UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

FACULTAD 6

"Estación de Monitorización Especializado para Video Vigilancia."

Trabajo de Diploma para optar por el Título de
Ingeniero en Ciencias Informáticas.

Autores: Merlín Milián Díaz

Eduardo Merino Hernández

Tutor: Ing. Heliodoro Rodríguez Milián

Ciudad de La Habana, 15 de junio de 2011
"Año 53 de la Revolución"

DECLARACION DE AUTORIA

Declaramos que somos los únicos autores del presente trabajo y autorizamos a la Universidad de las Ciencias Informáticas los derechos patrimoniales de la misma, con carácter exclusivo.

Para que así conste firmamos la presente a los ___ días del mes de _____ del año __2011___.

Autores:

_____ _____

Merlín Milián Díaz Eduardo Merino Hernández

Tutor:

_____

Ing. Heliodoro Rodríguez Milián.

DATOS DE CONTACTO

Tutor: Ing. Heliodoro Rodríguez Milián (hrodriguezm@uci.cu)

Graduado de Ingeniero en Ciencias Informáticas en la UCI en el año 2007; es profesor instructor, durante su trayectoria como profesor ha impartido las asignaturas Gráfico por Computadoras, Programación Web, Práctica Profesional 1 e Historia de la Informática. Trabajador del GEYSED en el Proyecto Sistema de Video Vigilancia en el cual se desempeña como Líder de Proyecto.

AGRADECIMIENTOS

De Merlín:

Primeramente, agradezco a mis padres por confiar en mí y guiarme por el camino correcto, por enseñarme cuanto hay que esforzarse para alcanzar un sueño.

A mi papá Norberto por estar a mi lado en cada pequeño momento de mi vida y apoyarme incondicionalmente. Gracias por estar siempre ahí.

A mis hermanas Maylín y Melissa, por estar siempre disponibles en mi vida.

A toda la familia: mis abuelos, mis tíos y primos, a mi tía Mirayda a todos gracias por estar siempre a mi lado y que hoy puedan compartir conmigo este importante momento de mi vida.

A mi compañero de tesis Eduardo por estar disponible siempre que lo necesité y por demostrarme que los amigos se llevan en el corazón.

A mi tutor y su esposa Aíslen que han estado a mi lado incondicionalmente en todo mi recorrido en la universidad.

A mis mejores amigos por demostrarme que los amigos se llevan en el corazón y que la lejanía no opaca los recuerdos.

A todos mis compañeros de la UCI, de mi pueblo, a mis compañeros de clases, a los profesores y estudiantes del proyecto de Video Vigilancia y a todos aquellos que han estado incondicionalmente siempre que los necesité.

A los miembros del tribunal por el sacrificio y la abnegación para que cada día fuéramos mejores.

A todos ustedes… Muchas Gracias.

De Eduardo:

Agradezco a toda mi familia en particular a mis padres por confiar en mí, guiarme y enseñarme todo lo que se en la vida.

A mi novia Arianna por su comprensión, apoyo en todas mis decisiones y el amor que me ha ofrecido en todo este tiempo.

A mis mejores amigos: Julio, Yadiel, Arturo.

A todos los profesores y estudiantes del proyecto Video Vigilancia por el sacrificio y la abnegación para que fuéramos mejores profesionales.

A mis compañeros de aula y profesores que estuvieron ayudándome en las diferentes facultades donde tuve el privilegio de estudiar durante estos 5 años.

A Heliodoro, Deivis y Merlin por su ayuda incondicional en todo este tiempo y ayudarme a cumplir este sueño.

A todos ustedes muchas gracias por ser parte importante de mi vida.

DEDICATORIA

De Merlín:

Dedico este trabajo:

A mi mamá que ha luchado mucho por verme triunfar en la vida.

A mis papás José y Norberto que siempre me han hecho sentirme orgullosa de ellos.

A mis hermanas que siempre están cuando las necesito.

A toda mi familia y a aquellos amigos que ya son parte de ella.

A todos ellos; dedico este sueño hecho realidad.

De Eduardo:

Quisiera dedicar este trabajo:

A mi mamá y mi papá que han dado todo por mí y que siempre me han hecho sentirme orgulloso de ellos.

A mi familia que tanto me apoya y siempre están junto a mí en todo momento.

A mi novia que ha sabido ganarse mi corazón con amor y cariño.

A mi hijo y más grande tesoro que tengo en la vida, que el tiempo que no he podido pasar a su lado por cumplir este sueño sea recompensado con más amor y un mejor futuro para él.

RESUMEN

El ministerio de Turismo tiene hoy en día la necesidad de preservar todos los bienes que la revolución le ha puesto a su disposición, así como velar por la integridad de los turistas y las instalaciones. Con este objetivo en la UCI se ha comenzado el desarrollo de un sistema de Video Vigilancia SURIA, el cual en la actualidad cuenta con las primeras versiones de la estación de monitorización, grabación de los flujos de video y del módulo central orquestador de todo el sistema. Uno de los principales componentes de los sistemas de video vigilancia es la estación de monitorización de flujos de video; este es el componente de monitorización del sistema que tiene la capacidad de reflejar todo el aspecto organizativo con que el sistema maneja las cámaras internamente, es decir, que la forma de presentación responda a la disposición física de las cámaras en el lugar del despliegue de la aplicación.

El presente trabajo propone implementar nuevas funcionalidades para convertir la estación de monitorización de SURIA en una estación de monitorización especializada.

Las nuevas funcionalidades que se proponen permitirán la gestión de roles y usuarios en el sistema así como la autenticación de los mismos, ladetección de movimientoy generación de alarmas sonoras y visuales a partir de eventos.

La estación de monitorización de SURIA se convertirá en una herramienta de mayor potencia que permitirá mejorar la vigilancia y control de los recursos en las instituciones del país.

Palabras Claves: video vigilancia, cámaras, estación de monitorización.

ABSTRACT

The Ministry of Tourism has the need to preserve all resources that the Cuban Revolution has offered to it, as well as ensuring the integrity of the tourists and facilities. For this objective, in the Informatics Science University has begun developing a Video Surveillance System SURIA, which currently has early versions of the monitoring station, recording module and central module orchestrator of the whole system. One of the main components of the surveillance systems, is the monitoring station of video streams, this is the system monitoring component that has the ability to capture every organizational aspect that handles the camera system internally, i.e. that the presentation meets the physical layout of the cameras at the site of application deployment.

This thesis proposes to implement new functionality, to convert SURIA monitoring station in a specialized monitoring station. The new features add to this system will allow the manage roles and users in the system and authentication of them, motion detection and generation of audible and visual alarms from events.

The SURIA monitoring station will be a powerful tool that will improve the monitoring and control of resources in the country's institutions.

Keywords: video surveillance, cameras, monitoring station.

CONTENIDO

CONTENIDO

Introducción

Hay ojos en todas partes y no pertenecen solo a los seres humanos. En el acelerado mundo moderno de hoy día, la video vigilancia se ha convertido en algo esencial para la sociedad como controladores de acceso y guardias de seguridad. Al mencionar video vigilancia las personas promedio asocian instantáneamente el término a las cámaras de video montadas en bancos, grandes almacenes, vías públicas, aeropuertos o cintas de video de una pareja errante, en un proceso complicado de divorcio.

De hecho, se remonta mucho más allá en el tiempo de lo que la mayoría de los seres humanos se pueden dar cuenta. Informes de prensa indican que ya en 1965, la policía de los Estados Unidos estuvo usando videovigilancia en lugares públicos. Para 1969, las cámaras de la policía se habían montado en áreas estratégicas de la ciudad de Nueva York como el Edificio Municipal. Esto sentó un precedente fuerte, y no pasó mucho tiempo antes de que la práctica se extendiera a otras ciudades y los agentes de policía vigilaban de cerca en áreas claves, creando así los primeros Sistemas de circuito cerrado de televisión (CCTV).

Los video casetes de cintas magnéticas son en gran parte responsables de la popularidad de la video vigilancia. En un principio se utilizaba la tecnología analógica en la grabación de cintas de video, esta dio a los encargados de tomar decisiones una visión innovadora ya que contaban con pruebas preservadas en dicha cinta. En 1975, Inglaterra instaló sistemas de video vigilancia en cuatro de sus principales estaciones de tren subterráneo. Al mismo tiempo, también se comenzó a monitorear el flujo del tráfico en las carreteras principales. Los Estados Unidos hicieron lo mismo durante la década de 1980, y aunque no fueron tan rápidos como Inglaterra en la utilización de cámaras de vigilancia, se dieron a la tarea de recuperar el tiempo perdido y comenzaron a desplegar ampliamente sistemas de video vigilancia en las zonas públicas. (1)

Una de las desventajas de la tecnología analógica es que los usuarios tenían que cambiar las cintas diariamente. Esto se solucionó en la década de 1990, con la introducción de la multiplexación digital. Esta permitió un gran ahorro de espacio en cinta. Además, permitió realizar grabaciones simultáneas desde varias cámaras. La digitalización presentaba también capacidad de compresión y bajo costo, permitiendo a los usuarios grabar todo un mes de videos de vigilancia en el disco duro. Las imágenes digitalizadas eran más claras y permitían la manipulación para mejorar su calidad.

Los acontecimientos del 11 de septiembre de 2001 cambiaron la percepción para el público de la video vigilancia. Los desarrolladores de software crearon programas que permitían mejorar la vigilancia por video cámaras; una de estas mejoras fueron los programas de reconocimiento facial. En diciembre de 2003, el Royal Palm MiddleSchool en Phoenix, Arizona, instaló un sistema para el reconocimiento de rostros por video vigilancia. Este fue un programa piloto para el registro de delincuentes sexuales y el seguimiento de los niños desaparecidos. Sucesivamente con el auge de internet y el surgimiento de las cámaras IP se incrementó aún más lavideo vigilancia, ya que se fueron eliminando todos los impedimentos para la visualización y control de cámaras desde cualquier lugar del mundo. (1)

Con esta intención se han destinado muchos esfuerzos y recursos a las actividades relacionadas con la vigilancia. Los sistemas de video vigilancia han atravesado por varias etapas de su desarrollo, desde simples sistemas constituidos básicamente por una cámara conectada a un monitor y a un grabador de cinta, para de ser necesario, grabar un determinado acontecimiento delictivo, hasta los modernos sistemas actuales de tercera generación, basados en cámaras IP[1] y redes de alta velocidad. Estos sistemas de tercera generación cuentan con varias partes fundamentales: la dedicada a la visualización en tiempo real de los flujos de video, la de grabación de estos en dispositivos de almacenamiento, así como una gran variedad de video sensores (detección de movimiento, detección de rostros, conteo de personas, extracción de matrículas de vehículos, entre otras) que utilizan el reconocimiento de patrones y el procesamiento de imágenes para brindar un producto de alto valor agregado.

En el País, se han realizado grandes inversiones en varios de sus sectores. Instituciones como hospitales, bancos, escuelas, empresas, entre otras, hoy cuentan con equipos tecnológicos de altos costos. La Universidad de las Ciencias Informáticas (UCI) es también un ejemplo donde se evidencia el uso de esta gran variedad y cantidad de nuevas tecnologías, cuenta con una gran red de computadoras, refrigeradores, televisores, aires acondicionados y ventiladores en sus áreas, además de almacenes de equipos y piezas de reparación para todos estos medios, todos potenciales motivadores de actos delictivos. De aquí que la seguridad es un tema de vital importancia para el país y las instituciones tienen que preservar los recursos con que cuentan por su importancia, alto costo y valor social de los mismos.

[1] IP: Internet Protocol, Protocolo de Internet.

El Ministerio del Turismo (MINTUR**)** por su capacidad de generar ingresos a la economía del país ha sido uno de los sectores más favorecidos en las inversiones que se han estado llevando a cabo. De ahí que hoy tiene la necesidad de preservar todos estos bienes que la revolución le ha puesto a su disposición, así como velar por la integridad de los turistas y sus instalaciones. Con este objetivo en la UCI se ha comenzado el desarrollo de un sistema de Video Vigilancia, el cual en la actualidad cuenta con las primeras versiones de la estación de monitorización, grabación de los flujos de video y del módulo central orquestador de todo el sistema. Uno de los principales componentes de los sistemas de video vigilancia es la estación de monitorización de flujos de video; este es el componente de monitorización del sistema que tiene la capacidad de reflejar todo el aspecto organizativo con que el sistema maneja las cámaras internamente, es decir, que la forma de presentación responda a la disposición física de las cámaras en el lugar del despliegue de la aplicación, además de poder visualizarlas de manera independiente o colectiva(a manera de vistas); esta puede trabajar cooperativamente con el recuperador, tras previa coordinación del orquestador, para la recuperación de video almacenado de un grupo determinado de cámaras.

La situación planteada anteriormente lleva a formular el siguiente **problema a resolver:** La aplicación estación de monitorización del sistema SURIA no cuenta con las funcionalidades necesarias para proteger los recursos de alto valor agregado existentes en las instalaciones del MINTUR. Para darle solución a este problema se toma como **objeto de estudio:** El proceso de monitorización y procesamiento de flujos de video digital desde cámaras IP, delimitando como **campo de acción:** El proceso de monitorización y procesamiento de flujos de video digital provenientes de cámaras IP que maneja el sistema SURIA.

Para guiar la investigación se plantea la siguiente **idea a defender:** Si se desarrolla una estación de monitorización especializada para el sistema SURIA mejorará la calidad de la vigilancia en las Instituciones del MINTUR.

Para dar solución a la situación problemática descrita y al problema planteado, así como al objeto y campo de investigación, la presente tesis se estructura y desarrolla en función del siguiente **objetivo general:** Implementar las herramientas necesarias para convertir la estación de monitorización de SURIA en una estación de monitorización especializada.

Los métodos utilizados en la investigación se explican a continuación:

Métodos Teóricos.

Para el análisis de las características históricas de las estaciones de monitorización se emplea el **análisis histórico – lógico** realizando un estudio sobre su evolución, desarrollo, los principales hechos y sus consecuencias, así como la relación entre estos. Se emplea también el método **analítico - sintético** para el análisis y comprensión de documentos y bibliografías de diferentes autores; realizando una amplia investigación sobre los elementos que se relacionan con el objeto de estudio. Además se usa la **modelación** para la comprensión de los objetos y sus relaciones, para determinar la estructura, jerarquía y dinámica de cada componente en el módulo propuesto respectivamente.

Métodos Empíricos.

De los métodos empíricos se utilizó la **observación** para la realización de valoraciones y obtención de información sobre el funcionamiento de sistemas similares, brindando una visión de cómo tiene que ser el sistema a realizar en su forma externa.

El presente documento consta de cuatro capítulos:

Capítulo 1: Describe algunas de las características de las diferentes estaciones de monitorización de flujos de Video Digital, surgimiento y desarrollo de estos, así como una referencia al estado del arte de los proyectos existentes en el mundo, semejantes al que se va a desarrollar. Además, se realiza la selección de las tecnologías, metodologías y herramientas actuales, que se van a utilizar para el desarrollo del sistema.

Capítulo 2: Describe las principales características del sistema, haciendo comparaciones con otras aplicaciones informáticas de este tipo, existentes en el mundo. Además, se ofrece el modelo de dominio de la aplicación, conjuntamente con la especificación de los requerimientos funcionales y no funcionales, y el modelo de casos de usos del sistema.

Capítulo 3: Muestra los resultados obtenidos en el desarrollo de los procesos de análisis y diseño del sistema, así como los diagramas que fueron necesarios para obtener una mayor claridad a la hora de elaborar la solución que se propone.

Capítulo 4: Contiene el modelo de implementación como resultado del análisis y diseño estando compuesto por su respectivo diagrama de despliegue, y por su diagrama de componentes. Además de las pruebas que se le realizaron al sistema.

Cápitulo1: Fundamentación teórica.

1.1 Introducción

En este capítulo se abordan aspectos relacionados con la evolución de los sistemas de estaciones de monitorización de flujos de Video Digital. También, se da una panorámica del estado en que se encuentran en el mundo estas tecnologías. Además, se realiza una breve descripción sobre las principales metodologías y herramientas utilizadas en la aplicación.

1.2 Evolución de las estaciones de monitorización de los sistemas de video vigilancia.

Existen reportes periodísticos que ubican el uso del Primer Sistema de Video Vigilancia en el año 1969 por la policía de Nueva York, basado en un simple CCTV, desde entonces hasta la fecha, los sistemas de video vigilancia han tenido un gran desarrollo hasta llegar a los modernos sistemas digitales. El origen de CCTV se remonta a los 60, con grandes avances en los 70, concretamente los sistemas de grabación análoga, impulsaron a las tecnologías dedicadas a la seguridad, vigilancia y control. (1)

Desde el punto de vista tecnológico, los sistemas de vigilancia han evolucionado atravesando diferentes etapas en las últimas décadas:

- La primera generación de sistemas de vigilancia basada en video emplea señales y transmisión analógicas. Este tipo de sistema usaba cable coaxial de 75 Ohm. Las cámaras se conectaban por medio de este cableado. Se podían visualizar las imágenes en tiempo real en monitores, con un solo monitor y un switch para cambiar a la cámara deseada, o con monitores capaces de aceptar múltiples fuentes de video en ventanas separadas. Una desventaja esencial de este método era el alto costo de los centros de monitorización de seguridad. Este centro de seguridad centralizado constituía un punto crítico dentro de la infraestructura de seguridad. Todas las alimentaciones de video y los cables de control tenían que estar conectados hacia ese punto. Si una cámara era reubicada, frecuentemente se requería un nuevo tendido de cable. Las videotecas requerían muchas cintas y, debido a que los medios magnéticos son susceptibles a descargas magnéticas o electroestáticas, estos sistemas no siempre proporcionaban la funcionalidad para la cual fueron

diseñados. El factor humano también era parte importante de este sistema, ya que una persona debía cambiar físicamente las cintas y monitorizar las sesiones de grabación.

Este procedimiento limita la duración de video que puede guardarse y hace que el tiempo necesario para su revisión sea elevado, después de haberse producido un delito, asalto en una tienda o robo de un auto los investigadores pueden buscar el suceso en el video y ver qué ocurrió, pero ya es tarde para evitarlo. Sería necesario un seguimiento continuo, durante las 24 horas del día, del video generado para alertar al personal de seguridad mientras el delito está en progreso, cuando aún existen opciones de evitarlo. (2)

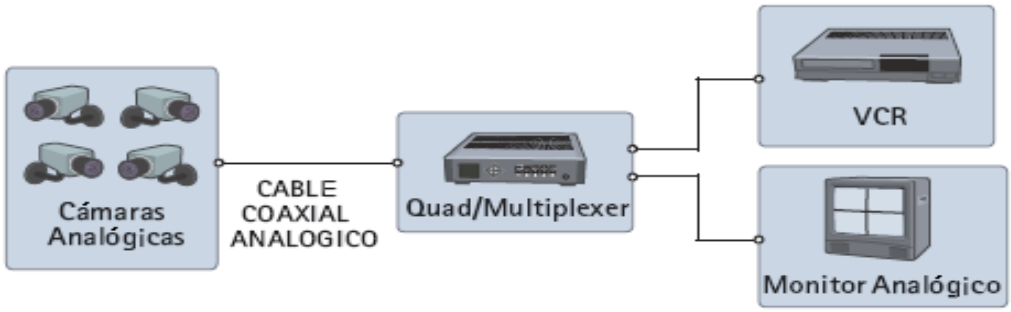


Figura 1. Sistema de Video Vigilancia Analógico.

Los sistemas analógicos emplean amplificadores de baja potencia y cables coaxiales para ver de forma remota las imágenes de las cámaras de seguridad. Las cámaras y los monitores están interconectados mediante una red de conmutación y distribución de video complejo y caro, que direcciona las imágenes de cada cámara hacia un monitor. Esta tecnología tiene demasiadas limitaciones y defectos. El video analógico solo se puede distribuir en una red local de cables coaxiales.

- La segunda generación de sistemas de vigilancia se basa, principalmente, en métodos de procesamiento y comunicación híbridos analógico-digitales, o completamente digitales. Aprovechan la flexibilidad ofrecida por los primeros algoritmos de procesado de video que permiten centrar la atención del operador humano en un grupo de situaciones de interés y, además, las facilidades proporcionadas por los primeros métodos de compresión digital para aprovechar el ancho de banda de transmisión. En esta segunda generación es que se comienza a utilizar por primera vez software para visualizar y manejar las cámaras de vigilancia, este tipo de software es conocido como estaciones de monitorización, en este momento solo gestionaban información

referente a las cámaras y usuarios, brindaban la funcionalidad de visualizar y manipular las cámaras que permitían las funciones PTZ[2]. Las cámaras IP PTZ pueden ser incorporadas actualmente en la infraestructura de red existente en los edificios. Estos sistemas explotan los beneficios de esta infraestructura a diferencia del cable coaxial.

