PROYECTO DE INGENIERÍA DE SOFTWARE I

NOMBRES

JEFERSON BENJUMEA MORALES

JUAN DIEGO PAZ SERNA

TRABAJO

TRABAJO ESCRITO PARA INGENIERÍA DE SOFTWARE I

DOCENTE

PIEDAD MARÍA METAUTE PANIAGUA

FECHA

5/11/2024

CORPORACIÓN UNIVERSITARIA REMINGTON

FACULTAD DE INGENIERÍAS

MEDELLÍN

2024

Contenido

[GLOSARIO 5](#_Toc646313206)

[INTRODUCCION 6](#_Toc1460407045)

[JUSTIFICACION DEL PROYECTO 6](#_Toc92428905)

[MISION 7](#_Toc106775633)

[VISION 7](#_Toc1165985629)

[Contextualización del tema 8](#_Toc1608200611)

[Inteligencia Artificial aplicada a la vigilancia en unidades residenciales 8](#_Toc1700432192)

[Cómo se alimenta una IA para aprender 8](#_Toc1443482772)

[IA aplicada a la vigilancia 8](#_Toc808910187)

[Sistemas de vigilancia en unidades residenciales 9](#_Toc643868692)

[Cómo la IA detecta comportamientos sospechosos 9](#_Toc995592553)

[Conclusión 9](#_Toc1000954828)

[Extracción de requisitos 10](#_Toc429165718)

[Formulario 10](#_Toc1194052902)

[Formato de la entrevista 10](#_Toc304724723)

[Desarrollo de la entrevista 10](#_Toc587983939)

[Conclusión 18](#_Toc1714938265)

[Definición del problema 18](#_Toc1984095496)

[Antecedentes del problema 18](#_Toc511884022)

[Justificación del problema 19](#_Toc2119544894)

[Pregunta problemática 20](#_Toc1280062046)

[Listado de necesidades y características 20](#_Toc1551705772)

[Fuente: elaboración propia 21](#_Toc915301344)

[Objetivó general 21](#_Toc1303925946)

[Objetivos específicos 21](#_Toc358074880)

[Fuente: elaboración propia 23](#_Toc929892989)

[Nombre que se le colocará al sistema de software 23](#_Toc950594066)

[Cronograma de actividades 24](#_Toc1604492766)

[Fuente: elaboración propia 25](#_Toc1587220059)

[Análisis de riesgos 26](#_Toc13295724)

[Fuente: elaboración propia 28](#_Toc1269440808)

[Análisis de requisitos 28](#_Toc959099981)

[Tabla general para casos de uso. 28](#_Toc972751669)

[Fuente: elaboración propia 30](#_Toc783249303)

[Requisitos de Usuario 30](#_Toc1986369930)

[Fuente: elaboración propia 31](#_Toc1229156721)

[Requisitos Funcionales 31](#_Toc682730761)

[Fuente: elaboración propia 33](#_Toc286477889)

[Requisitos No funcionales 33](#_Toc618719798)

[Facilidad de uso (“usability”) 33](#_Toc504695507)

[Confiabilidad 34](#_Toc810891192)

[Ambiente de Trabajo (“Performance”) 34](#_Toc652703616)

[Restricciones de Diseño 34](#_Toc427955306)

[Seguridad 34](#_Toc893695103)

[Documentación de Usuario y Sistemas de Ayuda 35](#_Toc1995688370)

[Interfaces 35](#_Toc1054215388)

[Interfaz de Usuario 35](#_Toc90315244)

[Interfaces de Comunicación 35](#_Toc1038564556)

[Modelo de Casos de Uso 35](#_Toc1402215637)

[Descripciones Generales de Actores 35](#_Toc1872594101)

[Fuente: elaboración propia 36](#_Toc321303722)

[Especificación del requisito 36](#_Toc1477942427)

[Documentación o especificación de los Casos de Uso (Plantillas o escenarios) 43](#_Toc80649267)

[Fuente: elaboración propia **¡Error! Marcador no definido.**](#_Toc1701896250)

[Fuente: elaboración propia 48](#_Toc1230825475)

[Fuente: elaboración propia 54](#_Toc5077581)

[Fuente: elaboración propia **¡Error! Marcador no definido.**](#_Toc1250783200)

[Mapa de navegación (Diseño del menú que se utilizará en el sistema) 60](#_Toc1966759054)

[Recursos (hardware, Software, Talento Humano) 60](#_Toc1631355859)

[Conclusiones 62](#_Toc2145785564)

[Referentes **¡Error! Marcador no definido.**](#_Toc1418011893)

### GLOSARIO

\* **Inteligencia Artificial (IA)**: Rama de la informática que se ocupa de crear sistemas capaces de realizar tareas que normalmente requieren inteligencia humana, como el análisis de datos, reconocimiento de patrones y aprendizaje automático.

\* **Monitoreo 24/7**: Vigilancia constante durante las 24 horas del día, los 7 días de la semana, garantizando que no haya interrupciones en el control de seguridad.

\* **Análisis de Imágenes**: Proceso de examinar las imágenes captadas por las cámaras para identificar patrones y comportamientos inusuales, utilizando algoritmos de IA.

\* **Alertas en Tiempo Real**: Notificaciones instantáneas enviadas al personal de seguridad cuando se detectan actividades sospechosas o situaciones que requieren atención inmediata.

\* **Patrones de Comportamiento**: Comportamientos recurrentes que pueden ser analizados por la IA para identificar actividades inusuales o potencialmente peligrosas.

\* **Interfaz Intuitiva**: Diseño de software que permite a los usuarios interactuar de manera sencilla y eficiente, facilitando su uso y comprensión.

\* **Aplicación Móvil**: Software diseñado para ser utilizado en dispositivos móviles, permitiendo a los vigilantes gestionar las cámaras y recibir notificaciones de forma remota.

\* **Reconocimiento Facial**: Tecnología que permite identificar a las personas mediante el análisis de sus características faciales, útil para detectar la presencia de personas no autorizadas.

\* **Automatización**: Proceso de utilizar tecnología para realizar tareas de forma automática, reduciendo la necesidad de intervención humana.

\* **Generación de Reportes**: Creación automática de documentos que contienen información relevante sobre eventos de seguridad, análisis de datos y comportamiento de las cámaras.

\* **Compatibilidad**: Capacidad del software para integrarse y funcionar con otros sistemas de seguridad, como alarmas y dispositivos de control de acceso.

\* **Feedback de Usuarios**: Comentarios y sugerencias proporcionados por los usuarios sobre el funcionamiento del software, utilizados para realizar mejoras continuas.

\* **Gestión de Alertas**: Proceso de creación, modificación y consulta de alertas dentro del sistema para asegurar un monitoreo efectivo.

\* **Configuraciones del Sistema**: Ajustes y parámetros que permiten personalizar el funcionamiento del software según las necesidades del usuario o de la instalación.

\* **Historial de Equipos**: Registro de información sobre los dispositivos que ingresan o salen de una instalación, incluyendo detalles como marca, serie y propietario.

# INTRODUCCION

Siempre es importante mantener un control de vigilancia constante, en los lugares donde se requieren un mayor control del orden público; por eso queremos aprovechar el fortalecimiento de la inteligencia artificial para entrenar una IA para encargarse de analizar estos patrones de comportamiento y alertar al guardia, para llevar a cabo su debida acción.

Las cámaras de seguridad son un tema importante y algo en que considerar las personas que requieran un sistema más confiable y eficiente, en estos tiempos “una cámara con IA aportará beneficios a la seguridad, la protección y la eficiencia operativa desde el mismo momento en que se despliegue la cámara” (Alberto Alonso, 09/10/2023).

Este software analizaría las 24 horas de los 7 días de la semana, sin perder de vista su objetivo como si lo haría un humano.

Esta aplicación sería una solución para la falta de atención constante de los guardias, y brindaría una solución más ágil a un problema existente.

Analizando los comportamientos que se ven en las cámaras con una inteligencia artificial, que se encarga de ver los comportamientos, y mediante un entrenamiento de la IA para reconocer dichos comportamientos, y así notificar al portero mediante su respectiva aplicación.

## JUSTIFICACION DEL PROYECTO

Este proyecto se hace porque se ve la necesidad de desarrollar un software capaz de vigilar las cámaras como lo haría un vigilante, reportando problemas y trabajando con el vigilante para agilizar este proceso.

Se hace para que el vigilante tenga una herramienta la cual pueda usar de manera fácil, que mejore su trabajo y le libere de una carga laboral adicional, con este software podrá despreocuparse y confiar en que recibirá una notificación al menor indicio de problemas que requieran atención.

Con estos puntos a querer implementar podríamos actuar más rápidamente en tales situaciones, el sistema analiza constantemente las cámaras, analizando patrones y acciones sospechas, así las cámaras siempre estarán en revisión y no como lo estarían si una persona las revisara.

El proyecto se haría con una inteligencia artificial entrenada para vigilar la imagen de las cámaras, la cual analiza los comportamientos de las personas, para así determinar si la acción que se esta visualizando sea dicha de mención, mediante una notificación al celular del vigilante, la cual intentara describir el problema a solucionar.

## MISION

Desarrollar e implementar soluciones innovadoras de vigilancia basadas en inteligencia artificial, capaces de analizar y detectar actividades sospechosas en tiempo real a través de cámaras de seguridad, mejorando la seguridad de los edificios mediante la automatización del monitoreo y la reducción de la dependencia humana.

## VISION

Ser líderes en el desarrollo de tecnologías inteligentes para la seguridad, ofreciendo soluciones avanzadas que transformen la forma en que se vigilan los espacios, proporcionando una vigilancia más eficiente, precisa y confiable, que sea accesible y adaptable a múltiples sectores y entornos.

## Contextualización del tema

### Inteligencia Artificial aplicada a la vigilancia en unidades residenciales

La Inteligencia Artificial (IA) ha transformado múltiples industrias y ha encontrado un campo particularmente relevante en el área de la seguridad y vigilancia. Desde sus inicios, la IA ha sido diseñada para aprender a partir de datos y mejorar sus capacidades predictivas y de análisis en diversos contextos, incluyendo la seguridad en unidades residenciales. Esta contextualización explora cómo se alimenta una IA para aprender, su aplicación en la vigilancia, los sistemas de vigilancia existentes y el rol de la IA en la detección de comportamientos sospechosos.

### Cómo se alimenta una IA para aprender

La IA requiere grandes volúmenes de datos para entrenarse y mejorar su capacidad de toma de decisiones. Estos datos pueden incluir imágenes, videos, registros de audio o texto, que son procesados mediante algoritmos de aprendizaje automático. Según Goodfellow, Bengio y Courville (2016), el aprendizaje supervisado, no supervisado y el aprendizaje por refuerzo son algunos de los métodos clave que permiten que una IA identifique patrones, clasifique información y prediga resultados basados en los datos recibidos. Para que una IA pueda aprender, los desarrolladores diseñan modelos matemáticos que se ajustan a los datos de entrenamiento y se perfeccionan a través de iteraciones y retroalimentación constante, mejorando así su precisión y efectividad (Russell & Norvig, 2020).

### IA aplicada a la vigilancia

La IA aplicada a la vigilancia se utiliza para monitorear, analizar y reaccionar en tiempo real ante situaciones de seguridad. Las soluciones de vigilancia impulsadas por IA son capaces de identificar y responder automáticamente a eventos sospechosos, alertando al personal de seguridad o ejecutando acciones preprogramadas. Estas aplicaciones son especialmente útiles en entornos donde la vigilancia constante es necesaria, como en las unidades residenciales, y pueden reducir la dependencia de personal humano en tareas de observación continua (Badii et al., 2021). La IA en vigilancia también permite una cobertura más amplia y un análisis detallado de patrones de comportamiento en lugares de alta circulación, donde se pueden detectar anomalías o comportamientos inusuales.

### Sistemas de vigilancia en unidades residenciales

En el contexto de unidades residenciales, existen sistemas de vigilancia tradicionales, como cámaras de seguridad, sensores de movimiento y alarmas, que han sido ampliamente utilizados para proteger a los residentes. Sin embargo, los sistemas de vigilancia modernos ahora integran tecnologías avanzadas de IA que les permiten "aprender" patrones normales de actividad y detectar comportamientos inusuales. Según García y Sánchez (2022), estos sistemas de IA pueden analizar grandes cantidades de datos de video en tiempo real y generar alertas automáticas ante eventos inusuales, como personas merodeando o entradas no autorizadas en zonas restringidas. Estos sistemas de vigilancia aumentan la eficacia y la cobertura de seguridad al realizar análisis automatizados y generar reportes detallados.

### Cómo la IA detecta comportamientos sospechosos

La detección de comportamientos sospechosos es una de las funciones más avanzadas de la IA en el ámbito de la vigilancia. Los sistemas de IA utilizan algoritmos de visión por computadora y aprendizaje profundo para analizar los patrones de movimiento y acciones de las personas dentro de un área monitoreada. A través de la identificación de patrones de comportamiento previamente definidos como "anormales", la IA puede emitir alertas para que el personal de seguridad investigue más a fondo la situación. Por ejemplo, el sistema puede detectar comportamientos inusuales, como movimientos erráticos, permanencia prolongada en áreas restringidas, o intentos de acceso a áreas no autorizadas (Zhang et al., 2019). Al basarse en modelos de detección de anomalías, la IA es capaz de identificar eventos que escapan al monitoreo humano, mejorando así la prevención de posibles incidentes de seguridad.

### Conclusión

La implementación de la IA en los sistemas de vigilancia en unidades residenciales representa un avance significativo en la seguridad y protección de estos espacios. Los sistemas de IA aprenden de grandes volúmenes de datos y pueden integrarse en entornos de vigilancia para detectar comportamientos sospechosos y generar alertas automáticas. A medida que las tecnologías avanzan, se espera que la IA continúe perfeccionando sus capacidades predictivas, lo que hará que los sistemas de vigilancia en las unidades residenciales sean cada vez más eficientes y autónomos en la detección de riesgos.

## Extracción de requisitos

### Formulario

<https://docs.google.com/forms/d/e/1FAIpQLSeLaswtV1KfqWuhxUZCTbflMf9-tE0Pwn23HMnbhmyoaZpHeg/viewform?usp=sf_link>

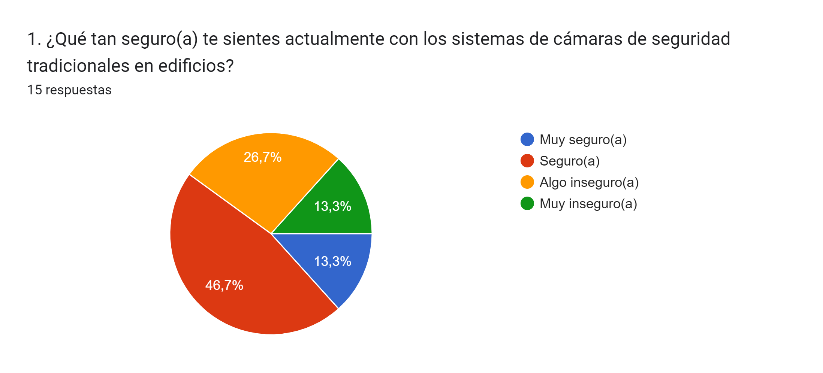
### Formato de la entrevista

La encuesta fue diseñada en Google Forms con un **total de 15 preguntas**, donde 14 son de opción múltiple o selección múltiple, y **una pregunta final abierta** para que los encuestados puedan dejar comentarios o sugerencias adicionales.

