

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR



FACULTAD DE INGENIERÍA MAESTRÍA EN REDES DE COMUNICACIONES

**PERFIL DEL TRABAJO PREVIO LA OBTENCIÓN DEL TÍTULO DE:
MÁSTER EN REDES DE COMUNICACIONES**

TEMA:

**“ANÁLISIS TÉCNICO DE LA IMPLEMENTACIÓN DE UN SISTEMA DE
SEGURIDAD DE VIDEO VIGILANCIA, CASO DE ESTUDIO AEROPUERTO
INTERNACIONAL MARISCAL SUCRE DEL ECUADOR.”**

ING. PAVÓN ANRANGO JUAN CARLOS

DIRECTOR: DR. GUSTAVO CHAFLA

Quito – Septiembre 2016

DEDICATORIA.

La familia es una de las joyas más preciadas que uno puede tener, sin la familia uno no puede tener la fuerza necesaria para lograr las metas. Es por eso que dedico esta tesis a mis padres Magdalena Anrango, Remberto Anibal Pavón, y a todos mis hermanos que me han sabido apoyar en este camino de sacrificio y estudio.

Muchas gracias Familia Pavón.

Hijo mío Juan Francisco Pavón Martínez, posiblemente en este momento no entiendas mis palabras, pero para cuando seas capaz, quiero que te des cuenta de lo que significas para mí. Eres la razón que me levanta cada día, a esforzarme por un mejor presente y mañana, eres mi principal motivación.

Como en todos mis logros, en este has estado presente.

Muchas gracias Panchito Pavón M.

Agradezco a una persona muy especial dentro de mi vida, que confio en mí para poder dar inicio en este sueño cumplido y anhelado. Dedico de igual manera este sacrificio de estudio cumplido.

Gracias por todo.

CONTENIDO

CAPÍTULO I	11
Definición del proyecto.....	11
Introducción	11
Justificación e Importancia.	12
Antecedentes	14
Objetivos.	15
Objetivo General.....	15
Objetivos Específicos.....	15
CAPÍTULO II	16
2.1 Estudio del estado del arte de sistemas de seguridad de video vigilancia...	16
2.1.1 Sistemas de CCTV	16
2.1.2 Introducción a los sistemas de CCTV	16
2.1.3 Sistemas de CCTV sobre IP	18
2.1.4 Sistemas de vigilancia IP y su evolución	18
2.1.5 Compresión de video Digital Códec de vídeo	20
2.1.6 Compresión de imagen vs. Compresión de vídeo	21
2.1.7 Formatos de compresión	22
2.2 Características y ventajas de los sistemas de video vigilancia IP	24
2.2.1 Capacidad de escalamiento del sistema de seguridad	24
2.2.2 Manejo de servidores de video en las Redes LAN	26
2.2.3 Compatibilidad con aplicaciones y facilidad de integración	27
2.2.4 Potente herramienta de análisis de Video	27
2.2.5 Esquema redundante	27
2.2.6 Grabación usando NVR	28
2.3 Características de almacenamiento en los sistemas de video vigilancia	28

2.3.1	Seguridad y monitoreo utilizando cámaras IP.....	28
2.3.2	Sistemas de video supervisión y control a través de cámaras IP.....	29
2.3.2.1	Ventajas de los DVR de RED.	30
2.3.3	Servidores de video dentro de los sistemas de CCTV.	31
2.4	Sistemas de video vigilancia en licitación para el AIMS.	32
2.4.1	Software de control y administración.	32
2.4.1.1	XProtect VDI.	34
2.4.1.2	GENETEC (Security Center).	37
2.4.1.3	OMNICAST (Sistema De Administración De Videos).	39
2.4.1.4	SYNERGIS, Sistema de Control de Acceso.	40
2.4.1.5	Arquitectura de Security Center.	41
CAPITULO III.....		53
3.1.	Funciones Tecnicas De Los Sistemas De Video Vigilancia IP.....	53
3.1.1.	Comparación Funcional de los Sistemas.	53
3.2.	Elección de Tecnología entre VDI vs GENETEC.	57
3.2.1.	Sistema de Gestión Monitoreo GENETEC.	57
3.2.2.	Sistema de Codificación/Grabación/Transmisión	73
3.2.3.	Sistema de Grabación.....	77
3.3.	Cámaras de seguridad FIJAS y PTZ.	78
3.3.1.	Tipos de Cámaras.	78
3.1.5.1.	Historia de Construcción del Aeropuerto.	79
3.1.5.2	Terminal de Pasajeros.....	82
3.1.5.3	Edificio Del Nodo De Comunicaciones De CNT.	83
3.1.5.4	Estacionamientos.	84
3.1.5.5	Lineas Aereas.	84
3.1.5.6	Terraza.	85
3.1.5.7	Corredor de mangas.....	85

3.1.5.8 Torre de Control.....	86
3.1.6 Distribución de las Cámaras en cada nivel del Aeropuerto.....	87
3.1.6.2 Niveles 0, 1, 2, 4 del Aeropuerto (Cámaras DOMOS PTZ).....	88
3.1.6.3 Niveles 0, 1 ,2 ,3 ,4 Cámaras FIJAS	89
CAPÍTULO IV	94
4.1. Requerimientos tecnológicos del sistema de video vigilancia.....	94
4.1.1 Descripción Técnica Del Equipos de Red.	94
4.1.2 Servidores de bases de datos.....	94
4.1.3 Equipos de Comunicaiones Switchs Core.	95
4.1.4 Switchs de Distribución.....	97
4.1.5 Detalle de Vlans y Direccionamiento IP.	99
4.1.6 QoS o Calidad de Servicio.....	100
4.1.7 Ancho De Banda.	100
4.1.8 Sistemas de redundancia y alta disponibilidad.....	103
4.1.9 Especificaciones Técnicas de las cámaras IP.	107
4.1.9.1 Cámaras fijas.	107
4.1.9.2 Cámaras móviles. (PTZ Giratoria)	107
4.1.9.3 Equipo de administración y grabación digital.....	108
4.1.9.4 Servidores de Grabaciones.	108
4.1.10 Equipos de cómputo para el centro de control y monitore CCTV. ...	109
4.1.10.1 Estaciones de Trabajo para los Operadores.	110
4.1.10.2 Especificaciones Generales.	111
4.1.10.3 Estaciones de Trabajo para el sistema Video Wall.	111
4.1.10.4 Pantallas para el Video Walls.....	112
4.1.10.5 Monitor.....	113
4.1.10.6 Joystick.....	113
4.1.11 Diagrama de red de las Cámaras IP.....	114

4.1.12 Diagrama de RED LAN DEL AIMS.	115
CAPÍTULO V	116
5.1. Estudio Económico.	116
CAPITULO VI	121
6.1. CONCLUSIONES	121
6.2. RECOMENDACIONES	123
BIBLIOGRAFÍA	124
ANEXOS	126

INDICE DE FIGURAS	PAGINA
Figura N° 1. Inicio Del CCTV.	19
Figura N° 2. Formato Motion JPEG.	21
Figura N° 3. Codificación diferencial.	22
Figura N° 4. La tecnología de Servidor de Vídeo.	25
Figura N° 5. Manejo de servidores de video en las Redes LAN.	27
Figura N° 6. Red de cámaras IP	29
Figura N° 7. Circuito cerrado de TV analógico usando DVR de red	31
Figura N° 8. Sistema de vídeo IP que utiliza servidor de vídeo.	31
Figura N° 9. Aeropuerto Internacional Mariscal Sucre.	32
Figura N° 10. Aeropuerto Internacional Mariscal Sucre	33
Figura N° 11. Gama de software Milestone.	35
Figura N° 12. Partners de XProjet	35
Figura N° 13. Dispositivos de acceso al Sistema.	36
Figura N° 14. Herramienta de búsqueda de vídeo.	37
Figura N° 15. Sistemas Básicos de Security Center.	38
Figura N° 16. Arquitectura de Security Center - GENETEC.	41

Figura N° 17. Componentes de Security Center – GENETEC.....	41
Figura N° 18. Herramientas y Componentes de Security Center.	42
Figura N° 19. Herramienta de Config Tool.	43
Figura N° 20. Herramienta Security Desk.....	43
Figura N° 21. Función Del Archiver.....	45
Figura N° 22. Método de Trasmisión Unicast.	47
Figura N° 23. Método de Trasmisión Multicast	48
Figura N° 24. Portal de Asistencia Técnica de Genetec - GTAP.	51
Figura N° 25. Portal de Asistencia Técnica de Genetec - GTAP.	51
Figura N° 26. Socios de Cámaras.	52
Figura N° 27. Herramientas y Componentes de Security Center.	58
Figura N° 28. Acceso como Administrador de GENETEC.....	58
Figura N° 29. Herramienta Security Desk del Cliente.....	59
Figura N° 30. Herramienta Config Tool.	59
Figura N° 31. Herramienta del Servidor Principal.....	60
Figura N° 32. Funciones Del Servidor Genetec.....	61
Figura N° 33. Particiones de Usuarios	62
Figura N° 34. Grupos de Usuarios.....	63
Figura N° 35. Roles y Usuarios.	64
Figura N° 36. Privilegio de Usuarios GENETEC.....	64
Figura N° 37. Roles y Usuarios.	65
Figura N° 38. Autodeteccion de IP dentro de la Red LAN.	66
Figura N° 39. Capacidad de la Red LAN.	66
Figura N° 40. Failover Ridirector.	67
Figura N° 41. Configuración del Failover del Servidor Principal de GENETEC. ...	68
Figura N° 42. Configuración del Failover del Servidor Principal de GENdETEC. .	69