Con este sistema el costo de una estación de monitorización central se reduce, los movimientos, adiciones y cambios son más fáciles, ya que las cámaras pueden instalarse dondequiera que exista una toma de red. El cableado viaja hacia un multiplexor que soporta conectores RJ45. Los videos digitales se graban en unidades de discos duros de la misma forma en que un archivo se almacena en una PC. Esto permite obtener monitorizacióndescentralizada, mejor calidad de imagen y mayor conservación de las grabaciones. Las transmisiones digitales pueden almacenarse sin la necesidad de intervención humana o cambio de cintas. Los tiempos de grabación son mayores y, gracias a algoritmos de compresión dentro de los dispositivos y secuencias de video, estas grabaciones son accesibles de forma instantánea y virtualmente; pueden ser visualizadas desde cualquier lugar del mundo a través de internet. Un diseño típico de red para una solución de video vigilancia IP se muestra en la Figura 2.

La solución de video vigilancia IP rompió con las barreras de la video vigilancia tradicional, elevando el alcance de la solución y minimizando los costos de la infraestructura de comunicaciones, al utilizar las redes LAN/WAN, las redes telefónicas, inalámbricas e Internet como vía de comunicación y transmisión de datos. (3)

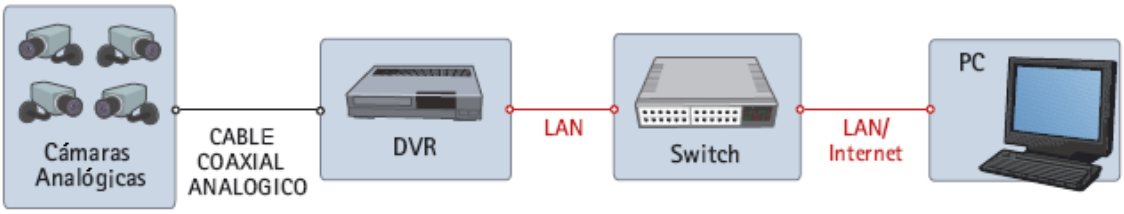


Figura 2. Sistema de Video Vigilancia Mixto Analógico-Digital.

- Actualmente, se está produciendo una migración de los sistemas de vídeo clásicos a los sistemas de tercera generación. Los sistemas de tercera generación aprovecharán el progreso de las redes

[2] PTZ: Pan, Tilt y Zoom.

de ordenadores de bajo costo y alto rendimiento, y las comunicaciones multimedia fijas y móviles. La investigación en este campo trabaja en técnicas distribuidas de procesamiento de video, para el procesado de secuencias de video en tiempo real con la intención de conseguir sistemas robustos de transmisión de imagen, procesamiento de imagen en color, generación de alarmas basada en eventos, reconstrucción de secuencias a partir de modelos, segmentación y análisis en tiempo real de secuencias de imágenes 2D, identificación y seguimiento de múltiples objetos en escenas complejas, reconocimiento de comportamientos humanos, etc. Se prevé que todos estos trabajos proporcionen a las aplicaciones de vigilancia resultados cada vez más interesantes, gracias a la disponibilidad de una potencia de cálculo muy elevada a unos precios aceptables.

Las estaciones de monitorización que incorporan esta generación utiliza un software más complejo ya que además de tener las mismas funciones que el de la generación anterior estos permiten gestionar eventos complejos como son los avisos a o desde otros sistemas o personas y la representación del procesamiento que se realiza de forma descentralizada a los flujos de video. En la actualidad aunque hay muchas empresas que se dedican a la fabricación de software de video vigilancia, estos tienen un alto costo en el mercado internacional.

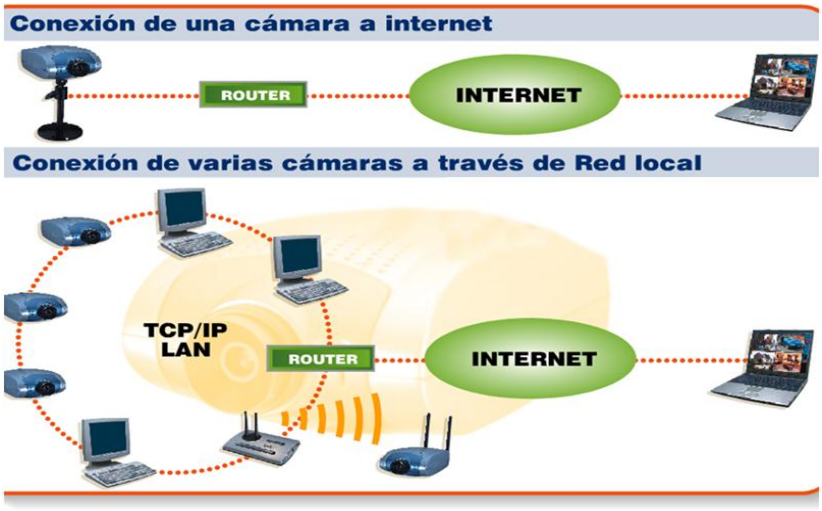


Figura 2. Sistemas de Video Vigilancia Modernos.

1.3 Estado del Arte de las estaciones de monitorización de los sistemas de video vigilancia.

En la actualidad se hallan en el mercado una gran variedad de sistemas de video vigilancia, todas estassoluciones, tienen lógicamente como el primer objetivo en el mercado a las grandes empresas, aunque no son las únicas que pueden obtener provecho de sus posibilidades. La experiencia de los fabricantes de este sector posibilita que actividades como: gestionar recursos, realizar inventarios, analizar conductas de compradores, controlar procesos industriales, además de realizar prácticas de tiro a distancia e incluso para controlar y fotografiar las migraciones de la fauna de un parque natural sin tener que molestarla, son ejemplos reales de tareas que pueden realizarse con un uso intensivo de estas herramientas. De manera que quizás solo la imaginación sea una limitación a su aplicación a diversos campos.

Las posibilidades que ofrecen los sistemas de video vigilancia, dependerán del nivel de la seguridad que demande el consumidor. Como en toda tecnología hay sectores que parecen más interesados y son más proclives a la adopción e incorporación de dichas herramientas. Por citar sólo algunos de estos se encuentran: administraciones públicas (protección de edificios públicos , para el control del tráfico y el Patrimonio), la industria (control de procesos), relaciones públicas (acciones delictivas, prevención de actos terroristas), el comercio minorista (conteo de personas, análisis de conductas de compradores, control del manejo de las cajas), en la educación (para la detección y análisis de conductas delictivas o control de asistencias), el medio ambiente (controlar y fotografiar las migraciones de la fauna), así como otros.

Principales empresas productoras de estaciones de monitorización de los sistemas de video vigilancia en el ámbito nacional:

DATYS, Tecnología y Sistemas, creada desde el año 2005, sustenta sus soluciones en el expertise que tienen sus especialistas para diferentes sectores. Uno de sus productos es XYMA SAFE VISION, el cual permite e monitorización y control en tiempo real y de forma histórica de cada uno de los movimientos que ocurren en áreas e inmuebles, desde cualquier parte del mundo, aumentando su seguridad y protegiéndolo de intrusos o movimientos peligrosos. Este producto es un software de video vigilancia profesional basado en tecnología IP, con un alto grado de modularidad, adaptable a una gran cantidad de entornos, flexible, escalable y que admite también el uso de tecnologías analógicas. (3)

Principales ventajas de XYMA SAFE VISION:

Permite ver y grabar múltiples cámaras continuamente.
Posibilidad de unicasting y multicasting.
Arquitectura modular, que le permite adaptar su configuración, según las exigencias de los escenarios de despliegue.
Utiliza componentes estándares (servidores, switches, cámaras, etc.)
Independencia del hardware dando la oportunidad de elegir el más adecuado a sus propósitos.
Permite la interacción con otros sistemas incluso de tipo analógico.
Control de acceso y asignación de permisos a los usuarios.
Realiza trazas de las incidencias del sistema y de su uso.
Módulo de Alertas que actúa como un vigilante, chequeando el funcionamiento de los módulos del sistema, y generando avisos a los usuarios y administradores de los eventos detectados.

Principales empresas productoras de estaciones de monitorización de los sistemas de video vigilancia en el ámbito internacional:

Una de las empresas productoras a nivel internacional es SCATI LABS, S.A., fundada en 1998, nace con el claro objetivo de ser especialista en el diseño, desarrollo y fabricación de soluciones globales para vídeo en el campo de la seguridad.SCATI LABs es una empresa que se dedica a la fabricación de sistemas de video vigilancia que permiten la gestión de múltiples cámaras de seguridad para el control y supervisión de instalaciones locales y remotas (4). Esta presenta al mercado su completa Suite de Gestión Remota VisionSurfer para la explotación y mantenimiento eficaz de grandes parques de videograbación digital o de instalaciones singulares. Esta suite, está compuesta por un potente conjunto de aplicaciones integrables entre sí, tales como grabación, explotación, gestión local y/o remota, control y monitorización. Esto unido a otras aplicaciones de terceros, como control de accesos, sistemas de conteo, alarmas de incendios, etc. y cámaras Megapíxel es capaz de dar una respuesta integral y simplificada a cualquier proyecto de CCTV.

La suite VisionSurfer está orientado a ofrecer a sus clientes soluciones integrales de CCTV en entornos multisectoriales tales como: banca, logística, industria, administración públicas (militar, gobierno…etc.), sanidad, educación, etc.(4). El módulo que se encarga de la video vigilancia es el SurferWatcher, pero ningún módulo se comercializa de manera independiente.

Figura 4. SCATI LABS S.A SurferWatcher

Axis, compañía sueca de Tecnologías de la Información que ofrece soluciones de vídeo IP dirigidas al mercado profesional, fundada en 1984. La compañía es líder del mercado del video IP, conduciendo el cambio del video vigilancia analógica hacia las soluciones digitales, la cual coopera con socios comerciales en más de 70 países de todo el mundo. Los productos de video de red de Axis permiten un rentable monitorización remoto de personas, lugares y propiedades, así como la transmisión de imágenes y sonido en tiempo real para aplicaciones de seguridad física, industriales y otras y están basados en la innovación y en lo estándares abiertos. (5) Gracias al uso de los servidores de cámaras y video de red Axis, los usuarios autorizados en diversas ubicaciones pueden acceder de manera simultánea a imágenes de la misma cámara, con lo que se mejora la eficacia y seguridad en general. Los productos y soluciones de Axis están diseñados para los sectores de la vigilancia, la seguridad y la monitorización remota, y están basados en la innovación y en lo estándares abiertos. El nombre del producto como tal es Axis Camera Station.

AXIS Camera Station es un software de vigilancia IP que funciona con cámaras de red y codificadores de vídeo de Axis y proporciona funciones de supervisión de vídeo, grabación y gestión de eventos. Los usuarios pueden realizar una grabación de vídeo continua, programada, activada por alarma y/o por detección de movimiento. El software dispone de múltiples funciones de búsqueda de eventos grabados. También es posible la visualización y reproducción remota mediante el cliente para Windows de AXIS Camera Station.

Otras características:

- Visualización y control remoto de uno o varios emplazamientos.
- Diseñado para sistemas pequeños y medianos.
- Manejo sencillo e intuitivo.
- Excelente calidad de imagen; permite ver, grabar y exportar vídeo de alta calidad en los formatos de compresión H.264, MPEG-4 y Motion JPEG.
- Configuración flexible de la visualización en directo, incluyendo un mapa del sitio para la visión completa.
- Fácil control de las cámaras de red PTZ y PTZ domo.

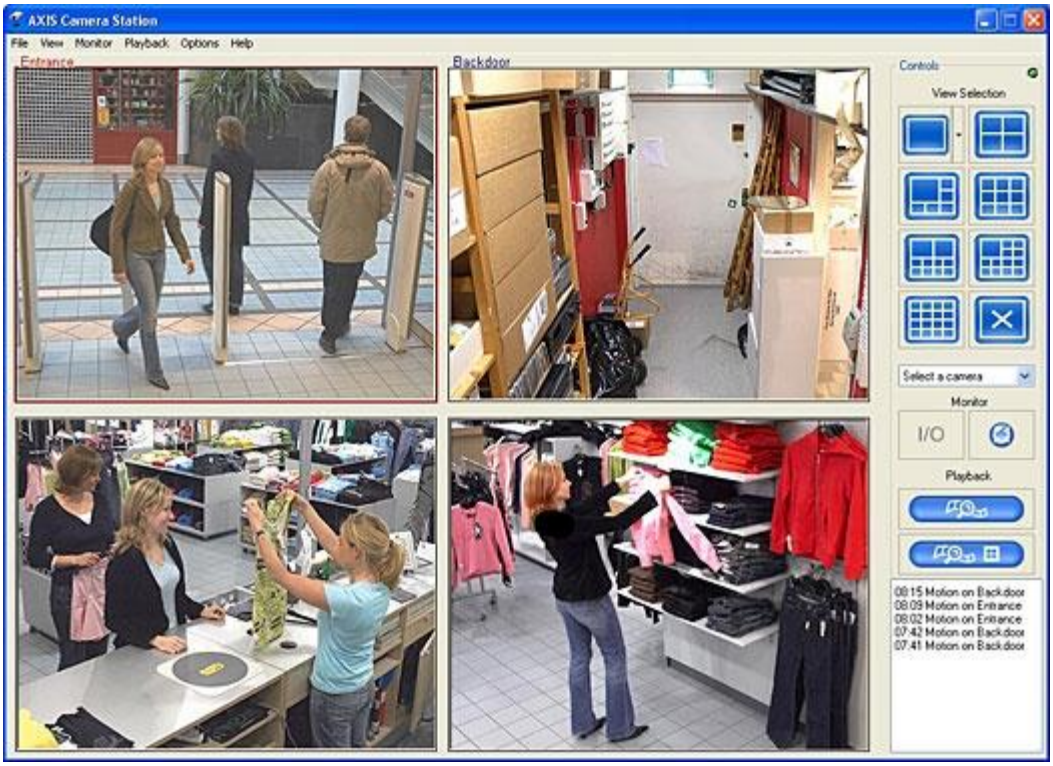


Figura 5. Axis Camera Station.

VIVOTEK INC., establecido en 2000, se ganó su lugar rápidamente como fabricante líder en la industria de la vigilancia IP. VIVOTEK se especializa en la integración de componentes audiovisuales en la operación de redes. Mediante sofisticadas tecnologías de códec, el innovador equipo de investigación y desarrollo de VIVOTEK inventa y produce una amplia gama de productos de vigilancia IP que comprende cámaras de red, servidores de video, receptores de video y software de grabación que son fáciles de instalar, utilizar y mantener. VIVOTEK ofrece software de gestión y grabación central, VAST, siendo una grabación fiable, además de fácil administración del sistema, y una gran escalabilidad para las diversas aplicaciones de vigilancia IP. Con la estructura cliente / servidor, los usuarios pueden llevar a cabo la administración remota en un sistema a gran escala y los beneficios de un sistema de vigilancia IP robusta, la avanzada tecnología de códec de VIVOTEK permite visualizar, controlar y administrar fácilmente todas las cámaras de red usando cualquier navegador estándar desde cualquier PC en la red. Agregando

además que la empresa proporciona 3 series de software de grabación: ST2403, ST3402 y ST7501, ambos gratuitos. El ST2403 destinado a las cámaras de red y servidores de video VIVOTEK de la serie 2000 y el ST7501 y ST3402 destinado a las cámaras de red de serie 3000, 6000, 7000y 8000 y servidores video de serie 3000. (6)

Figura 6. VIVOTEK ST7501.

Una vez analizadas algunas de las principales empresas en la fabricación de estaciones de monitorización de los sistemas de video vigilancia se aprecia que los sistemas actuales tienen características comunes como son: la capacidad de gestionar las cámaras presentes en el sistema (adicionar, eliminar y configurar las cámaras), visualizar flujos de video de varias cámaras de manera individual o conjunta y exportar secuencias de video. Todo esto sobre una interfaz de usuario amigable e intuitiva.

Al valorar críticamente los productos de estas empresas, los autores concluyen que la mayoría son sistemas provistos por fabricantes de hardware, y tienen gran dependencia del hardware del fabricante en cuestión. La mayoría de las funcionalidades del sistema vienen implementadas en el hardware y el software solo se encarga de gestionarlas. Lo que encarece el costo del sistema y dificulta su extensión con cámaras u otro equipo que no sea del fabricante que lo proveyó, ya que existe una muy baja compatibilidad.

1.4 Metodologías, herramientas y tecnologías a utilizar para el desarrollo de la solución.

1.4.1 Tecnologías a usar para el desarrollo del sistema.

Las tecnologías a usar a la hora de desarrollar cualquier aplicación están en estrecha dependencia con respecto a los lenguajes de programación a utilizar. Debido a las características que tiene el sistema, los autores consideraron que el desarrollo de la aplicación se realice con C# 2.0 como lenguaje de desarrollo ya que este es el lenguaje estrella de la plataforma de desarrollo .NET. Cuenta con una extensa biblioteca de clases base para el desarrollo de todo tipo de aplicaciones. C# 2.0 es un lenguaje de programación simple pero eficaz, este toma las mejores características de lenguajes preexistentes como Visual Basic, Java o C++ y las combina en un solo lenguaje.

C# presenta entre otras características:

- ✓ Sencillez.
- ✓ Modernidad.
- ✓ Orientación a Objetos.
- ✓ Orientación a componentes.
- ✓ Gestión automática de memoria.
- ✓ Seguridad de tipos.
- ✓ Instrucciones seguras.
- ✓ Sistema de tipos unificado.
- ✓ Extensibilidad de tipos básicos.
- ✓ Extensibilidad de operadores.
- ✓ Extensibilidad de modificadores.
- ✓ Posibilidad de crear versiones.
- ✓ Eficiencia
- ✓ Compatibilidad.

1.4.2 Herramientas.

Para el desarrollo de esta estación de monitorización se seleccionó como herramienta CASE[3] a utilizar Enterprise Architect (EA) ya que es una herramienta comprensible de diseño y análisis UML[4], cubriendo el desarrollo de software desde el paso de los requerimientos a través de las etapas del análisis, modelos de diseño, pruebas y mantenimiento. EA es una herramienta multi-usuario, basada en Windows, diseñada para ayudar a construir software robusto y fácil de mantener. Ofrece salida de documentación flexible y de alta calidad.

Provee trazabilidad completa desde el análisis de requerimientos hasta los artefactos de análisis y diseño, a través de la implementación y el despliegue. Combinados con la ubicación de recursos y tareas incorporados, los equipos de Administradores de Proyectos y Calidad están equipados con la información que ellos necesitan para ayudarles a entregar proyectos en tiempo. (7)

Control de Versiones

Subversion: Es un sistema de control de versiones diseñado para acceder al repositorio a través de redes, lo que le permite ser usado por personas que se encuentran en distintos ordenadores. A cierto nivel, la posibilidad de que varias personas puedan modificar y administrar el mismo conjunto de datos desde sus respectivas ubicaciones fomenta la colaboración. Es software libre bajo una licencia de tipo Apache/BSD y se le conoce también como **svn** por ser el nombre de la herramienta utilizada en la línea de órdenes.

Existen varias interfaces a **Subversion**, ya sea programas individuales como interfaces que lo integran en entornos de desarrollo, para el control de versiones del sistema se utilizó **TortoiseSVN** el cual provee integración con el explorador de Microsoft Windows, además de **AnkhSVN**, extensión para Visual Studio 2010.

[3]CASE: ComputerAided Software Engineering, Ingeniería de Software Asistida por Ordenador.

[4]UML: UnifiedModelingLanguage, Lenguaje Unificado de Modelado.

IDE[5] de desarrollo

Los IDEs se deben seleccionar en dependencia del lenguaje en que se piensa desarrollar. Como se ha seleccionado el C# 2.0 se eligió como IDE de desarrollo **Microsoft Visual Studio 2010** ya que este entorno de desarrollo integrado puede ser utilizado para desarrollar tanto librerías de código necesarias para los plugins de las cámaras como controles de usuario personalizados e interfaces de usuario de calidad para alcanzar una alta usabilidad por el usuario final.

1.4.3 Tecnologías a usar para la comunicación.

Conjuntamente con los lenguajes de desarrollo se utilizan tecnologías que; apoyadas en las herramientas de desarrollo, permiten de manera integral desarrollar el sistema. Para el sistema se necesita fundamentalmente tecnología de comunicaciones.

Comunicación: Tecnologías que permiten la transmisión de datos sobre la red, están condicionadas por el lenguaje de desarrollo a utilizar.

Microsoft .NET Remoting 2.0: .NET Remoting permite crear fácilmente aplicaciones ampliamente distribuidas, tanto si los componentes de las aplicaciones están todos en un equipo como si están repartidos por el mundo. Se pueden crear aplicaciones de cliente que utilicen objetos en otros procesos del mismo equipo o en cualquier otro equipo disponible en la red. También se puede utilizar .NET Remoting para comunicarse con otros dominios de aplicación en el mismo proceso.

Características de .Net Remoting:

- ✓ Gran flexibilidad.
- ✓ Tecnologías independientes del lenguaje de programación y con las comunicaciones en un nivel de abstracción elevado.
- ✓ Modelo de programación sencillo y eficaz, así como compatibilidad en tiempo de ejecución que permite interacciones transparentes.

[5]IDE: IntegratedDevelopEnvironment, Entorno Integrado de Desarrollo, software para desarrollar aplicaciones en distintos lenguajes.

Se seleccionó Microsoft **.NET Remoting 2.0** para la comunicación entre los módulos del sistema debido a que es una tecnología de alto nivel, inherente a la plataforma .NET que ya se había seleccionado anteriormente y por su probada eficacia en aplicaciones desktop distribuidas.