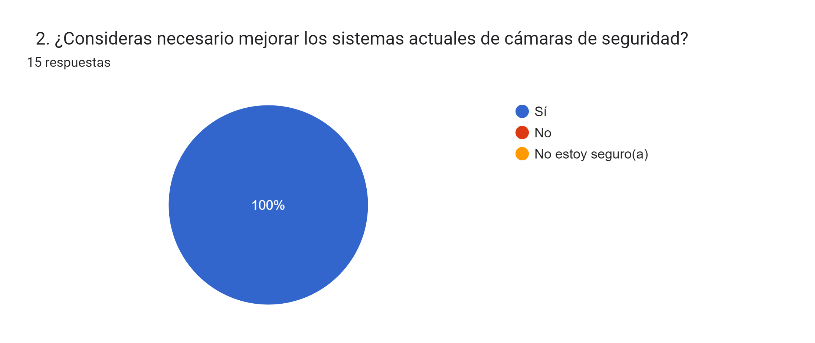
**Participantes:** La encuesta fue respondida por **15 personas**, brindando así una muestra preliminar de opiniones sobre la implementación de un sistema de vigilancia basado en inteligencia artificial.

### Desarrollo de la entrevista

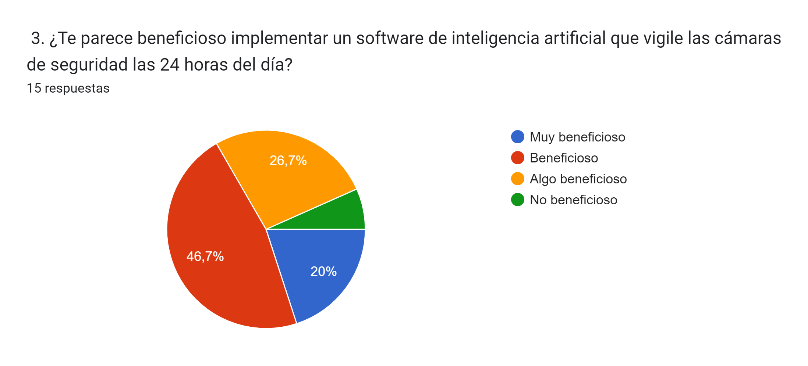
#### Análisis de la entrevista



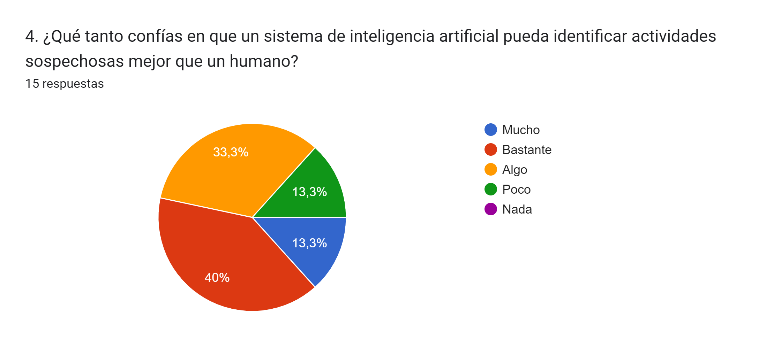
* **Resultados**:
* Muy seguro(a): 13,3%
* Seguro(a): 46,7%
* Algo inseguro(a): 26,7%
* Muy inseguro(a): 13,3%
* **Análisis**: La mayoría de los usuarios (60%) se siente segura o algo segura con los sistemas tradicionales de cámaras de seguridad. Sin embargo, un porcentaje significativo (40%) de los encuestados muestra cierta inseguridad, lo que podría indicar una percepción de que las cámaras tradicionales no son suficientes para garantizar una seguridad total. Este dato sugiere que la confianza en la tecnología actual es moderada, y algunos usuarios podrían estar abiertos a alternativas más avanzadas.



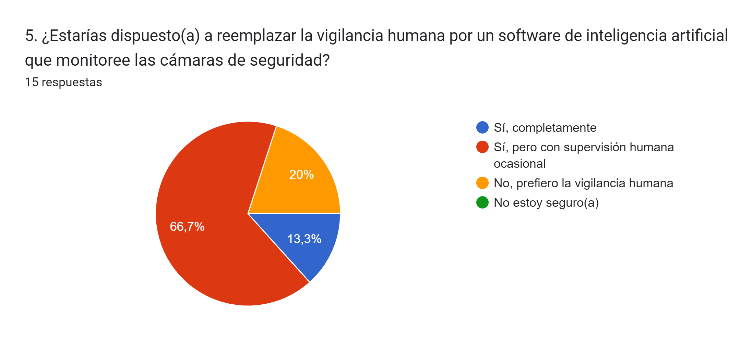
* **Resultados**:
* Sí: 100%
* **Análisis**: Todos los encuestados consideran que es necesario mejorar los sistemas actuales. Este resultado refleja un consenso claro sobre la necesidad de actualizar la tecnología de vigilancia, lo que puede ser un punto a favor para la implementación de un software con inteligencia artificial (IA) que ofrezca mejores características y mayor eficiencia.



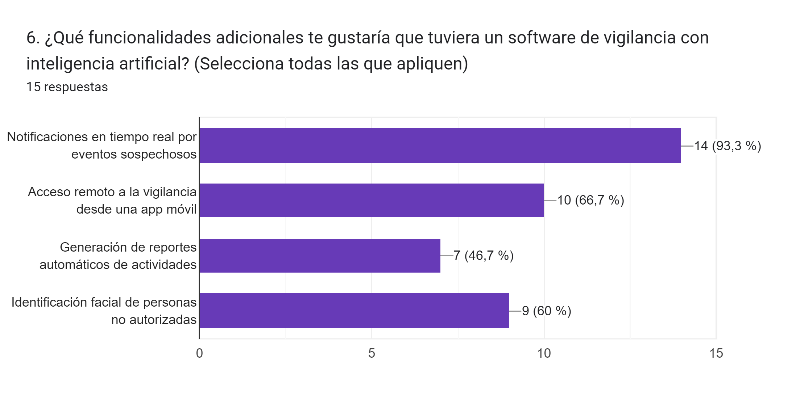
* **Resultados**:
  + Muy beneficioso: 20%
  + Beneficioso: 46,7%
  + Algo beneficioso: 26,7%
  + No beneficioso: 0%
* **Análisis**: La gran mayoría (93,4%) de los encuestados considera que implementar un software de IA es beneficioso, lo que muestra un alto nivel de aceptación hacia esta tecnología. Esto sugiere que los usuarios ven un valor significativo en la vigilancia continua y en la capacidad que la IA tiene para mejorar la seguridad.



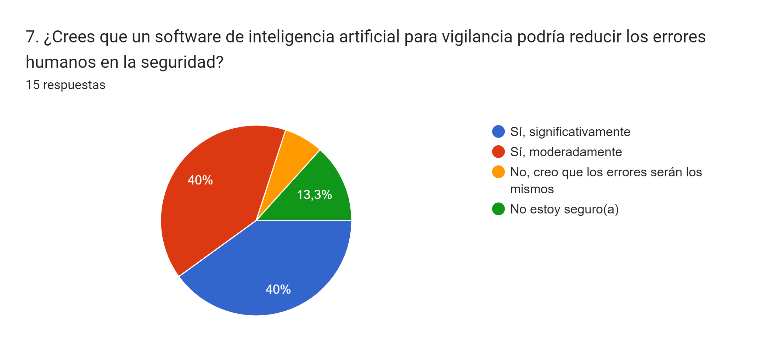
* **Resultados**:
* Mucho: 13,3%
* Bastante: 40%
* Algo: 33,3%
* Poco: 13,3%
* Nada: 0%
* **Análisis**: La confianza en la capacidad de la IA para identificar actividades sospechosas varía, con la mayoría (53,3%) confiando bastante o algo en ella. Sin embargo, un 26,6% de los encuestados tiene dudas, lo que refleja una cierta preocupación sobre la efectividad de la IA en comparación con la supervisión humana.



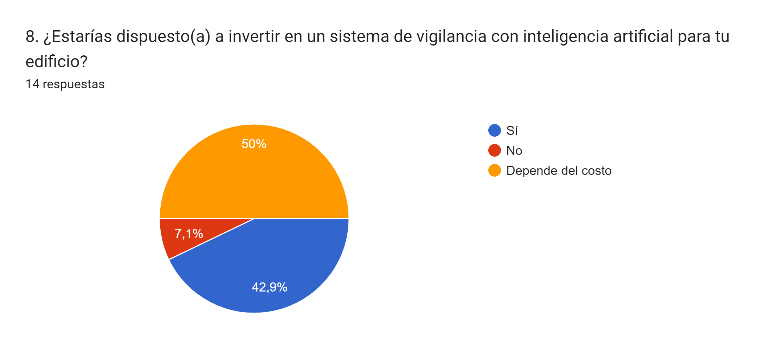
* **Resultados**:
* Sí, completamente: 13,3%
* Sí, pero con supervisión humana ocasional: 66,7%
* No, prefiero la vigilancia humana: 20%
* No estoy seguro(a): 0%
* **Análisis**: La mayoría de los encuestados (66,7%) prefiere mantener la supervisión humana, aunque aceptaría un sistema de IA con supervisión ocasional. Esto sugiere que, aunque los usuarios ven el valor en la IA, aún confían en la intervención humana para garantizar una seguridad completa.



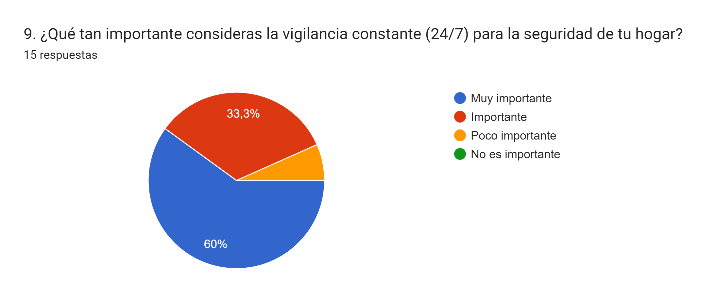
* **Resultados**:
* Notificaciones en tiempo real por eventos sospechosos: 14
* Acceso remoto a la vigilancia desde una app móvil: 10
* Generación de reportes automáticos de actividades: 7
* Identificación facial de personas no autorizadas: 9
* **Análisis**: Las funcionalidades más solicitadas son las notificaciones en tiempo real (14 votos) y el acceso remoto desde una app móvil (10 votos), lo que refleja un interés por la comodidad y la capacidad de actuar rápidamente ante situaciones sospechosas. También hay un interés moderado por la generación de reportes y la identificación facial.



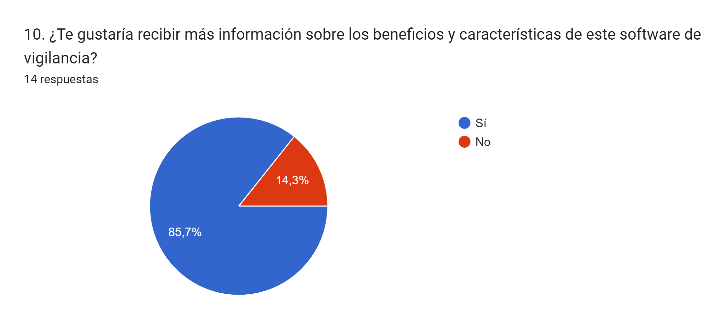
* **Resultados**:
* Sí, significativamente: 40%
* Sí, moderadamente: 40%
* No, creo que los errores serán los mismos: 0%
* No estoy seguro(a): 13,3%
* **Análisis**: La mayoría (80%) cree que la IA puede reducir significativamente o moderadamente los errores humanos, lo que indica una fuerte confianza en la capacidad de la IA para mejorar la precisión de la vigilancia y reducir fallos humanos.



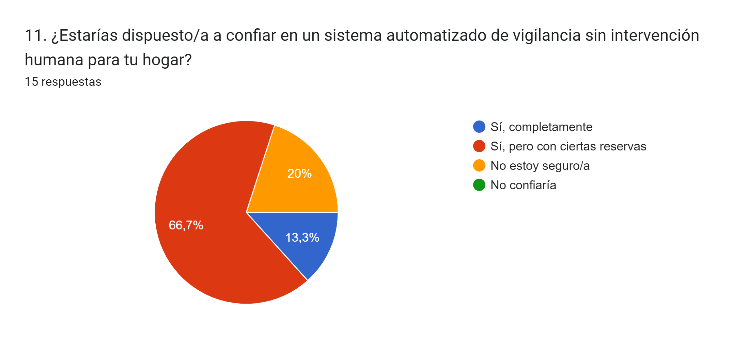
* **Resultados**:
* Sí: 42,9%
* No: 7,1%
* Depende del costo: 42,9%
* **Análisis**: La disposición a invertir en un sistema de IA es alta (85,8% en total), pero también hay una clara preocupación por el costo. Este dato sugiere que, aunque hay un interés general por la tecnología, los usuarios están atentos a los precios y probablemente buscarán una relación calidad-precio adecuada.



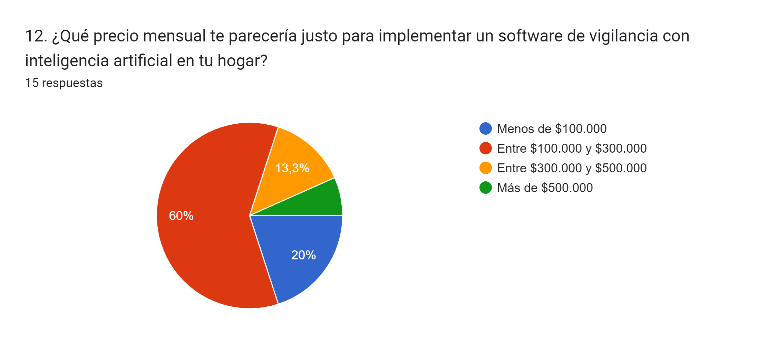
* **Resultados**:
* Muy importante: 60%
* Importante: 33%
* Poco importante: 0%
* No es importante: 0%
* **Análisis**: La gran mayoría (93%) considera que la vigilancia constante es crucial para la seguridad, lo que refuerza la necesidad de una solución de IA que pueda operar de manera continua sin intervención humana.