Figura N° 43. Mozaicos de la Herramienta Security Desk.....	70
Figura N° 44. Reproductores de la Herramienta Security Desk	71
Figura N° 45. Informacion del Video	72
Figura N° 46. Botones de Control del Video	72
Figura N° 47. Esquema de codificación H.264.....	73
Figura N° 48. Configuración Del Grabador.....	74
Figura N° 49. NVR Sistema GENETEC.	74
Figura N° 50. Cámara Analógica.....	75
Figura N° 51. Cámara Analógica en la pista del AIMS.....	75
Figura N° 52. Sistema de Gestión CCTV del AIMS.	76
Figura N° 53. Fotografía la Pista del AIMS.	76
Figura N° 54. BCDVideo PART NUMBER—BCD360V8-M-MP-C.	77
Figura N° 55. BCDVideo PART NUMBER—BCD360V8-M-MP-C.	77
Figura N° 56. Cámara AXIS P3215-VE Network Camera.....	78
Figura N° 57. AXIS P3215-VE - Para Exteriores.....	79
Figura N° 58. Toma Aerea de la Superficie en Construcción Del Aeropuerto.....	80
Figura N° 59 Toma Satelital Del Aeropuerto.	81
Figura N° 60. Toma Fotografía desde la Torre de Control.....	82
Figura N° 61. Tomas Fotograficas de los diferentes areas del AIMS.	83
Figura N° 62. Tomas Fotograficas Del Nodo de Comunicaciones de CNT.....	83
Figura N° 63. Tomas Fotograficas Parqueaderos del AIMS.	84
Figura N° 64. Tomas fotograficas de las oficinas de las lineas Aereas del AIMS.	84
Figura N° 65. Tomas Fotograficas de la Terraza del AIMS	85
Figura N° 66. Tomas Fotograficas Del Corredor de Mangas del AIMS.	85
Figura N° 67. Tomas Fotograficas de la torre de Control AIMS.....	86
Figura N° 68. Servidores de Bases de datos GENETEC security Center.....	95

Figura N° 69. Cisco Core Catalyst 4503-E - WS-C4503-E.....	96
Figura N° 70. Cuarto de Comunicaciones MCR1 del AIMS.....	98
Figura N° 71. Cableado Estructurado CAT6A del AIMS	98
Figura N° 72. Calculo del Ancho de Banda.....	101
Figura N° 73. Calculo del Ancho de Banda y Almacenamiento.	102
Figura N° 74. Calculo del Almacenamiento.....	102
Figura N° 75. Herramienta para la medición de ancho de banda AXIS	103
Figura N° 76. Cuarto de Comunicaciones del MCR1.....	103
Figura N° 77. Sistemas de Redundancia en Redes LAN	104
Figura N° 78. Cámaras ubicadas en arribos Internacional.....	107
Figura N° 79. Cámaras ubicadas los Corredores.	108
Figura N° 80. Espacio de Almacenamiento del los Servidores de video.....	109
Figura N° 81. Estaciones de Trabajo.	110
Figura N° 82. Video Wall Operativos dentro del Centro de Control del AIMS.....	112
Figura N° 83. Pantalla de 42” Operativas dentro Del CCTV AIMS.	113
Figura N° 84. Fotografía de los Equipos del Centro de Control CCTV	113
Figura N° 85. Diagrama de la Red Lan del AIMS.....	115

TABLAS	PAGINA
Tabla No. 1 Roles Predeterminados.....	44
Tabla N° 2. Modos de Grabación.....	46
Tabla N° 3. Comparación técnica de los sistemas de video vigilancia.	53
Tabla N° 4. Cámaras Operativas Dentro Del AIMS.....	87
Tabla N° 5. Camaras Domoz PTZ (Cámaras Instaladas).....	88
Tabla N° 6. Cámaras Fijas	89
Tabla N° 7. El Cisco Catalyst 4500 y Series y Modelos de Switch Catalyst.....	96

Tabla N° 8. Detalle de Vlans y direccionamiento IP.	99
Tabla N° 9. Licencias y Software GENETEC	116
Tabla N° 10. Cableado Estructurado.	117
Tabla No. 11 Cuartos de Comunicaciones y Networking.	117
Tabla N° 12. Costo Total de Red LAN del AIMS.	118
Tabla No. 13 Equipos tecnologicos Del CCTV.	119

CAPÍTULO I

Definición del proyecto.

Introducción

Actualmente el incremento de atentados llevados a cabo por diferentes grupos terroristas, los delitos cometidos por pequeñas y grandes bandas organizadas de narcotráfico, y el aumento del vandalismo en las grandes ciudades, son algunas de las principales fuentes de preocupación e incertidumbre. Tanto es así, que un gran número de instituciones públicas, privadas y municipales han tomado la decisión de reforzar las medidas de seguridad instalando sistemas de video vigilancia como una posible solución. Hoy en día los sistemas de video vigilancia son una herramienta útil e indispensable para disminuir la delincuencia, como en bancos, centros comerciales, aeropuertos, instalaciones militares, grandes empresas, calles conflictivas, etc.

Existen grandes avances en el área de video vigilancia IP, que hacen completamente importante la utilización de nuevas tecnologías de redes IP, razón por la cual el Aeropuerto Internacional Mariscal Sucre AIMS tiene como prioridad optimizar su sistema de video vigilancia utilizando equipos de comunicación IP.

Los sistemas de video vigilancia IP orientados a Aeropuertos requieren a gran escala un despliegue muy importante de una infraestructura y componentes tecnológicos que comprende principalmente de un centro de monitoreo (CCTV), cableado estructurado, servidores de vídeo, fibra óptica por las largas distancias que hay que instalar los dispositivos y sobre pasan la distancia que determina el estándar TIA/EIA del cableado estructurado UTP.

Este proyecto comprende el estudio de los sistemas de seguridad de video vigilancia IP,

diseñados para la seguridad aeroportuaria, y gracias a los avances de la tecnología nos permiten consolidar este requerimiento de video vigilancia desde un solo sistema central dando lugar a optimizar la plataforma de seguridad aeroportuaria.

Justificación e Importancia.

Los sistemas de televisión de circuito cerrado (CCTV) y los de video vigilancia se están volviendo más habituales evitando robos, en los edificios de oficinas, centros comerciales, escuelas, incluso en las calles principales de la ciudad.

El Aereopuerto Internacional Mariscal Sucre, tiene como requerimiento optimizar el sistema de video vigilancia mediante el manejo de nuevas tecnologías y comunicaciones IP, que en la actualidad ofrecen un óptimo servicio de comunicaciones, razón por la cual se detalla el propósito y los beneficios que tiene como objetivo alcanzar:

Requerimientos del sistema.

- Mantener la vigilancia remota de varios lugares simultáneamente desde un solo sitio a través de conexiones de red IP.
- Grabación de video por cada cámara (Continuo, por detección de movimiento por 30 días).
- Integración con otros sistemas electrónicos de seguridad para hacer más eficiente la vigilancia. (Control de accesos para las diferentes áreas)
- Configuración de patrones de movimientos inteligentes a las cámaras giratorias, (rotación y grabación de 360°).
- Instalar cámaras mediante la utilización de fibra óptica para monitorear la pista del AIMS.

Las redes IP brindan un desarrollo importante a los sistemas de video vigilancia a la vez

existe un desafío con la utilización de las nuevas tendencias tecnológicas que son:

Beneficios de la automatización del sistema.

- Cuidar y vigilar a las personas.
- Evitar el robo de productos.
- Protección de activos fijos.
- Dar seguridad a personas (empleados, visitantes, etc.)
- Ayudar al seguimiento visual de sospechosos
- Disuadir robos y asaltos.
- Vigilancia en estacionamientos.
- Cuidado de niños y pacientes.
- Ver la actividad de empleados.
- Controlar actos de violencia.
- Monitoreo de áreas específicas.
- Control de seguimientos a personas sospechosas.

El propósito del presente proyecto es realizar el estudio técnico y funcional de un sistema de video vigilancia sobre una red IP, como una alternativa al servicio de seguridad y detección de intrusos que al momento se tiene como exigencia el AIMS.

El nuevo sistema de video vigilancia tiene como necesidad la instalación de cámaras domo (PTZ- Giratorias de gran alcance), cámaras fijas para la grabación por movimiento mediante activación interna y externa. Las cámaras serán conectadas a un servidor de video, través de cable UTP CAT6A o fibra óptica, dependiendo de las distancias que esté instalado el componente IP.

Los videos serán almacenados en los grabadores de video en red (NVR), los cuales estarán en capacidad de almacenar todos los acontecimientos ocurridos durante las 24 horas del día y por un tiempo determinado de 30 días.

Es importante tomar en cuenta estos requerimientos ya que será las soluciones para automatizar el sistema de video seguridad, manteniendo presente todo lo que se requiere en el mundo de las redes IP, y con el fin de mantener sostenible el proyecto tecnológico de video vigilancia y ayudar así a conseguir los objetivos empresariales propuestas por el Aeropuerto Internacional Mariscal Sucre.

Antecedentes

La condición actual del sistema de video vigilancia del Aeropuerto Internacional Mariscal Sucre presenta muchas vulnerabilidades que deja muchos puntos sensibles dentro de las diferentes áreas, razón por la cual se ha elaborado un estudio explícito para optimizar la seguridad integral de todo el aeropuerto con la implementación de un nuevo sistema de seguridad de video vigilancia basado en nuevas tecnologías IP.