1.4.4 Metodologías.

En el ciclo de vida del software se deben completar una serie de tareas para obtener un producto de software. Cada una de esas tareas puede ser abordada y resuelta de múltiples maneras, con distintas herramientas y utilizando distintas técnicas. Es necesario saber cuándo podemos dar por concluida una tarea, quién debe realizarla, qué tareas preceden o anteceden a una dada, qué documentación utilizaremos para llevar a cabo esa tarea. Estamos hablando de detalles organizativos, de un estilo de hacer las cosas. Formalizando ese estilo; añadiendo algo de rigurosidad y normas obtenemos una metodología.

Se entiende por metodología de desarrollo una colección de documentación formal referente a los procesos, las políticas y los procedimientos que intervienen en el desarrollo del software. La finalidad de una metodología de desarrollo es garantizar la eficacia (ej. cumplir los requisitos iniciales) y la eficiencia (ej. minimizar las pérdidas de tiempo) en el proceso de generación de software. (8)

Las metodologías de desarrollo de software se dividen en dos grandes grupos estos son Metodologías Ágiles de Desarrollo y Metodologías Tradicionales o Robustas. Tenemos entre las metodologías tradicionales RUP[6] el cual se seleccionó como metodología de desarrollo a utilizar debido a que es la más utilizada en el mundo para el desarrollo de sistemas orientados a objeto, ya que utiliza UML para el modelado y la herramienta CASE a utilizar, Enterprise Architect, lo soporta completamente.

RUP: Es un proceso de desarrollo de software y junto con el UML, constituye la metodología estándar más utilizada para el análisis, implementación y documentación de sistemas orientados a objetos. El RUP no es un sistema con pasos firmemente establecidos, sino un conjunto de metodologías adaptables al contexto y necesidades de cada organización. Se caracteriza por ser iterativo e incremental, estar centrado en la arquitectura y guiado por los casos de uso. Incluye artefactos (que son los productos tangibles del proceso como por ejemplo, el modelo de casos de uso, el código fuente, etc.) y roles (papel

[6] RUP: RationalUnifiedProcess, Proceso Unificado Racional.

que desempeña una persona en un determinado momento, una persona puede desempeñar distintos roles a lo largo del proceso). (9)

El RUP está basado en 5 principios claves que son:

- ✓ **Adaptar el proceso:** El proceso deberá adaptarse a las características propias del proyecto u organización. El tamaño del mismo, así como su tipo o las regulaciones que lo condicionen, influirán en su diseño específico. También se deberá tener en cuenta el alcance del proyecto.
- ✓ **Balancear prioridades:** Los requerimientos de los diversos participantes pueden ser diferentes, contradictorios o disputarse recursos limitados. Debe encontrarse un balance que satisfaga los deseos de todos. Debido a este balanceo se podrán corregir desacuerdos que surjan en el futuro.
- ✓ **Demostrar valor iterativamente:** Los proyectos se entregan, aunque sea de un modo interno, en etapas iteradas. En cada iteración se analiza la opinión de los inversores, la estabilidad y calidad del producto, y se refina la dirección del proyecto así como también los riesgos involucrados.
- ✓ **Elevar el nivel de abstracción:** Este principio dominante, motiva el uso de conceptos reutilizables tales como patrón del software, lenguajes 4GL o marcos de referencia (Frameworks) por nombrar algunos. Esto evita que los ingenieros de software vayan directamente de los requisitos a la codificación de software a la medida del cliente, sin saber con certeza qué codificar para satisfacer de la mejor manera los requerimientos y sin comenzar desde un principio pensando en la reutilización del código. Un alto nivel de abstracción también permite discusiones sobre diversos niveles y soluciones arquitectónicas. Estas se pueden acompañar por las representaciones visuales de la arquitectura, por ejemplo con el lenguaje UML.
- ✓ **Enfocarse en la calidad:** El control de calidad no debe realizarse al final de cada iteración, sino en todos los aspectos de la producción. El aseguramiento de la calidad forma parte del proceso de desarrollo y no de un grupo independiente.

Principales características:

- ✓ Forma disciplinada de asignar tareas y responsabilidades (quién hace qué, cuándo y cómo).
- ✓ Pretende implementar las mejores prácticas en Ingeniería de Software.
- ✓ Desarrollo iterativo.
- ✓ Administración de requisitos.

- ✓ Uso de arquitectura basada en componentes.
- ✓ Control de cambios.
- ✓ Modelado visual del software.
- ✓ Verificación de la calidad del software.

1.5 Conclusiones.

En el capítulo se presentaron los fundamentos teóricos que constituyen la base de esta investigación sobre los sistemas de video vigilancia, abordando desde los sistemas analógicos que fueron los primeros hasta los modernos sistemas digitales. Se analizaron algunas de las principales empresas del mundo en la fabricación de sistemas de este tipo. Se realizó un estudio en cuanto a las desventajas, tecnologías y herramientas que serán utilizadas para el desarrollo del software propuesto.

Capítulo 2: Características del sistema.

2.1 Introducción

Con motivo de la poca estructuración de los procesos del negocio y para poder comprender el contexto en el cual se desarrolla el sistema se determinó desarrollar un Modelo de Dominio, donde se expone un marco conceptual y las relaciones entre estas definiciones. Por otra parte, se enumeran los requerimientos funcionales y no funcionales, agrupándose los primeros en Casos de Uso, con el fin de estructurar el Diagrama de Casos de Uso del Sistema.

2.2Modelo de Dominio.

El Modelo de Dominio o Modelo Conceptual, permite de manera visual mostrar al usuario los principales conceptos que se manejan en el dominio del sistema en desarrollo. Un Modelo de Dominio es una representación visual de los conceptos u objetosdel mundo real significativos para un problema o área de interés. Representa clases conceptuales deldominio del problema; representa conceptos del mundo real, no de los componentes de software. El modelo desarrollado no se trata de un conjunto de diagramas que describen clases de software u objetos de software con responsabilidades, sino que puede considerarse como un diccionario visual de las abstracciones relevantes, vocabulario e información del dominio. Aprovechando las bondades de los diagramas UML para representar conceptos, el Modelo de Dominio se presenta en forma de diagrama de clases donde figuran los principales conceptos y roles del sistema en cuestión.

*2.2.1*Conceptos Fundamentales.

Para un mejor entendimiento del Diagrama de Modelo de Dominio conformado, en este punto se proporciona un marco conceptual con las definiciones identificadas, las cuales son:

Estación de Monitorización:Módulo encargado de la visualización y manejo de los flujos de video de las cámaras.

Agente Externo (Orquestador):Módulo orquestador del sistema, controla el tráfico de información entre el resto de los módulos del mismo.

Petición: Acción, evento, tarea generada por un usuario, estación de monitorización u orquestador para cumplir un objetivo deseado.

Respuesta: Información generada a partir de una petición recibida.

Administrador: Persona encargada de la vigilancia en la entidad el cual tiene permisos de administración en el sistema.

Operador: Persona encargada de la vigilancia en la entidad.

2.2.2 Diagrama del Modelo de Dominio.

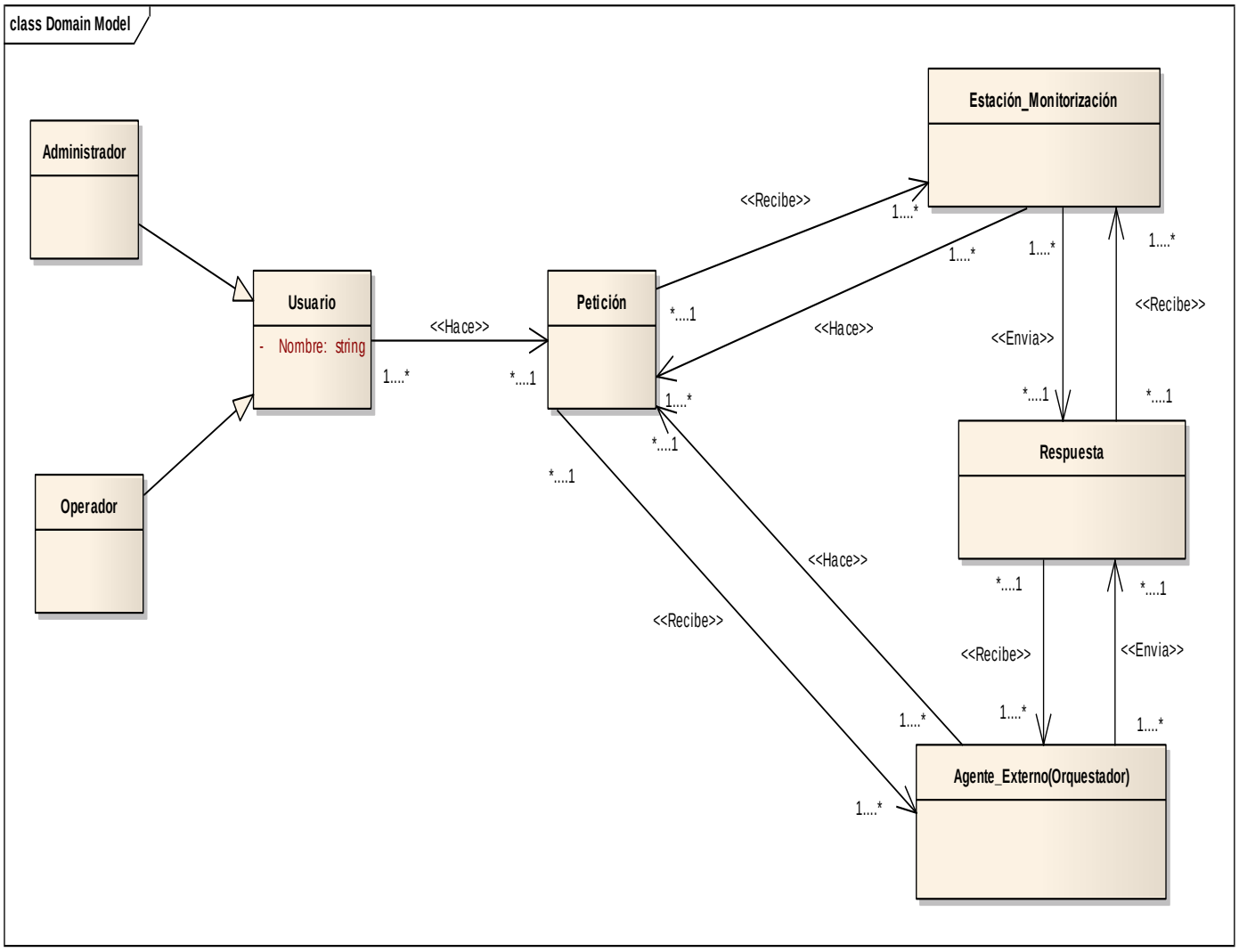


Figura 7. Modelo de Dominio.

2.3 Breve descripción del sistema.

El módulo Estación de Monitorización permitirá a los operadores manipular las cámaras, visualizar los flujos de video obtenidos de cada una de ellas de manera individual o en grupo. De esta forma se podrá centrar la vigilancia de un determinado número de puntos de interés en una sola estación de visualización. Cuando se active elmódulo Estación de Monitorización este descargará del orquestador toda la información relacionada a las cámaras y otros elementos de configuración necesarios para su funcionamiento. El operador podrá entonces manipular las cámaras o hacer cambios sobre este si es un administrador. Cualquier modificación a los datos existentes se le solicita al orquestadorque la procesa y avisa a las demás instancias del módulo de monitorización que se encuentren activas, para que reflejen dicho cambio.Este módulo será capaz de manipular diversos tipos de cámaras que a la vez pueden ser de distintos fabricantes. Para esto el sistema soportará cada hardware a través de plugins, que serán desarrollados de manera específica para cada cámara, pero que funcionarán de manera semejante, de forma tal que el sistema puede utilizar cualquiera de estos plugins de la misma forma, no importa la cámara que sea, manteniéndose así la sencillez del diseño y la flexibilidad del sistema.El mismo debe tener una interfaz amigable, de manera que sea atractivo al usuario y que brinde además un fácil acceso a todas las operaciones del sistema. Debe de ser un diseño basado en ventanas plegables, para también dejar disponible la mayor cantidad de área expositiva para la visualización de las cámaras.

Los Sistemas de Vigilancia se caracterizan por tener en cada estación de monitorización varios monitores y televisores conectados a la PC, el sistema debe de ser capaz de enviar la señal de una cámara o de un grupo de cámaras determinado hacia cualquier monitor o televisor. Para ello se propone además el desarrollo de controles gráficos específicos para la aplicación utilizando la plataforma .NET, que brinden la posibilidad de visualizar en cada uno de ellos cámaras individuales o grupos de ellas y que esos controles entonces puedan ser enviados a cada monitor o televisor como ventanas apartes.

2.4 Requerimientos Funcionales del Sistema.

Los requerimientos funcionales son capacidades o condiciones que el sistema debe cumplir.

*Nota: Se usa el prefijo **RF** en su nomenclatura-*

Se debe agregar las siguientes funcionalidades a la Estación de Monitorización del sistema SURIA:

RF1 Autenticar usuario.

RF2 Gestionar Usuario.

2.1 Adicionar Usuario.

2.2Eliminar Usuario.

2.3Actualizar Usuario.

RF3 Mostrar Bitácora de sucesos en el Sistema.

RF4 Generar Reporte.

RF5 Hacer Zoom sobre flujo de Video.

RF6 Generar Alarma Visual.

RF7 Gestionar Roles.

7.1 Adicionar Rol.

7.2 Actualizar Rol.

7.3 Eliminar Rol.

RF8 Generar Alarma Sonora.

RF9 Realizar Detección de rostro.

RF10 Realizar Detección de Movimiento.

RF11 Chequeo de Cámaras offline.

2.5 Requerimientos No Funcionales del Sistema.

Los requerimientos no funcionales son propiedades o cualidades que el producto debe tener. Son características que hacen al producto atractivo, usable, rápido o confiable. Estos requerimientos se agrupan en varias categorías:

Requerimientos de Usabilidad.

*Nota: Se usa el prefijo **RNU** en su nomenclatura*

RNU 1 La interfaz debe ser configurable para lograr la comodidad del usuario.

RNU 2 El usuario debe poder configurar el sistema, sin necesidad de acceder manualmente a los ficheros de configuración.

RNU 3 El Sistema debe mostrar mensajes al usuario, que le ayuden a llevar a cabo la tarea que realiza.

RNU 4 Se debe hacer uso de botones, con imágenes que indiquen de modo intuitivo la función que realizan.

RNU 5 Los controles visuales deben mostrar mensajes que indiquen su función.

RNU 6 La configuración predeterminada debe brindar buena comodidad.

RNU 7 Los parámetros de funcionamiento del módulo deben ser configurables.

Requerimientos de Fiabilidad.
*Nota: Se usa el prefijo **RNF** en su nomenclatura.*

RNF 7 El sistema debe estar disponible de forma permanente.
RNF 8 Debe funcionar sin necesidad de la intervención del usuario.

Requerimientos de Eficiencia.
*Nota: Se usa el prefijo **RNE** en su nomenclatura.*

RNE 9 Debe usar programación concurrente para lograr un óptimo aprovechamiento de los recursos de hardware.

Requerimientos de Diseño e Implementación.
*Nota: Se usa el prefijo **RNDI** en su nomenclatura.*

RNDI 10 Debe ser implementado en C#2.0 ajustándose a las funcionalidades del Framework 2.0.

RNDI 11 Resolución de 1024 x 768.

Requerimientos de Soporte.
*Nota: Se usa el prefijo **RNSO** en su nomenclatura.*

RNSO 12 El sistema permitirá la modificación o agregarle módulos cuando sea necesario, asegurando su extensibilidad y lograr mejores prestaciones. Además el sistema debe permitir distribuir la carga de trabajo en tantas estaciones como se requiera para llevarla a cabo.

Requerimientos de Interfaz de usuario.
*Nota: Se usa el prefijo **RNIU** en su nomenclatura.*

RNIU 13 Se requiere que el Cliente tenga una interfaz gráfica que permita la interacción con el usuario.

Requerimientos de Interconexión.
*Nota: Se usa el prefijo **RNI** en su nomenclatura.*

RNI 14 Debe poder comunicarse con cualquier aplicación que implemente las interfaces definidas para el Gestor.

RNI 15 Debe brindar una interfaz fija para la comunicación con sistemas externos que usen las funciones que la estación de monitorización brinda.

Requerimientos de Funcionamiento.
*Nota: Se usa el prefijo **RNFO** en su nomenclatura.*

RNFO 16 Se debe tener instalado .NET Framework 2.0 o superior.

RNFO 17 Usar como sistema operativo Windows XP SP2 o superior: Determinado por los requerimientos del .NET Framework 2.0. (32)

Requerimientos de Seguridad.
*Nota: Se usa el prefijo **RNS** en su nomenclatura.*

RNS 18 Se garantizará la accesibilidad a diferentes controles según los privilegios de usuarios.

2.6 Definición de los casos de uso.

2.6.1 Definición de los actores.

Actor	Descripción
Administrador	***Rol responsable de velar por el funcionamiento apropiado del sistema, configurarlo y realizar todas las demás funcionalidades que permite el sistema.***
Operador	***Rol que se beneficia de diversas funcionalidades del sistema pero no tiene acceso a las configuraciones del mismo.***
Estación de Monitorización	***Rol que representa la Estación de Monitorización que controla y visualiza el flujo de video obtenidos de las cámaras IP.***
Orquestador	***Rol que representa el orquestador del sistema, controlador del tráfico de información entre el resto de los agentes autónomos del mismo.***

2.6.2 Listado de los casos de uso.

De acuerdo a las nuevas funcionalidades que se le agregarán a la Estación de Monitorización quedan conformados los siguientes Casos de Uso:

Caso de Uso:	***Autenticar usuario***
Actores:	***Operador***
Descripción:	***Se inicia cuando el actor introduce su usuario y contraseña para acceder al sistema, los mismos se verifican contra la base de datos.***
Referencia:	***RF1***

Caso de Uso:	***Gestionar Usuario***
Actores:	***Administrador***
Descripción:	***El usuario accede al administrador de usuarios del sistema donde puede seleccionartanto la opción de adicionar, eliminar o editar un usuario.***
Referencia:	***RF2.1, RF2.2, RF2.3***

Caso de Uso:	***Mostrar Bitácora de sucesos en el Sistema***
Actores:	***Administrador***
Descripción:	***El administrador selecciona la opción de Visualizar Logs del Sistema, donde aparecerán los eventos ocurridos en el mismo.***
Referencia:	***RF3***

Caso de Uso:	***Generar Reporte***
Actores:	***Operador***
Descripción:	***El usuario selecciona la opción de Generar un Reporte la cual generará de forma automática un informe detallado de los sucesos y eventos en el Sistema.***
Referencia:	***RF4***

Caso de Uso:	***Hacer Zoom sobre flujo de Video***
Actores:	***Operador***
Descripción:	***El usuario selecciona el control que le permite el manejo del zoom sobre la cámara que se encuentra visualizándose.***
Referencia:	***RF5***

Caso de Uso:	***Generar Alarma Visual***
Actores:	***Orquestador***
Descripción:	***El sistema muestra gráficamente una alarma a partir de la detección de algún evento.***
Referencia:	***RF6***

Caso de Uso:	***Gestionar Roles***
Actores:	***Administrador***
Descripción:	***El usuario accede al administrador de usuarios del sistema donde puede seleccionar tanto la opción de adicionar, eliminar o editar un rol.***
Referencia:	***RF7.1, RF7.2, RF7.3***

Caso de Uso:	***Generar Alarma Sonora***
Actores:	***Orquestador***
Descripción:	***El sistema genera una alarma sonora a partir de la detección de algún evento.***
Referencia:	***RF8***

Caso de Uso:	***Realizar Detección de rostro***
Actores:	***Administrador***
Descripción:	***El Usuario abre un formulario especializado con opciones de detección de rostro.***
Referencia:	***RF9***

Caso de Uso:	***RealizarDetección de Movimiento***
Actores:	***Operador***
Descripción:	***El Usuario abre un formulario especializado con opciones de detección de movimiento.***
Referencia:	***RF10***

Caso de Uso:	***Chequeo de Cámaras offline***
Actores:	***Estación de Monitorización***
Descripción:	***El sistema chequea el estado de la conexión de las cámaras en visualización en un intervalo de tiempo predeterminado.***
Referencia:	***RF11***

2.7Diagrama de Casos de Uso.