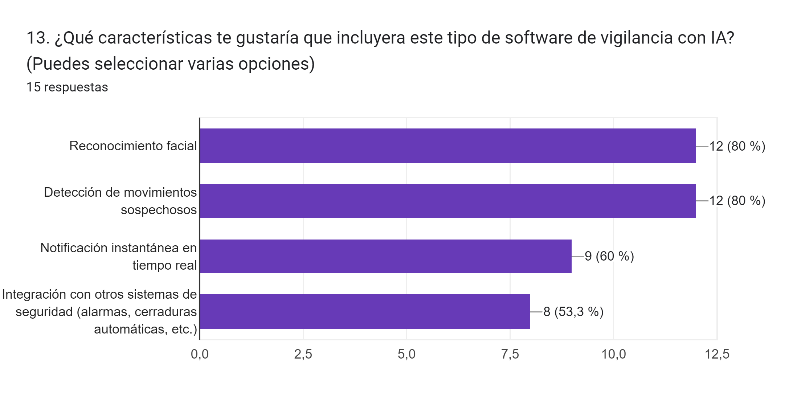
* **Resultados**:
* Sí: 85,7%
* No: 14,3%
* **Análisis**: Un porcentaje alto de encuestados está interesado en recibir más información, lo que muestra un interés en profundizar en los detalles de cómo la IA puede mejorar la seguridad y cómo funciona este tipo de software.



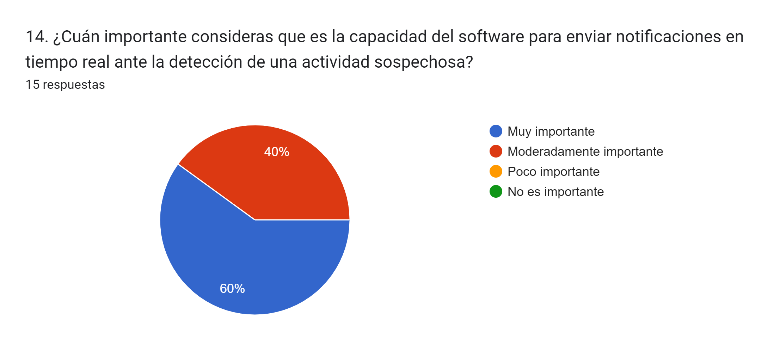
* **Resultados**:
* Sí, completamente: 13,3%
* Sí, pero con ciertas reservas: 66,7%
* No estoy seguro/a: 20%
* No confiaría: 0%
* **Análisis**: La mayoría de los usuarios (66,7%) estaría dispuesta a confiar en un sistema automatizado de vigilancia, aunque con algunas reservas. Esto sugiere que, aunque hay una aceptación de la tecnología, las personas aún valoran algún tipo de control humano.



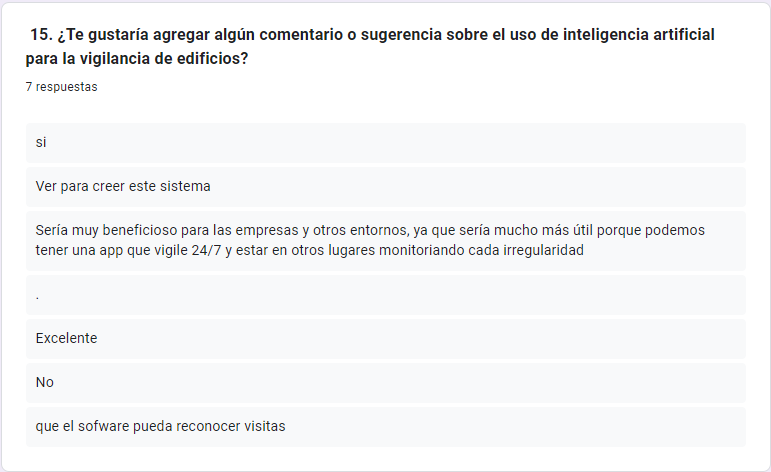
* **Resultados**:
* Menos de $100.000: 20%
* Entre $100.000 y $300.000: 60%
* Entre $300.000 y $500.000: 13,3%
* Más de $500.000: 0%
* **Análisis**: La mayoría de los encuestados está dispuesta a pagar entre $100.000 y $300.000 al mes por el servicio, lo que indica que existe un rango de precios aceptable para este tipo de tecnología, siempre que se mantenga dentro de una cantidad razonable.



* **Resultados**:
* Reconocimiento facial: 12
* Detección de movimientos sospechosos: 12
* Notificación instantánea en tiempo real: 9
* Integración con otros sistemas de seguridad (alarmas, cerraduras automáticas, etc.): 8
* **Análisis**: El reconocimiento facial y la detección de movimientos sospechosos son las características más solicitadas, lo que muestra un interés por la personalización y la capacidad de identificar amenazas específicas. Las notificaciones en tiempo real y la integración con otros sistemas de seguridad también son valoradas, lo que refuerza la idea de que los usuarios buscan un sistema integral.



* **Resultados**:
* Muy importante: 60%
* Moderadamente importante: 40%
* Poco importante: 0%
* No es importante: 0%
* **Análisis**: La capacidad de recibir notificaciones instantáneas es considerada muy importante por la mayoría (100%) de los usuarios, lo que subraya la necesidad de una respuesta rápida ante situaciones sospechosas.



* **Resultados**:
* Comentarios varios, como:
  + "Ver para creer este sistema."
  + "Sería muy beneficioso para las empresas y otros entornos."
  + "Que el software pueda reconocer visitas."
* **Análisis**: Los comentarios sugieren un interés por probar el sistema en la práctica y también destacan el valor potencial de la IA para entornos empresariales y residenciales. La sugerencia de reconocer visitas refleja un interés por mejorar la personalización y la efectividad del sistema.

### Conclusión

La encuesta refleja una **alta aceptación** hacia la implementación de un software de vigilancia con inteligencia artificial, considerando que esta tecnología puede **mejorar la seguridad en edificios** y reducir la necesidad de vigilancia humana. La mayoría de los encuestados confía en que la IA puede **detectar actividades sospechosas de forma más eficiente** que un vigilante humano, y las características más demandadas son el **reconocimiento facial, la detección de movimientos y notificaciones en tiempo real**.

A pesar de su aceptación, **persisten algunas preocupaciones** relacionadas con la **privacidad de los datos, fallos técnicos y la necesidad de supervisión humana** para validar las alertas. Esto sugiere que el software debe complementar, más que sustituir, la intervención humana.

En cuanto al costo, los encuestados muestran disposición a pagar entre **$100.000 y $300.000 mensuales**, lo que indica una expectativa razonable para su comercialización. En general, la encuesta destaca que un **enfoque híbrido**, combinando IA y personal humano, podría ser el más adecuado para garantizar una implementación exitosa.

### Definición del problema

En la actualidad, los sistemas de vigilancia tradicionales presentan limitaciones significativas en la capacidad de monitoreo constante. Los vigilantes humanos, aunque esenciales, no pueden mantener un control permanente sobre las cámaras de seguridad, lo que genera brechas en la detección de comportamientos sospechosos o situaciones de riesgo. Esta falta de atención continua puede ocasionar retrasos en la toma de decisiones críticas, comprometiendo la seguridad en los edificios.

Con el avance de la inteligencia artificial (IA), surge la oportunidad de desarrollar soluciones más eficientes y automatizadas. Un software basado en IA puede monitorear las cámaras las 24 horas del día, los 7 días de la semana, analizando patrones y comportamientos sospechosos de manera continua. La necesidad de una vigilancia más efectiva, ágil y precisa motiva este proyecto, que busca reducir la carga de trabajo de los guardias y mejorar su capacidad de respuesta mediante notificaciones en tiempo real sobre eventos que requieran su intervención.

### Antecedentes del problema

A lo largo del tiempo, la vigilancia ha sido una herramienta fundamental para la seguridad en edificios, instituciones y espacios públicos. Tradicionalmente, esta tarea ha dependido de la presencia de guardias que monitorean cámaras de seguridad o realizan rondas periódicas. Sin embargo, este enfoque presenta limitaciones claras, ya que los seres humanos, por naturaleza, no pueden mantener un nivel constante de atención durante largos periodos. Esto ha generado desafíos en la detección oportuna de incidentes, como robos, vandalismo o intrusiones.

En los últimos años, los avances tecnológicos, especialmente en inteligencia artificial (IA) y análisis de imágenes, han abierto nuevas posibilidades para optimizar los sistemas de vigilancia. Empresas y organizaciones han comenzado a experimentar con soluciones que combinan cámaras de seguridad con IA, permitiendo que los sistemas identifiquen patrones de comportamiento y alerten sobre actividades sospechosas de forma automática.

Algunos estudios de casos han demostrado que la integración de inteligencia artificial mejora la precisión en la detección de eventos inusuales y reduce los tiempos de respuesta. Por ejemplo, sistemas de vigilancia con reconocimiento facial y detección de movimientos no autorizados ya se utilizan en aeropuertos, centros comerciales y complejos residenciales, facilitando un control más eficiente.

Sin embargo, la dependencia exclusiva del personal humano sigue siendo un reto en muchos entornos. Esto no solo aumenta el riesgo de omisión de eventos importantes, sino que también genera sobrecarga laboral y fatiga en los vigilantes, afectando su desempeño. Por ello, existe una necesidad creciente de adoptar tecnologías de automatización que garanticen una vigilancia continua sin interrupciones.

La integración de IA en los sistemas de vigilancia se presenta como una solución prometedora para estos problemas. Un software capaz de analizar en tiempo real las imágenes de las cámaras, identificar patrones sospechosos y notificar de inmediato al personal encargado podría transformar la forma en que se gestionan los sistemas de seguridad en edificios. Este enfoque no solo reduce la dependencia de los vigilantes, sino que también asegura una respuesta más rápida y eficiente ante situaciones críticas.

### Justificación del problema

La vigilancia tradicional presenta limitaciones debido a la fatiga y distracción de los guardias, lo que puede comprometer la seguridad en edificios. Por ello, es necesario implementar un software de inteligencia artificial (IA) capaz de analizar las cámaras las 24/7, identificando comportamientos sospechosos y notificando en tiempo real al personal encargado.

Este sistema complementará la labor del vigilante, aliviando su carga y mejorando la eficiencia en la respuesta ante incidentes. La integración de IA garantiza una vigilancia constante y precisa, minimizando errores humanos y ofreciendo mayor confianza y seguridad en los entornos monitoreados.

### Pregunta problemática

¿cómo se podría implementar un software para tener un mejor control de vigilancia en las unidades residenciales, implementando una cámara capaz de analizar situaciones y realizar informes para el vigilante?

## Listado de necesidades y características

|  |  |
| --- | --- |
| **Necesidades** | **Características** |
| **Manejo de información de propietarios** | **idp, nom1, nom2, ape1, ape2, direccion, telefono, email** |
| **Manejo de información de unidades residenciales** | |  | | --- | | **id\_unidad, nombre\_unidad, direccion, ciudad** |  |  | | --- | |  | |
| |  | | --- | | **Manejo de información de torres** |  |  | | --- | |  | | |  | | --- | | **id\_torre, num\_pisos, num\_aptos\_por\_piso, id\_unidad** |  |  | | --- | |  | |
| |  | | --- | | **Manejo de información de apartamentos** |  |  | | --- | |  | | |  | | --- | | **id\_apto, num\_apto, id\_torre** |  |  | | --- | |  | |
| |  | | --- | | **Manejo de información de personas** |  |  | | --- | |  | | |  | | --- | | **id\_persona, nom1, nom2, ape1, ape2, tipo\_persona, fecha\_nacimiento, tel\_fijo, tel\_movil, email** |  |  | | --- | |  | |
| |  | | --- | | **Manejo de información de cámaras** |  |  | | --- | |  | | |  | | --- | | **id\_camara, ubicacion, tipo\_camara, id\_torre** |  |  | | --- | |  | |
| |  | | --- | | **Manejo de información de comportamientos** |  |  | | --- | |  | | |  | | --- | | **id\_comportamiento, descripcion, nivel\_riesgo** |  |  | | --- | |  | |
| |  | | --- | | **Registro de comportamientos** |  |  | | --- | |  | | |  | | --- | | **id\_registro, fecha\_hora, id\_comportamiento, id\_camara, id\_persona** |  |  | | --- | |  | |
| |  | | --- | | **Manejo de información de soluciones** |  |  | | --- | |  | | |  | | --- | | **id\_solucion, descripcio** |  |  | | --- | |  | |
| |  | | --- | | **Registro de aplicación de soluciones** |  |  | | --- | |  | | **id\_aplicacion\_solucion, fecha\_aplicacion, descripcion, id\_persona, resultado\_esperado** |
| **Manejo de avisos** | **id\_aviso, descripcion, fecha\_hora, tipo\_autoridad, persona\_notificada** |
| **Manejo de información de autoridades** | **id\_autoridad, tipo\_autoridad, empresa\_autoridad** |
| **Manejo de reportes de sucesos** | **id\_reporte, fecha\_hora, descripcion, id\_camara, id\_persona, medidas\_tomadas** |

## Fuente: elaboración propia

## Objetivó general

Desarrollar un software de inteligencia artificial entrenado para analizar las imágenes captadas por cámaras de seguridad, analizar su comportamiento y detectar actividades que requieran atención especial.

## Objetivos específicos

- Establecer una vigilancia continua de 24/7 mediante el software, garantizando la detección oportuna de situaciones sospechosas o inusuales.

- Automatizar el proceso de vigilancia, minimizando la dependencia de personal humano para el monitoreo de cámaras de seguridad.

- Mejorar la eficiencia en la respuesta ante eventos de seguridad, proporcionando alertas en tiempo real cuando se detecten comportamientos sospechosos.