Con el fin de automatizar de forma dinámica el monitoreo y seguridad de las personas que están circulando en dichas áreas es primordial automatizar el sistema de video vigilancia basados en IP, brindando un apoyo muy importante al agente de seguridad aeroportuario que no puede cubrir todas las áreas vulnerables como son: filtros, mangas, arribos nacionales, áreas estériles, áreas restringidas, áreas públicas y administrativas etc.

Es de suma importancia contar con un sistema de video vigilancia IP Inteligente, además de mantener con los objetivos de la seguridad aeroportuaria que se enfocada en la necesidad de cumplir con los requisitos de seguridad empresariales y brindar un mejor servicio de seguridad física a todas las áreas del aeropuerto.

Para mantener un control de monitoreo de todas las áreas del Aeropuerto Internacional Mariscal Sucre, AIMS, es necesario tener un centro de monitoreo CCTV, que brindara apoyo a los agentes de seguridad que están encargados de la seguridad y chequeo de los pasajeros en las diferentes áreas como son: arcos detectores de metales, detectores de explosivos, la separación de las operaciones de llegada y salida, cercas y puertas de seguridad, máquinas de rayos X, cámaras de vigilancia, monitores, puestos de control de seguridad, centros de comunicaciones, sistemas de control de acceso, sistemas de identificación de equipaje, y otras equipos de seguridad.

Objetivos.

Objetivo General.

Análisis técnico de la implementación de un sistema de video vigilancia basado en tecnología IP, caso de estudio Aeropuerto Internacional Mariscal Sucre del Ecuador.

Objetivos Específicos.

1. Realizar el estudio del estado del arte de los sistemas de seguridad de video vigilancia, basado en tecnología IP.
2. Analizar las funcionalidades de los sistemas de video vigilancia IP.
3. Determinar los requerimientos tecnológicos de infraestructura de red para implementación del sistema de seguridad aeroportuario.
4. Pruebas de funcionalidad del sistema implementado de Video Vigilancia.
5. Estudio económico sobre la implementación del sistema de Video Vigilancia.

CAPÍTULO II

2.1 Estudio del estado del arte de sistemas de seguridad de video vigilancia.

2.1.1 Sistemas de CCTV

Las siglas CCTV vienen del inglés “*Closed Circuit Television*” que traducido se conoce como “Circuito cerrado de televisión”. Es una tecnología de video vigilancia diseñada para supervisar áreas específicas y en diferentes ambientes internos o externos, en la actualidad los sistemas CCTV están operativos en, micromercados, aeropuertos, centros comerciales, bancos, edificios públicos, etc.¹

Un sistema de seguridad está constituido por un conjunto de dispositivos que se interrelacionan entre sí, cuya función principal es prevenir, alertar y verificar intrusiones o actos delictivos, y de acuerdo a esto, tomar medidas de prevención sobre los actos ilícitos.

Un sistema de video vigilancia utiliza cámaras IP para su monitoreo, las cuales pueden ser colocadas en lugares públicos y privados para la prevención del crimen y/o combate del crimen. Es una tecnología multifuncional, inicialmente usada para el manejo de riesgos en caso de embotellamientos de tráfico, incendios, accidentes y crimen, los sistemas de CCTV están siendo usados cada vez más para varios propósitos y lugares como el control de acceso, y el control de conducta ante los actos delictivos.

2.1.2 Introducción a los sistemas de CCTV.

Los sistemas de videovigilancia pueden ser evocados a los años 50 con la expansión de la tecnología de la información y las comunicaciones. Para esta fecha, las cámaras eran principalmente usadas para el manejo del tráfico, en bancos y tiendas, fue sólo hasta la

¹CCTV. Recuperado de: https://es.wikipedia.org/wiki/Circuito_cerrado_de_televisión.

década de los 60 que los sistemas de video-tecnología comenzaron a expandirse en las ciudades, principalmente en el Reino Unido y los Estados Unidos. Aunque el padre real de la implementación del CCTV es el Reino Unido, ya que desde los 80s el gobierno de este país ha instalado cámaras a una tasa de 500 camaras por semana.

Con el crecimiento de las áreas urbanas y la sociedad en los años 70s, el sistema de video vigilancia masiva se adopto como herramienta para monitorear hurtos, actos ilicistos, eventos masivos, propiedad privada, trasporte público urbano, hospitales y escuelas. En el Reino Unido, se instalaron cámaras de video vigilancia en cuatro grandes estaciones de tren subterráneo y al mismo tiempo se comenzó a monitorizar el flujo vehicular en las grandes carreteras.

En los Estados Unidos, el uso de los sistemas de videovigilancia no era prevalente hasta los años 80 para las áreas públicas, pero los propietarios de tiendas y bancos entendieron rápidamente el valor de los sistemas de seguridad y los implementaron.

Países como Suiza han adoptado ampliamente la tecnología de CCTV como herramienta para el manejo operativo de áreas públicas, en los 90, la estación principal de trenes de Zúrich, la más grande de Suiza, se convirtió en empresa pública debido a su rol en el trasporte interno y externo, la estación se convirtió en una ubicación importante para las cámaras de CCTV para monitorear la considerable cantidad de actividad.²

Por medio de un sistema de vigilancia IP, es posible que varias personas revisen la misma imagen desde computadores y lugares diferentes ya que las cámaras de vigilancia de hoy poseen una mejor tecnología, pueden ser inalámbricas o cableadas, con diferentes ángulos de movimiento, *pan* (rotación en sentido horizontal), *tilt* (rotación en sentido vertical), *zoom*

²http://www2.congreso.gob.pe/Sicr/TraDocEstProc/Contdoc03_2011.nsf/.

(acercamiento o alejamiento de la imagen), visión nocturna y poseer audio unidireccional o bidireccional (con micrófono y parlante incorporado).

2.1.3 Sistemas de CCTV sobre IP.

La vigilancia, la supervisión y seguridad son temas que han adquirido importancia en la actualidad, tanto en el área privada como en la doméstica. Todos quisieran contar con un completo sistema de vigilancia, que permita evitar los delitos, poder identificar a los autores de un robo, de una conducta indebida, o simplemente una supervisión de actividades.

El vídeo IP, a menudo conocido como vigilancia IP para determinadas aplicaciones en el ámbito de la vigilancia en seguridad y la monitorización remota, es un sistema que ofrece a los usuarios la posibilidad de controlar y grabar en vídeo a través de una red IP. La tecnología de CCTV es cada vez más asequible y ha sido considerada exitosa para mejorar la eficiencia de la vigilancia en áreas públicas y privadas.

2.1.4 Sistemas de vigilancia IP y su evolución.

La primera referencia sobre el Circuito Cerrado de Televisión fue en 1942 y desarrollado por la empresa Siemens AG para el ejército Alemán.³

Estos sistemas comenzaron a ser implementados en los años 50 en forma muy básica, durante los años 70 mejoraron significativamente y actualmente se han complementado con equipos tales como VCR y monitores.⁴

³ <http://seguridadig.com/historia-del-circuito-cerrado-de-television-cctv/>.

⁴ <http://camarasdeseguridad.jimdo.com/historia-e-información-del-sistema-dvr/>.



Fuente: el Autor

Figura N° 1. Inicio Del CCTV.

Los sistemas de seguridad de video vigilancia se clasifican en tres generaciones de acuerdo a las ventajas y problemas que presentan y en el uso de tecnologías que emplean.

Primera Generación.

El procesamiento y grabación de video en la primera generación, lo realizaban de forma analógica con la ayuda de equipos llamados VHS. La aparición del VHS dio una ventaja para el almacenamiento de la información, y revisión posterior de los videos.⁵

La primera generación está formada por sistemas de circuito cerrado de televisión, cuyo acrónimo es CCTV (Closed Circuit Television). Todos los componentes son parte de un mismo circuito, por lo cual se lo denomina circuito cerrado de television. Están formados por un conjunto de cámaras distribuidas a lo largo del entorno vigilado y conectadas a un conjunto de monitores que suelen estar ubicados en una sala central de monitoreo.

- **La Segunda Generación.**

Los sistemas de vigilancia de la segunda generación combinan las tecnologías de los sistemas CCTV y vigilancia-IP, la segunda generación de CCTV vino con la digitalización de las imágenes, algo que permitió tratar los datos digitales con un equipo “inteligente” (CPU). La segunda generación brinda procesos mas sencillos para grabar los video en un DVR,

⁵ Primera Generacion:

http://www.novenca.com/site/index.php?option=com_content&view=article&id=257&Itemid=159 (2016).

detección de movimiento, búsqueda más rápida de un video guardado sin degeneración de la calidad del video al momento de relizar un respaldo.⁶

Los DVR tienen una entrada analógica por cada camara habilitada dentro del sistema de video vigilancia para luego ser procesada y almacenada la información.

- **La Tercera Generación**

En la tercera generación del CCTV, los sistemas IP han evolucionado y tienen un grado de procesamiento de la información, convirtiéndose en una solución automatizada inteligente dentro de la tercera generación adquieren el nombre de *DVMS “Sistema Digital de Manejo de Video”*.⁷

En la tercera generación los sistemas IP han obtenido una madurez en su desarrollo, en la cual brindan la característica de operar de forma integrada con sistemas de control de accesos, cajeros automáticos o puntos de venta, esta integración de los sistemas hace que se pueda automatizar la seguridad.