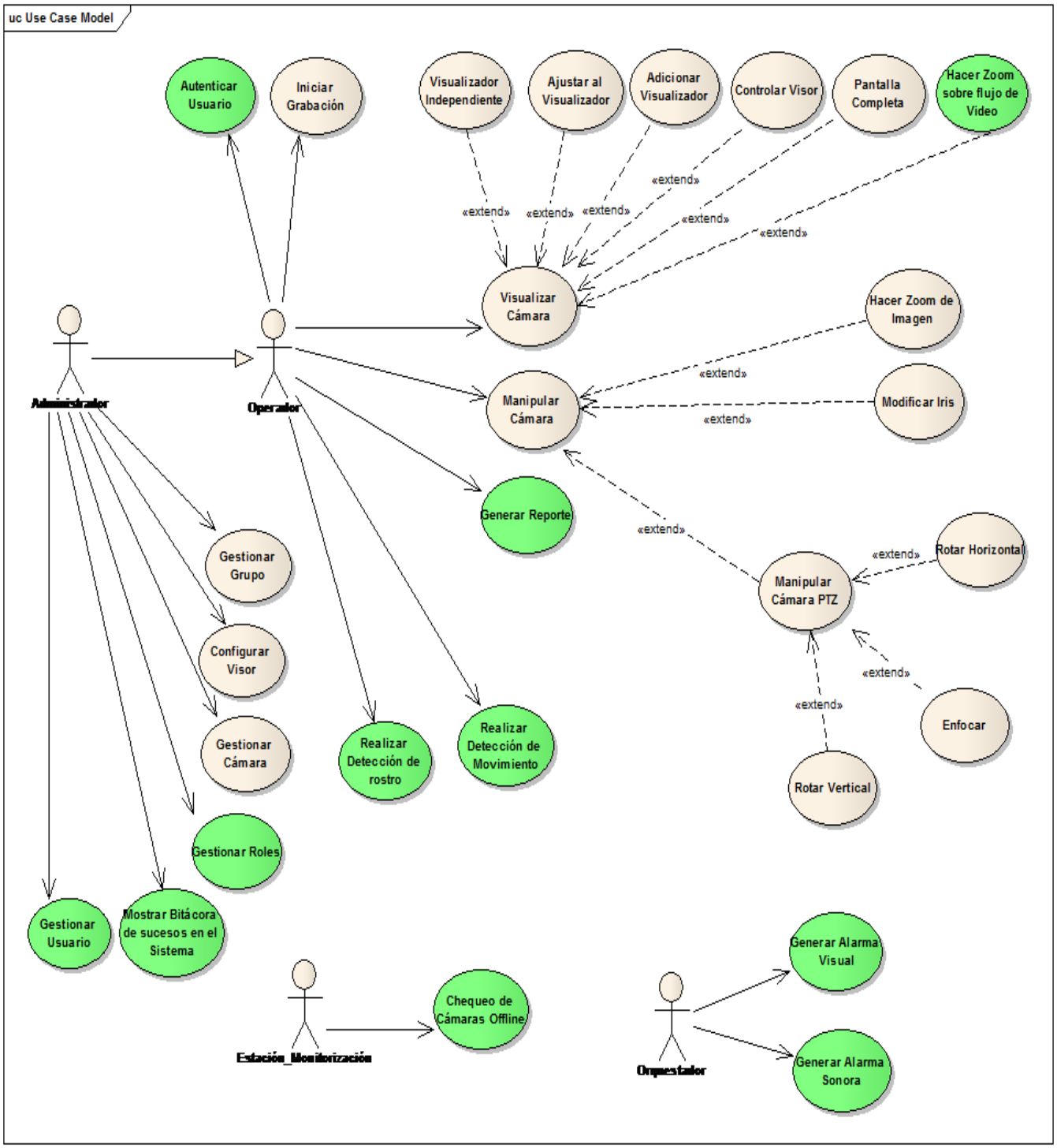


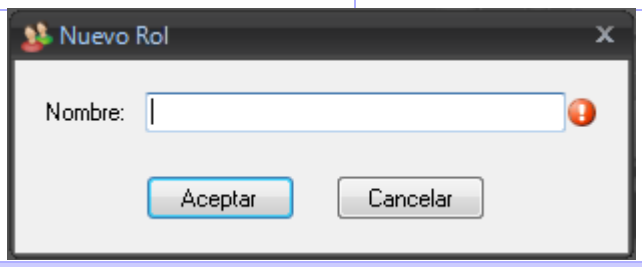
Figura8. Diagrama de Casos de Uso.

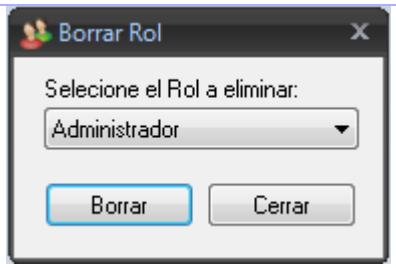
2.8 Casos de Uso Expandidos.

Caso de Uso:	Autenticar usuario
Actores:	Operador
Propósito:	Garantizar la seguridad en el Sistema mediante el uso autenticación.
Resumen:	El caso de uso se inicia cuando el Operador abre la Estación de Monitorización.
Referencias	RF7

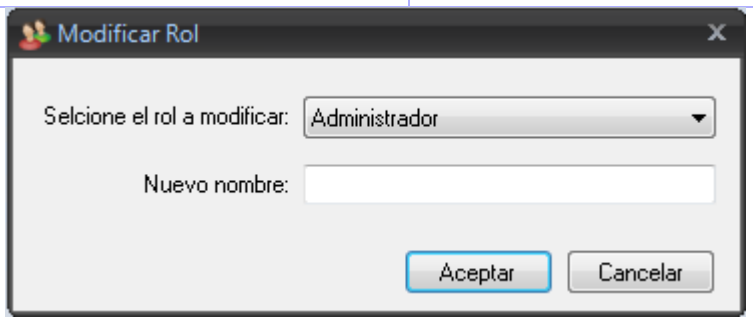
Flujo Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
Escenario Autenticarse	
1.- El Operador abre la Estación de Monitorización.	2.- El Sistema le muestra la forma para Autenticarse.
3.- El Operador selecciona el nombre de usuario y escribe la contraseña correspondiente.	4.- El Sistema verifica la validez de los datos introducidos.
	5.- El Sistema muestra la forma principal de la Estación de Monitorización.
Flujos Alternos	
Escenario contraseña introducida incorrecta.	
Acción del Actor	**Respuesta del Sistema**
	4.- El Sistema muestra una advertencia en la forma para Autenticarse informando que la contraseña es incorrecta.

Caso de Uso:	Gestionar Roles
Actores:	Administrador
Propósito:	Garantizar la seguridad en el Sistema mediante el uso de roles con distintos privilegios.
Resumen:	El caso de uso se inicia cuando el Administrador selecciona la opción de adicionar, eliminar o actualizar un rol determinado en el Administrador de Seguridad previamente abierto.
Referencias	RF13.1, RF13.2, RF13.3

Flujo Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
Escenario Adicionar	
1.- El Administrador abre el Administrador de Seguridad.	2.- El Sistema le muestra la forma del Administrador de Seguridad.
3.- El Administrador selecciona la opción de adicionar un rol.	4.- El Sistema le muestra una forma para introducir los datos necesarios.
5.- El Administrador entra los datos necesarios y acepta la entrada.	6.- El Sistema almacena los nuevos datos.
	
Escenario Eliminar	
1.- El Administrador abre el Administrador de Seguridad.	2.- El Sistema le muestra la forma del Administrador de Seguridad.
3.- El Administrador selecciona la opción de eliminar un rol.	4.- El Sistema muestra los roles que existen.
5.-El Administrador selecciona un rol y acepta.	6.- El Sistema muestra una advertencia.
7.-El Administrador elige continuar con la operación.	8.- El Sistema elimina el rol.

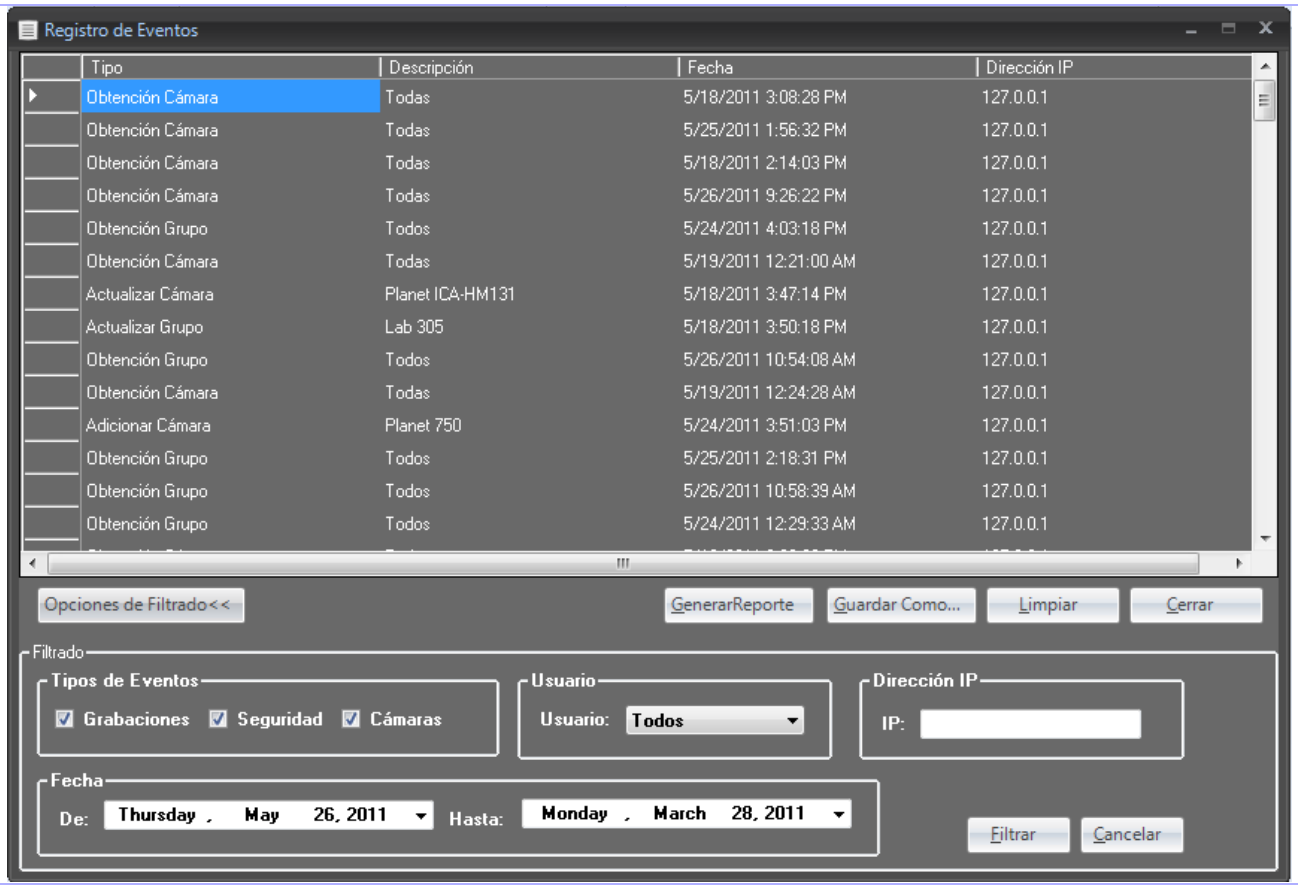


Escenario Actualizar	
1.- El Administrador abre el Administrador de Seguridad.	2.- El Sistema le muestra la forma del Administrador de Seguridad.
3.- El Administrador selecciona la opción de editar un rol.	4.- El Sistema muestra los roles que existen.
5.-El Administrador selecciona un rol.	6.- El Sistema muestra los datos del rol.
7. El Administrador modifica los datos y acepta.	8.-El Sistema almacena los datos modificados.



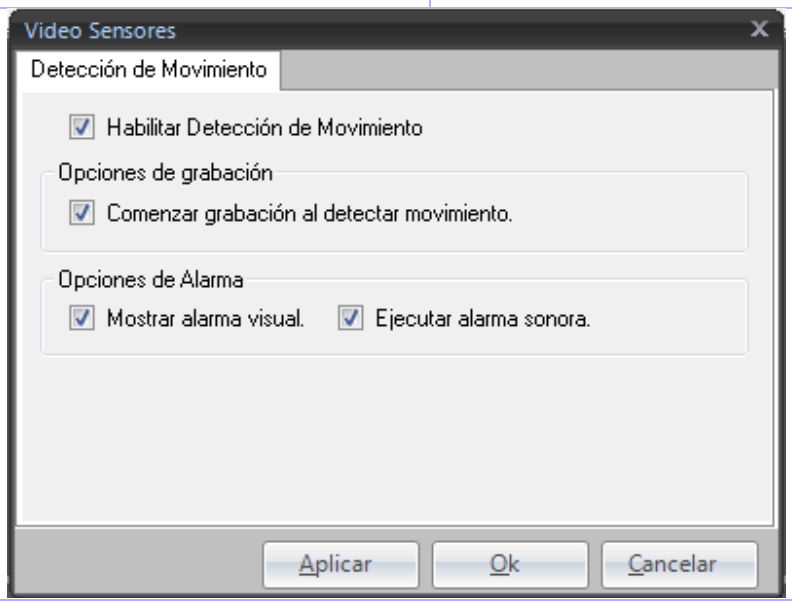
Caso de Uso:	Mostrar Bitácora de sucesos en el Sistema
Actores:	Administrador
Propósito:	Mostrar una lista de eventos ocurridos en el Sistema.
Resumen:	El caso de uso se inicia cuando el Administrador selecciona la opción de Mostrar Bitácora de sucesos en el Sistema.
Referencias	RF9

Flujo Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
Escenario Mostrar Bitácora de sucesos en el Sistema	
1.- El Administrador selecciona la opción de Mostrar Bitácora de sucesos en el Sistema.	2.- El Sistema muestra una forma con todos los datos de los sucesos ocurridos en el Sistema.



Caso de Uso:	Generar Alarma Sonora
Actores:	Orquestador
Propósito:	Mostrar una alarma sonora para alertar sobre un suceso ocurrido.
Resumen:	El caso de uso se inicia cuando la Estación de Monitorización recibe una notificación sobre algún evento a alertar.
Referencias	RF14
Flujo Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
Escenario Generar Alarma Sonora	
1.- ElOrquestador recibe una notificación sobre algún evento a alertar.	2.- El Sistema genera una alarma sonora para alertar sobre el suceso.

Caso de Uso:	Realizar Detección de Movimiento
Actores:	Operador
Propósito:	Habilitar un formulario con opciones especializadas para la detección de movimiento.
Resumen:	El caso de uso se inicia cuando el Usuarioselecciona la opción de abrir Visor Especializado.
Referencias	RF17
Flujo Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
Escenario Realizar Detección de Movimiento	
1.- El Operador selecciona la opción de abrir Visor Especializado.	2.- El Sistema muestra un formulario con las opciones especializadas para la detección de movimiento.



Nota: Las restantes descripciones de los Casos de uso Expandidos, por su extensión se encuentran en el Anexo I.

2.9 Conclusiones.

En este capítulo se establecieron las características principales del sistema así como el proceso para su funcionamiento.Se obtuvo el modelo del dominio, conjuntamente con la especificación de los requisitos funcionales y no funcionales.Se elaboró el modelo de casos de uso del sistema.

Capítulo 3: Análisis y diseño del sistema.

3.1 Arquitectura.

***3.1.1* Arquitectura del sistema de video vigilancia SURIA.**

Primeramente antes de exponer la propuesta del sistema que se presenta como solución en la presente investigación, es necesario analizar las particularidades de la arquitectura del sistema SURIA, el mismo está diseñado para seguir una arquitectura primaria, en forma de pizarra en su variante de tablero de control. Esta desacopla el sistema en componentes denominados agentes autónomos, los cuales son independientes en la realización atómica de su funcionalidad. (2) Pero dependen de una entrada de información externa, que es provista por otros agentes, y a su vez, producen un resultado que puede ser entrada de otros agentes.

Cada agente se rige por interfaces estándares que permiten cambios en el ambiente externo del mismo sin que este sufra cambios en su funcionamiento interno. Todo el funcionamiento de los agentes autónomos, está coordinado por un elemento central, denominado Repositorio Activo, el cual entrega y recibe información de los agentes y coordina su funcionamiento.En el caso del sistema de video vigilancia SURIA, el **Orquestador** cumple con la función de Repositorio activo al que se pueden conectar diferentes agentes autónomos.

Aunque el Sistema mantiene una Arquitectura de Pizarra a manera global, en cada uno de los módulos o sea los agentes autónomos se usa el estilo Modelo-Vista-Controlador (MVC).

3.1.2 Patrones Arquitectónicos usados.

- **Patrón arquitectónico Modelo-Vista-Controlador**

El patrón Modelo-Vista-Controlador (MVC) afronta una de las consecuencias de los cambios frecuentes en los soportes de hardware y de añadir nuevas funcionalidades, que es la de constantes modificaciones en la interfaz de usuario. Se separa los módulos en 3 componentes fundamentales, el Modelo, la Vista y el Controlador. El Modelo es inmutable a los cambios en la interfaz de usuario, se encarga de toda la gestión interna del negocio, la Vista se encarga de presentar los datos y de interactuar con el usuario, mientras que el controlador maneja todos los cambios de estado de la Vista. Mediante el uso de este

patrón la Estación de Monitorización es capaz de utilizar diferentes interfaces de usuario manteniendo la misma lógica de negocio.

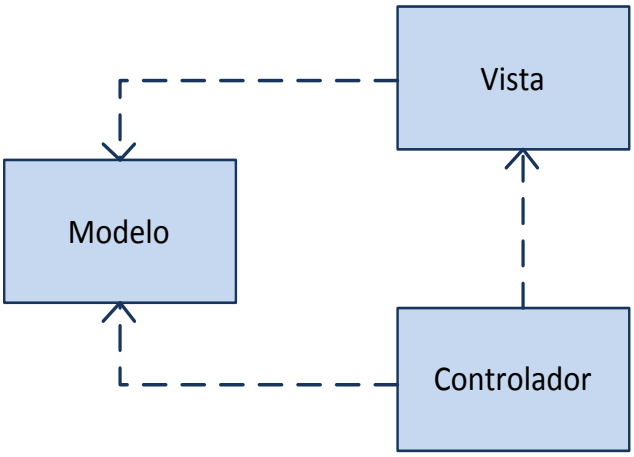


Figura 9 Patrón Modelo-Vista-Controlador.

- **Arquitectura basada en plugins**

Las funcionalidades de agregar y visualizar cámaras de un tipo en específico se implementan en plugins, lo que brinda ventajas como:

Extensibilidad del sistema: Se pueden agregar plugins al sistema para dar soporte a nuevos modelos de cámaras sin tener que recompilar todo el sistema.

Ambiente controlado: Cada plugin implementa un ambiente controlado de visualización. En caso de que ocurra un error, este puede ser descargado sin afectar al resto de la aplicación.

3.1.3 Arquitectura del Módulo Estación de Monitorización.

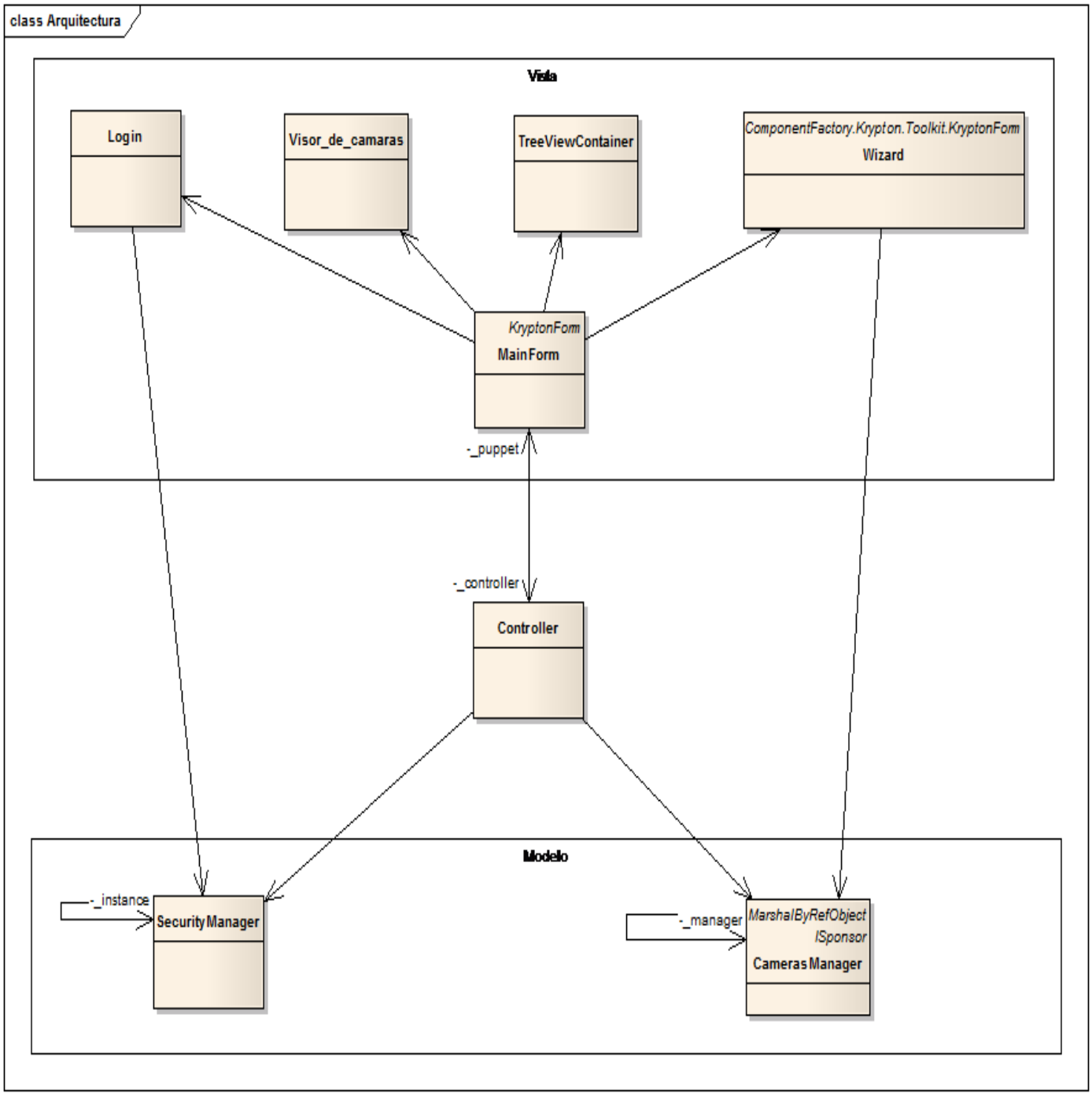


Figura 10. Arquitectura Estación de Monitorización.