Alcance del sistema propuesto en términos de (entradas, procesos y salidas)

|  |  |  |
| --- | --- | --- |
| **Entradas** | **Procesos** | **Salidas** |
| |  | | --- | | **Datos de propietarios (idp, nom1, nom2, ape1, ape2, direccion, telefono, email)** |  |  | | --- | |  | | |  | | --- | | **Registrar y gestionar la información de propietarios** |  |  | | --- | |  | | |  | | --- | | **Información de propietarios actualizada y accesible** |  |  | | --- | |  | |
| |  | | --- | | **Datos de unidades residenciales (id\_unidad, nombre\_unidad, direccion, ciudad)** |  |  | | --- | |  | | |  | | --- | | **Registrar y gestionar las unidades residenciales** |  |  | | --- | |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | **Listado de unidades residenciales** |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |
| |  |  |  | | --- | --- | --- | | |  | | --- | | **Datos de torres (id\_torre, num\_pisos, num\_aptos\_por\_piso, id\_unidad)** |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | **Registrar y gestionar las torres en cada unidad residencial** |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | **Listado de torres con detalles** |  |  | | --- | |  | |  |  | | --- | |  | |  |  | | --- | |  | |
| |  |  |  | | --- | --- | --- | | |  | | --- | | **Datos de apartamentos (id\_apto, num\_apto, id\_torre)** |  |  | | --- | |  | |  |  | | --- | |  | | |  | | --- | | **Gestión de alertas**: Notificación al vigilante a través de una aplicación móvil. |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | **Listado de apartamentos por torre** |  |  | | --- | |  | |  |  | | --- | |  | |
| |  |  |  | | --- | --- | --- | | |  | | --- | | **Datos de personas (id\_persona, nom1, nom2, ape1, ape2, tipo\_persona, fecha\_nacimiento, tel\_fijo, tel\_movil, email)** |  |  | | --- | |  | |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | **Registrar y gestionar la información de personas** |  |  | | --- | |  | |  |  | | --- | |  | | |  | | --- | | **Información detallada de personas** |  |  | | --- | |  | |
| |  | | --- | | **Datos de cámaras (id\_camara, ubicacion, tipo\_camara, id\_torre)** |  |  | | --- | |  | | |  | | --- | | **Registrar y gestionar la información de cámaras** |  |  | | --- | |  | | |  | | --- | | **Listado de cámaras con ubicación y tipo** |  |  | | --- | |  | |
| |  | | --- | | **Datos de comportamientos (id\_comportamiento, descripcion, nivel\_riesgo)** |  |  | | --- | |  | | |  | | --- | | **Registrar y gestionar tipos de comportamientos** |  |  | | --- | |  | | |  | | --- | | **Listado de comportamientos y niveles de riesgo** |  |  | | --- | |  | |
| |  | | --- | | **Datos de soluciones (id\_solucion, descripcion)** |  |  | | --- | |  | | |  | | --- | | **Registrar y gestionar tipos de soluciones aplicables** |  |  | | --- | |  | | |  | | --- | | **Listado de soluciones** |  |  | | --- | |  | |
| |  | | --- | | **Aplicación de soluciones (id\_aplicacion\_solucion, fecha\_aplicacion, descripcion, id\_persona, resultado\_esperado)** |  |  | | --- | |  | | |  | | --- | | **Registrar y gestionar la aplicación de soluciones** |  |  | | --- | |  | | |  | | --- | | **Registro de soluciones aplicadas y resultados** |  |  | | --- | |  | |
| **Datos de avisos (id\_aviso, descripcion, fecha\_hora, tipo\_autoridad, persona\_notificada)** | |  | | --- | | **Registrar y gestionar avisos de seguridad** |  |  | | --- | |  | | |  | | --- | | **Notificaciones enviadas al personal o autoridades** |  |  | | --- | |  | |
| |  | | --- | | **Datos de autoridades (id\_autoridad, tipo\_autoridad, empresa\_autoridad)** |  |  | | --- | |  | | |  | | --- | | **Registrar y gestionar información de autoridades** |  |  | | --- | |  | | |  | | --- | | **Listado de autoridades** |  |  | | --- | |  | |
| |  | | --- | | **Datos de reportes de sucesos (id\_reporte, fecha\_hora, descripcion, id\_camara, id\_persona, medidas\_tomadas)** |  |  | | --- | |  | | |  | | --- | | **Generar reportes de sucesos registrados** |  |  | | --- | |  | | Reportes detallados de sucesos |

## Fuente: elaboración propia

## Nombre que se le colocará al sistema de software

##### **watchful eye**

## Cronograma de actividades

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Actividad | fecha  Inicio | Fecha  Final | T.E  (hra) | T.R  (hra) | responsable | recursos | Observación |
| Investigación y recopilación de información sobre sistemas de vigilancia y IA | 01-01-24 | 15-01-24 | 20 | 25 | Equipo de investigación | Internet, bibliografía, portátiles | Revisión de estudios y literatura relevante sobre IA aplicada a vigilancia y seguridad en unidades residenciales. |
| Definición de requisitos del proyecto | 16-01-24 | 20-01-24 | 15 | 18 | Equipo de desarrollo y cliente | Portátil, software de documentación | Reuniones con cliente para definir objetivos y alcance del proyecto de acuerdo con sus necesidades de vigilancia. |
| Selección de herramientas y tecnologías para el desarrollo del software | 21-01-24 | 25-01-24 | 10 | 12 | Equipo de desarrollo | Internet, análisis de herramientas, documentación técnica | Evaluación de plataformas de IA, cámaras compatibles y lenguajes de programación adecuados para el proyecto |
| Diseño de arquitectura del software | 26-01-24 | 10-02-24 | 25 | 30 | Arquitecto de software | Herramientas de diseño de software (e.g., UML, diagramas de flujo) | Creación del esquema de arquitectura general del software, incluyendo módulos de análisis y notificación. |
| Desarrollo de módulos de análisis de comportamiento | 11-02-24 | 10-03-24 | 50 | 60 | Desarrolladores de IA | IDE de programación, bibliotecas de IA y visión artificial | Implementación de algoritmos de IA para análisis de video en tiempo real, detección de patrones y anomalías. |
| Entrenamiento y ajuste del modelo de IA para detección de comportamientos sospechosos | 11-03-24 | 30-03-24 | 40 | 50 | Especialistas en IA | Datos de entrenamiento, hardware de procesamiento | El modelo se entrena con datos reales y se ajusta para mejorar su precisión en la detección de comportamientos. |
| Integración de módulos de notificación y alertas en tiempo real | 01-04-24 | 15-04-24 | 20 | 25 | Desarrolladores de back-end | Software de notificación, plataforma de integración | Desarrollo de la funcionalidad de notificación para alertar al vigilante sobre eventos sospechosos detectados. |
| Pruebas iniciales de funcionalidad y detección de errores | 16-04-24 | 30-04-24 | 20 | 25 | Equipo de pruebas | Cámara, software, protocolo de pruebas | Validación de la funcionalidad y detección de errores en los módulos de análisis y notificación. |
| Implementación en un entorno de prueba en la unidad residencial | 01-05-24 | 15-05-24 | 20 | 25 | Ingeniero de sistemas | Equipos de vigilancia, acceso a cámaras del lugar | Instalación del software y pruebas en un entorno simulado para evaluar la eficiencia del sistema en tiempo real. |
| Revisión de feedback y ajustes finales | 16-05-24 | 30-05-24 | 15 | 20 | Equipo de desarrollo y cliente | Portátil, software de ajuste y análisis | Ajuste del sistema según el feedback recibido de las pruebas en el entorno de prueba. |
| Capacitación del personal de vigilancia | 01-06-24 | 10-06-24 | 10 | 12 | Especialistas en IA | Material de capacitación, manuales del software | Capacitación del equipo de vigilancia en el uso del software de IA y respuesta a las notificaciones. |
| Lanzamiento final y monitoreo inicial | 11-06-24 | 20-06-24 | 10 | 12 | Todo el equipo | Recursos de soporte, manuales del sistema | Lanzamiento oficial del software en la unidad residencial y monitoreo de su funcionamiento inicial. |

## Fuente: elaboración propia

\*TE (Tiempo Estimado)

\*\*TR (Tiempo Real)

## Análisis de riesgos

|  |  |  |  |
| --- | --- | --- | --- |
| Análisis de riesgos | | | |
| Descripción del riesgo | Tipo de riesgo | Probabilidad que ocurra | Plan de acción |
| Fallo en el servidor que podría causar la interrupción de las operaciones del sistema | Técnico | Alta | Realizar mantenimiento preventivo y programado en el servidor. Mantener respaldo en un servidor secundario. |
| Pérdida de datos importantes por error humano (por ejemplo, eliminación accidental de información crítica) | Humano | Media | Implementar permisos de acceso para usuarios con diferentes niveles de privilegios y crear respaldos automáticos diarios |
| Vulnerabilidad en la seguridad del sistema que pueda permitir accesos no autorizados | Seguridad | Alta | Implementar protocolos de seguridad, como autenticación multifactor, encriptación de datos, y auditorías regulares de seguridad |
| Fallo en el sistema de cámaras de vigilancia, afectando la capacidad de monitoreo en tiempo real | Técnico | Media | Realizar mantenimiento preventivo en el sistema de cámaras y monitorear regularmente su funcionamiento |
| Baja aceptación del sistema por parte de los usuarios debido a una interfaz poco intuitiva | Usabilidad | Media | Realizar pruebas de usabilidad y adaptar el diseño de la interfaz basado en las sugerencias de los usuarios. |
| Errores en el sistema de notificaciones que podrían retrasar la comunicación de alertas de seguridad | Técnico | Media | Realizar pruebas de funcionamiento del sistema de notificaciones de forma periódica. |
| Riesgo de retrasos en la implementación por falta de capacitación del equipo de usuarios | Operativo | Media | Proveer capacitación adecuada y temprana al equipo de usuarios. |
| Dependencia de proveedores externos para el mantenimiento del sistema, lo cual podría generar retrasos en el soporte | Operacional | Alta | Establecer contratos con tiempos de respuesta claros y prever proveedores alternativos para soporte. |
| Desgaste o daño en los equipos de hardware, como cámaras o servidores, lo cual podría reducir la efectividad del sistema | Técnico | Media | Implementar un plan de mantenimiento preventivo para el hardware. |
| Incompatibilidad entre el sistema y otras herramientas o sistemas de seguridad externos | Técnico | Baja | Realizar pruebas de integración y asegurar que el sistema sea compatible con los sistemas de seguridad existentes. |

## Fuente: elaboración propia

## Análisis de requisitos

### Tabla general para casos de uso.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tabla general para casos de uso** | | | | | | |
| **Gestión** | **Actividades** | **Actores** | | | | |
| **Técnico** | **usuarios** | **Seguridad** | **Administrador** | **vigilante** |
| **Gestión de Propietarios** | Crear | **x** | **x** |  | **x** |  |
| Modificar | **X** | **x** |  | **x** |  |
| Consultar | **X** | **x** | **x** | **x** | **x** |
| Inhabilitar | **X** | x |  | x |  |
| Guardar | x | x |  | x |  |
| Salir | **X** | **x** |  | **x** |  |
| **Gestión de Unidad Residencial** | Crear | **X** |  | **x** | **x** | **x** |
| Modificar | **X** |  | **x** | **x** | **x** |
| Consultar | **X** | **x** | **x** | **x** | **X** |
| Inhabilitar | **X** |  | x | x | x |
| Guardar | x |  | x | x | x |
| Salir | **X** |  | **x** | **x** | **x** |
| **Gestión de Torres** | Crear | **X** |  | **x** | **x** | **X** |
| Modificar | **X** |  | **x** | **x** | **X** |
| Consultar | **X** | **x** | **x** | **x** | **X** |
| Inhabilitar | **X** |  | x | x | x |
| Guardar | x |  | x | x | x |
| Salir | **X** |  | **x** | **x** | **X** |
| **Gestión de Apartamentos** | Crear |  |  | **x** | **x** |  |
| Modificar |  |  | **x** | **x** |  |
| Consultar | **X** |  | **x** | **x** | **X** |
| Inhabilitar |  |  | x | x |  |
| Guardar |  |  | x | x |  |
| Salir |  |  | **x** | **x** |  |
| **Gestión de Personas** | Crear |  |  | **x** | **x** | **X** |
| Modificar |  |  | **x** | **x** | **X** |
| Consultar | **X** |  | **x** | **x** | **X** |
| Inhabilitar |  |  | x | x | x |
| Guardar |  |  | x | x | x |
| Salir |  |  | **x** | **x** | **X** |
| **Gestión de Cámaras** | Crear | **X** |  | **x** | **x** | **X** |
| Modificar | **X** |  | **x** | **x** | **X** |
| Consultar | **X** | **x** | **x** | **x** | **X** |
| Inhabilitar | **X** |  | x | x | x |
| Guardar | x |  | x | x | x |
| Salir | **X** |  | **x** | **x** | **X** |
| **Gestión de Comportamientos** | Crear | **X** |  | **x** |  | **X** |
| Modificar | **X** |  | **x** |  | **X** |
| Consultar | **X** |  | **x** | **x** | **X** |
| Inhabilitar | **X** |  | x |  | x |
| Guardar | x |  | x |  | x |
| Salir | **X** |  | **x** |  | **X** |
| **Registro de Comportamientos** | Crear | **X** |  | **x** |  | **X** |
| Modificar | **X** |  | **x** |  | **X** |
| Consultar | **X** |  | **x** | **x** | **X** |
| Inhabilitar | **X** |  | x |  | x |
| Guardar | x |  | x |  | x |
| Salir | **X** |  | **x** |  | **X** |
| **Gestión de Soluciones** | Crear | **x** |  |  | **x** |  |
| Modificar | **X** |  |  | **x** |  |
| Consultar | **X** |  | **x** | **x** |  |
| Inhabilitar | **X** |  |  | x |  |
| Guardar | x |  |  | x |  |
| Salir | **X** |  |  | **x** |  |
| **Aplicación de Soluciones** | Crear | **X** |  |  | **x** |  |
| Modificar | **X** |  |  | **x** |  |
| Consultar | **X** | **x** | **x** | **x** |  |
| Inhabilitar | **X** |  |  | x |  |
| Guardar | x |  |  | x |  |
| Salir | **X** |  |  | **x** |  |
| **Gestión de Avisos** | Crear |  |  | **x** |  | **X** |
| Modificar |  |  | **x** |  | **X** |
| Consultar | **X** |  | **x** | **x** | **X** |
| Inhabilitar |  |  | x |  | x |
| Guardar |  |  | x |  | x |
| Salir |  |  | **x** |  | **X** |
| **Gestión de Autoridades** | Crear |  |  |  |  | **X** |
| Modificar |  |  |  |  | **X** |
| Consultar | **X** | **x** | **x** | **x** | **X** |
| Inhabilitar |  |  |  |  | x |
| Guardar |  |  |  |  | x |
| Salir |  |  |  |  | **X** |
| **Gestión de Reportes de Sucesos** | Crear |  |  | **x** |  | **X** |
| Modificar |  |  | **x** |  | **X** |
| Consultar | **X** |  | **x** | **x** | **X** |
| Inhabilitar |  |  | x |  | x |
| Guardar |  |  | x |  | x |
| Salir |  |  | **x** |  | **X** |

