventivo para extender la vida útil.

Medidas del dispositivo

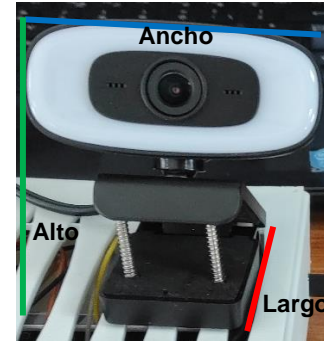
El sistema de seguridad se compone de 3 elementos, las medidas de cada uno de estos elementos se detallan a continuación.



Largo: 9.5cm
 Ancho: 8.5cm
 Alto: 6.0cm



Largo: 4.3cm
 Ancho: 5.1cm
 Alto: 3.0cm



Largo: 4.8cm
 Ancho: 5.6cm
 Alto: 7.6cm

Requerimientos del sistema

Los aspectos que se deben tener en cuenta en la instalación del prototipo son:

- Se necesita de una conexión eléctrica para enchufar el dispositivo.
- La Raspberry Pi 4 B tiene que estar conectada a internet, la conexión puede ser mediante WiFi o Ethernet. Si la señal WiFi es débil, se recomienda conectar mediante Ethernet para asegurar que el sistema funcione correctamente y de manera inmediata.
- Se necesita de cable AWG 22 para la conexión al sensor y al relé.
- Para la instalación de la cámara, sensor y Raspberry Pi, se requiere de case con orificios para poder fijarlos en la pared o en el lugar que se crea conveniente colocar.
- Las configuraciones iniciales requieren de una computadora con programas como PuTTY y TeamViewer instalados, o bien, un smartphone con estas aplicaciones disponibles para establecer la conexión remota necesaria.

Instalación

1. Realizar los respectivos orificios en el case del sensor en los puntos que se indican a continuación.



2. Tomar la medida exacta de la distancia que existe entre los orificios del case del sensor para que se puedan realizar las perforaciones en el material sobre el cual se va a fijar el sensor (madera, concreto, metal).
3. Repetir el paso 1 y 2 para la instalación de la cámara. Antes de proceder, es importante evaluar cuidadosamente el lugar donde se colocará la cámara para asegurarse de que cubra todo lo necesario. De esta manera, se puede garantizar una cobertura adecuada y maximizar la efectividad del sistema.



4. Suministrar energía eléctrica al sistema, para ello se debe conectar el cable de alimentación propio del sistema.

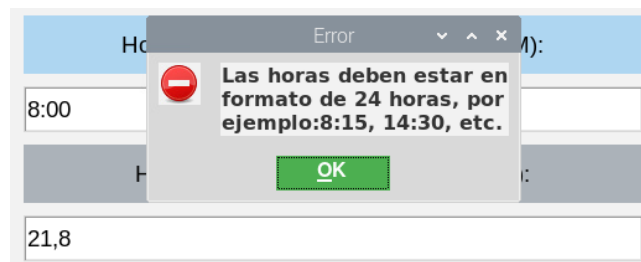
Uso del sistema de seguridad

- Presionar el botón que se indica en la siguiente figura para encender el dispositivo.



- Al encender el dispositivo automáticamente se ejecutará el sistema de seguridad de antirrobo e intrusión. Ingresar a la Raspberry por medio de TeamViewer con el ID: 1506416429 y la contraseña especificada por el personal técnico, en la pantalla principal aparecerá la interfaz de configuración que se muestra en la siguiente imagen.

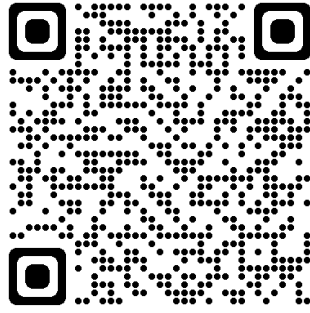
- En los recuadros de color blanco colorar la hora en la que se requiere que se inicie el sistema, así como la hora de finalización del mismo. Se debe colocar la hora en formato de 24 horas de la siguiente manera: 8:30, 12:00, 23:59, etc. En caso de que se coloque la hora de manera errónea aparece un mensaje indicando la manera correcta en la que se debe colocar para que dé inicio el sistema.