2.1.5 Compresión de video Digital Códec de vídeo

Las técnicas de compresión de video consisten en reducir y eliminar datos redundantes del video para que el archivo de video digital se pueda enviar a través de la red y recolectar en servidores apropiados para su almacenamiento. Con técnicas de compresión eficaces se puede reducir considerablemente el tamaño del fichero sin que ello afecte muy poco, o en absoluto, la calidad de la imagen.

⁶ La Segunda Generación Del CCTV:

http://www.novenca.com/site/index.php?option=com_content&view=article&id=257&Itemid=159

⁷ La tercera generación del CCTV:

http://www.seguridad-online.com.ar/index.php?mod=Home&ac=verNota&id_nota=435&id_seccion=149

Existen diferentes técnicas de compresión, tanto patentadas como estándar. Hoy en día, la mayoría de proveedores de video en red utilizan técnicas de compresión estándar. Los estándares son importantes para asegurar la compatibilidad y la interoperabilidad de los componentes y sistemas de seguridad basados en IP.

2.1.6 Compresión de imagen vs. Compresión de vídeo.

Los diferentes estándares de compresión utilizan métodos distintos para reducir los datos y, en consecuencia, los resultados en cuanto a la frecuencia de los bits y latencia son diferentes. Existen dos tipos de algoritmos de compresión:

- **Compresión de imágenes**
- **Compresión de vídeo.**

La compresión de imagen, utiliza la tecnología de codificación intrafotograma. Los datos se reducen a un fotograma de imagen con el fin de eliminar la información innecesaria que puede ser imperceptible para el ojo humano. Motion JPEG es un ejemplo de este tipo de estándar de compresión. En una secuencia Motion JPEG codifican, o comprimen como imágenes JPEG individuales.



Figura N° 2. Formato Motion JPEG.

Fuente: el autor.

Los algoritmos de compresión de vídeo-4 como el MPEG-4 y el H.264 utilizan la predicción interfotograma para reducir los datos de vídeo entre las series de fotogramas.

El par de algoritmos que funcionan conjuntamente se denomina códec de video (codificador/decodificador). Los *códec's* de video de estándares diferentes no suelen ser compatibles entre sí, es decir, el contenido de video comprimido con un estándar no se puede descomprimir con otro estándar diferente. Esto ocurre simplemente porque un algoritmo no puede decodificar correctamente los datos de salida del otro algoritmo.

Compresión de video, Los algoritmos de compresión de video utilizan la predicción inter-fotograma para reducir los datos de video entre las series de fotogramas. Ésta consiste en técnicas como la codificación diferencial, en la que un fotograma se compara con un fotograma de referencia y sólo se codifican los píxeles que han cambiado con respecto al fotograma de referencia.



Fuente: el autor.

Figura N° 3. Codificación diferencial.

2.1.7 Formatos de compresión.

Motion JPEG

“*Motion JPEG o M-JPEG es una secuencia de video digital compuesta por una 35 serie de imágenes JPEG individuales (Joint Photographic Experts Group)*”⁸. Cuando el ser humano observa la cantidad de 16 o más imágenes por segundo, el ojo humano percibe como un video en movimiento.

Un video en completo movimiento se percibe a 30 imágenes por segundo en el estándar

⁸ https://es.wikipedia.org/wiki/Joint_Photographic_Experts_Group.

NTSC o a 25 imágenes por segundo en el estándar. Una de las ventajas de Motion JPEG es que cada imagen de una secuencia de vídeo puede conservar la misma calidad garantizada que se determina mediante el nivel de compresión elegido para la cámara de red o codificador de vídeo. Cuanto más alto es el nivel de compresión, menor es el tamaño del archivo y la calidad de imagen. En algunas situaciones, como cuando hay poca luz o la escena es compleja, el tamaño del archivo puede ser bastante grande y, por lo tanto, usar más ancho de banda y espacio de almacenamiento.⁹

Motion JPEG es un estándar libre que no necesita licencia. Su uso es muy habitual en aplicaciones donde se requieren fotogramas individuales en una secuencia de vídeo y donde se utiliza una frecuencia de imagen de 5 fotogramas por segundo o inferior. Motion JPEG también puede ser útil para aplicaciones que requieren integración con sistemas que sólo son compatibles con Motion JPEG.

Motion JPEG no utiliza ninguna técnica de compresión ya que consiste en una serie de imágenes individuales fijas y completas. El resultado es una frecuencia de bits relativamente alta o una relación de compresión baja para la calidad proporcionada, en comparación con estándares de compresión de vídeo como MPEG-4 y H.264¹⁰.

MPEG-4.

Cuando se menciona MPEG-4 en las aplicaciones de video vigilancia, normalmente nos referimos a MPEG-4 Parte 2, también conocido como MPEG-4 Visual. Como todos los estándares *MPEG (Moving Picture Experts Group)*, requiere una licencia, es decir, los usuarios deben pagar una tasa de licencia por cada estación de supervisión.

⁹ <http://www.axis.com/ve/es/learning/web-articles/technical-guide-to-network-video/compression-formats>

¹⁰ https://es.wikipedia.org/wiki/H.264/MPEG-4_AVC.

MPEG-4 es compatible con aplicaciones de ancho de banda reducido y aplicaciones que requieren imágenes de alta calidad, sin limitaciones de frecuencia de imagen y con un ancho de banda virtualmente ilimitado.

H.264 o MPEG-4 Part 10/AVC.

El H.264, también conocido como MPEG-4 Parte 10/AVC para Codificación de Vídeo Avanzada, es el estándar MPEG más actual para la codificación de vídeo y puede comprimir en mas de del 80%.

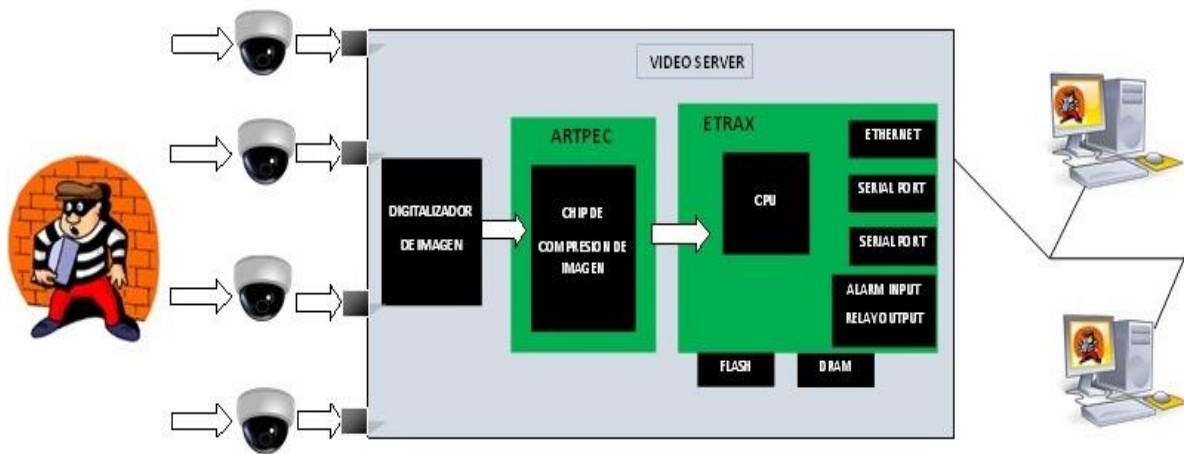
El H.264 ha sido definido conjuntamente por organizaciones de normalización del sector de las telecomunicaciones (ITU-T's Video Coding Experts Group) y de las tecnologías de la información (ISO/IEC Moving Picture Experts Group), tiene una mayor protección que respecto a los estándares anteriores.

2.2 Características y ventajas de los sistemas de video vigilancia IP.

2.2.1 Capacidad de escalamiento del sistema de seguridad.

Un sistema de seguridad IP esta conformado por una o varias cámaras que son parte de una red, estos dispositivos están conectados a varios monitores o televisores. Los cuales reproducen las imágenes capturadas, estas imágenes pueden ser simultáneamente, almacenadas en medios analógicos o digitales según lo requiera el usuario. Los componentes de este circuito pueden ser entonces: cámaras, servidores de video, grabadores digitales (DVR).¹¹

¹¹ https://es.wikipedia.org/wiki/Grabador_de_video_digital.



Fuente: el autor.

Figura N° 4. La tecnología de Servidor de Vídeo.

Administración del vídeo.

1. El Servidor de Vídeo recibe la señal de vídeo analógico de la cámara analógica en el digitalizador de imágenes. El digitalizador convierte el vídeo analógico al formato digital.
2. El vídeo digital se transfiere al chip de compresión, donde las imágenes de vídeo se comprimen en imágenes fijas JPEG o en vídeo MPEG. La conversión al formato digital y la compresión en imágenes JPEG las realiza el chip controlador de cámara y de compresión de vídeo de Axis.
3. El Chip ETRAX de Axis contiene la CPU, la conexión Ethernet, los puertos serie y la entrada de alarmas y la salida, lo que representa “el cerebro” o las funciones del servidor de vídeo. Gestiona la comunicación con la red. La CPU procesa las acciones del servidor web y las de todo el software (por ejemplo los controladores de diferentes cámaras Pan/Tilt/Zoom).
4. La conexión Ethernet permite la conexión directa a la red.
5. Los puertos serie (RS-232 y RS-485) permiten el control de las funciones

Pan/Tilt/Zoom de las cámaras o de equipos de vigilancia como el grabador de lapsos de tiempo (time-lapse recorder). También permite la conexión de un módem.