## Fuente: elaboración propia

## Requisitos de Usuario

|  |  |  |  |
| --- | --- | --- | --- |
| Requisitos de usuario (RU) | | | |
| Id requisito | Nombre del requisito | Descripción del requisito | usuario |
| RU-01 | |  | | --- | | Gestión de propietarios |  |  | | --- | |  | | |  | | --- | | Permite agregar, modificar, eliminar y consultar información de propietarios (ID, nombres, datos de contacto). |  |  | | --- | |  | | Administrador |
| |  | | --- | | RU-02 |  |  | | --- | |  | | Gestión de comportamientos | Permite registrar y consultar comportamientos asociados a residentes o visitantes (fecha, descripción, tipo). | Seguridad, Administrador |
| RU-03 | Gestión de cámaras | Permite administrar y monitorear el tipo y ubicación de cámaras en el sistema. | Técnico, Administrador |
| RU-04 | Gestión de autoridades | Permite registrar y consultar información sobre autoridades (nombre, empresa, contacto) para notificación rápida. | Administrador |
| RU-05 | Generación de reportes | Genera informes automáticos sobre sucesos, comportamientos y datos de residentes para análisis y auditoría. | Administrador |
| RU-06 | Notificaciones de incidentes | Notifica en tiempo real al personal de seguridad sobre incidentes o comportamientos sospechosos detectados. | |  | | --- | | Seguridad |  |  | | --- | |  | |
| RU-07 | Acceso remoto a información | Proporciona acceso móvil para consultar y gestionar cámaras y registros de comportamientos. | Administrador, Seguridad |
| RU-08 | Integración con sistemas de seguridad | Sincroniza alertas y datos con otros sistemas de seguridad instalados en la unidad residencial. | Administrador, Técnico |
| RU-09 | Administración de permisos de usuario | Permite definir roles y permisos para los usuarios según sus funciones en el sistema. | Administrador |
| RU-10 | Revisión y retroalimentación del sistema | Captura comentarios de usuarios para mejora continua del sistema. | Todos los usuarios |

## Fuente: elaboración propia

## Requisitos Funcionales

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Requisitos funcionales (RF) | | | | |
| Id requisito | Nombre del requisito | Descripción del requisito | usuario | id requisito de usuario |
| RF-1 | Crear propietario | Permite registrar nuevos propietarios en el sistema con sus datos personales y de contacto. | Administrador | RU1 |
| RF-2 | Modificar propietario | Permite actualizar la información de un propietario existente. | Administrador | |  | | --- | | RU1 |  |  | | --- | |  | |
| RF-3 | Eliminar propietario | Permite eliminar el registro de un propietario del sistema. | Administrador | RU1 |
| RF-4 | Consultar propietario | Permite buscar y visualizar la información de propietarios en el sistema. | Administrador | RU1 |
| RF-5 | Registrar comportamiento | Permite ingresar y registrar un comportamiento o incidencia asociada a un residente o visitante. | Seguridad, Administrador | RU2 |
| RF-6 | Consultar comportamientos | Permite buscar y visualizar registros de comportamientos de residentes y visitantes. | Seguridad, Administrador | RU2 |
| RF-7 | Administrar cámaras | Permite registrar, actualizar y eliminar información sobre el tipo y ubicación de cámaras en la unidad residencial. | Técnico, Administrador | RU3 |
| RF-8 | Monitoreo de cámaras | Permite acceder al monitoreo en tiempo real de las cámaras. | Técnico, Administrador | RU3 |
| RF-9 | Registrar autoridades | Permite registrar datos de autoridades relevantes para el sistema (nombre, empresa, contacto). | Administrador | RU4 |
| RF-10 | Generar reportes | Crea informes automáticos de sucesos, comportamientos y estadísticas para análisis. | Administrador | RU5 |
| RF-11 | Notificación de incidentes | Envía alertas inmediatas al personal de seguridad en caso de incidentes o comportamientos | Seguridad | RU6 |
| RF-12 | Acceso móvil | Permite a usuarios autorizados acceder a la información y gestionar cámaras desde dispositivos móviles. | Administrador, Seguridad | RU7 |
| RF-13 | Integración de seguridad | Sincroniza datos y alertas con otros sistemas de seguridad para mejorar la cobertura y protección de la unidad. | Técnico, Administrador | RU8 |
| RF-14 | Gestión de permisos | Define roles y permisos de acceso para cada usuario según su rol en el sistema. | Administrador | RU9 |
| RF-15 | Feedback de usuarios | Recoge sugerencias de los usuarios sobre el sistema para promover mejoras continuas. | Todos los usuarios | RU10 |

## Fuente: elaboración propia

## Requisitos No funcionales

### Facilidad de uso (“usability”)

|  |  |
| --- | --- |
| ID Requisito | Descripción del Requisito |
| RNF-001 | La interfaz del sistema debe ser intuitiva y fácil de usar para todos los roles (Administrador, Seguridad, Técnico). |
| RNF-002 | El sistema debe ser accesible desde múltiples dispositivos, incluyendo computadoras y dispositivos móviles. |
| RNF-003 | El sistema debe ofrecer una guía rápida o tutorial para la capacitación de los nuevos usuarios. |

### Confiabilidad

|  |  |
| --- | --- |
| ID Requisito | Descripción del Requisito |
| RNF-004 | Los datos deben ser respaldados automáticamente cada 24 horas para evitar pérdida de información crítica. |
| RNF-005 | El sistema debe estar disponible el 99.9% del tiempo, minimizando los tiempos de inactividad. |

### Ambiente de Trabajo (“Performance”)

|  |  |
| --- | --- |
| ID Requisito | Descripción del Requisito |
| RNF-006 | El sistema debe responder en menos de 2 segundos para las funciones de monitoreo y consulta de alertas. |
| RNF-007 | El sistema debe ser escalable para soportar hasta 1000 usuarios concurrentes sin afectar el rendimiento. |
| RNF-008 | El sistema debe tener capacidad para almacenar hasta 1 año de grabaciones y datos históricos. |

### Restricciones de Diseño

|  |  |
| --- | --- |
| ID Requisito | Descripción del Requisito |
| RNF-009 | El sistema debe ser compatible con cámaras de video IP de diferentes marcas y modelos. |
| RNF-010 | El sistema debe tener un diseño modular para permitir futuras actualizaciones y mejoras sin afectar su estabilidad. |

### Seguridad

|  |  |
| --- | --- |
| ID Requisito | Descripción del Requisito |
| RNF-011 | El sistema debe requerir autenticación mediante usuario y contraseña para todos los roles. |
| RNF-012 | Los permisos deben estar claramente definidos según el rol (Administrador, Seguridad, Técnico). |
| RNF-013 | Todos los datos sensibles deben ser encriptados para proteger la privacidad y seguridad de los usuarios. |

### Documentación de Usuario y Sistemas de Ayuda

|  |  |
| --- | --- |
| ID Requisito | Descripción del Requisito |
| RNF-014 | Debe incluir un manual de usuario detallado para cada rol en el sistema (Administrador, Seguridad, Técnico). |
| RNF-015 | El sistema debe contar con un sistema de ayuda en línea accesible para resolver dudas y problemas. |

### Interfaces

### Interfaz de Usuario

|  |  |
| --- | --- |
| ID Requisito | Descripción del Requisito |
| RNF-016 | La interfaz de usuario debe adaptarse a diferentes tamaños de pantalla (computadoras, tabletas, móviles). |
| RNF-017 | La interfaz debe mostrar notificaciones visuales para incidentes y alertas en tiempo real. |
| RNF-018 | |  | | --- | |  | | El usuario debe poder personalizar su tablero de control según sus necesidades (por ejemplo, colores, alertas). | |

Interfaces de Comunicación

|  |  |
| --- | --- |
| ID Requisito | Descripción del Requisito |
| RNF-018 | El sistema debe ofrecer una API para integrarse con otros sistemas de seguridad en la unidad residencial. |
| RNF-018 | Las notificaciones de alertas deben poder enviarse por SMS o correo electrónico a los usuarios autorizados. |

### Modelo de Casos de Uso

### Descripciones Generales de Actores

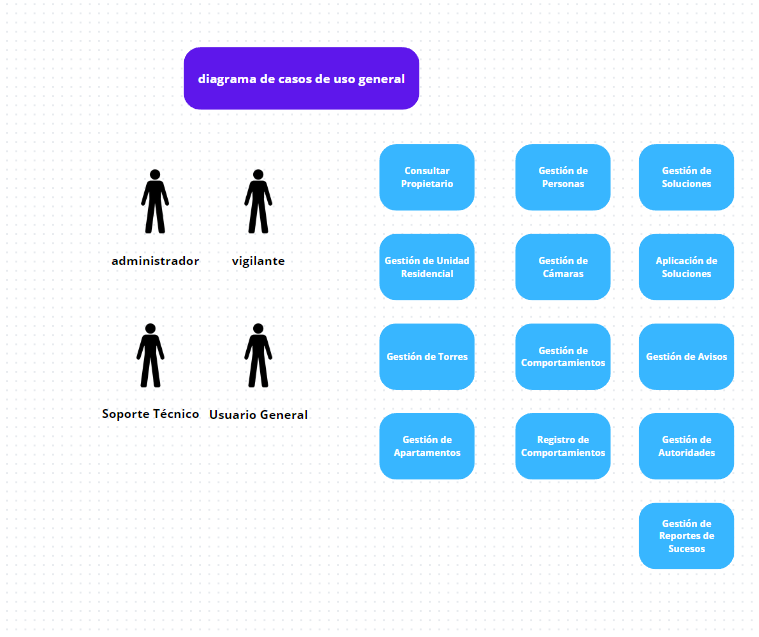
|  |  |
| --- | --- |
| Actor | Descripción |
| Administrador | Responsable de gestionar los usuarios, configuraciones y reportes del sistema. Tiene control completo sobre el sistema y sus funcionalidades. |
| Vigilante | Encargado de monitorear las cámaras y responder a las alertas en tiempo real. Tiene acceso limitado a funciones de consulta y notificación de incidentes. |
| Soporte Técnico | Responsable de la administración de las cámaras y el mantenimiento técnico del sistema. Puede modificar configuraciones y gestionar el acceso remoto. |
| Usuario General | Incluye a los residentes y visitantes autorizados que pueden interactuar con el sistema en ciertos aspectos (por ejemplo, recibir notificaciones de alerta). |

## Fuente: elaboración propia

### Especificación del requisito

#### Diagramas del Modelo de Casos de Uso.

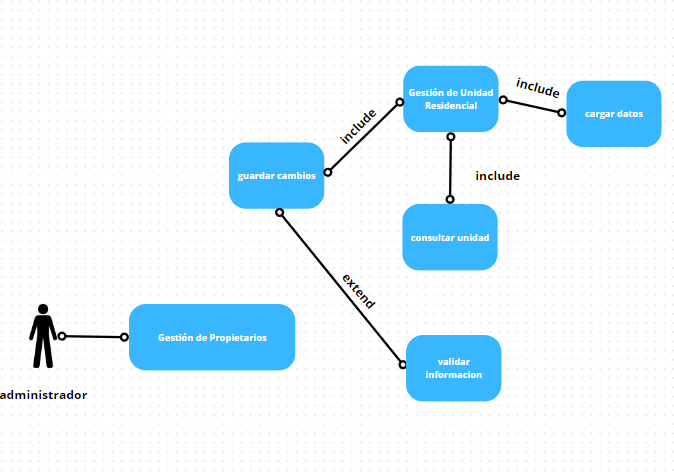
#### Diagrama general del sistema



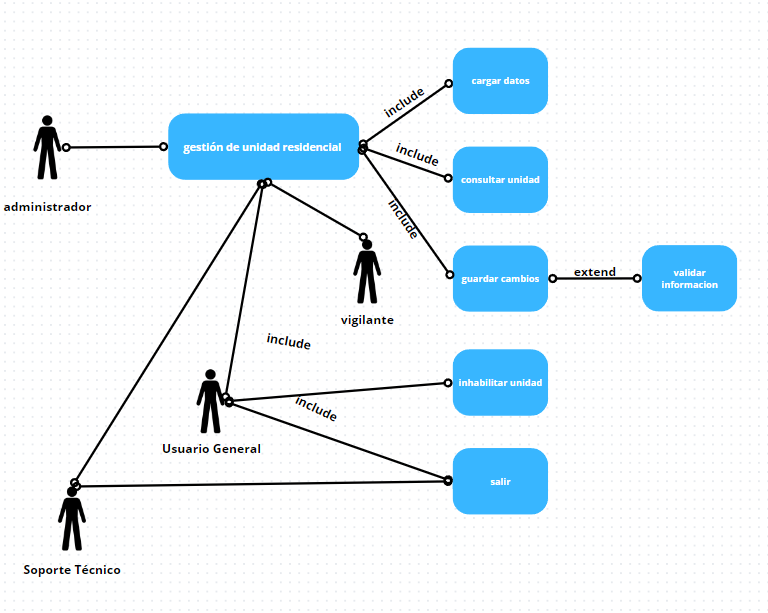
#### Fuente: Diseño propio

### Diagramas de casos de uso extendidos

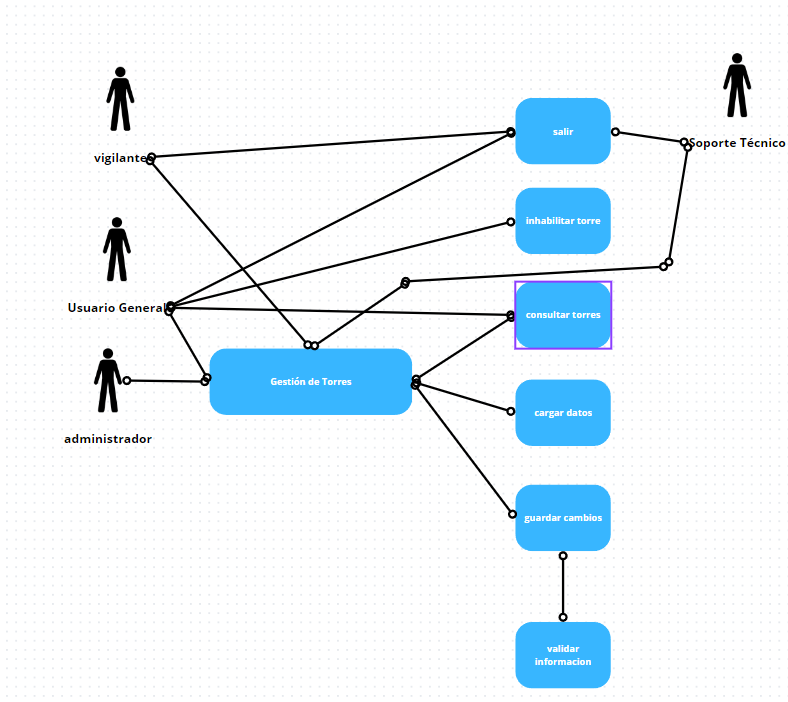
#### Diagrama de casos de uso extendido para la Gestión Cliente