- Una vez que se haya especificado las respectivas horas de inicio y de fin, se debe presionar el botón **Iniciar** que se encuentra en la parte inferior de la interfaz. Existe la posibilidad de pausar la ejecución del sistema con el botón **Pausar**, de igual manera se podrá reanudar la ejecución del sistema presionando el botón **Reanudar**.
- Para monitorear las incidencias desde la aplicación web, se deberá ingresar al siguiente enlace:

<https://www.seguridadi2tec.click/>

O puede escanear el siguiente código Qr



- Al ingresar se mostrará la siguiente ventana

Acceso

Usuario

Contraseña

Acceder

Para permitir el acceso a la aplicación web, es necesario colocar las credenciales proporcionadas por el personal técnico. Al ingresar estas credenciales en el formulario correspondiente, el sistema puede verificar la identidad del usuario y permitir el acceso a las funciones y datos correspondientes.

Una vez que se logró ingresar aparece la ventana principal, en donde se muestran:

Muestra la información con la que se inició sesión

Muestra la información de soporte técnico

Salir de la aplicación web

Muestra los datos de fecha y hora de la intrusión

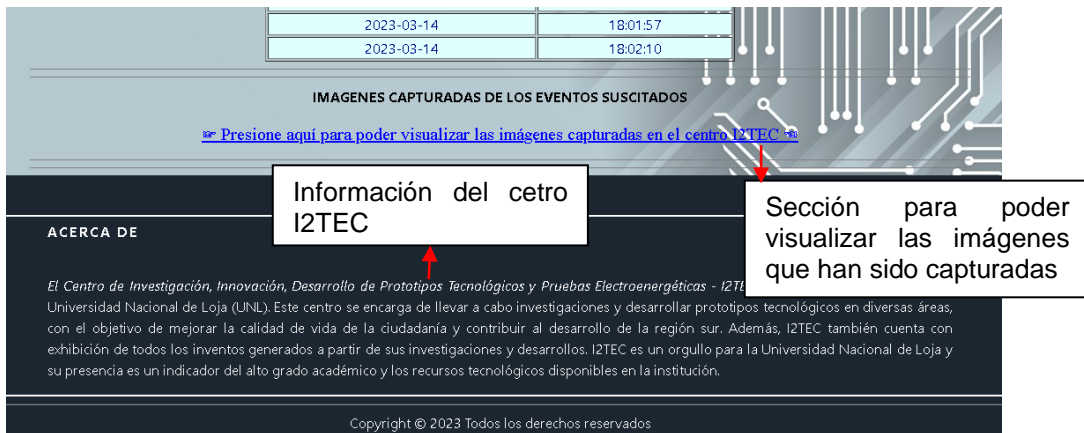
I²TEC UNL Información de usuario Soporte Cerrar sesión

Investigación innovación Tecnología

Bienvenid@, aquí podras visualizar las incidencias dentro del centro, usted ha iniciado sesión como: I2TEC

TABLA RESUMEN DE EVENTOS SUCITADOS

FECHA	HORA
2023-02-15	17:42:29



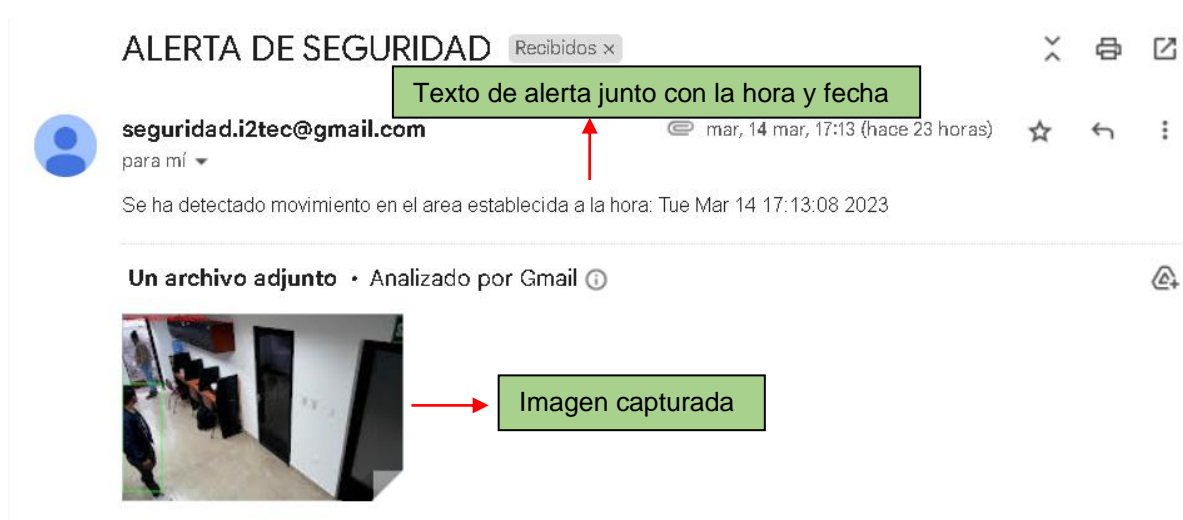
Al ingresar a la sección de visualización de las imágenes se mostrará la siguiente ventana:



Es importante destacar que las imágenes han sido agrupadas según el día en que fueron capturadas, y que además las más recientes se muestran en la parte superior, con la finalidad de que sea más fácil identificarlas.

- Para recibir las alertas de los eventos suscitados por correo electrónico, en primer lugar, se debe iniciar sesión con la cuenta seleccionada para ser la receptora y se tiene que habilitar las notificaciones de la plataforma de correo electrónico.

En la siguiente imagen se muestra cómo llegan las alertas por correo electrónico



- Para visualizar el backup de todas las imágenes capturadas se necesita visitar el siguiente enlace <https://console.firebase.google.com/> y acceder con las credenciales de correo electrónico de Gmail proporcionadas para Firebase storage.
- Como medida disuasiva se activará automáticamente por unos segundos la alarma sonora.
- Si se desea apagar el dispositivo se tendrá que presionar nuevamente el botón que se indicó en el punto 1.
- Si se requiere monitorear de manera remota es necesario tener instalado TeamViewer en cualquier dispositivo (portátil, celular, Tablet, etc.). Para ello se requiere del ID y de la contraseña que deberá ser proporcionada por el personal técnico, de esa manera se accede al contenido de la cámara en tiempo real.

Mantenimiento

Para asegurar el correcto funcionamiento del sistema es esencial realizar un mantenimiento preventivo de manera periódica. Sin un mantenimiento adecuado, el sistema podría experimentar fallas o errores en la actuación del sistema.

A. Limpieza

En donde se debe poner mayor atención es en la cámara y en la Raspberry ya que se pueden ver afectados por factores, como la suciedad, el polvo o deterioro natural del hardware.

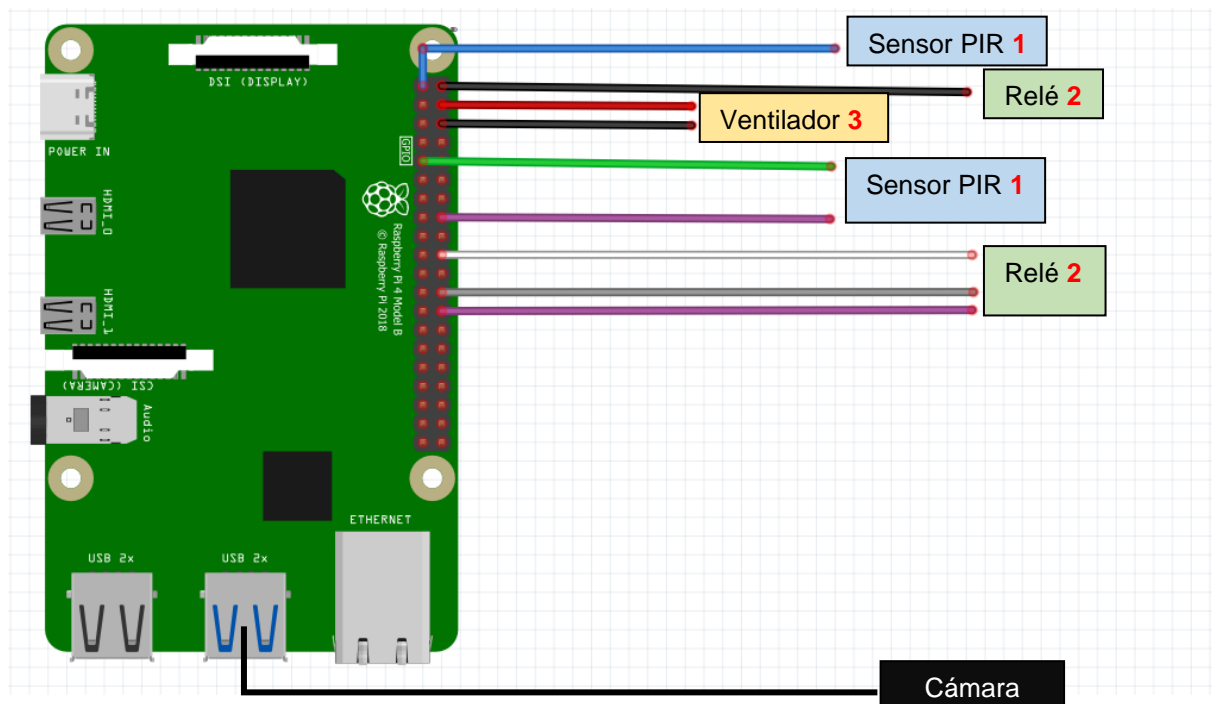
Para ello es necesario seguir las siguientes instrucciones:

- Apagar el sistema presionando el mismo botón con el que se encendió.
- Retirar los tornillos con un destornillador tipo estrella.

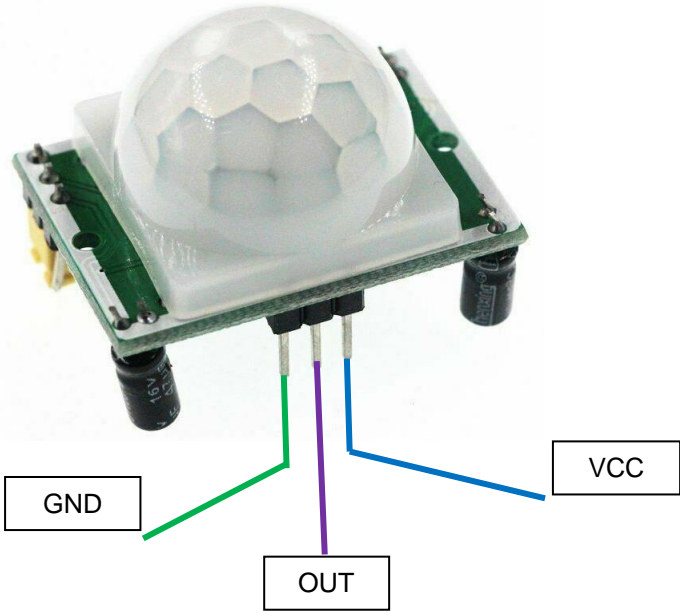
- Retirar el case de la Raspberry Pi para acceder a las partes internas del dispositivo, se recomienda utilizar un cepillo de cerdas suaves o un pincel para limpiar cuidadosamente las áreas donde se haya acumulado polvo y otras partículas. Es importante prestar mayor atención en el ventilador y en las áreas que están cerca de los puertos de entrada y salida, ya que es común que se acumule polvo y suciedad en estas áreas.
- Una vez finalizada la limpieza de la Raspberry Pi, es importante asegurarse de volver a colocar el case y los tornillos en sus lugares respectivos. Esto permitirá que la Raspberry Pi esté debidamente protegida.
- Para limpiar el lente de una cámara de manera efectiva, es importante utilizar un paño de microfibra limpio y seco. Se recomienda evitar tocar el lente directamente con los dedos, ya que esto puede dejar huellas dactilares y otros residuos que afectan la calidad de la imagen. En su lugar, se deben realizar movimientos circulares y muy suaves con el paño de microfibra para eliminar cualquier suciedad o polvo que haya en el lente.