3.2 Modelo de Análisis.

El análisis consiste en obtener una visión del sistema que se preocupa de lo que hace el mismo. El modelo de análisis es la entrada fundamental para el comienzo del diseño. A continuación se listan los diagramas de análisis de los CU más significativos en el sistema. El resto de los diagramas de análisis por su extensión se encuentran en el *fichero "**EstaciónMonitorizacion.eap**" elaborado en Enterprise Architect 7.5 para una información más detallada sobre los Diagramas de Análisis.*

Diagrama de clases de análisis.

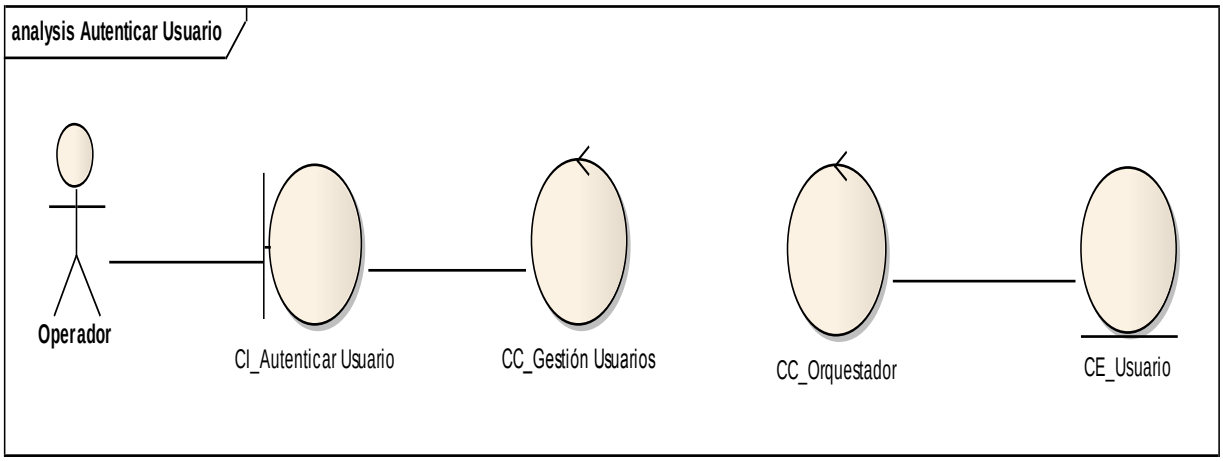


Figura 11. CU Autenticar usuario.

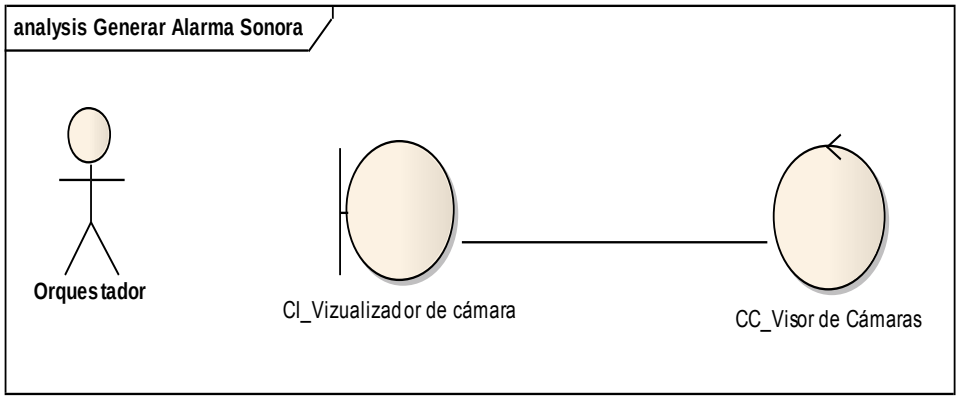


Figura 12. CU Generar Alarma Sonora.

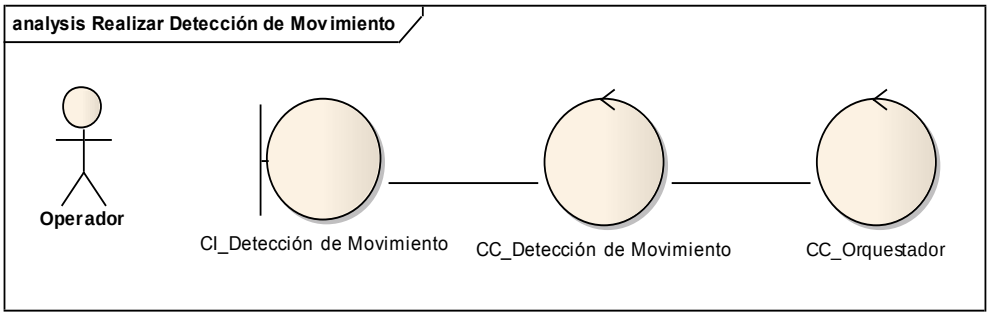


Figura 13. CU Realizar Detección de Movimiento.

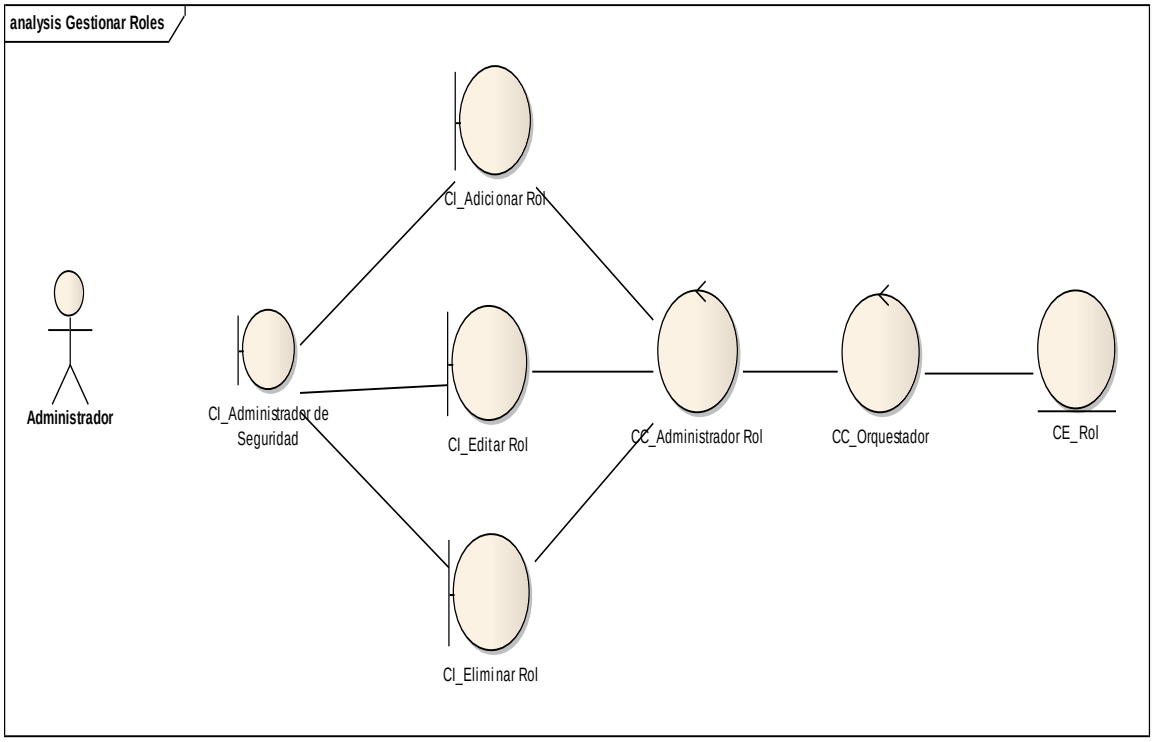


Figura 14. CU Gestionar Roles.

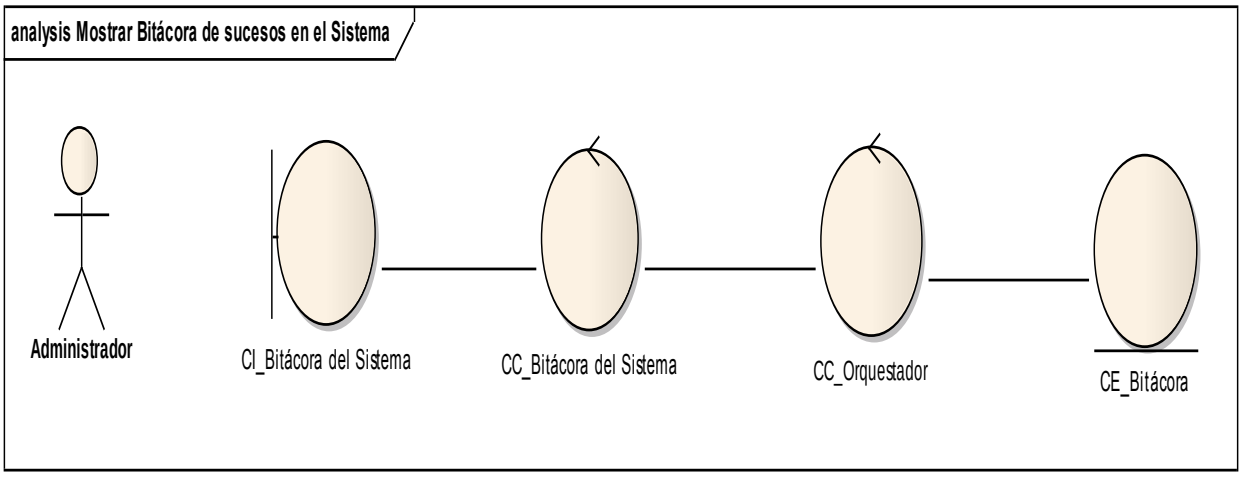


Figura 15. CU Mostrar Bitácora de Sucesos en el Sistema.

3.3 Modelo de Diseño.

Un Modelo de Diseño es un modelo de objetos que describe la realización física de los casos de uso, centrándose en cómo los requisitos funcionales y no funcionales, junto con otras restricciones relacionadas con el entorno de implementación, tienen impacto en el sistema. Este artefacto constituye la entrada fundamental utilizada para el correcto desarrollo de la implementación.

A continuación se presenta el diagrama de diseño delsistema y una brevedescripciónde las principales clases involucradas en el mismo. Los diagramas de clases del diseño por casos de uso, por su extensión se encuentran en el **Anexo II** los diagramasde secuenciay en el **Anexo III** los diagramasdeClases. Además v*er fichero "**Estación Monitorizacion.eap**"*

3.3.1 Diagrama de Diseño del Sistema.

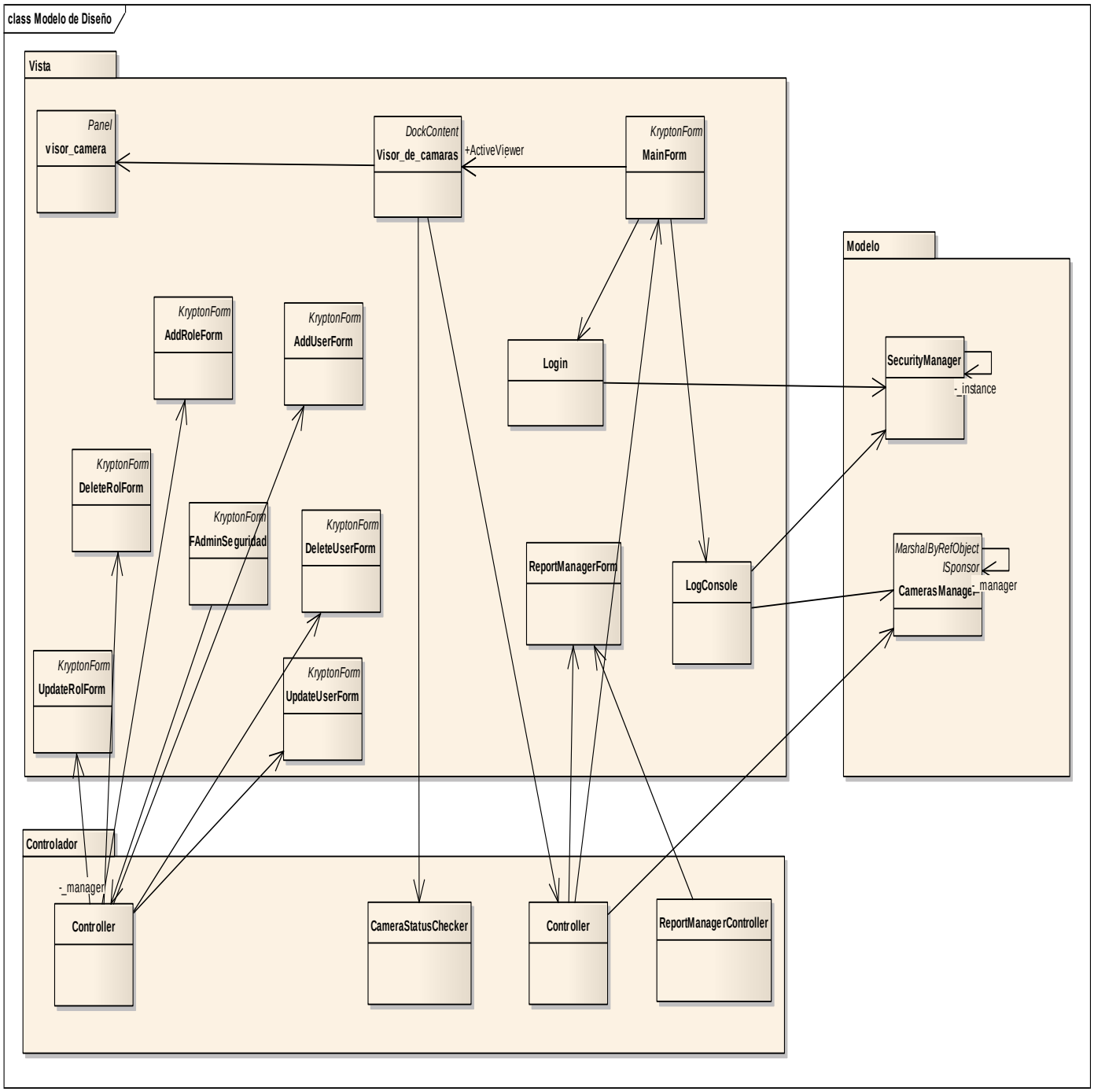


Figura 16. Diagrama de Diseño del Sistema.

En el paquete Vista residen todos los formularios, los cuales son los encargados de brindarles la información a los usuarios en forma de interfaces para viabilizar la interacción de los mismos con el sistema. Como formulario e interfaz principal se encuentra el MainForm, encargado de recibir todos los eventos y acciones generados por el usuario sobre el sistema, este, mediante el Visor de Cámaras visualiza el flujo de video obtenido desde las cámaras en forma de grupos o individualmente. La interfaz Login permite el acceso mediante autenticación de usuario y contraseña mientras que LogConsole hace la función de Bitácora mostrando todos los eventos ocurridos en el sistema. Mediante el formulario ReportManagerForm el usuario podrá editar y componer todos los datos necesarios para la generación de reportes de los sucesos en el sistema. Mediante el uso de interfaces visuales como FAdminSeguridad, AddRoleForm, UpdateRoleForm, DeleteRoleForm, AddUserForm, UpdateUserForm y DeleteUserForm se podrá adicionar, modificar y eliminar tanto roles como usuarios. Dentro de las clases controladoras como las representadas en el paquete Controlador, se encuentran implementadas todas las funcionalidades que garantizarán el cumplimiento de todos los eventos generados desde las interfaces en el paquete Vista logrando así el correcto funcionamiento del sistema. Por su parte el paquete Modelo contiene las clases de acceso al Orquestador del sistema, utilizándose la clase SecurityManager para obtener y modificar datos de la seguridad en el sistema y la clase CamerasManager para datos relacionados a las cámaras y grupos.

3.4 Conclusiones.

El desarrollo de este capítulo facilitó una mejor comprensión de todo el proceso a automatizar mediante la descripción de la arquitectura del sistema, lográndose una propuesta certera del mismo.
Se obtuvo una visión más clara en términos de desarrollo del sistema a desarrollar que servirá como base o plano para el modelo de implementación, garantizando de esta manera una arquitectura sólida y estable gracias a los diagramas de clases del análisis y el modelo de diseño.

Capítulo 4: Implementación y Pruebas del Sistema.

4.1 Introducción.

En la implementación, se parte de los resultados obtenidos en el diseño y se implementa el sistema en términos de componentes, como son los ficheros de código fuente, ficheros de código binario, ejecutables, entre otros. Primeramente, se detalla el modelo de datos del sistema, que es el modelo donde se ve la estructura en la cual se almacenan toda la información requerida en el sistema. Luego se muestra el modelo de implementación que está compuesto por el diagrama de despliegue y el diagrama de componentes. Estos diagramas, describen los componentes a construir, su organización y dependencias entre los nodos físicos en la que funcionará la aplicación.

4.3 Modelo de implementación.

4.3.1 Diagrama de despliegue.

ElDiagrama de Despliegue/Distribución muestra la disposición física de los distintos nodos que componen un sistema y el reparto de los componentes sobre dichos nodos. La vista de despliegue representa la disposición de las instancias de componentes de ejecución en instancias de nodos conectados por enlaces de comunicación. (10)
Nota: Un nodo es un recurso de ejecución tal como un computador, un dispositivo o memoria.

El diagrama de despliegue que se muestra se utiliza para capturar los elementos de configuración del procesamiento y las conexiones entre esos elementos. Se utiliza además para visualizar la distribución de los componentes de software en los nodos físicos.

La aplicación desarrollada tiene tres elementos fundamentales: Estación de Monitorización, el Orquestador y las Cámaras IP, además son imprescindibles en su despliegue el Servidor de Base de Datos.

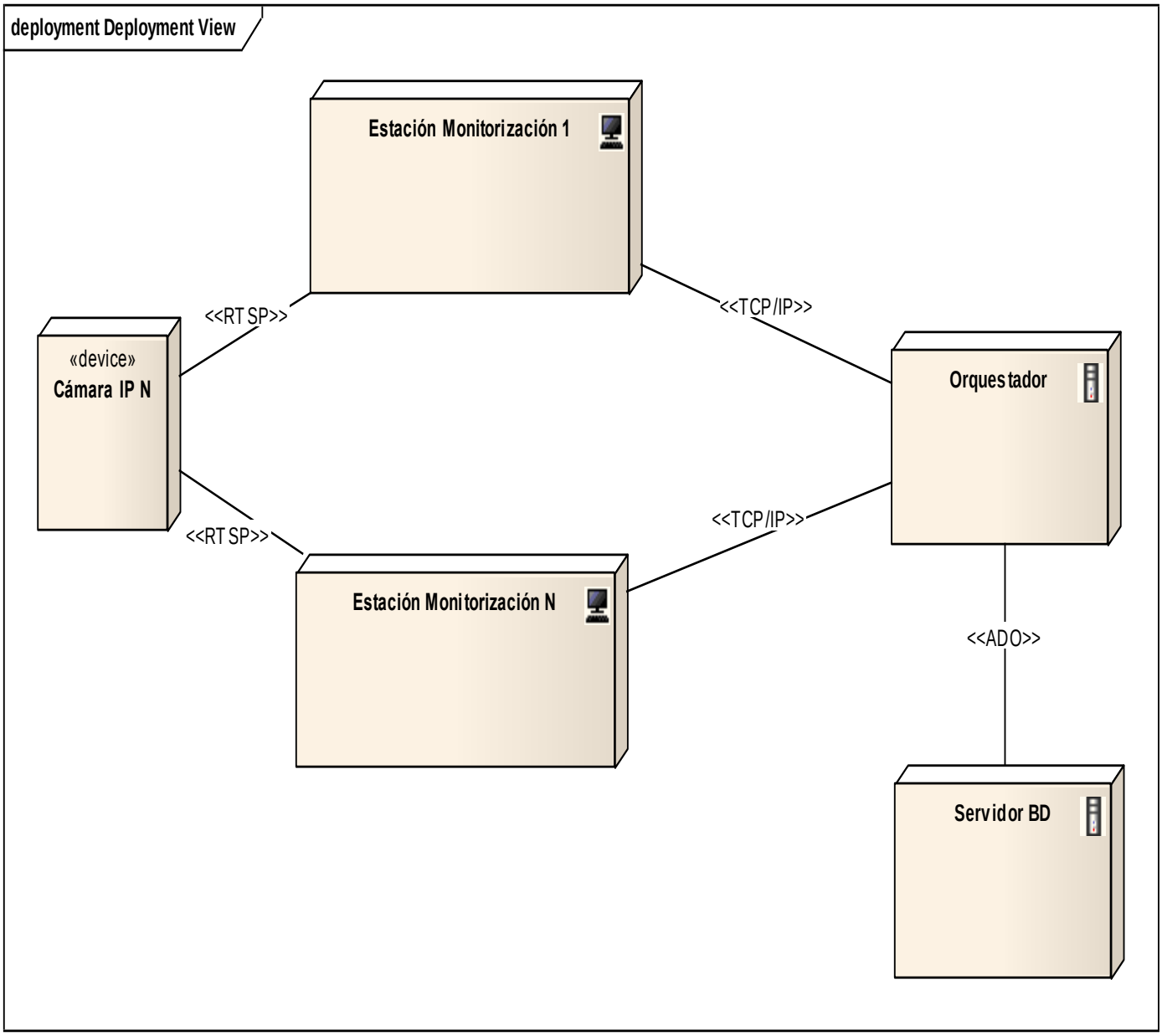


Figura 17. Diagrama de Despliegue del Sistema.