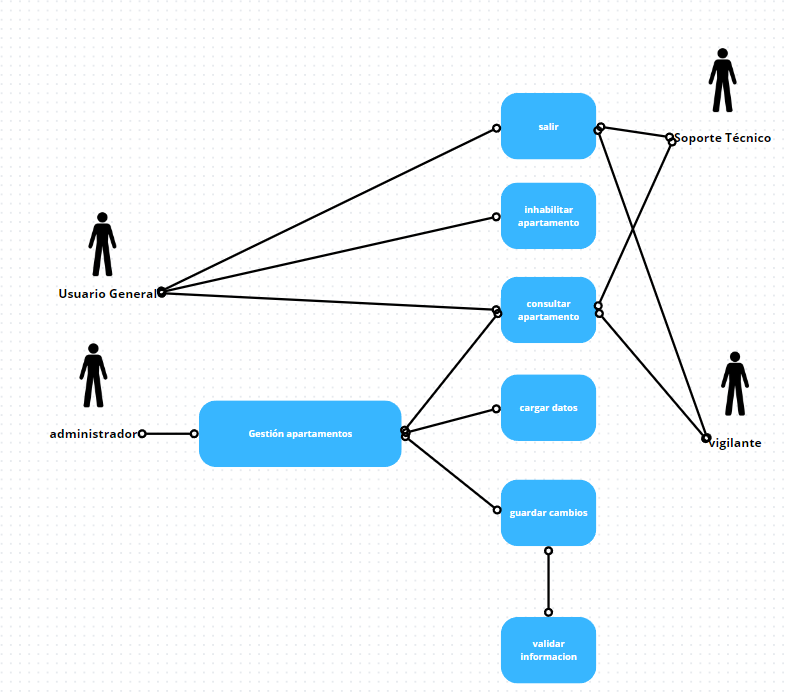
#### Fuente: elaboración propia



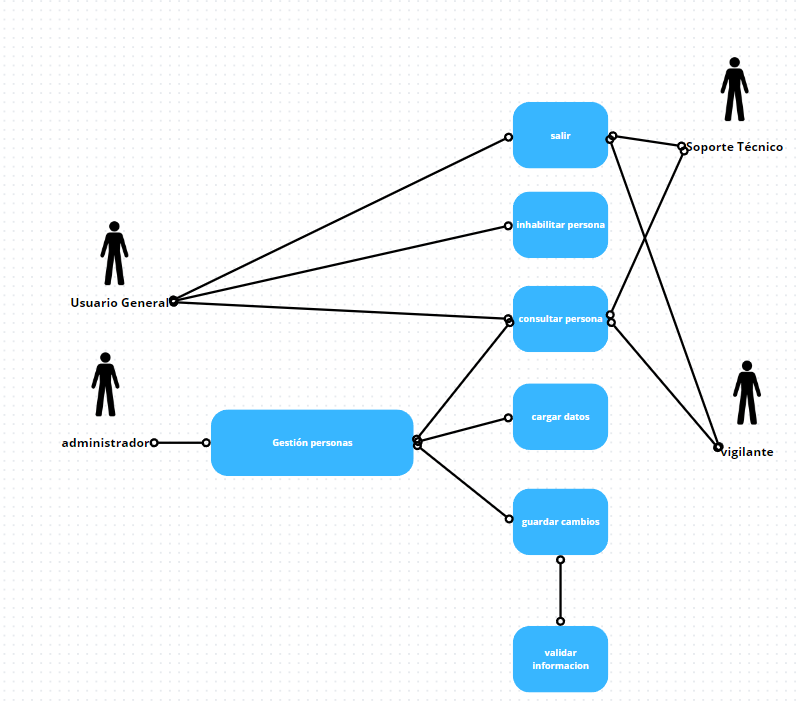
#### Fuente: elaboración propia



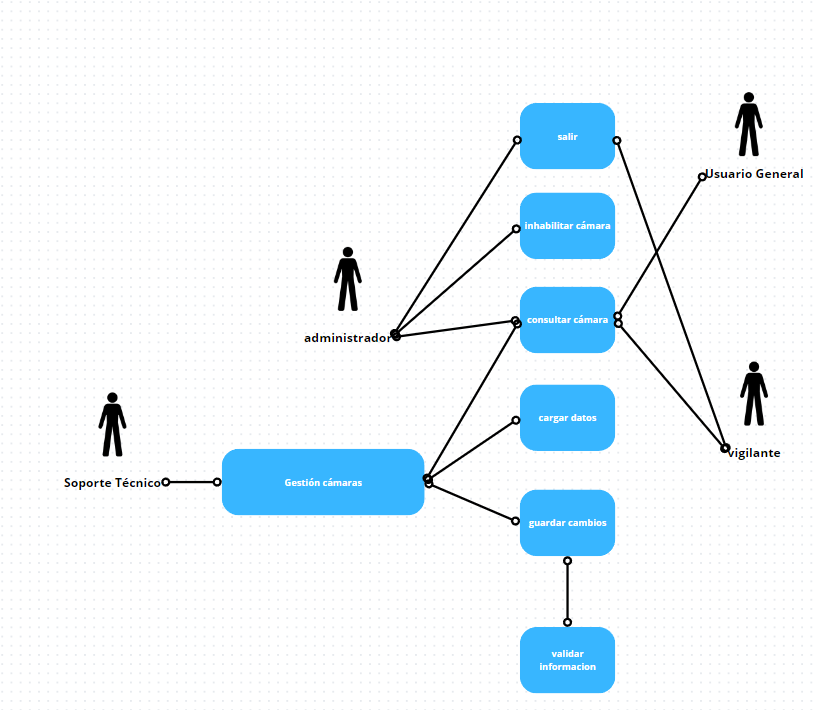
#### Fuente: Diseño propio



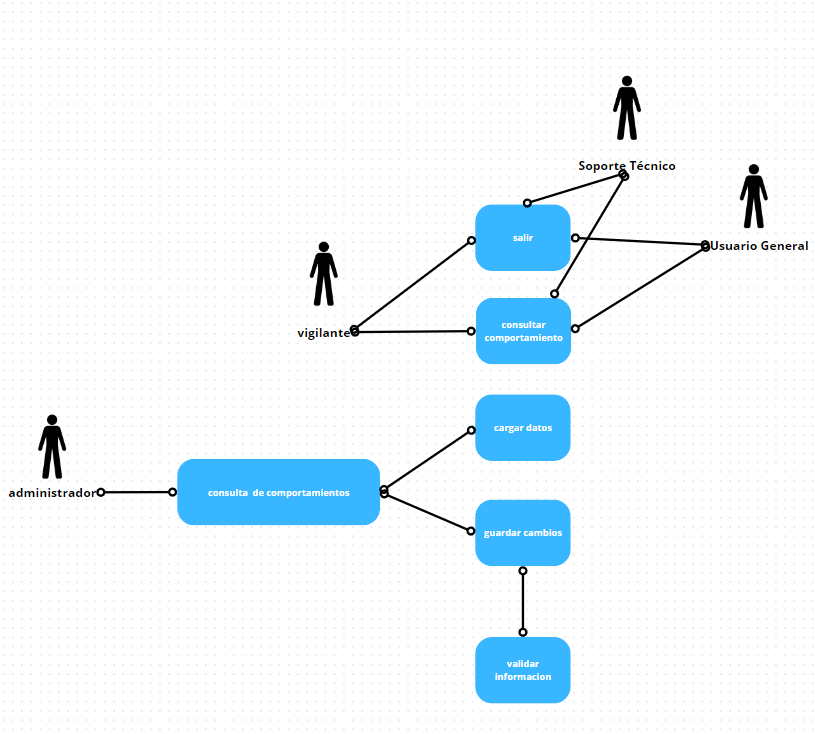
#### Fuente: Diseño propio



#### Fuente: Diseño propio



#### Fuente: Diseño propio

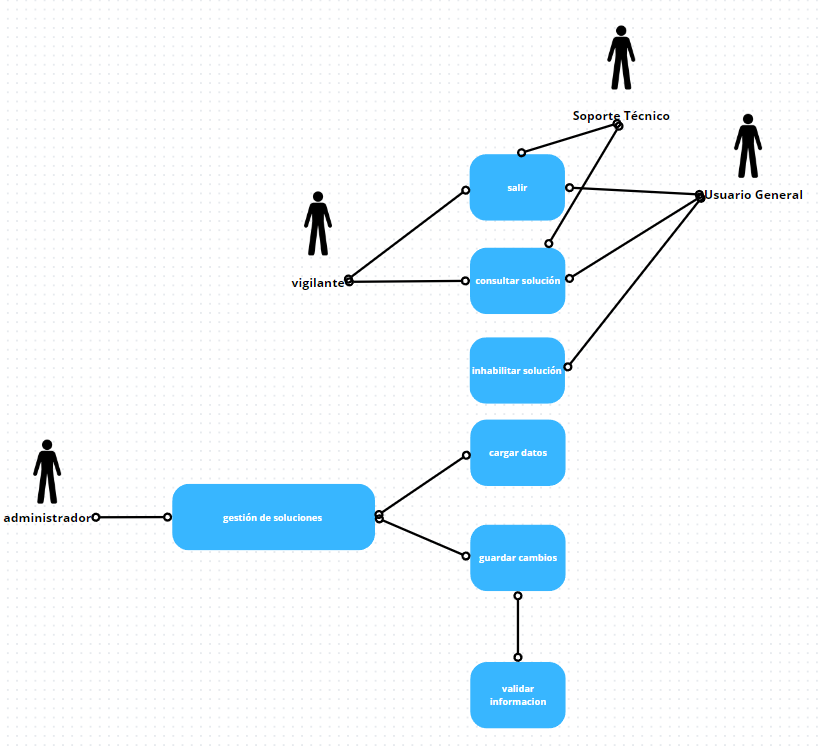


#### Fuente: Diseño propio

Diagrama

Descripción generada automáticamente

#### Fuente: Diseño propio

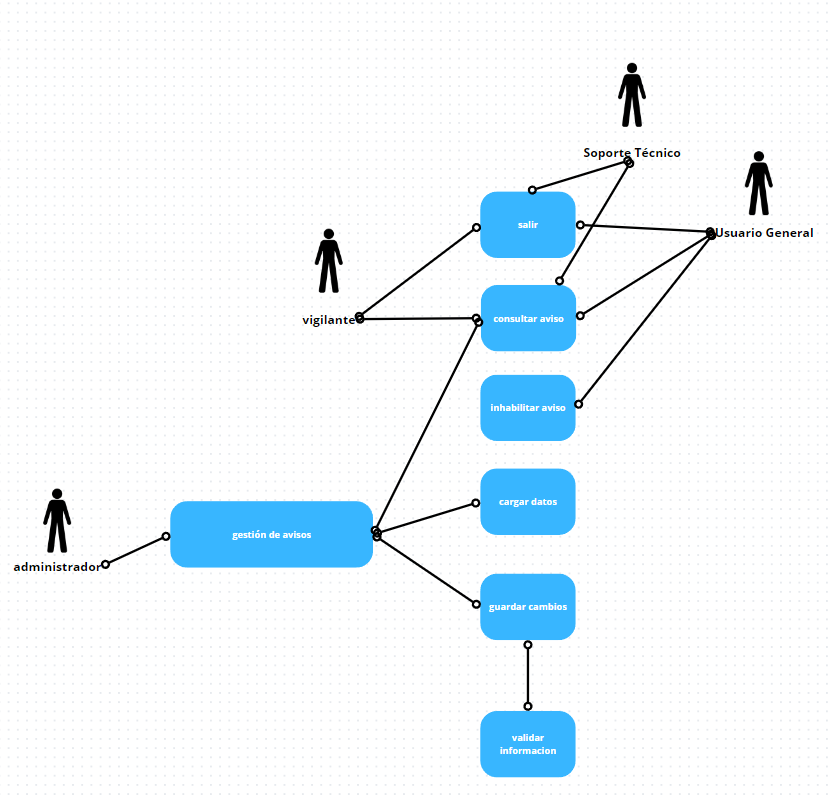


#### Fuente: Diseño propio

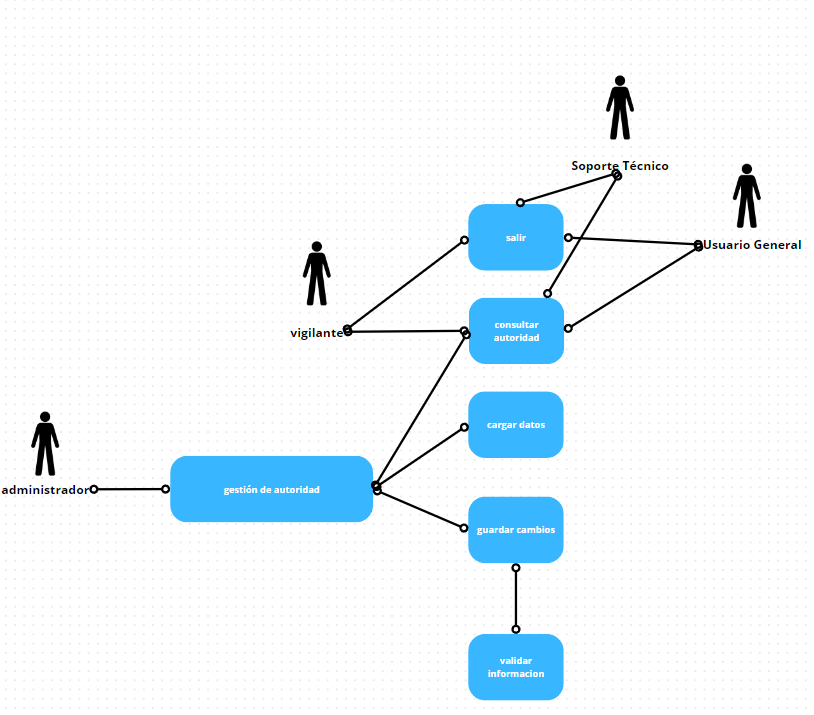
Diagrama

Descripción generada automáticamente

#### Fuente: Diseño propio



#### Fuente: Diseño propio



#### Fuente: Diseño propio

Diagrama

Descripción generada automáticamente

#### Fuente: Diseño propio

## Documentación o especificación de los Casos de Uso (Plantillas o escenarios)

|  |  |  |
| --- | --- | --- |
| **NOMBRE** | Crear Propietario | |
| **DESCRIPCION** | Permite registrar nuevos propietarios en el sistema con sus datos personales y de contacto. | |
| **ACTOR** | Administrador | |
| **PRECONDICIONES** | El usuario debe estar logueado en el sistema con permisos de administrador. | |
| **FLUJO BASICO** | | |
|  | **ACTOR** | **SISTEMA** |
| PASOS | 1. Ingresa al menú de propietarios. | El sistema muestra el formulario para registrar un nuevo propietario. |
| 2. Completa los datos personales y de contacto del propietario. | El sistema permite la entrada de los datos requeridos, como nombre, identificación, dirección, teléfono, etc. |
| 3. Da clic en el botón "Guardar". | El sistema valida los datos ingresados y guarda el nuevo registro del propietario en la base de datos. |
| 4. El sistema confirma el registro. | Muestra un mensaje de confirmación indicando que el propietario ha sido registrado exitosamente. |
| **FLUJO ALTERNATIVO** | | |
| PASOS | **ACTOR** | **SISTEMA** |
| 7. Si faltan datos obligatorios o el formato es incorrecto. | **Muestra un mensaje de alerta indicando que no existe el propietario.** |
| **Post-Condiciones** | El nuevo propietario ha sido registrado correctamente en el sistema. |  |
| **Requisito Funcional** | RF-001 |  |