6. La entrada de Alarmas y la salida, la entrada de Alarmas puede ser utilizada para activar el Servidor de Vídeo y que empiece a transmitir imágenes entre la cámara y los monitores donde están a disposición del CCTV.

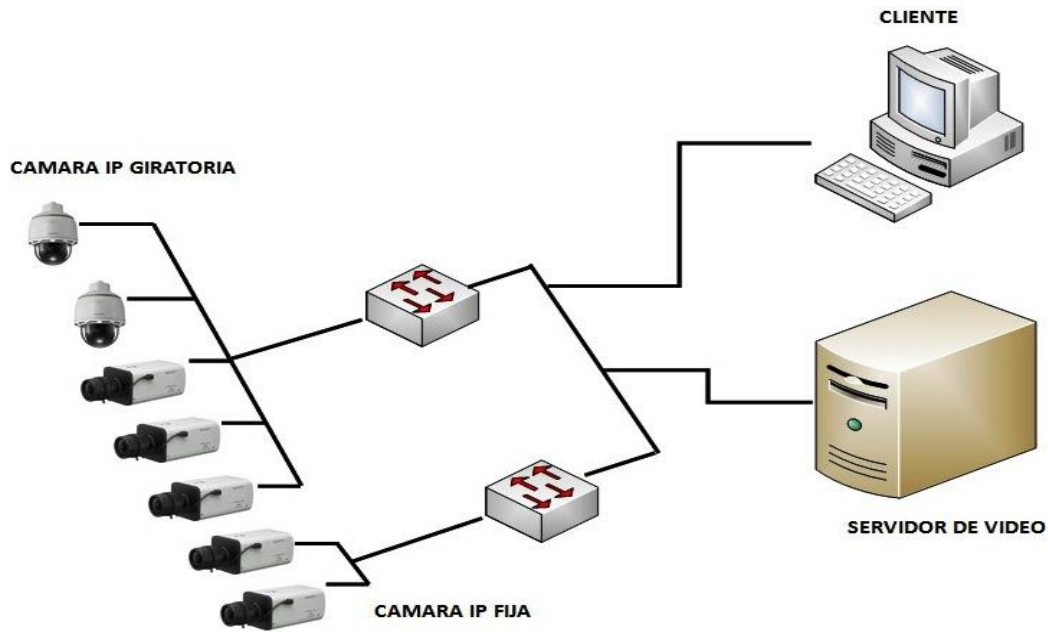
2.2.2 Manejo de servidores de video en las Redes LAN.

Los servidores de video en red, al igual que muchos otros tipos de comunicaciones se realiza a través de redes IP cableadas. El video en red y las transmisiones de audio, así como otros datos, se efectúan a través de la misma infraestructura de red.

El video en red proporciona a los usuarios, en particular a los del sector de vigilancia y seguridad, muchas ventajas con respecto a los sistemas CCTV.

Los sistemas de seguridad basados en tecnología IP tienen la funcionalidad de poder controlar las cámaras de forma remota. Las diferentes cámaras que conforman el circuito de video vigilancia tienen características fijas y PTZ.

Las cámaras tienen la funcionalidad de operar en ambientes extremos, visión nocturna, detección de movimiento, control remoto, configuración de patrones de movimiento de las cámaras giratorias (PTZ).



Fuente: el autor.

Figura N° 5. Manejo de servidores de video en las Redes LAN.

2.2.3 Compatibilidad con aplicaciones y facilidad de integración.

- **Arquitectura Distribuida y Centralizada:** La arquitectura flexible de un sistema de seguridad permite la implementación de distintas topologías de acuerdo a los requerimientos técnicos de la solución. Pudiéndose instalar todos los servicios en un único equipo o armar una arquitectura distribuida, dependiendo del tamaño de la red.
- **Modular:** El sistema de seguridad está basado en servicios, lo cual brinda una insuperable modularidad que corren en un único servidor o en varios.

2.2.4 Potente herramienta de análisis de Video.

La aplicación cliente incluye una potente herramienta de búsqueda de video grabado basada en eventos.

2.2.5 Esquema redundante.

La solución permite definir servidores que actúen como redundancia de otros, ya sea

reemplazando al servidor principal en caso de que éste quede fuera de servicio o definiendo un servidor alternativo asociado a cada cámara.

2.2.6 Grabación usando NVR¹².

Este método de grabación es sumamente flexible y permite alcanzar capacidades de almacenamiento del orden de Terabytes, utilizando tecnologías absolutamente maduras y probadas en IT, como por ejemplo SAN, RAID, SATA, etc.

2.3 Características de almacenamiento en los sistemas de video vigilancia.

2.3.1 Seguridad y monitoreo utilizando cámaras IP.

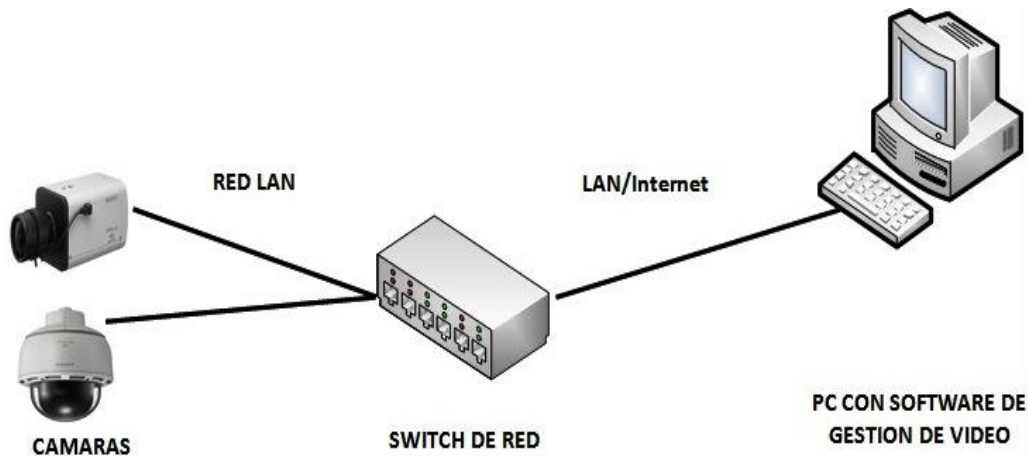
Las imágenes y videos que captura una camara, es transmitido por una infraestructura de red LAN, existen servidores que brindan el almacenamiento de la información. Dentro de un sistema de video vigilancia basado en tecnología IP.

Ventajas:

- Resolución de megapíxel.
- Definición de imágenes.
- Alimentacion POE¹³ (Power Over Ethernet).
- Entrada y salida de audio.
- Algunas cámaras IP tienen sensor de movimiento.

¹² NVR (Network Video Recorder), Grabador de Video en Red.

¹³ https://es.wikipedia.org/wiki/Power_over_Ethernet.



Fuente: el autor.

Figura N° 6. Red de cámaras IP

La figura N° 6 muestra un sistema de vídeo IP, este sistema brinda un servicio optimo de la tecnología digital, y brinda una calidad de imagen eficiente y constante desde la cámara hasta el centro de control.

2.3.2 Sistemas de video supervisión y control a través de cámaras IP.

La transmisión de video en la actualidad son sistemas que utilizan tecnología IP, por lo tanto se toma la decisión de incorporar este tipo de soluciones, es importante considerar los factores que permitan realizar la mejor elección de los equipos.

- Calidad De Imagen.
- Posibilidad de ampliar el sistema.
- Compatibilidad con aplicaciones y facilidad de integración.
- Compresión compatible con los estándares Jpeg y Mpeg4.
- Herramientas de administración para grandes instalaciones.
- Múltiples opciones de funcionalidad y seguridad en red.
- Sensor de barrido progresivo.
- Alimentación a través de PoE (Power over Ethernet).

- Historial y prioridades del fabricante.
- Sistemas de CCTV usando DVR de RED.

2.3.2.1 Ventajas de los DVR de RED.

Los codificadores de vídeo son un componente clave en este proceso de conversión por parte del mercado de los sistemas de videovigilancia analógicos a los sistemas en red.

En un sistema IP es muy fácil incorporar cámaras nuevas y cambiarlas de sitio; esto facilita tanto la instalación como una posible ampliación del sistema. Como la grabación y la gestión se realizan con un equipo informático estándar, el operador puede elegir entre una multitud de fabricantes y proveedores siempre que necesite más espacio de almacenamiento o deba actualizar otras partes de la infraestructura.¹⁴

Ventajas de los DVR:

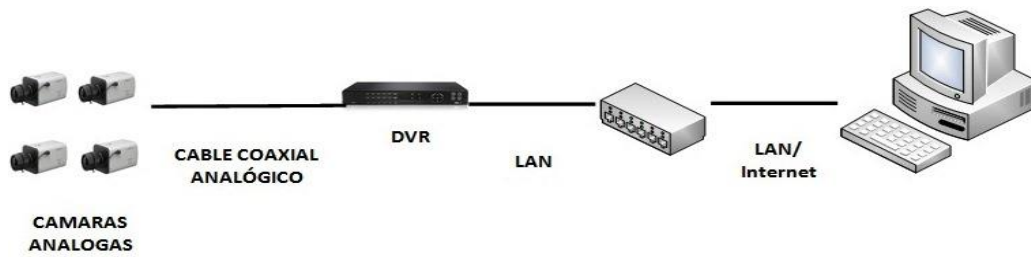
- **Acceso Remoto:**

La tecnología IP brinda la potestad de poder verificar los videos de forma remota.