4.3.2 Diagrama de Componentes.

Un diagrama de componentes representa cómo un sistema de software es dividido en componentes y muestra las dependencias entre estos componentes. Los componentes físicos incluyen archivos, cabeceras, bibliotecas compartidas, módulos, ejecutables, o paquetes. Desde el punto de vista del diagrama de componentes se tienen en consideración los requisitos relacionados con la facilidad de desarrollo, la gestión de software, la reutilización, y las restricciones impuestas por los lenguajes de programación.

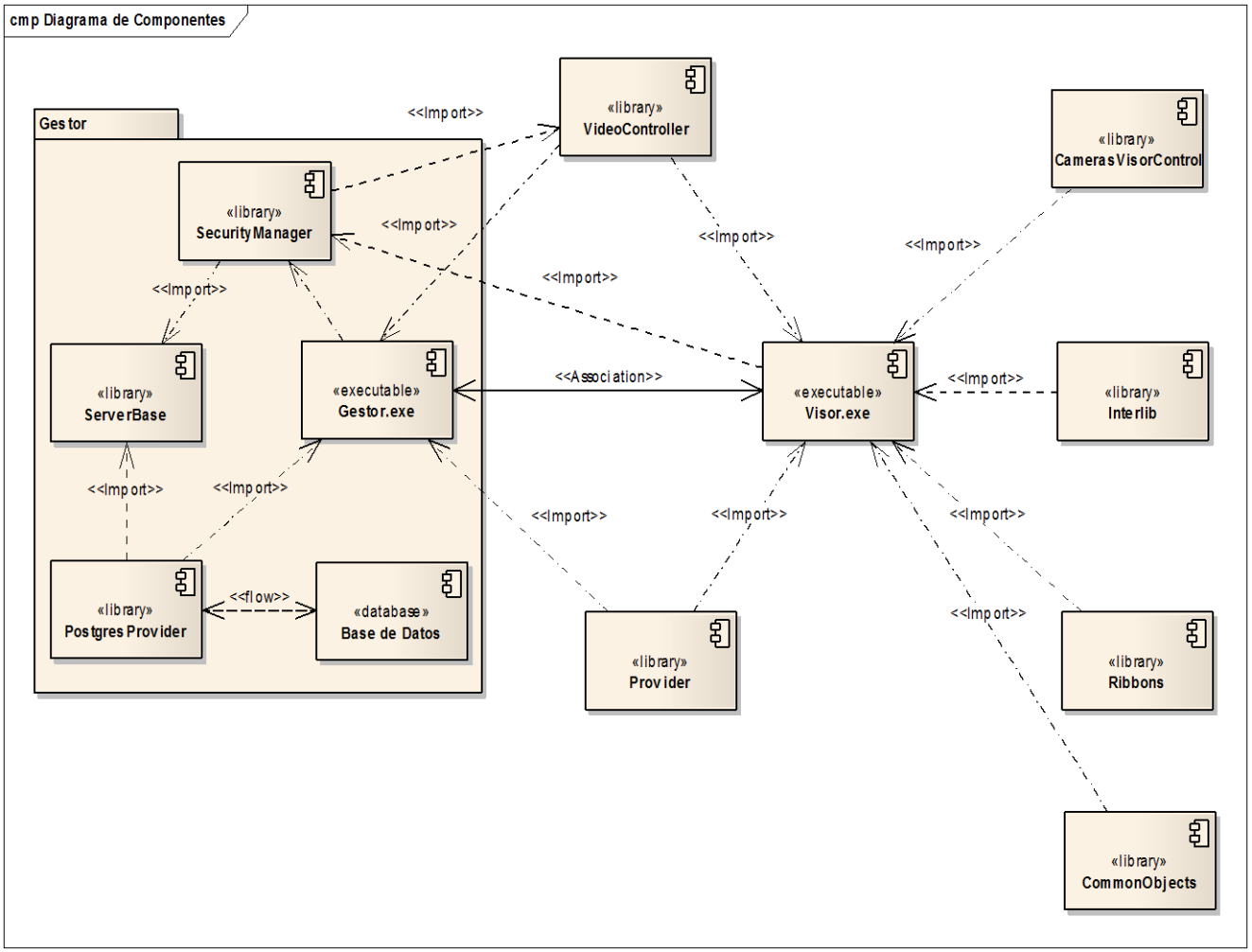


Figura 18. Diagrama de Componentes del Sistema.

4.4 Pruebas al Sistema.

Desde la creación de los primeros sistemas informáticos, aparecieron los procesos de pruebas de los sistemas. Las pruebas se le realizan a un software con la finalidad de descubrir errores, tanto en la lógica interna como en funciones externas del mismo. Las pruebas son un elemento crítico para garantizar la calidad del software, estas no mejoran ni aseguran la calidad del software, pero sí lo hace indirectamente previendo un grupo de debilidades asociadas a la organización y sus riesgos.

Existen varios tipos de prueba, los dos métodos más utilizados son las Pruebas de Caja Blanca (CB), y las Pruebas de Caja Negra (CN).

Técnicas de caja blanca o estructural, se basan en un minucioso examen de los detalles procedimentales del código a evaluar, por lo que es necesario conocer la lógica del programa.(11)

Técnicas de caja negra o funcionales, realizan pruebas sobre la interfaz del programa aprobar, entendiendo por interfaz las entradas y salidas de dicho programa. No es necesario conocer la lógica del programa, únicamente la funcionalidad que debe realizar. (11)

Luego de implementada las nuevas funcionalidades a la aplicación se realizaron las pruebas de caja negra pues estas se centran en los requisitos funcionales del software. O sea, permiten al ingeniero del software obtener conjuntos de condiciones de entrada que ejerciten completamente todos los requisitos funcionales de un programa. Estas no son una alternativa a las técnicas de prueba de caja blanca; más bien se trata de un enfoque complementario que intenta descubrir diferentes tipos de errores que los métodos de caja blanca.

Al realizar una primera iteración de las pruebas de caja negra al módulo estación de monitorización se arrojó como resultado un total de 25 no conformidades. Para dar respuesta a las no conformidades identificadas se dio un plazo de 10 días en los cuales se resolvieron estas no conformidades identificadas y se procedió a una segunda iteración identificando un total de 5 no conformidades. Para darle solución a las mismas se dio un término de 7 días en los cuales se resolvieron estas no conformidades identificadas.

Fueron probados 11 requisitos funcionales, los que representan el cien por ciento del total de requisitos. Para cada requisito se tuvo en cuenta varios escenarios que implican cada una de las posibles interacciones del usuario o combinaciones de situaciones posibles con el fin de evaluar el comportamiento del sistema ante cada funcionalidad.
El resultado de cada prueba coincide con la especificación de cada requisito funcional lo que demuestra la correcta implementación de los mismos.

NOTA: Ver el anexo IV para obtener mayor información sobre como quedaron confeccionados los casos de prueba (CP).

4.5 Conclusiones.

Se obtuvo como resultado que todos los componentes se implementaron cumpliendo con esta etapa de desarrollo. Se estableció una visión general de cómo quedó finalmente implementada la aplicación.

Se mostró la aplicación en términos de componentes, su ubicación y utilización a la hora de la implementación final.

Al realizar las pruebas de software al sistema, los resultados obtenidos validaron que el sistema cumplía con las funcionalidades esperadas.

Conclusiones Generales.

Con el desarrollo del presente trabajo de diploma, se cumplió con las tareas y objetivos trazados. Lo que permitió llegar a las siguientes conclusiones:

- ✓ Se realizó un análisis sobre los principales sistemas de video vigilancia existente en la actualidad. Las principales limitaciones estuvieron en que estos software tienen en su funcionamiento gran dependencia del fabricante.
- ✓ Se valoraron las principales tecnologías y herramientas actuales lo que permitió seleccionar las adecuadas para el desarrollo del sistema permitiendo que el producto final tenga la calidad requerida.
- ✓ Se agregaron nuevas funcionalidades al módulo estación de monitorización las cuales permitieron convertir la estación de monitorización de SURIA en una herramienta de mayor potencia para tareas de video vigilancia, estas nuevas funcionalidades fueron probadasobteniéndose resultados satisfactorios.
- ✓ Se logró que la estación de monitorización esté preparada para evolucionar hacia nuevas funcionalidades y actualizar las ya existentes.

Es importante destacar la capacidad de la estación de monitorización de soportar hardware de diversos fabricantes, que es una de las delimitaciones actuales de la mayoría de los sistemas en el mercado.

Recomendaciones.

Sobre el presente trabajo los autores recomiendan:

- ✓ Implementar nuevas herramientas y funcionalidades que al agregarlas a la estación de monitorización, amplíe las prestaciones que brinda esta y viabilice el proceso de video vigilancia en las instituciones donde fueran requeridos estos servicios.
- ✓ Integración con los videos sensores pertenecientes al módulo SURIA Analytic.

Referencia Bibliográfica

1. All-Seeing Eye La Historia de Video Vigilancia.htm. [Online] 2010. [Cited: 10 20, 2010.] htto://www.All-Seeing Eye La Historia de Video Vigilancia.htm.
2. **Edmis Deivis Semanat Aldana, Leonor Verdecia Four.***Sistema de Video Vigilancia.* La Habana : s.n., 2009.
3. **DATYS.** Sistemas, D. T. (s.f.). [Online] [Cited: 10 17, 2010.] http://www.datys.cu/.
4. **(s.f.). Scati Labs,.** S.A. Sistemas de Videovigilancia Inteligente CCTV. [Online] http://www.scati.com/.
5. **Axis Communications.** Axis Communications. *Axis Communications.* [Online] 11 21, 2008. [Cited: 11 21, 2008.] http://www.axis.com.
6. **VIVOTEK .***Inc, V. (s.f.).VIVOTEK build with reliability.* [Online] [Cited: 10 17, 2010.] http://www.vivotek.com.
7. Enterprise Architect - Herramienta de diseño UML. *Enterprise Architect - Herramienta de diseño UML.* [Online] [Cited: 12 2, 2010.] http://www.sparxsystems.com.ar/products/ea.html.
8. *Introducción a la Ingeniería de Software.*
9. **Wikipedia.** Proceso Unificado de Rational. *Wikipedia.* [Online] Noviembre 19, 2008. [Cited: Noviembre 29, 2008.] http://es.wikipedia.org/wiki/RUP.
10. **Marca Huallpara, Hugo Michael.***ANALISIS Y DISEÑO DE SISTEMAS II.*
11. **Natalia Juristo, Ana M. Moreno, Sira Vegas.***TÉCNICAS DE EVALUACIÓN DE SOFTWARE.* 2006.

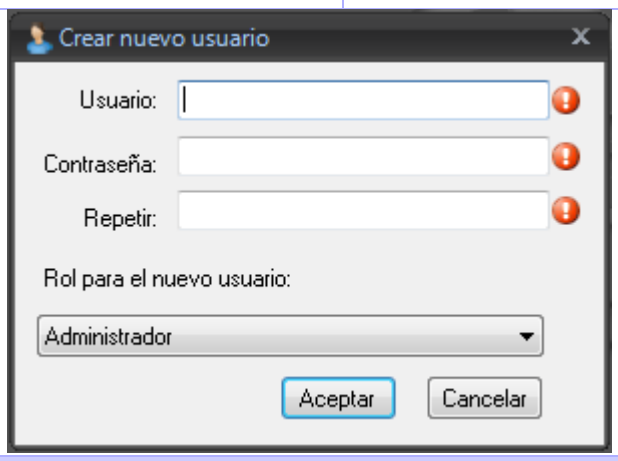
Bibliografía

1. All-Seeing Eye La Historia de Video Vigilancia.htm. [Online] 2010. [Cited: 10 20, 2010.] htto://www.All-Seeing Eye La Historia de Video Vigilancia.htm.
2. **Edmis Deivis Semanat Aldana, Leonor Verdecia Four.***Sistema de Video Vigilancia.* La Habana : s.n., 2009.
3. **DATYS.** Sistemas, D. T. (s.f.). [Online] [Cited: 10 17, 2010.] http://www.datys.cu/.
4. **(s.f.). Scati Labs,.** S.A. Sistemas de Videovigilancia Inteligente CCTV. [Online] http://www.scati.com/.
5. **Axis Communications.** Axis Communications. *Axis Communications.* [Online] 11 21, 2008. [Cited: 11 21, 2008.] http://www.axis.com.
6. **VIVOTEK .***Inc, V. (s.f.).VIVOTEK build with reliability.* [Online] [Cited: 10 17, 2010.] http://www.vivotek.com.
7. Enterprise Architect - Herramienta de diseño UML. *Enterprise Architect - Herramienta de diseño UML.* [Online] [Cited: 12 2, 2010.] http://www.sparxsystems.com.ar/products/ea.html.
8. *Introducción a la Ingeniería de Software.*
9. **Wikipedia.** Proceso Unificado de Rational. *Wikipedia.* [Online] Noviembre 19, 2008. [Cited: Noviembre 29, 2008.] http://es.wikipedia.org/wiki/RUP.
10. **Marca Huallpara, Hugo Michael.***ANALISIS Y DISEÑO DE SISTEMAS II.*
11. **Natalia Juristo, Ana M. Moreno, Sira Vegas.***TÉCNICAS DE EVALUACIÓN DE SOFTWARE.* 2006.
12. **Rivero, Magdiel Gonzalez y Rivas, Juan Carlos Ferrer.***Suria Recorder: Grabador de flujos de video.* Ciudad de la Habana : s.n., 2010.
13. **Datys.***Datys. [Online] DATYS le brinda un Sistema de Video Vigilancia profesional.* 2010.
14. Communications, A. (s.f.). Obtenido de Axis Communications: . [Online] http://www.axis.com/es/.
15. **Microsoft Corp.** MSDN. MSDN. [Online] Microsoft Corp. . [Online] [Cited: 10 20, 2010.] http://www.msdn.com..
16. XYMA SAVE VISION SISTEMA DE VIDEO VIGILANCIA IP. [Online] [Cited: 11 8, 2010.] http://www.datys.cu/docs/Documentación%20Productos/Xyma.
17. D_ Link Software de gestión de Cámaras IP. [Online] [Cited: 11 8, 2010.] http://www.dlink.es/.
18. Microsoft Visual Studio. [Online] [Cited: 11 8, 2010.] http://en.wikipedia.org/wiki/Microsoft_Visual_Studio.
19. **Jiménez, Javier Alonso Albusac.***Vigilancia Inteligente: Modelado de Entornos Reales e.* l 2008.
20. Rational Rose Enterprise Edition Suite 2003. [Online] Marzo 20, 2010. [Cited: 11 12, 2010.] http://www.intercambiosvirtuales.org/software/rational-rose-enterprise-edition-suite-2003.
21. Sitio de descargas de software. [Online] [Cited: 11 12, 2010.] http://www.freedownloadmanager.org/es/downloads/Paradigma_Visual_para_UML_(M%C3%8D)_14720_p/.
22. Rational Software Rational Software IBM online. *Rational Software Rational Software IBM online.* [Online] [Cited: 11 24, 2010.] http://www-01.ibm.com/software/awdtools/rup/..
23. VIVOTEK - Cámaras de red. *VIVOTEK - Cámaras de red.* [Online] [Cited: 12 2, 2010.] http://www.vivotek.com/.../network_cameras.php?newlang.
24. **Herranz, Arantxa.** Video Vigilancia IP. *PCWORLD PROFESIONAL.* [Online] July 24, 2008. [Cited: November 23, 2008.]

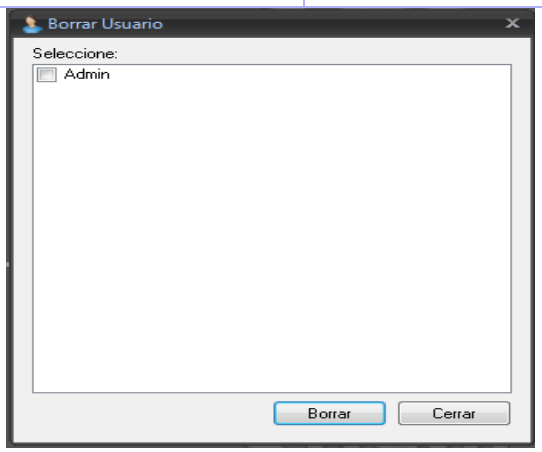
http://www.idg.es/pcworldtech/Video_vigilancia_IP:_un_Gran_Hermano_en_nuestra_re/art191729-comunicaciones.htm.
25. **Panasonic.** Construnario.com - Notiweb: Sistemas de Seguridad Panasonic: 50 años haciendo la vida más fácil. *Construnario >> Notiweb.* [Online] April 25, 2007. [Cited: November 25, 2008.] http://www.construnario.es/notiweb/titulares_resultado.asp?regi=15902.
26. Scati Labs - Wikipedia, la enciclopedia libre. *Wikipedia, la enciclopedia libre.* [Online] [Cited: November 25, 2008.] http://es.wikipedia.org/wiki/Scati_Labs.
27. Sony: Vigilancia inteligente en Verbania: España. *Sony: Soluciones profesionales, corporativas y de broadcast: España.* [Online] [Cited: November 25, 2008.] http://www.sony.es/biz/view/ShowContent.action?site=biz_es_ES&contentId=1189437949251&sectiontype=NVM+CaseStudies.
28. Las 10 ventajas principales de Microsoft Office Visio 2007. *Microsoft Office Online.* [Online] [Cited: November 25, 2008.] http://office.microsoft.com/es-es/visio/HA101650313082.aspx.
29. Microsoft Visual Studio - Wikipedia, la enciclopedia libre. *Wikipedia, la enciclopedia libre.* [Online] [Cited: November 25, 2008.] http://es.wikipedia.org/wiki/Microsoft_Visual_Studio#Visual_Studio_2008.
30. Información general de .NET Framework Remoting. *Visual Studio.* [Online] [Cited: November 25, 2008.] http://msdn.microsoft.com/es-es/library/kwdt6w2k(VS.80).aspx .
31. Visual SourceSafe 2005. *Visual Studio.* [Online] [Cited: November 25, 2008.] http://msdn.microsoft.com/es-es/vcsharp/aa718670.aspx.
32. PostgreSQL8.3 ya disponible. *Portal de Astra NTi.* [Online] [Cited: November 25, 2008.] http://www.astra.es/noticias/postgresql-8-3-ya-disponible.
33. **MPEG LA®.** MPEG-4 Visual. *MPEG LA.* [Online] MPEG LA, 2004. [Cited: Noviembre 20, 2008.] http://www.mpegla.com/m4v/m4v-licensees.cfm.
34. **Wikipedia.** Programación Extrema. *Wikipedia La Enciclopedia Libre.* [Online] Noviembre 22, 2008. [Cited: Noviembre 29, 2008.] http://es.wikipedia.org/wiki/Programaci%C3%B3n_Extrema.
35. **Axis Communications.***Coste total de propiedad(TCO) Comparativa entre los sistemas de vigilancia con cámaras IP y cámaras analógicas.* s.l. : Axis Communications, 2008.
36. Videovigilancia. *TELENORMA Solucines en comunicación.* [Online] [Cited: November 30, 2008.] http://www.telenorma.com.co/index.php?option=com_content&view=section&layout=blog&id=3&Itemid=7.

Anexos
Anexo I. Casos de Uso Expandidos.