## Fuente: elaboración propia

|  |  |  |
| --- | --- | --- |
| **NOMBRE** | Modificar Propietario | |
| **DESCRIPCION** | Permite actualizar la información de un propietario existente en el sistema. | |
| **ACTOR** | Administrador | |
| **PRECONDICIONES** | El usuario debe estar logueado en el sistema con permisos de administrador y el propietario debe existir en el sistema. | |
| **FLUJO BASICO** | | |
|  | **ACTOR** | **SISTEMA** |
| PASOS | 1. Ingresa al menú de propietarios y selecciona la opción de modificar. | El sistema muestra una lista de propietarios registrados. |
| 2. Selecciona el propietario a modificar. | El sistema despliega la información actual del propietario en un formulario editable. |
| 3. Realiza las modificaciones necesarias en los datos. | El sistema permite la edición de los campos seleccionados. |
| 4. Da clic en el botón "Guardar". | El sistema valida los datos modificados y actualiza la información del propietario en la base de datos. |
| 5. El sistema confirma la actualización. | Muestra un mensaje de confirmación indicando que la información del propietario ha sido actualizada correctamente. |
| **FLUJO ALTERNATIVO** | | |
| PASOS | **ACTOR** | **SISTEMA** |
| Si algún campo modificado tiene un error de formato o está incompleto. | Muestra un mensaje de error solicitando la corrección de los datos. |
| **Post-Condiciones** | La información del propietario ha sido actualizada correctamente en el sistema. |  |
| **Requisito Funcional** | RF-002 |  |

|  |  |  |
| --- | --- | --- |
| **NOMBRE** | Eliminar Propietario | |
| **DESCRIPCION** | Permite eliminar el registro de un propietario del sistema. | |
| **ACTOR** | Administrador | |
| **PRECONDICIONES** | El usuario debe estar logueado en el sistema con permisos de administrador y el propietario debe existir en el sistema. | |
| **FLUJO BASICO** | | |
|  | **ACTOR** | **SISTEMA** |
| PASOS | 1. Ingresa al menú de propietarios y selecciona la opción de eliminar. | El sistema muestra una lista de propietarios registrados. |
| 2. Selecciona el propietario a eliminar. | El sistema muestra los detalles del propietario seleccionado y solicita confirmación para eliminar. |
| 3. Confirma la eliminación del propietario. | El sistema elimina el registro del propietario de la base de datos. |
| |  | | --- | | 4. El sistema confirma la eliminación. | |  | | Muestra un mensaje de confirmación indicando que el propietario ha sido eliminado exitosamente. |
| **FLUJO ALTERNATIVO** | | |
| PASOS | **ACTOR** | **SISTEMA** |
| 7. Si el administrador cancela la acción. | El sistema regresa al menú de propietarios sin realizar cambios. |
| **Post-Condiciones** | El registro del propietario ha sido eliminado correctamente del sistema. |  |
| **Requisito Funcional** | RF-003 |  |

## Fuente: elaboración propia

|  |  |  |
| --- | --- | --- |
| **NOMBRE** | Consultar propietario | |
| **DESCRIPCION** | Permite buscar y visualizar la información de los propietarios registrados en el sistema. | |
| **ACTOR** | Administrador | |
| **PRECONDICIONES** | El usuario debe estar logueado en el sistema. | |
| **FLUJO BASICO** | | |
|  | **ACTOR** | **SISTEMA** |
| PASOS | 1.Ingresa al menú de propietarios. | El sistema despliega la interfaz con los campos de búsqueda: Número de ID, Nombre, y Apellido. |
| 2. Da clic en el botón "Consultar". | El sistema activa los campos de búsqueda para que el usuario pueda ingresar la información necesaria. |
| 3. Ingresa datos de búsqueda (ID | El sistema valida que los datos ingresados sean de un propietario registrado |
| 5. Da clic en "Salir". | El sistema cierra la pantalla de consulta de propietario. |
| 6. Muestra la información del propietario. | El sistema muestra la información del propietario en pantalla, incluyendo sus datos personales y de contacto. |
| **FLUJO ALTERNATIVO** | | |
| PASOS | **ACTOR** | **SISTEMA** |
| 7. Si los datos ingresados no corresponden a un propietario existente. | Muestra un mensaje de alerta indicando que no existe el propietario. |
| 8. El usuario ingresa los datos correctamente y da clic en "Consultar". | El sistema valida nuevamente los datos y muestra la información del propietario. |
| **Post-Condiciones** | Se consultó la información de un propietario existente. |  |
| **Requisito Funcional** | RF-004 |  |

## Fuente: elaboración propia

|  |  |  |
| --- | --- | --- |
| **NOMBRE** | Registrar Comportamiento | |
| **DESCRIPCION** | Permite ingresar y registrar un comportamiento o incidencia asociada a un residente o visitante. | |
| **ACTOR** | Seguridad, Administrador | |
| **PRECONDICIONES** | El usuario debe estar logueado en el sistema con permisos de seguridad o administrador. | |
| **FLUJO BASICO** | | |
|  | **ACTOR** | **SISTEMA** |
| PASOS | 1. Ingresa al menú de comportamientos e incidencias. | El sistema muestra el formulario para registrar un nuevo comportamiento o incidencia. |
| 2. Completa los detalles de la incidencia, incluyendo la descripción, tipo de comportamiento y persona involucrada. | El sistema permite la entrada de los datos requeridos para registrar la incidencia. |
| 3. Da clic en el botón "Guardar". | El sistema valida los datos ingresados y guarda el registro del comportamiento en la base de datos. |
| 4. El sistema confirma el registro. | Muestra un mensaje de confirmación indicando que el comportamiento ha sido registrado exitosamente |
| **FLUJO ALTERNATIVO** | | |
| PASOS | **ACTOR** | **SISTEMA** |
| Si faltan datos obligatorios o el formato es incorrecto. | Muestra un mensaje de error solicitando completar o corregir los datos. |
| **Post-Condiciones** | La incidencia o comportamiento ha sido registrado correctamente en el sistema. |  |
| **Requisito Funcional** | RF-005 |  |

## Fuente: elaboración propia

|  |  |  |
| --- | --- | --- |
| **NOMBRE** | Consultar Comportamientos | |
| **DESCRIPCION** | Permite buscar y visualizar registros de comportamientos de residentes y visitantes en el sistema. | |
| **ACTOR** | Seguridad, Administrador | |
| **PRECONDICIONES** | El usuario debe estar logueado en el sistema con permisos de seguridad o administrador. | |
| **FLUJO BASICO** | | |
|  | **ACTOR** | **SISTEMA** |
| PASOS | 1. Ingresa al menú de comportamientos y selecciona la opción de consulta. | El sistema muestra un formulario de búsqueda para filtrar comportamientos por criterios como fecha, tipo de comportamiento, o persona involucrada. |
| |  | | --- | | 2. Completa los filtros de búsqueda y da clic en el botón "Buscar". | |  | | |  | | --- | | El sistema busca en la base de datos los registros que cumplen con los filtros especificados. | |  | |
| |  | | --- | | 3. El sistema muestra los resultados de la búsqueda. | |  | | |  | | --- | | Muestra una lista de comportamientos que cumplen con los criterios, incluyendo detalles relevantes de cada uno. | |  | |
| |  | | --- | | 4. Selecciona un comportamiento de la lista para ver más detalles. | |  | | El sistema muestra la información completa del comportamiento seleccionado. |
| **FLUJO ALTERNATIVO** | | |
| PASOS | **ACTOR** | **SISTEMA** |
| Si no se encuentran registros con los filtros especificados. | Muestra un mensaje indicando que no se encontraron resultados. |
| **Post-Condiciones** | La incidencia o comportamiento ha sido registrado correctamente en el sistema. |  |
| **Requisito Funcional** | RF-006 |  |

## Fuente: elaboración propia

|  |  |  |
| --- | --- | --- |
| **NOMBRE** | Administrar Cámaras | |
| **DESCRIPCION** | Permite registrar, actualizar y eliminar información sobre el tipo y ubicación de cámaras en la unidad residencial. | |
| **ACTOR** | Seguridad, Administrador | |
| **PRECONDICIONES** | El usuario debe estar logueado en el sistema con permisos de técnico o administrador. | |
| **FLUJO BASICO** | | |
|  | **ACTOR** | **SISTEMA** |
| PASOS | |  | | --- | | 1. Ingresa al menú de administración de cámaras. | |  | | El sistema muestra una lista de cámaras registradas y la opción para agregar, modificar o eliminar cámaras. |
| |  | | --- | | 2. Selecciona la opción "Agregar cámara" y completa los datos (tipo, ubicación, etc.). | |  | | |  | | --- | | El sistema permite la entrada de datos para la nueva cámara y valida que la información esté completa y en el formato correcto. | |  | |
| |  | | --- | | 3. Da clic en el botón "Guardar". | |  | | |  | | --- | | El sistema guarda el registro de la nueva cámara en la base de datos. | |  | |
| |  | | --- | | 4. El sistema confirma el registro de la cámara. | |  | | Muestra un mensaje de confirmación indicando que la cámara ha sido registrada exitosamente. |
| **FLUJO ALTERNATIVO** | | |
| PASOS | **ACTOR** | **SISTEMA** |
| Si selecciona una cámara existente y elige "Modificar" o "Eliminar". | El sistema permite modificar los datos de la cámara seleccionada o eliminar su registro, mostrando una confirmación en caso de eliminación. |
| **Post-Condiciones** | La cámara ha sido registrada, actualizada o eliminada en el sistema correctamente. |  |
| **Requisito Funcional** | RF-007 |  |

## Fuente: elaboración propia

|  |  |  |
| --- | --- | --- |
| **NOMBRE** | Monitoreo de Cámaras | |
| **DESCRIPCION** | Permite acceder al monitoreo en tiempo real de las cámaras de seguridad | |
| **ACTOR** | Técnico, Administrador | |
| **PRECONDICIONES** | El usuario debe estar logueado en el sistema y tener acceso autorizado a las cámaras. | |
| **FLUJO BASICO** | | |
|  | **ACTOR** | **SISTEMA** |
| PASOS | 1. Ingresa al menú de monitoreo de cámaras. | El sistema despliega la interfaz de monitoreo en tiempo real. |
| 2. Selecciona una cámara o grupo de cámaras a visualizar. | El sistema muestra las imágenes en tiempo real de las cámaras seleccionadas. |
| 3. Observa las cámaras y toma acciones en caso de incidentes. | El sistema permite la visualización continua sin interrupciones. |
| **FLUJO ALTERNATIVO** | | |
| PASOS | **ACTOR** | **SISTEMA** |
| Si la cámara seleccionada no está operativa. | Muestra un mensaje de error indicando que la cámara no está disponible |
| **Post-Condiciones** | El usuario visualizó el monitoreo en tiempo real de las cámaras seleccionadas. |  |
| **Requisito Funcional** | RF-8 |  |

## Fuente: elaboración propia

|  |  |  |
| --- | --- | --- |
| **NOMBRE** | Registrar Autoridades | |
| **DESCRIPCION** | Permite registrar datos de autoridades relevantes para el sistema (nombre, empresa, contacto). | |
| **ACTOR** | Administrador | |
| **PRECONDICIONES** | El usuario debe estar logueado en el sistema con permisos de administrador. | |
| **FLUJO BASICO** | | |
|  | **ACTOR** | **SISTEMA** |
| PASOS | |  | | --- | | 1. Ingresa al menú de registro de autoridades. | |  | | El sistema muestra un formulario para ingresar los datos de la autoridad (nombre, empresa, contacto). |
| 2. Completa los campos requeridos con la información de la autoridad. | El sistema verifica que los campos estén completos y que los datos ingresados estén en el formato correcto. |
| |  | | --- | | 3. Da clic en el botón "Guardar". | |  | | El sistema guarda la información de la nueva autoridad en la base de datos. |
| 4. El sistema confirma el registro de la autoridad. | Muestra un mensaje de confirmación indicando que la autoridad ha sido registrada exitosamente. |
| **FLUJO ALTERNATIVO** | | |
| PASOS | **ACTOR** | **SISTEMA** |
| Si los datos están incompletos o en formato incorrecto. | Muestra un mensaje de error indicando los campos que deben corregirse o completarse. |
| **Post-Condiciones** | La autoridad ha sido registrada en el sistema correctamente. |  |
| **Requisito Funcional** | RF-009 |  |

## Fuente: elaboración propia

|  |  |  |
| --- | --- | --- |
| **NOMBRE** | Generar Reportes | |
| **DESCRIPCION** | Crea informes automáticos de sucesos, comportamientos y estadísticas para análisis. | |
| **ACTOR** | Administrador | |
| **PRECONDICIONES** | El usuario debe estar logueado en el sistema. | |
| **FLUJO BASICO** | | |
|  | **ACTOR** | **SISTEMA** |
| PASOS | 1. Ingresa al menú de reportes. | El sistema despliega las opciones de generación de reportes: tipo de reporte, rango de fechas, formato de salida. |
| 2. Selecciona el tipo de reporte y define el rango de fechas. | El sistema permite la selección de las opciones y habilita el botón "Generar Reporte". |
| 3. Da clic en "Generar Reporte". | El sistema procesa la información y genera el reporte solicitado en el formato seleccionado (PDF, Excel, etc.). |
| 4. Descarga o visualiza el reporte. | El sistema muestra una opción para descargar o visualizar el reporte generado. |
| **FLUJO ALTERNATIVO** | | |
| PASOS | **ACTOR** | **SISTEMA** |
| Si no se selecciona el rango de fechas o el tipo de reporte. | Muestra un mensaje de error solicitando completar las opciones para generar el reporte. |
| **Post-Condiciones** | Se generó el reporte con los datos solicitados. |  |
| **Requisito Funcional** | RF-10 |  |