- **Costo Reducido:**

La infraestructura de red existente brinda un costo beneficio al usuario a la hora de implementar equipos de gravacion basados en tecnología IP. Los sistemas de video vigilancia brindan la potestad de crecer en escalabilidad sin la necesidad de implementar un nuevo sistema de monitorización.

¹⁴ http://www.axis.com/files/whitepaper/wp_encoders_34384_es_0902_lo.pdf.



Fuente: el autor.

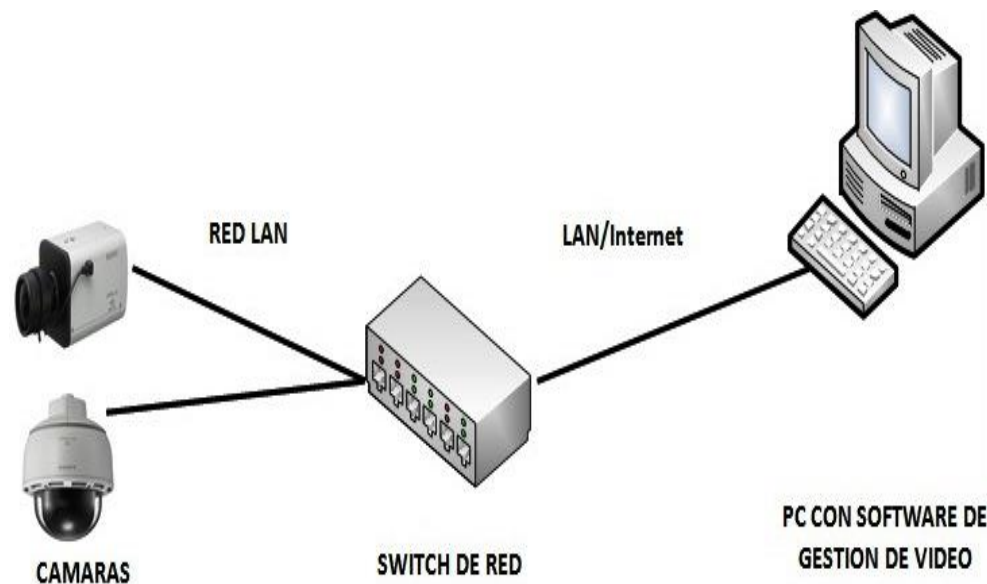
Figura N° 7. DVR de red

2.3.3 Servidores de vídeo dentro de los sistemas de CCTV.

El servidor de vídeo se conecta a una red y transmite el vídeo a través de un conmutador de red a un PC, y la información se almacena en los respectivos servidores.

Ventajas:

- Monitorización en vivo en los teléfonos Windows PDA phone, iPad, iPhone, iPod.
- Proporciona modos de grabación profesionales versátiles.¹⁵



Fuente: el autor

Figura N° 8. Sistema IP que utiliza servidor de vídeo.

¹⁵ <http://www.dointech.com.co/video-vigilancia-ip.html>.

2.4 Sistemas de video vigilancia en licitación para el AIMS.

2.4.1 Software de control y administración.



Fuente: el autor.

Figura N° 9. Aeropuerto Internacional Mariscal Sucre.

El Aeropuerto Internacional Mariscal Sucre, es el nuevo aeropuerto internacional de la ciudad de Quito y el principal aeropuerto del Ecuador. Está ubicado en una planicie en los suburbios orientales de la ciudad de Quito, en la localidad de Tababela, a 25 kilómetros del Centro Histórico de la ciudad, por lo que también se lo conoce como Aeropuerto de Tababela. El aeropuerto fue inaugurado el 20 de febrero de 2013, lo que significó el cierre del Antiguo AIMS¹⁶. El Programa Universal de Auditorías de seguridad, USAP¹⁷, es establecido por la Organización de la Aviación Civil Internacional, OACI¹⁸, para promover una mayor comprensión de los problemas de seguridad aéreos mundiales a través de auditorías para fomentar la confianza en la seguridad de la aviación.

¹⁶ AIMS. (Aeropuerto Internacional Mariscal Sucre).

¹⁷ USAP. (Programa de auditoría de la seguridad universal)

¹⁸ OACI. (Organización de la Aviación Civil Internacional)



Fuente: el autor

Figura N° 10. Aeropuerto Internacional Mariscal Sucre¹⁹

Su pista tiene 4.100 metros de longitud, lo que la hace la más larga de los aeropuertos de todas las capitales sudamericanas y de las ciudades ecuatorianas. Su torre de control posee 41 metros de alto. Se tiene previsto construir una segunda pista, para cubrir la demanda futura. En una segunda etapa, prevista para el 2023, se ampliará el terminal en 20 mil metros cuadrados más.

El Aeropuerto Internacional Mariscal Sucre, es el nuevo aeropuerto internacional de la ciudad de Quito y mediante la Empresa Pública Metropolitana de Servicios Aeroportuarios y Gestión de Zonas Francas y Regímenes Especiales tiene como propósito realizar el estudio técnico y funcional de un sistema de video vigilancia sobre tecnología IP, todo esto como una alternativa al servicio de seguridad y detección de intrusos, razón por la cual existe un análisis de licitación en software y hardware (cámaras) que cumpla con las necesidades del AIMS.

¹⁹ Toma Satelital del Aeropuerto Internacional Mariscal Sucre. Recuperada de: <https://www.google.com/maps/place/Aeropuerto+Internacional+Mariscal+Sucre/@-0.131836,-78.357239,12560m/data=!3m1!1e3!4m2!3m1!1s0x91d58db4352baa87:0x2f9f7623e0894b8b!6m1!1e1?hl=es>

El software en análisis para la instalación y gestión del sistema de video vigilancia dentro del Aeropuerto Internacional Mariscal Sucre son: XProtect VDI vs GENETEC.

2.4.1.1 XProtect VDI.

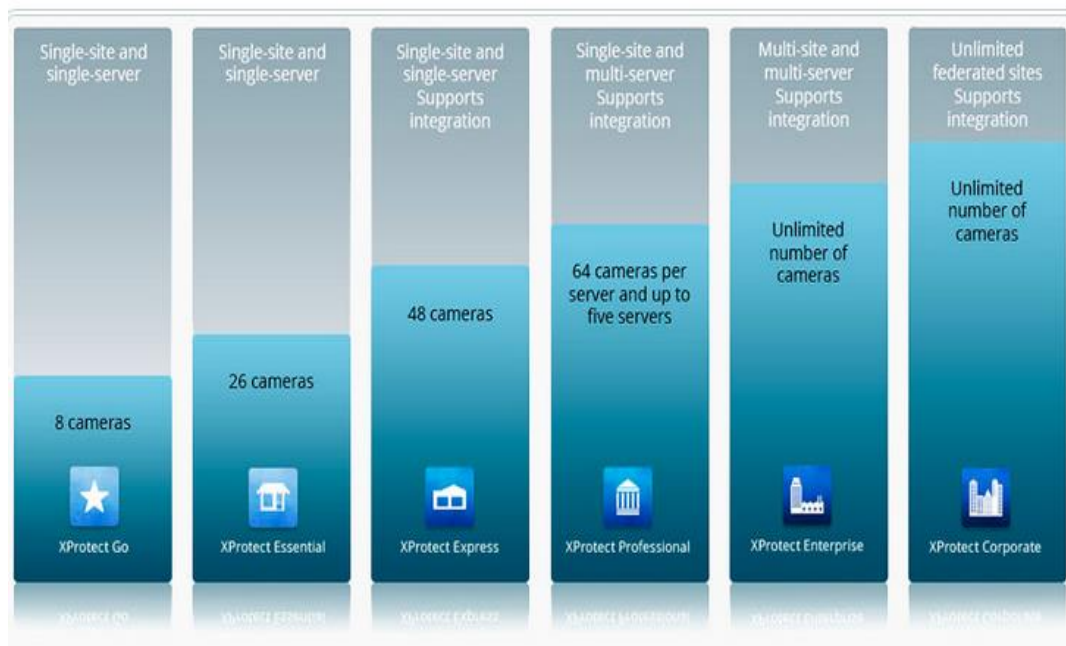
Información Corporativa XProtect VDI

EL sistema *VDI*, ofrece una solución para cualquier entorno de vídeo vigilancia, desde instalaciones de 5 ó 6 cámaras para pequeños comercios, hasta arquitecturas federadas con diferentes localizaciones y cientos de cámaras grabando 24 x 7, todo ello gestionado bajo un único administrador.

VDI ha considerado una alianza estratégica con **Milestone Systems ©**, *líder mundial en software para gestión de vídeo IP*, es la unión para asentar y desarrollar presencia en el mercado de la seguridad bajo tecnología IP.

El sistema *VDI*, es totalmente aplicable al entorno de vídeo vigilancia, proporcionando siempre la solución a medida más eficiente para la infraestructura de grabación requerida. La estrecha relación con Milestone y su canal de distribución permite ofrecer la mejor opción para cada caso, de forma personalizada e independiente.

El software Milestone abarca desde el servidor más sencillo para instalaciones pequeñas, a redes de almacenamiento con sistemas de grabación independientes a los servidores de gestión. Además de los puestos cliente de visionado, donde los requerimientos de procesador y potencia gráfica serán claves según número de cámaras a visionar y resolución.



Fuente: <https://www.milestonesys.com>

Figura N° 11. Gama de software Milestone.

Certificaciones.

VDI, trabaja con las mejores marcas del sector tecnológico, y éstas los avalan. Por ese motivo los profesionales realizan exámenes técnicos que los certifican para trabajar con tecnologías.