B. Cambio de componentes del sistema.

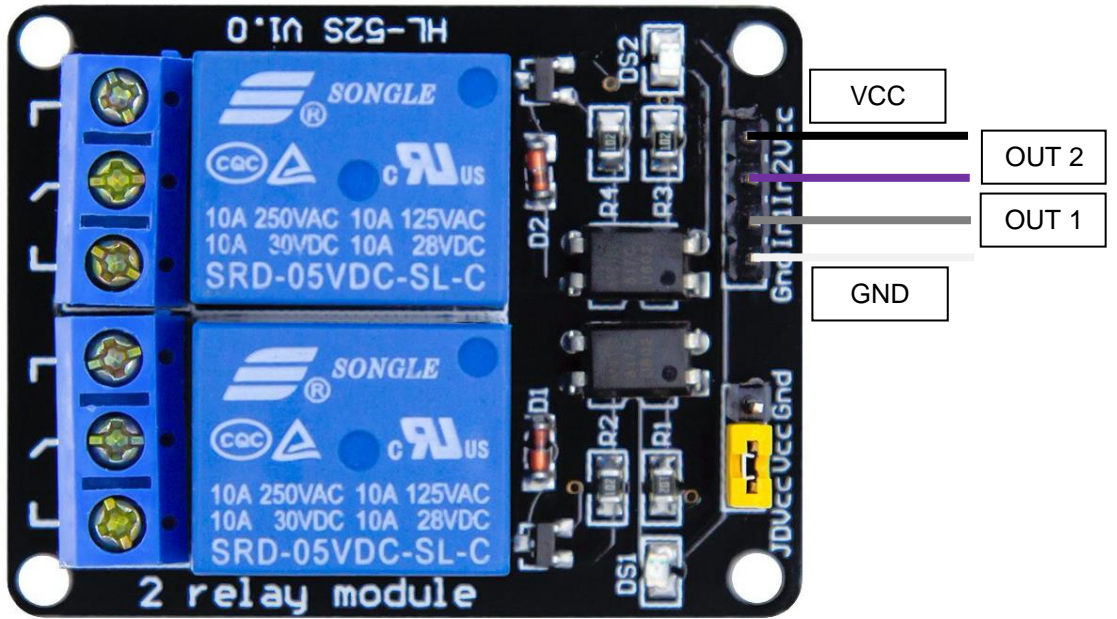
Para garantizar el correcto funcionamiento del sistema, es importante prestar atención al estado de sus componentes y dispositivos. Si alguno de ellos ha sufrido daños o ya no funciona de manera óptima debido al desgaste por el uso u otros factores, es necesario considerar su reemplazo. Para el cambio de cualquiera de estos se recomienda guiarse en la siguiente imagen, la cual indica la conexión correcta según el color de cable.



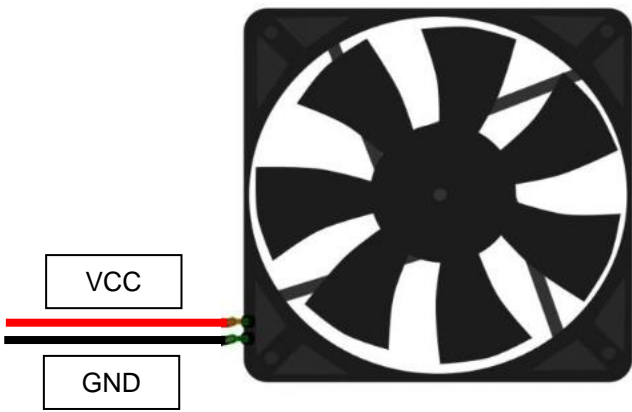
Sensor PIR 1



Relé 2



Ventilador 3



C. Consideraciones para un correcto funcionamiento

- Deben existir dos tomas de corriente eléctrica: una para el dispositivo y otra para la alarma sonora.
- El dispositivo debe estar conectado a internet todo el tiempo ya sea por WiFi o por Ethernet
- No manipular abruptamente el sensor o el relé.
- El dispositivo debe colocarse en una zona segura, no visible, libre de humedad o en entorno de altas temperaturas.
- Tener especial cuidado al conectar los cables del conmutador al relé, ya que se está manipulando corriente alterna.
- Apagar el dispositivo para realizar el respectivo mantenimiento

Información de contacto

En caso de tener alguna consulta, contactarse con Darwin Palacios

- Correo electrónico: darwin.a.palacios@unl.edu.ec / darwinagusto2000@gmail.com
- LinkedIn: [\(6\) Darwin Palacios | LinkedIn](#)
- Facebook: Darwin Palacios <https://www.facebook.com/darwinpalaciosD.P.24/>
- Telegram: https://t.me/darwin_palacios23

English Speak Up Center

Nosotros "English Speak Up Center"

CERTIFICAMOS que

La traducción del resumen de tesis "DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE SISTEMA DE SEGURIDAD INTELIGENTE, PARA EL CENTRO I2TEC DE LA UNL." documento adjunto solicitado por el señor Darwin Augusto Palacios Yunga con cédula de ciudadanía número 1150634788 ha sido realizada por el Centro Particular de Enseñanza de Idiomas "English Speak Up Center"

Esta es una traducción textual del documento adjunto. El traductor es competente y autorizado para realizar traducciones.

Loja, 9 de junio de 2023


Mg. Sc. Elizabeth Sánchez Burneo
DIRECTORA ACADÉMICA

DIRECCIÓN: SUCRE 207 45 ENTRE AZUAY Y MIGUEL RÍOFRÍO

TELÉFONO: 099 5263 264