## Fuente: elaboración propia

|  |  |  |
| --- | --- | --- |
| **NOMBRE** | Notificación de Incidentes | |
| **DESCRIPCION** | Envía alertas inmediatas al personal de seguridad en caso de incidentes o comportamientos inusuales. | |
| **ACTOR** | Seguridad | |
| **PRECONDICIONES** | El sistema debe estar en funcionamiento y conectado a los dispositivos de monitoreo de incidentes. | |
| **FLUJO BASICO** | | |
|  | **ACTOR** | **SISTEMA** |
| PASOS | 1. Detecta un incidente o comportamiento inusual a través de los dispositivos de monitoreo. | El sistema identifica el incidente y activa el proceso de notificación. |
| |  | | --- | | 2. Genera una alerta automática con los detalles del incidente. | |  | | La alerta incluye información relevante como ubicación, hora, y tipo de incidente. |
| |  | | --- | | 3. Envía la alerta al personal de seguridad mediante el canal de notificación configurado (app, SMS, etc.). | |  | | El sistema confirma el envío de la notificación y registra la alerta en la base de datos para su seguimiento. |
| |  | | --- | | 4. El personal de seguridad recibe la alerta y toma las acciones correspondientes. | |  | | El personal de seguridad puede visualizar los detalles del incidente y responder adecuadamente. |
| **FLUJO ALTERNATIVO** | | |
| PASOS | **ACTOR** | **SISTEMA** |
| Si el sistema falla al enviar la notificación. | Muestra un mensaje de error y reintenta el envío automáticamente o almacena la alerta en una lista de pendientes. |
| **Post-Condiciones** | El personal de seguridad ha sido notificado del incidente, y el sistema mantiene un registro del evento para futuros análisis. |  |
| **Requisito Funcional** | RF-11 |  |

## Fuente: elaboración propia

|  |  |  |
| --- | --- | --- |
| **NOMBRE** | Acceso Móvil | |
| **DESCRIPCION** | Permite a usuarios autorizados acceder a la información y gestionar cámaras desde dispositivos móviles. | |
| **ACTOR** | Administrador, Seguridad | |
| **PRECONDICIONES** | El usuario debe estar logueado en el sistema con permisos de administrador o seguridad y tener instalada la aplicación móvil. | |
| **FLUJO BASICO** | | |
|  | **ACTOR** | **SISTEMA** |
| PASOS | |  | | --- | | 1. Abre la aplicación móvil e inicia sesión. | |  | | |  | | --- | | El sistema verifica las credenciales del usuario. | |  | |
| |  | | --- | | 2. Selecciona la opción para gestionar cámaras o consultar información relevante. | |  | | |  | | --- | | El sistema despliega la interfaz con las opciones disponibles, como visualizar cámaras en tiempo real o consultar registros de seguridad. | |  | |
| |  | | --- | | 3. Escoge una cámara para monitorear en tiempo real. | |  | | El sistema activa la transmisión en tiempo real de la cámara seleccionada y muestra la imagen en el dispositivo móvil. |
| |  | | --- | | 4. Realiza otras consultas o gestiona las cámaras según sea necesario. | |  | | El sistema permite realizar otras gestiones, como registrar incidentes o modificar parámetros de visualización. |
| **FLUJO ALTERNATIVO** | | |
| PASOS | **ACTOR** | **SISTEMA** |
| Si el usuario no tiene permisos suficientes. | Muestra un mensaje indicando que el usuario no está autorizado para acceder a esa función. |
| **Post-Condiciones** | El usuario autorizado ha accedido a la gestión de cámaras desde el dispositivo móvil y ha consultado o gestionado la información necesaria. |  |
| **Requisito Funcional** | RF-12 |  |

## Fuente: elaboración propia

|  |  |  |
| --- | --- | --- |
| **NOMBRE** | Integración de Seguridad | |
| **DESCRIPCION** | Sincroniza datos y alertas con otros sistemas de seguridad para mejorar la cobertura y protección de la unidad residencial. | |
| **ACTOR** | Técnico, Administrador | |
| **PRECONDICIONES** | El sistema debe estar integrado correctamente con otros sistemas de seguridad y comunicación. | |
| **FLUJO BASICO** | | |
|  | **ACTOR** | **SISTEMA** |
| PASOS | |  | | --- | | 1. Configura la integración de seguridad seleccionando los sistemas con los que se sincronizarán los datos. | |  | | El sistema muestra una interfaz con las opciones de configuración de integración para seleccionar los sistemas de seguridad externos. |
| 2. Habilita la sincronización de datos en tiempo real. | El sistema establece una conexión segura con los sistemas externos y comienza a sincronizar los datos de seguridad y alertas. |
| |  | | --- | | 3. Verifica la sincronización exitosa de alertas y eventos de seguridad. | |  | | Notifica a los usuarios que la sincronización ha sido realizada y que los datos están integrados correctamente en el sistema. |
| **FLUJO ALTERNATIVO** | | |
| PASOS | **ACTOR** | **SISTEMA** |
| Si hay un error en la conexión con los sistemas externos. | Muestra un mensaje de error, detalla la causa del fallo y permite intentar la configuración nuevamente. |
| **Post-Condiciones** | Se generó el reporte con los datos solicitados. |  |
| **Requisito Funcional** | RF-13 |  |

## Fuente: elaboración propia

|  |  |  |
| --- | --- | --- |
| **NOMBRE** | Gestión de Permisos | |
| **DESCRIPCION** | Este caso de uso permite a los administradores del sistema definir roles y permisos de acceso para cada usuario, según su rol en el sistema. | |
| **ACTOR** | Administrador | |
| **PRECONDICIONES** | El usuario debe estar autenticado como administrador en el sistema. | |
| **FLUJO BASICO** | | |
|  | **ACTOR** | **SISTEMA** |
| PASOS | 1. El administrador ingresa al menú de configuración de permisos. | El sistema muestra las opciones de roles y permisos configurados. |
| |  | | --- | | 2. El administrador selecciona el rol o grupo de usuarios para gestionar permisos. | |  | | El sistema despliega una lista de usuarios o roles con opciones de permisos para asignar. |
| 3. El administrador asigna o modifica los permisos para el rol o usuario seleccionado. | El sistema valida los cambios y los guarda en el sistema. |
| 4. El administrador confirma la configuración de permisos. | El sistema guarda los cambios y muestra una confirmación de éxito. |
| **FLUJO ALTERNATIVO** | | |
| PASOS | **ACTOR** | **SISTEMA** |
| 1. El administrador intenta asignar permisos a un rol no existente. | El sistema muestra un mensaje de error indicando que el rol no existe. |
| **Post-Condiciones** | Los permisos para los usuarios o roles seleccionados han sido definidos correctamente en el sistema. |  |
| **Requisito Funcional** | RF-14 |  |

## Fuente: elaboración propia

|  |  |  |
| --- | --- | --- |
| **NOMBRE** | Feedback de Usuarios | |
| **DESCRIPCION** | Este caso de uso permite que los usuarios envíen sugerencias y comentarios sobre el sistema para promover mejoras continuas. | |
| **ACTOR** | Todos los usuarios | |
| **PRECONDICIONES** | El usuario debe estar autenticado en el sistema. | |
| **FLUJO BASICO** | | |
|  | **ACTOR** | **SISTEMA** |
| PASOS | 1. El usuario accede al menú de "Feedback" o "Sugerencias" en la interfaz del sistema. | El sistema despliega un formulario de retroalimentación para completar. |
| |  | | --- | | 2. El usuario ingresa su comentario o sugerencia. | |  | | El sistema valida el contenido del comentario para asegurarse de que no esté vacío. |
| |  | | --- | | 3. El usuario envía el formulario de retroalimentación. | |  | | El sistema guarda la sugerencia y muestra una confirmación de envío exitoso. |
| **FLUJO ALTERNATIVO** | | |
| PASOS | **ACTOR** | **SISTEMA** |
| El usuario intenta enviar el formulario vacío o con datos inválidos. | El sistema muestra un mensaje de error y solicita información válida. |
| **Post-Condiciones** | El comentario o sugerencia del usuario ha sido almacenado y se utilizará para la mejora continua del sistema. |  |
| **Requisito Funcional** | RF-15 |  |

## Fuente: elaboración propia

### Mapa de navegación (Diseño del menú que se utilizará en el sistema)

Fuente: elaboración propia

### Recursos (hardware, Software, Talento Humano)

#### Recursos para el Proyecto

Para la implementación de este sistema de vigilancia con inteligencia artificial, se requieren recursos en tres categorías principales: hardware, software y talento humano. A continuación, se especifican los recursos necesarios en cada área y se presentan tres cotizaciones estimadas para el proyecto.

#### 1. Hardware

* **Cámaras de Seguridad con IA Integrada:** Cámaras de alta resolución con capacidad de conexión a internet, compatibles con análisis en tiempo real.
* **Servidor de Procesamiento:** Servidores con GPU para el procesamiento de imágenes y la ejecución de modelos de inteligencia artificial. Es importante que los servidores tengan alta capacidad de procesamiento y almacenamiento.
* **Almacenamiento en la Nube o en Local:** Dependiendo de la capacidad del servidor, se puede necesitar almacenamiento adicional para guardar los videos y registros de incidentes.
* **Red de Comunicación:** Routers y switches que permitan una conectividad estable y de alta velocidad para el envío de datos desde las cámaras al servidor.
* **Dispositivos Móviles:** Dispositivos como teléfonos o tabletas para el personal de vigilancia, donde puedan recibir notificaciones en tiempo real sobre comportamientos sospechosos detectados por el sistema de IA.

#### **Cotización de Hardware:**

1. **Opción A:** Equipos de alta gama (marcas reconocidas) - $50,000 USD
2. **Opción B:** Equipos de gama media (buena calidad y confiabilidad) - $35,000 USD
3. **Opción C:** Equipos de entrada (marcas económicas) - $25,000 USD

#### 2. Software

* **Software de Inteligencia Artificial:** Herramientas de desarrollo y entrenamiento de modelos de IA, como TensorFlow, PyTorch o Keras, que permitirán entrenar la IA para el análisis de imágenes y detección de comportamientos sospechosos.
* **Sistema de Gestión de Seguridad:** Software para el monitoreo y administración de cámaras, integración con notificaciones en tiempo real, y panel de control accesible para el personal de seguridad.
* **Licencias de Nube (opcional):** En caso de que se opte por almacenamiento o procesamiento en la nube, es posible que se requieran servicios como AWS, Google Cloud o Microsoft Azure.
* **Aplicación de Notificaciones en Tiempo Real:** Desarrollo o integración de una aplicación móvil que permita a los guardias recibir alertas en tiempo real, con funcionalidades para visualizar la cámara y detalles del incidente.

#### Cotización de Software:

1. **Opción A:** Licencias comerciales y desarrollo de software personalizado - $30,000 USD
2. **Opción B:** Software de código abierto con personalización - $20,000 USD
3. **Opción C:** Soluciones básicas y económicas con limitadas personalizaciones - $15,000 USD

#### 3. Talento Humano

* **Ingeniero en Inteligencia Artificial y Machine Learning:** Responsable del diseño, desarrollo y entrenamiento de los modelos de IA que detectarán patrones de comportamiento.
* **Desarrollador de Software:** Encargado de implementar la integración entre las cámaras, el sistema de IA y la aplicación de notificaciones en tiempo real.
* **Especialista en Redes y Seguridad:** Responsable de la configuración y mantenimiento de la infraestructura de red y seguridad del sistema.
* **Analista de Seguridad:** Personal con experiencia en análisis de comportamientos y gestión de seguridad, que trabajará en colaboración con el equipo técnico para definir los patrones sospechosos a detectar.
* **Personal de Monitoreo:** Guardias y vigilantes entrenados en el uso de la aplicación y el sistema de vigilancia basado en IA.

#### **Cotización de Talento Humano:**

1. **Opción A:** Equipo altamente calificado y experimentado - $70,000 USD
2. **Opción B:** Equipo con experiencia intermedia - $50,000 USD
3. **Opción C:** Equipo de entrada o de menor costo - $35,000 USD

#### Resumen de Costos Totales por Opción

1. **Opción A:** $150,000 USD (Equipos de alta gama, software comercial, equipo experimentado)
2. **Opción B:** $105,000 USD (Equipos de gama media, software de código abierto, equipo intermedio)
3. **Opción C:** $75,000 USD (Equipos de entrada, software económico, equipo de menor costo)

## Conclusiones

La implementación de inteligencia artificial en sistemas de vigilancia representa un avance significativo en la optimización de la seguridad en edificios y espacios públicos. Gracias al monitoreo continuo que ofrece este tipo de tecnología, se logra una vigilancia constante y precisa, algo que resulta complicado para el personal humano debido a la fatiga y distracción. La IA puede detectar patrones sospechosos de manera automática, lo que permite actuar de forma rápida ante situaciones de riesgo, minimizando el tiempo de respuesta y aumentando la efectividad en la prevención de incidentes.

Además, este sistema complementa la labor de los vigilantes, liberándolos de la carga mental de estar atentos a múltiples cámaras durante largos periodos. Con la IA notificando en tiempo real cualquier actividad que requiera atención, los guardias pueden concentrarse en responder eficazmente a las alertas, mejorando la eficiencia de sus tareas y reduciendo el riesgo de errores humanos. La sinergia entre el vigilante y el sistema de IA crea un entorno de seguridad más robusto y confiable.

Finalmente, el desarrollo de esta solución tecnológica no solo tiene el potencial de transformar la manera en que se gestiona la seguridad, sino también de adaptarse a diferentes sectores y entornos. Ya sea en complejos residenciales, instalaciones industriales o espacios comerciales, el uso de IA en vigilancia puede establecer nuevos estándares de seguridad. Este proyecto resalta la importancia de adoptar herramientas innovadoras que contribuyan a un entorno más seguro y que estén en constante evolución para responder a los desafíos de seguridad actuales y futuros.

## Referentes

Badii, A., Guarnera, F., et al. (2021). *AI-based surveillance systems in residential areas: Enhancing security with advanced analytics*. Journal of Security and Surveillance, 32(4), 455-472.

García, P., & Sánchez, L. (2022). *Vigilancia residencial con inteligencia artificial: Una revisión de tecnologías emergentes*. Revista de Innovación Tecnológica, 15(2), 220-239.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

Russell, S., & Norvig, P. (2020). *Artificial Intelligence: A Modern Approach*. Pearson.

Zhang, H., Chen, X., & Li, P. (2019). *Anomaly detection in surveillance videos: Methods and applications*. Pattern Recognition Letters, 128, 47-58.

*¿Qué es una cámara AI y cuáles son sus ventajas? | Blog de Skylum | Skylum Blog*. (2024, 26 enero). <https://skylum.com/es/blog/what-is-an-ai-camera#:~:text=El%20significado%20de%20c%C3%A1mara%20AI,A15%20con%20triple%20c%C3%A1mara%20AI>.

Marta.Serrano. (2024, 28 mayo). *Cámaras con inteligencia artificial: revolucionan la seguridad y el rendimiento empresarial*. Seguritecnia. <https://www.seguritecnia.es/tecnologias-y-servicios/videovigilancia-y-cctv/camaras-con-inteligencia-artificial-ia-revolucionan-la-seguridad-y-el-rendimiento-empresarial_20240528.html>