Fuente: <https://www.milestonesys.com>

Figura N° 12. Partners de XProjet

XProtect Professional es una aplicación de software para video vigilancia a mediana escala de instituciones tales como museos, hospitales, campus universitarios y escuelas.²⁰

XProtect Professional

Es un Software de gestión de vídeo vigilancia sobre IP eficiente con capacidad para un número de cámaras ilimitado, XProtect Profesional es un software de gestión de vídeo, es una plataforma abierta integral para instalaciones de mediano tamaño con multiples edificios.

XProtect Professional ofrece a los usuarios una completa información visual de su instalación de vigilancia con mapas interactivos que revelan las ubicaciones de las cámaras. Las alarmas se muestran directamente en los mapas facilitando la rápida identificación y solución de incidentes en todo el sistema.



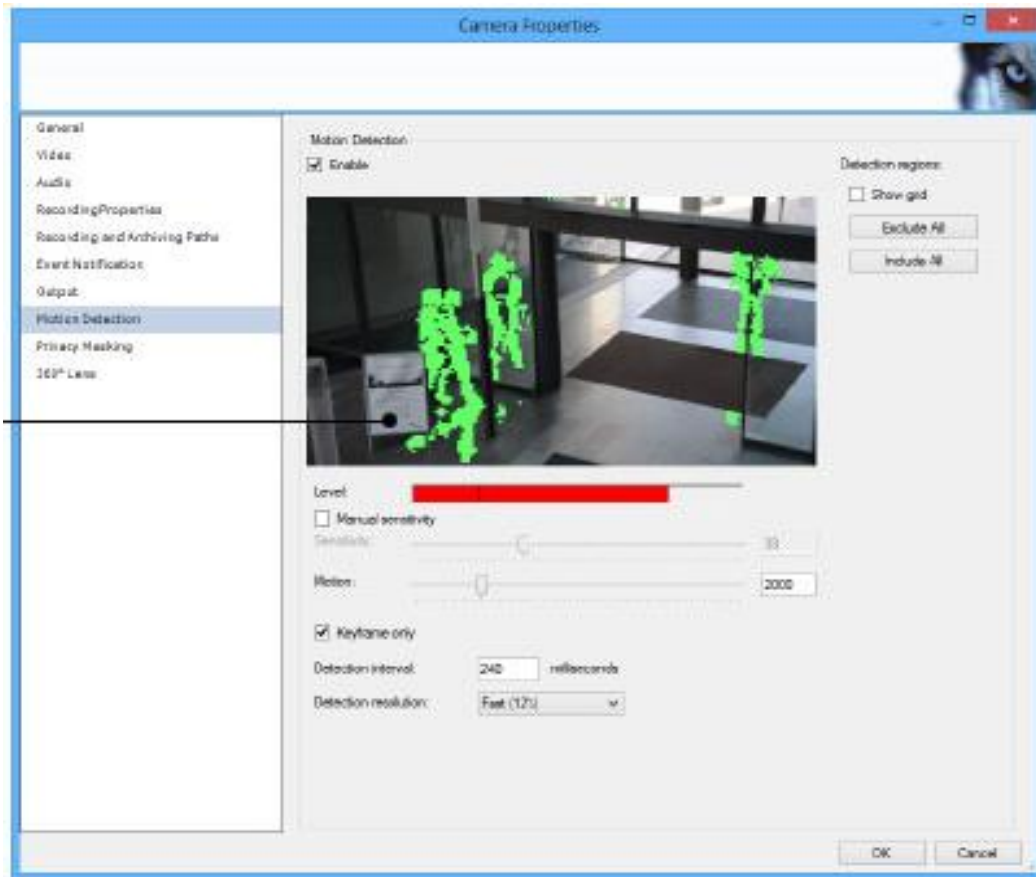
Fuente: <https://www.milestonesys.com>

Figura N° 13. Dispositivos de acceso al Sistema.

- **Detección de movimiento integrada:** las cámaras pueden grabar vídeo cuando detectan movimientos específicos como, por ejemplo, cuando alguien entra en el edificio por la noche.

²⁰ <https://www.milestonesys.com/es/productos/video-management-software/xprotect-professional/>.

- **Herramientas de búsqueda de vídeo:** la Búsqueda avanzada y el Explorador de secuencias permiten a los usuarios ordenar rápidamente grandes cantidades de evidencias para buscar exactamente lo que necesitan.



Fuente: <https://www.milestonesys.com>

Figura N° 14. Herramienta de búsqueda de vídeo.

XProtect: fácil de instalar.

Gracias a los asistentes de configuración automática y detección de cámaras es fácil configurar y empezar a trabajar con XProtect.²¹

2.4.1.2 GENETEC (Security Center).

Plataforma Unificada De Seguridad

²¹ <https://www.milestonesys.com/es/productos/video-management-software/xprotect-professional/>.

Sistema de Control de Sistema De Videos (Synergis)		
Sistema de Control de Sistema de Acceso Synergis		
Sistema de Reconocimiento de Placas de Matrícula (AutoVu)		

Fuente: www.genetec.com

Figura N° 15. Sistemas Básicos de Security Center.

Información Corporativa

Genetec es una plataforma unificada de seguridad fundada en 1997 en Montreal Canadá, Genetec es pionero en la industria de la seguridad física. Es el proveedor líder mundial de soluciones de seguridad unificadas basadas en IP, y tienen los siguientes módulos de seguridad.

- **Video vigilancia (Omnicast)**
- **Control de acceso (Synergis)**
- **Reconocimiento de matrículas de autos (AutoVu)**

Genetec ha liderado por más de 15 años el desarrollo de soluciones unificadas de seguridad

en redes IP de clase mundial. Comenzaron en el año 1997 siendo los pioneros en ofrecer el primer software de administración y gestión de videos en redes IP en la historia de la industria, lo que permitió proporcionarles a los clientes de aquel entonces algo nunca visto, un sistema flexible, la libertad de escoger el hardware, y la facilidad de expandir sus sistemas a través de soluciones poderosas y abiertas que eran muy fáciles de usar.

Hoy en día, Genetec²² es un proveedor global de soluciones de video vigilancia en redes IP, control de acceso, y reconocimiento de placas de vehículos unificadas en una sola plataforma denominada Security Center.

Genetec (Security Center), *“es la plataforma unificada de seguridad de Genetec que combina de manera transparente sistemas de seguridad en redes IP dentro de una única interfaz intuitiva para simplificar sus operaciones”*. Es una plataforma muy adaptable y flexible que brinda una solución de administración totalmente unificada.²³

2.4.1.3 OMNICAST (Sistema De Administración De Videos).

Omnicast es el sistema de administración de videos en redes IP de la plataforma unificada del Security Center que le proporciona a las organizaciones de todo tamaño la habilidad de instalar un sistema de videovigilancia que realmente se adapte a sus necesidades.

Con el soporte a una gran variedad de cámaras, codificadores y equipo CCTV que son líderes en el mercado, Omnicast se puede escalar y se adapta a las exigencias cambiantes de su departamento de seguridad.

²² Genetec Security Center. Sistema de Comunicaciones Unificadas IP.

²³ <https://www.genetec.com/es/soluciones/productos/security-center>.

Omnicast es el VMS líder en la industria IP que proporciona seguridad duradera y flexibilidad para sus instalaciones. Sistema de video que proporciona acceso al sistema ininterrumpido y protección de datos.

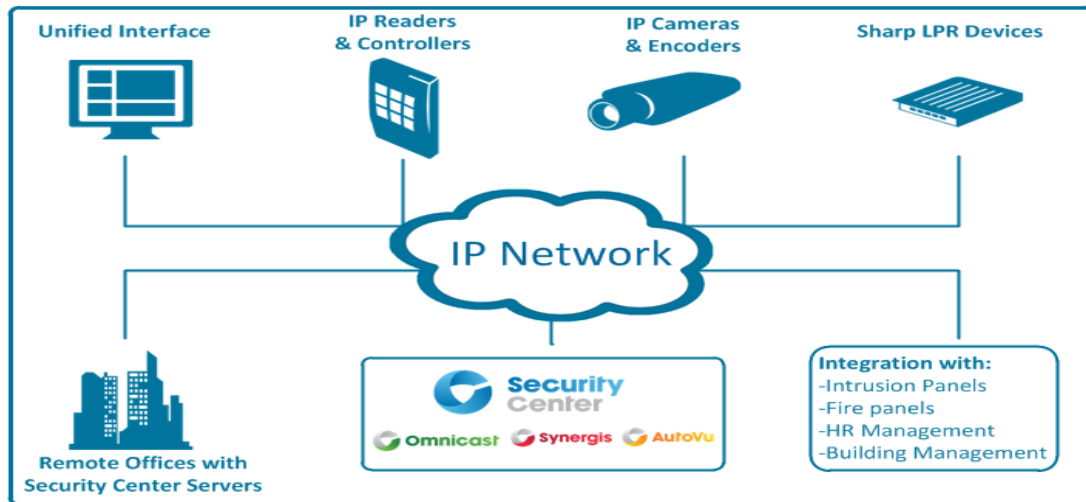
- Incorpora mecanismos de failover y redundancia para garantizar el acceso continuo
- Administrar con eficiencia más flujos de video HD a través de su red IP existente.
- Las capacidades avanzadas de gestión de ancho de banda aseguran que usted puede apoyar más canales de video, y reducir al mínimo los costos de red
- Proteger a las personas y bienes con capacidades de seguridad líderes
- Funciones avanzadas de seguridad permiten a los operadores detectar mejor las amenazas y los incidentes
- Seleccione el hardware que cumple con los requisitos de seguridad y presupuesto
- Amplio soporte para dispositivos de borde IP líderes en la industria y el hardware

2.4.1.4 SYNERGIS, Sistema de Control de Acceso.

Synergis es el sistema de control de acceso IP diseñado para reducir el tiempo de implementación y el costo de su entorno de seguridad.