Caso de Uso:	Gestionar Usuarios
Actores:	Administrador
Propósito:	Garantizar la seguridad en el Sistema mediante el uso de usuarios con distintos roles, que están protegidos por contraseña.
Resumen:	El caso de uso se inicia cuando el Administrador selecciona la opción de adicionar, eliminar o editar un usuario determinado en el Administrador de Seguridad previamente abierto.
Referencias	RF2.1, RF2.2, RF2.3

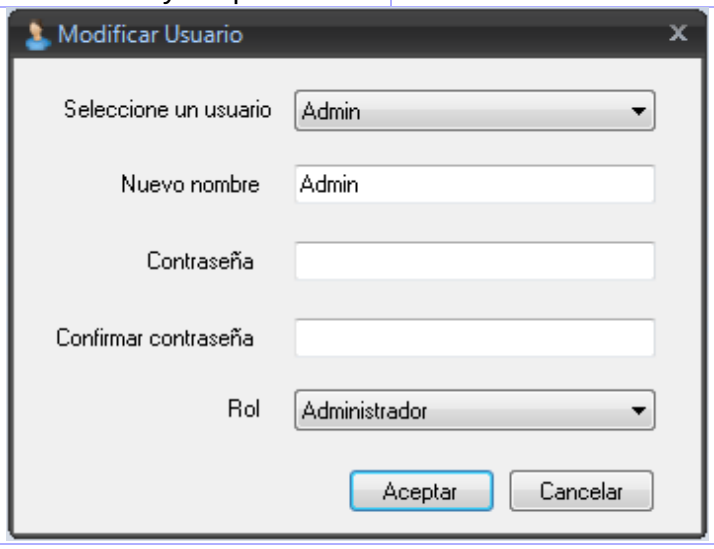
Flujo Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
Escenario Adicionar	
1.- El Administrador abre el Administrador de Seguridad.	2.- El Sistema le muestra la forma del Administrador de Seguridad.
3.- El Administrador selecciona la opción de adicionar un usuario.	4.- El Sistema le muestra una forma para introducir los datos necesarios.
5.- El Administrador entra los datos necesarios y acepta la entrada.	6.- El Sistema almacena los nuevos datos.
	
Escenario Eliminar	
1.- El Administrador abre el Administrador de Seguridad.	2.- El Sistema le muestra la forma del Administrador de Seguridad.
3.- El Administrador selecciona la opción de eliminar un usuario.	4.- El Sistema muestra los usuarios que existen.

5.-El Administrador selecciona un usuario y acepta.	6.- El Sistema muestra una advertencia.
7.-El Administrador elige continuar con la operación.	8.- El Sistema elimina el usuario.



Escenario Actualizar

1.- El Administrador abre el Administrador de Seguridad.	2.- El Sistema le muestra la forma del Administrador de Seguridad.
3.- El Administrador selecciona la opción de editar un usuario.	4.- El Sistema muestra los usuarios que existen.
5.-El Administrador selecciona un usuario.	6.- El Sistema muestra los datos del usuario.
7. El Administrador modifica los datos y acepta.	8.-El Sistema almacena los datos modificados.



Caso de Uso:	Generar Alarma Visual
Actores:	Orquestador
Propósito:	Mostrar una alarma visual para alertar al Usuario conectado al Sistema.
Resumen:	El caso de uso se inicia cuando elOrquestador recibe una notificación sobre algún evento a alertar.
Referencias	RF6

Flujo Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
Escenario Generar Alarma Visual	
1.- El Orquestador recibe una notificación sobre algún evento a alertar.	2.- El Sistema muestra una alarma visual sobre la cámara que se generó el evento.

Caso de Uso:	Chequeo de Cámaras offline
Actores:	Estación de Monitorización
Propósito:	Chequear el estado de las cámaras visualizadas que se encuentren sin brindar flujo de video.
Resumen:	El caso de uso se inicia cuando la Estación de Monitorización lanza cada cierto tiempo predefinido el evento de Chequear cámaras offline.
Referencias	RF12

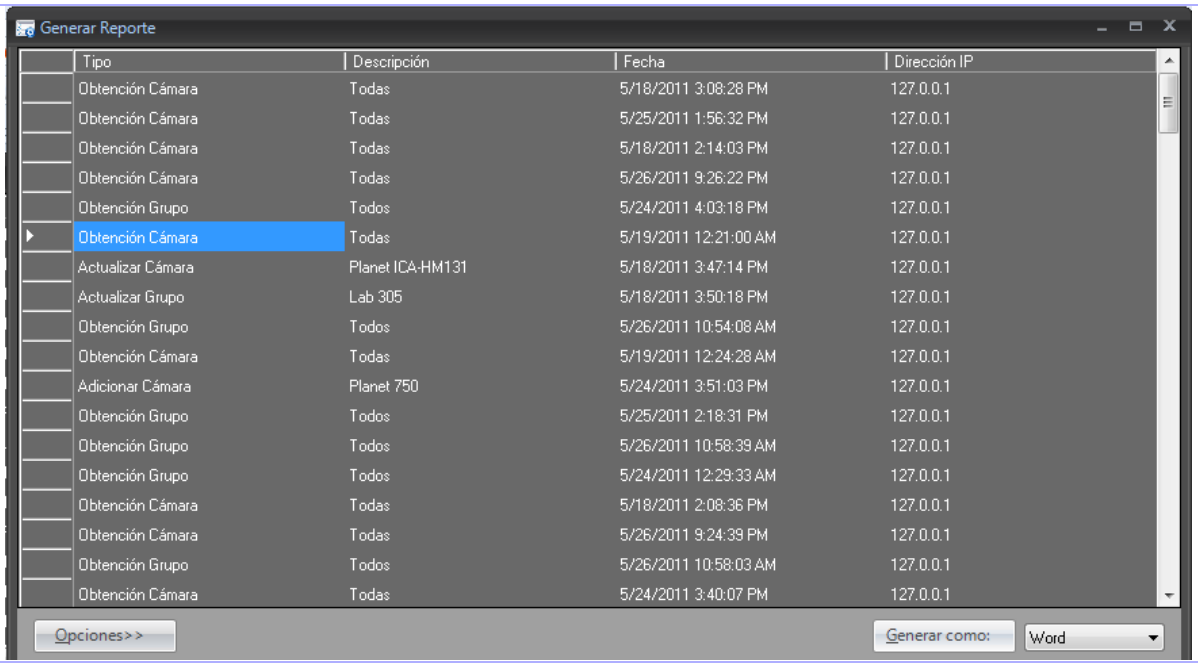
Flujo Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
Escenario Chequeo de Cámaras offline	
1.- La Estación de Monitorización lanza el evento de Chequear cámaras offline.	2.- El Sistema ejecuta la función de Chequear el estado de las cámaras conectadas a la Estación de Monitorización.

Caso de Uso:	Realizar Detección de Rostro.
Actores:	Operador
Propósito:	Habilitar un formulario con opciones especializadas para detección de rostro.
Resumen:	El caso de uso se inicia cuando el Operadorselecciona la opción de abrir Visor Especializado.
Referencias	RF9

Flujo Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
Escenario Realizar Detección de Rostro	
1.- El Operador selecciona la opción de abrir Visor Especializado.	2.- El Sistema muestra un formulario con las opciones especializadas para la detección de rostro.

Caso de Uso:	Generar Reporte
Actores:	Operador
Propósito:	Generar un informe detallado de los sucesos y eventos en el Sistema.
Resumen:	El caso de uso se inicia cuando el Operador selecciona la opción de Generar Reporte.
Referencias	RF4

Flujo Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
Escenario Generar Reporte	
1.- El Operador selecciona la opción de Generar Reporte.	2.- El Sistema muestra un formulario con los campos a seleccionar que formarán en el reporte.
3.- El Usuario selecciona los datos y campos que serán generados en el reporte.	4.- El Sistema genera un reporte a partir de los datos seleccionados por el Usuario.



Caso de Uso:	Hacer Zoom sobre flujo de Video
Actores:	Operador
Propósito:	Habilitar un control que permita hacer Zoom sobre el flujo de video de una cámara en visualización seleccionada.
Resumen:	El caso de uso se inicia cuando el Operadorhabilita el control para hacer Zoom sobre el flujode video de una cámara en visualización seleccionada.
Referencias	RF5

Flujo Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
Escenario Hacer Zoom sobre flujo de Video	
1.- El Operadorselecciona una cámara en visualización.	2.- El Sistema muestra un control para la cámara seleccionada el cual puede ser habilitado para hacer uso del Zoom.
3.- El Operador habilita el control para hacer Zoom.	4.- El Sistema habilita el control para hacer Zoom sobre el flujo de video de la cámara seleccionada.

Anexo II. Diagramas de Secuencia.

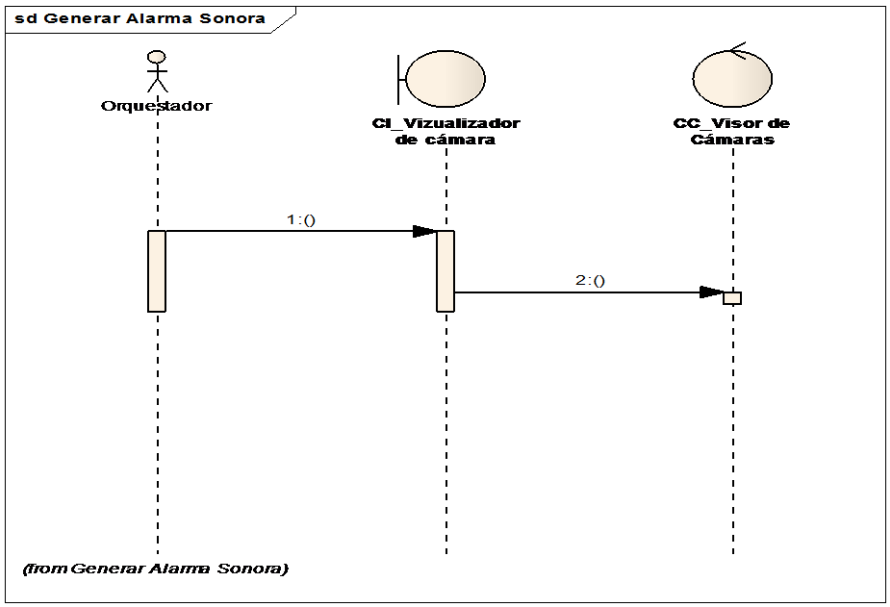


Figura 19. CU Generar Alarma Sonora.

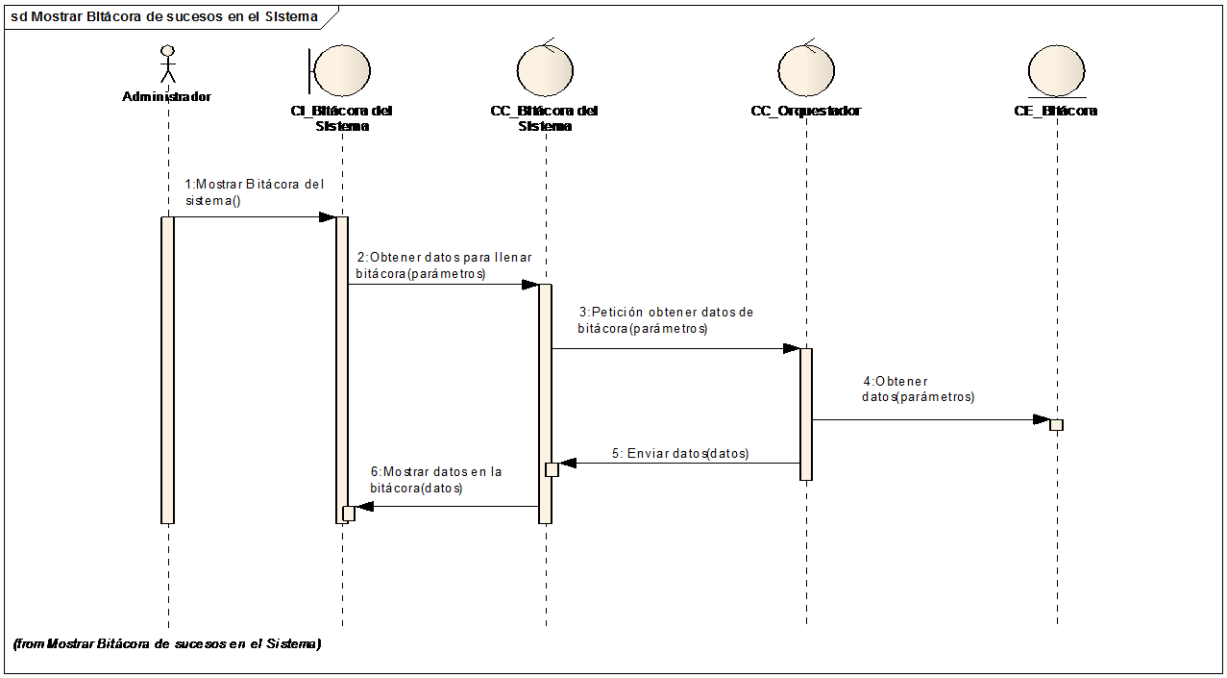


Figura 32. CU Mostrar Bitácora de sucesos del Sistema.

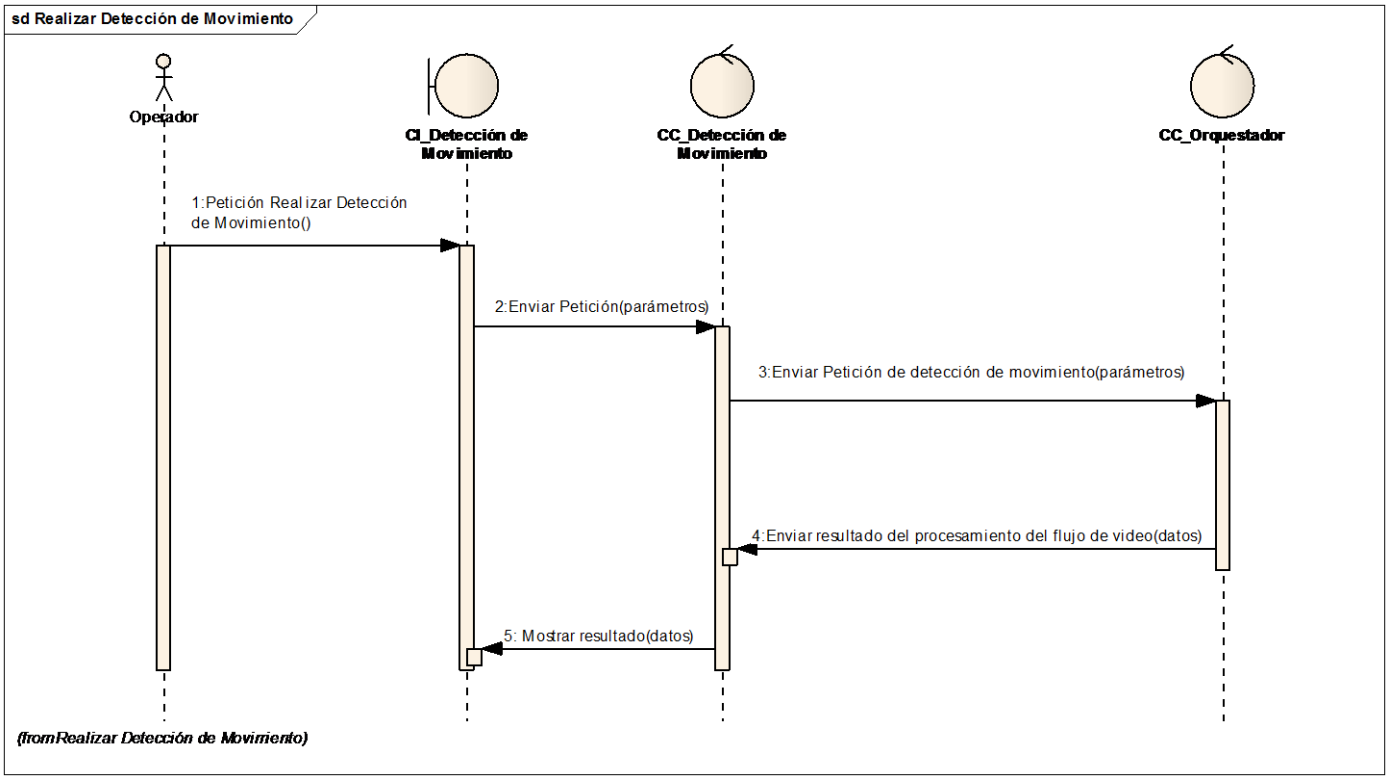


Figura 20. CU Realizar Detección de Movimiento.

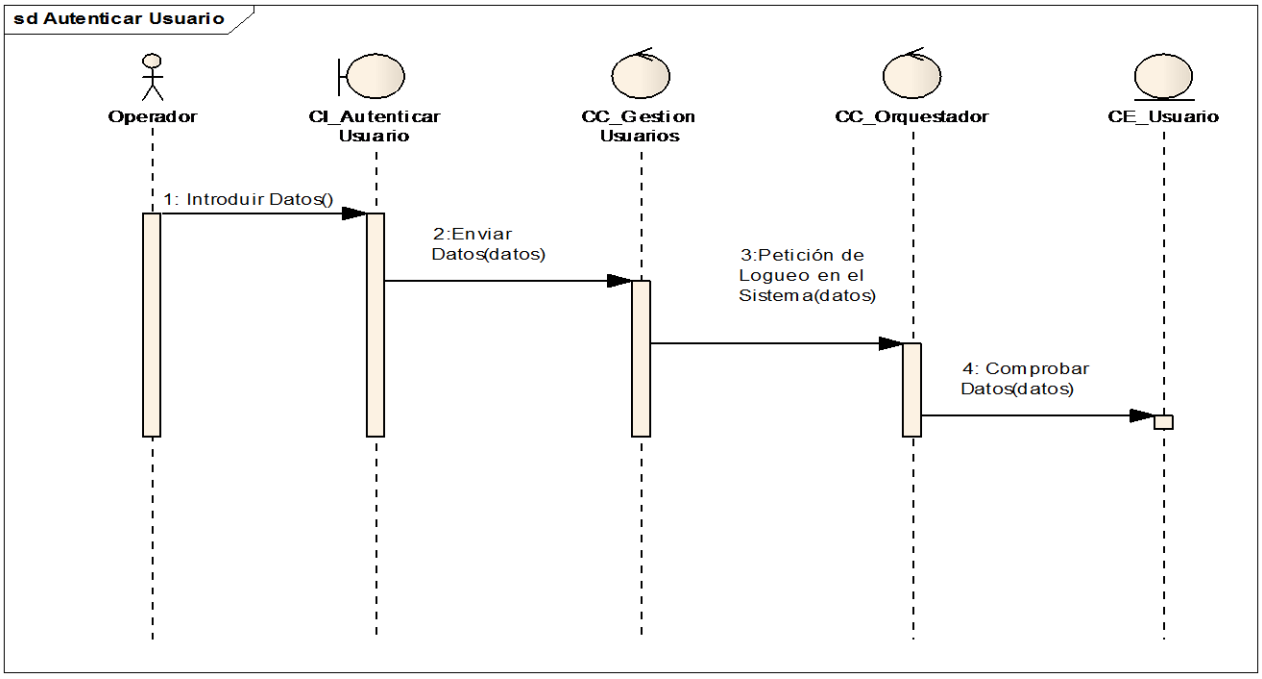


Figura 21. Diagrama de Secuencia CU Autenticar Usuario.

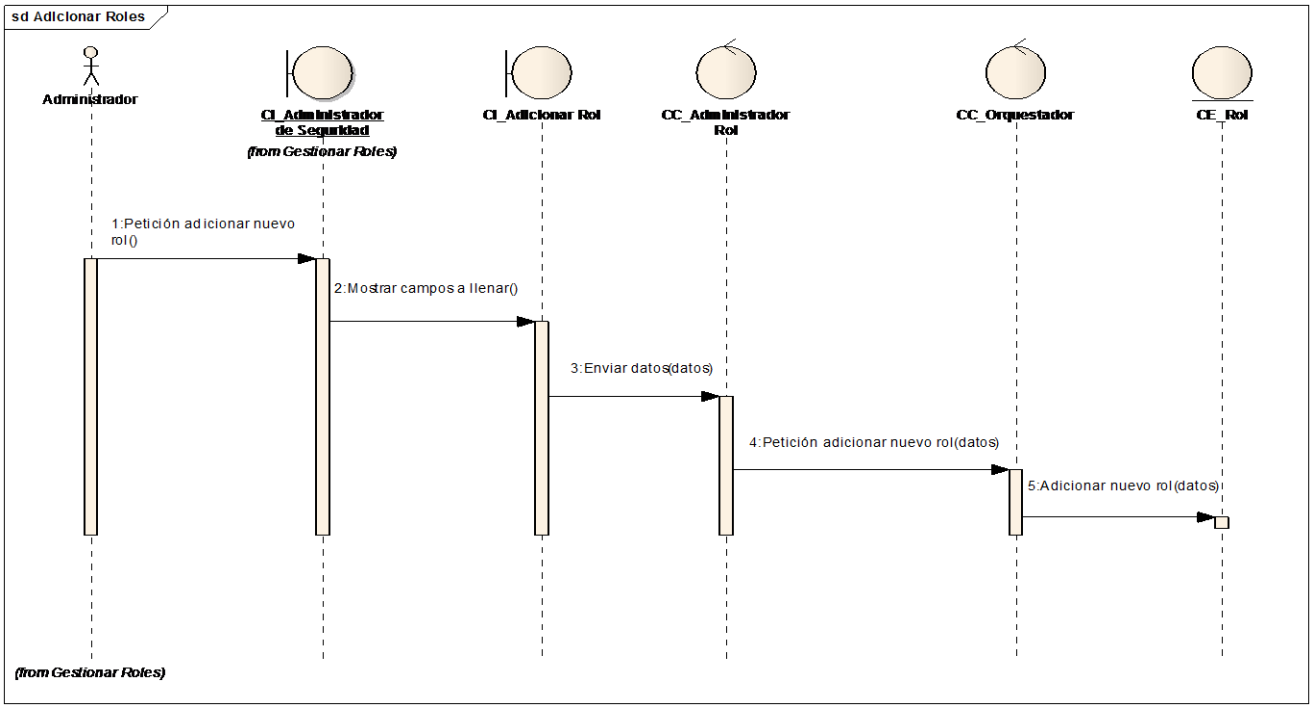


Figura 22. Diagrama de Secuencia CU Gestionar Roles, escenario Adicionar Rol.

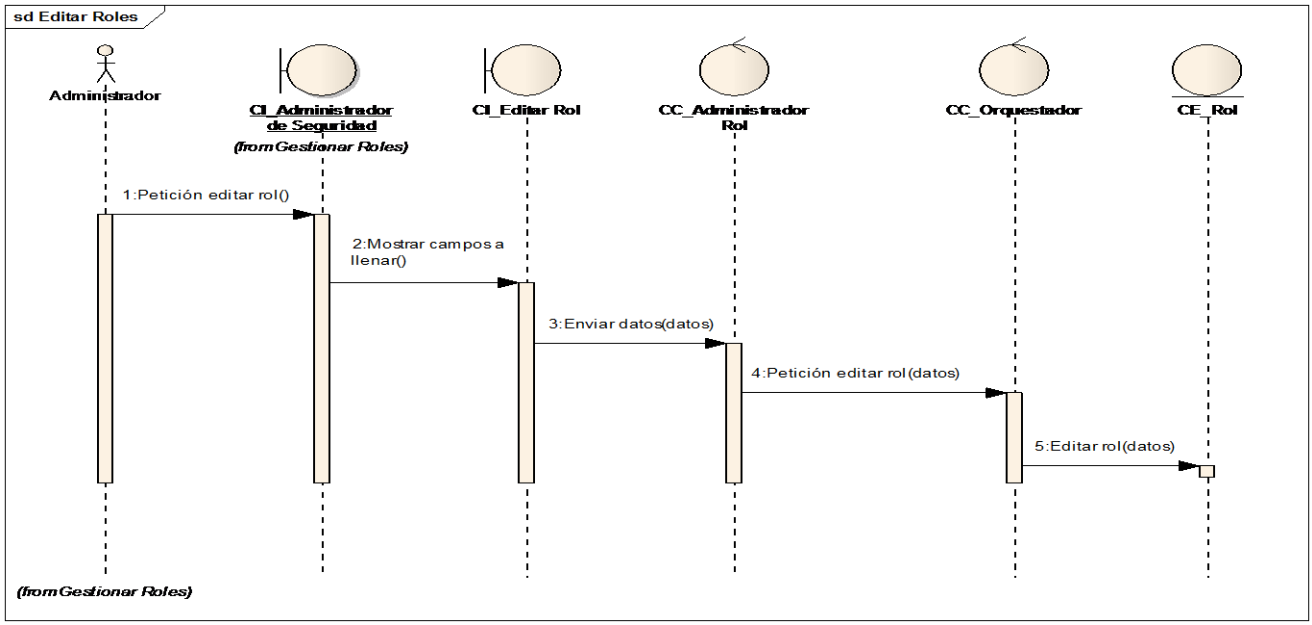


Figura 23. Diagrama de Secuencia CU Gestionar Roles, escenario Editar Rol.

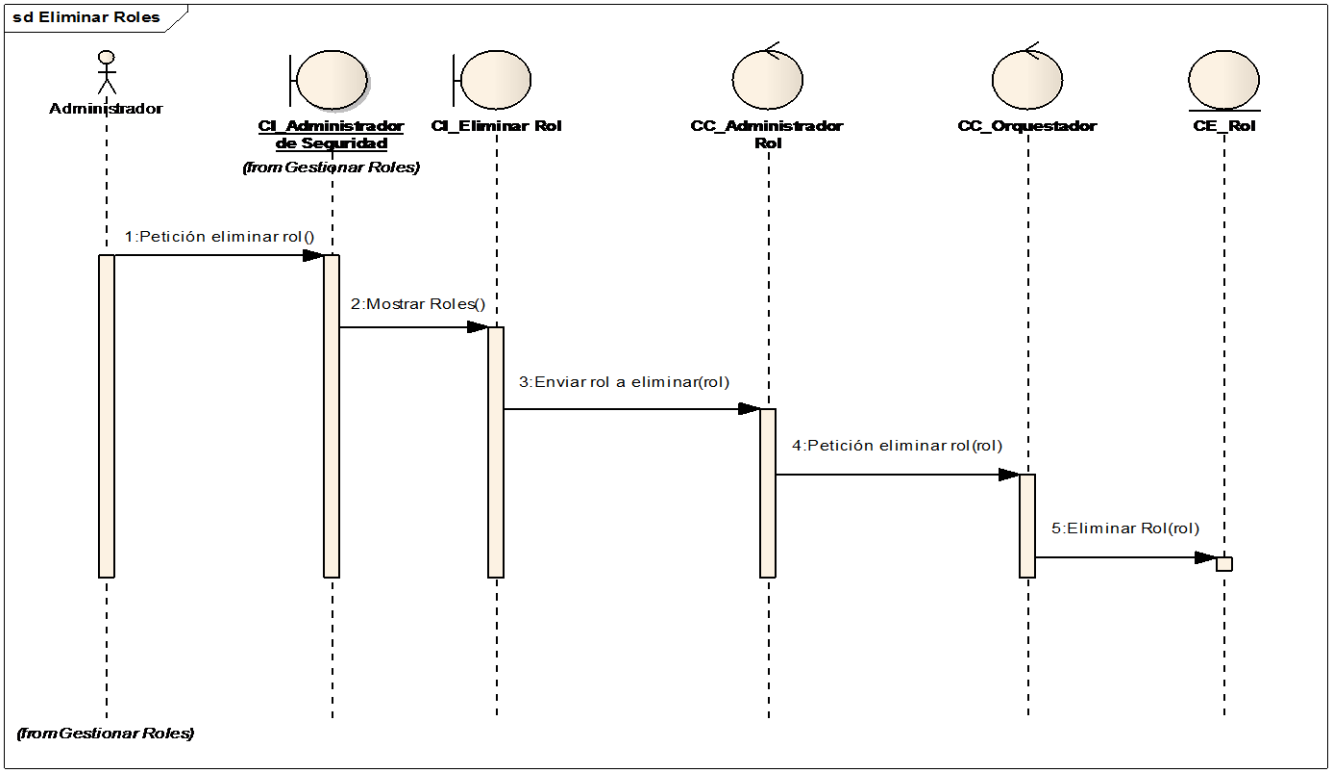


Figura 24. Diagrama de Secuencia CU Gestionar Roles, escenario Eliminar Rol.

Anexo III. Diagramas de Clases.

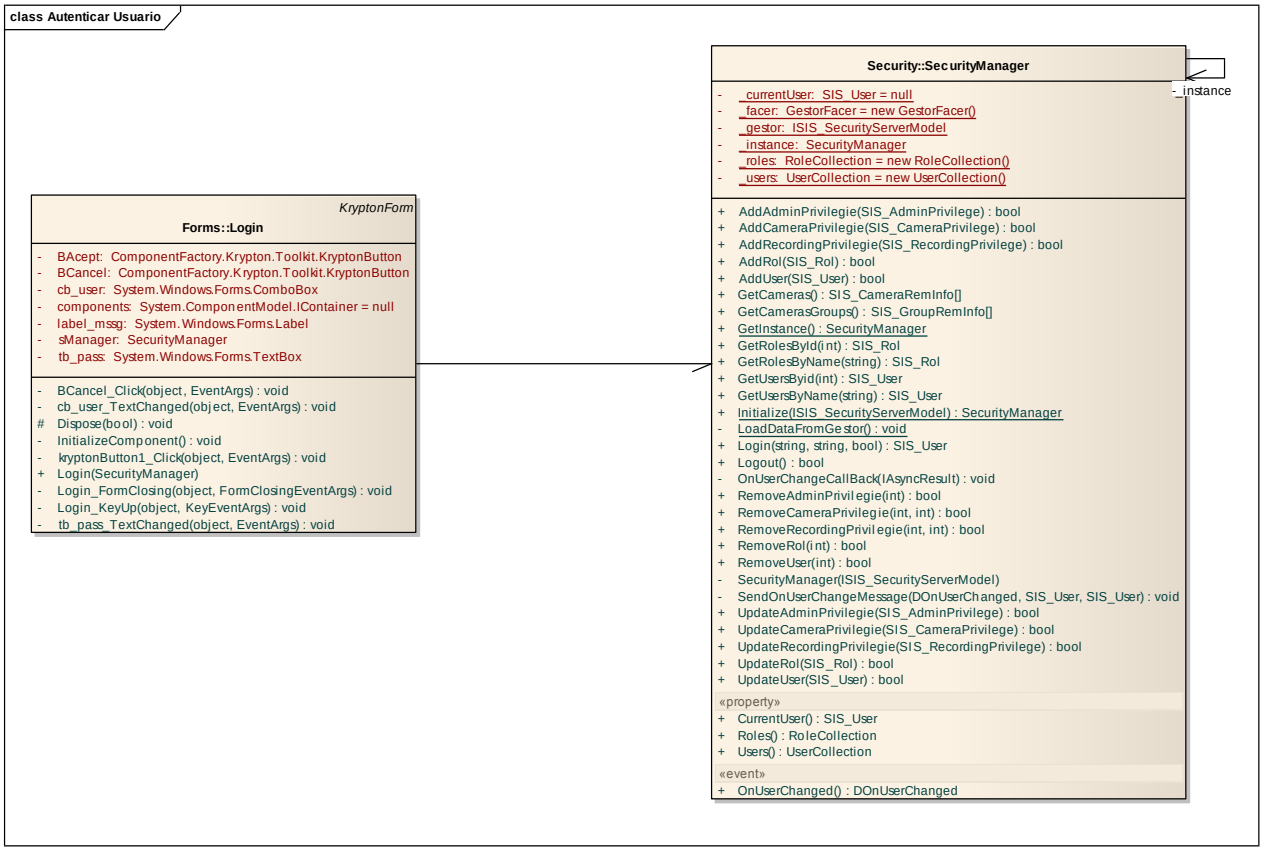


Figura 25. Diagrama de Clases CU Autenticar Usuario.

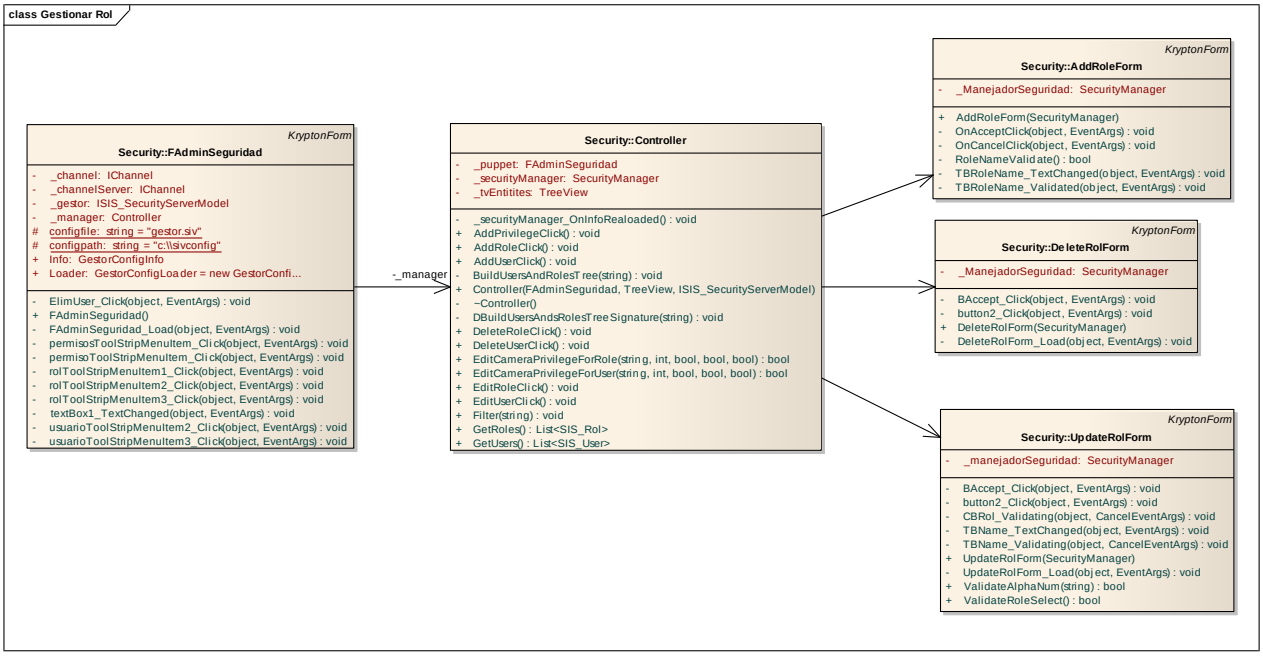


Figura 26. Diagrama de Clases CU Gestionar Roles.

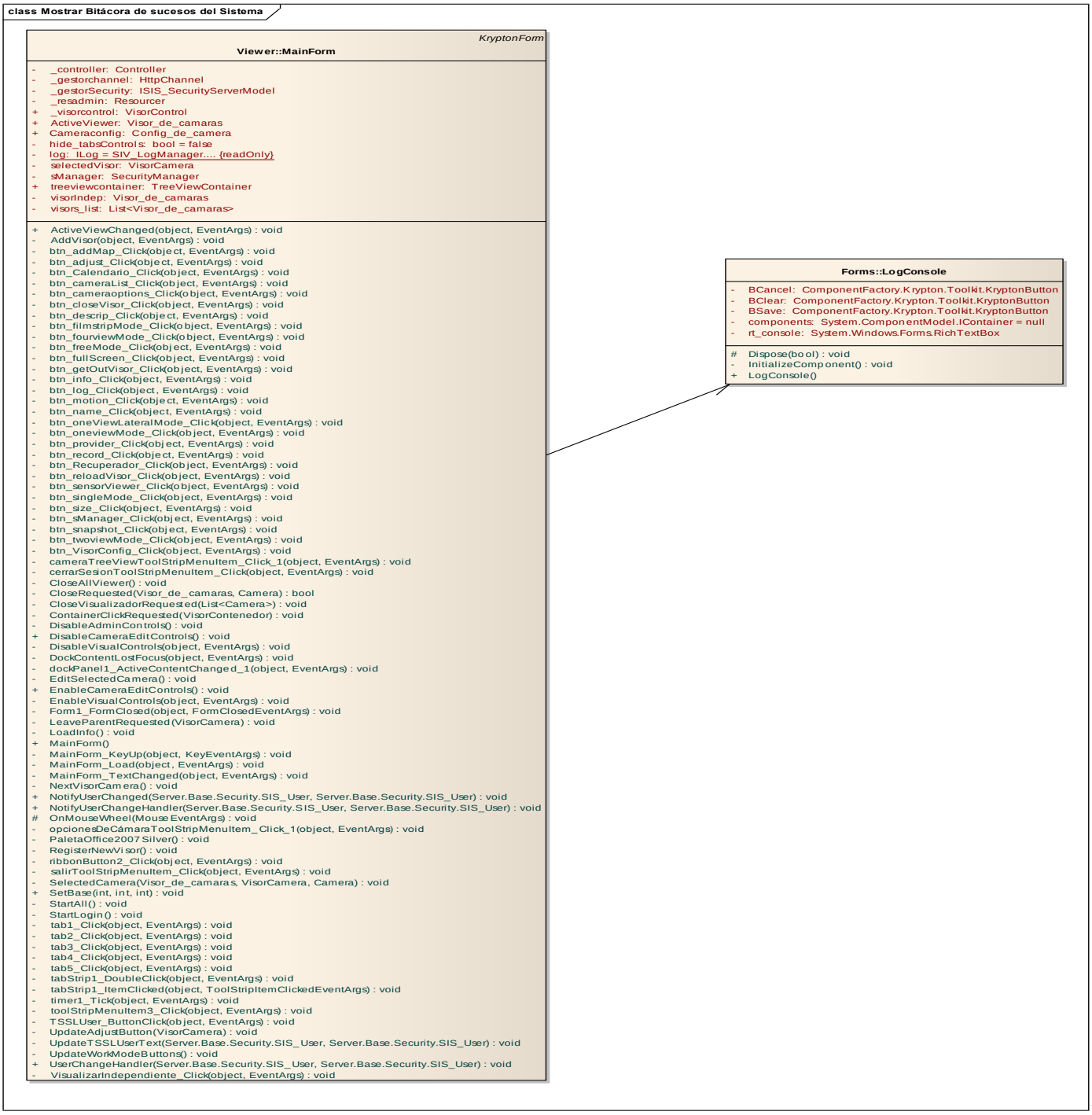


Figura27. Diagrama de Clases CU Mostrar Bitácora de Sucesos en el Sistema.

Figura 28. Diagrama de Clases CU Generar Alarma Sonora.

Anexo IV: Pruebas de Caja Negra

En la realización de los casos de prueba se utilizó la siguiente estructura para probar las funcionalidades requeridas:

Secciones a probar en el Caso de Uso.

CU Autenticar usuario.

Nombre de la sección	Escenarios de la sección	Descripción de la funcionalidad	Flujo Central
SC 1: Autenticar usuario.	EC 1.1: Autenticar usuariocorrectamente.	El usuario inserta su nombre y su contraseña en los campos correspondientes, el sistema busca el usuario en la base de datos y compara si la contraseña es la correcta, si es así se le permite el acceso al sistema con los permisos que tenga asignado según su rol.	Módulo Visor/ clic en “SuriaViewer”/ botón “Aceptar”.
	EC 1.2: Autenticar usuarioincorrectamente.	Si el nombre del usuario seleccionado no coincide con la contraseña proporcionada se muestra un mensaje de “Error, el usuario no existe o la contraseña es incorrecta”. Se ofrece la oportunidad de volver a introducir sus datos	Módulo Visor/ clic en “SuriaViewer”/ botón “Aceptar”.
	EC 1.3: Cancelar Autenticar usuario.	El usuario selecciona el botón “Cancelar”. El sistema cancela la operación y abre el Visor sin ninguna funcionalidad con la opción de volver a autenticarse.	Módulo Visor/ clic en “SuriaViewer”/ botón “Cancelar”.

Descripción de variable.

No	Nombre de campo	Clasificación	Valor Nulo	Descripción
1	Usuario	Lista desplegable.	No.	Se selecciona el rol en dependencia de los privilegios
2	Contraseña	Campo de texto.	*No.*	Se introduce la contraseña que el usuario tiene para su acceso al sistema.

Matriz de Datos

SC 1 Autenticar Usuario

ID del escenario	Escenario	Variable 1 Usuario	Variable 2 Contraseña	Respuesta del Sistema	Resultado de la Prueba
EC 1.1	Autenticar usuariocorrectamente.	V/Administrador	V/admin	El usuario accede al sistema con los permisos que le sean asignados	***Satisfactorio***
EC 1.2	Autenticar usuario incorrectamente	V/Administrador	I/administrador	El usuario no puede acceder al sistema, y se le da la opción de insertar sus datos nuevamente	***Satisfactorio***
EC 1.3	Cancelar Autenticar usuario.	V/Administrador	V/admin	Se abre el Visor sin ninguna funcionalidad con la opción de volver a autenticarse	***Satisfactorio***

AnexoV: Glosario de términos

Términos	Definiciones
IP	Protocolo de Internet (Internet Protocol),es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados no fiable de mejor entrega posible sin garantías.
PTZ	Es un acrónimo de pan-tilt-zoom y puede referirse sólo a las características de las cámaras de vigilancia específicas.
CASE	Ingeniería de Software Asistida por Ordenador (ComputerAided Software Engineering), Estas herramientas nos pueden ayudar en todos los aspectos del ciclo de vida de desarrollo del software en tareas como el proceso de realizar un diseño del proyecto, cálculo de costes, implementación de parte del código automáticamente con el diseño dado, compilación automática, documentación o detección de errores entre otras.
UML	Lenguaje Unificado de Modelado (UnifiedModelingLanguage),Es un lenguaje gráfico para visualizar, especificar, construir y documentar un sistema.
IDE	Entorno Integrado de Desarrollo (IntegratedDevelopEnvironment),es un entorno de programación que ha sido empaquetado como un programa de aplicación, es decir, consiste en un editor de código, un compilador, un depurador y un constructor de interfaz gráfica.
RUP	Proceso Unificado Racional (RationalUnifiedProcess), proceso de desarrollo de software, es la metodología estándar más utilizada para el análisis, implementación y documentación de sistemas orientados a objetos.