Se despliega rápidamente en su infraestructura de red IP existente, Reduce el tiempo y el costo de la implementación al aprovechar el hardware de control de acceso existente y la red IP.

2.4.1.5 Arquitectura de Security Center.



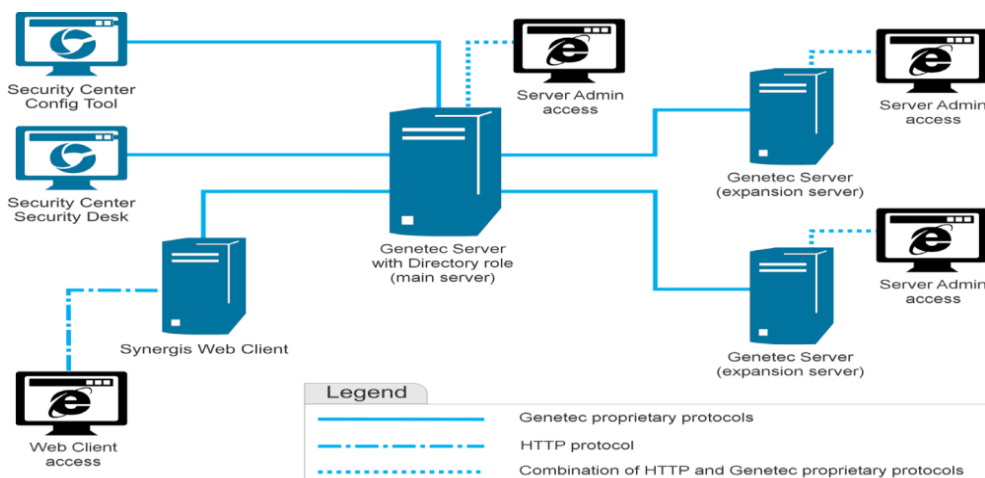
Fuente: <https://www.genetec.com>

Figura N° 16. Arquitectura de Security Center - GENETEC.

Componentes de Security Center

La arquitectura de Security Center se basa en un modelo cliente / servidor, donde todas las funciones del sistema son manejadas por un grupo de equipos servidores distribuidos sobre una red IP.

Cada sistema de Security Center debe tener su propio grupo de servidores. Su número puede variar desde una sola máquina para un pequeño sistema hasta cientos de máquinas para un sistema de gran escala.



Fuente: el autor.

Figura N° 17. Componentes de Security Center – GENETEC.

Los iconos de colores en azul representan los equipos donde están instalados los componentes de servidor y cliente del Centro de seguridad.

La misión de GENETEC es ser líderes en soluciones unificadas de seguridad basadas en redes IP, todo esto hace que se hagan merecedores del respeto y la lealtad de los clientes al proporcionarles valor y calidad con servicios técnicos garantizados a nivel de todo el mundo.

Herramientas y Componentes de Security Center



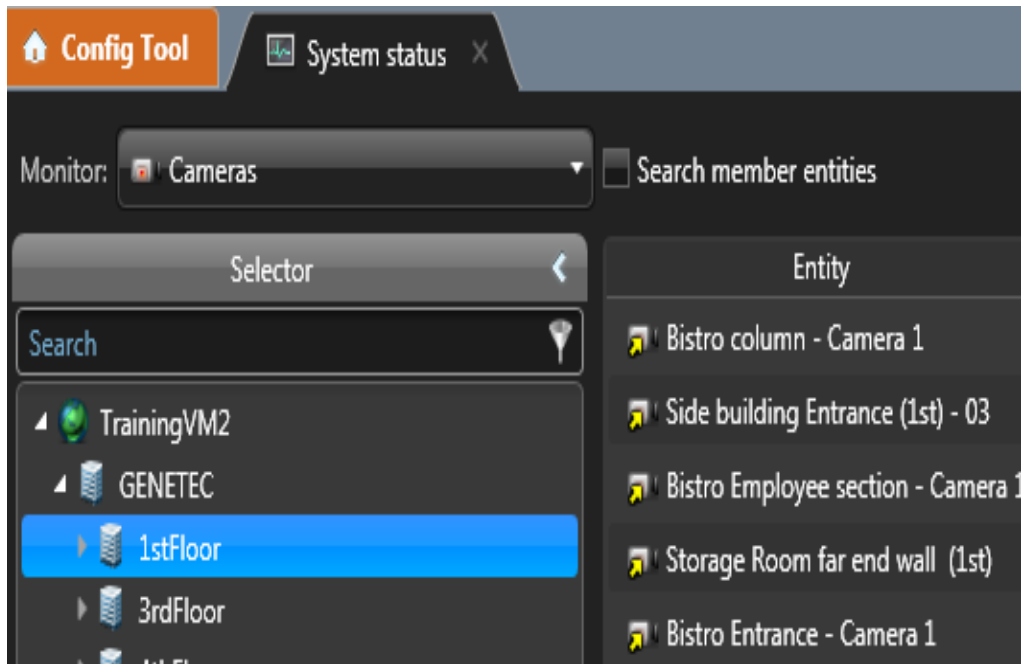
Fuente: el autor.

Figura N° 18. Herramientas y Componentes de Security Center.

Aplicaciones del sistema.

Las aplicaciones y herramientas de configuración del sistema de seguridad varían en su presentación ya que muestran sus nombres y aplicaciones en diferentes colores en la barra de herramientas.

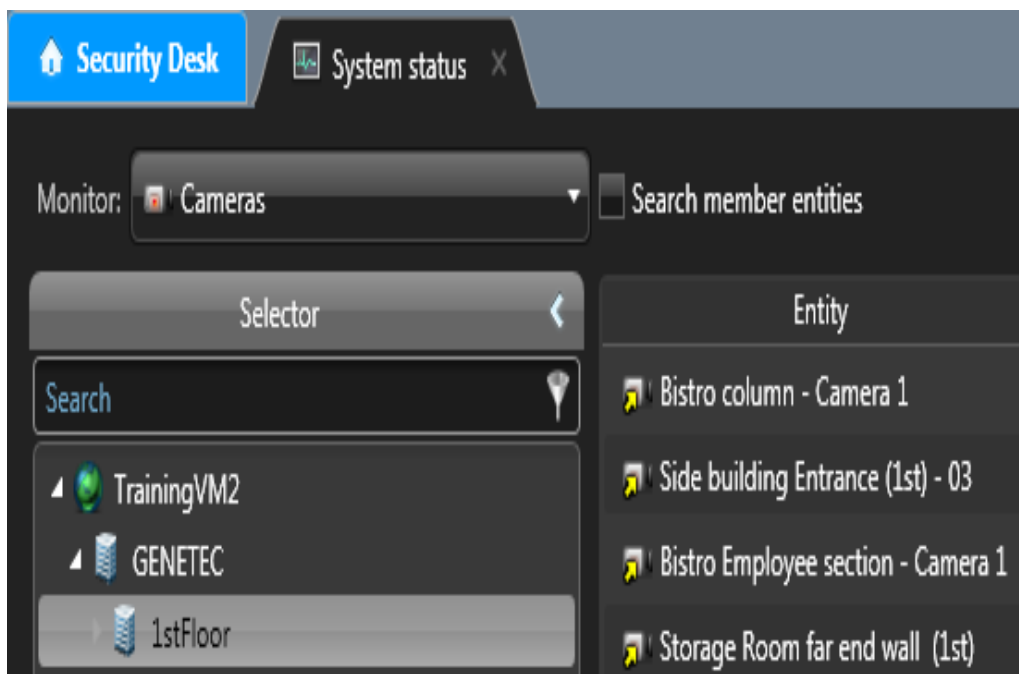
Config Tool es la principal herramienta utilizada para la configuración, la administración del sistema y solución de problemas y es de color tomate como muestra la Figura No. 19.



Fuente: el autor.

Figura N° 19. Herramienta de Config Tool.

Security Desk se utiliza principalmente por los usuarios finales (monitoreo, investigación, informes, etc.). Cuando el usuario ingresa al sistema la barra de herramientas es de color azul.











Fuente: el autor.

Figura N° 20. Herramienta Security Desk

Roles Predeterminados

Tabla No. 1 Roles Predeterminados.

ROLES	DESCRIPCIÓN
<p>Directorio</p> 	<p>Sólo un único Directorio se permite por sistema. El servidor que aloja el Directorio se conoce como el servidor principal. El directorio gestiona: licencias de la aplicación, las conexiones cliente / autenticación, la base de datos de configuración, eventos, auditoría, rastros de actividad, alarmas, incidencias, tareas programadas, macros.</p>
<p>Archiver</p> 	<p>El Archiver es una función específica de Omnicast que es responsable del descubrimiento, el estado, y el control de unidades de vídeo. Todas las comunicaciones entre el sistema y las unidades de vídeo se establecen a través de esta función. El Archiver también gestiona los archivos de vídeo, y lleva a cabo la detección de movimiento cuando no se realiza en la propia unidad de video.</p>
<p>Access Manager</p> 	<p>El Access Manager es una función específica de Synergis que controla y configura las unidades de control de acceso (controladores de puertas), aplica las reglas de acceso y las limitaciones a áreas seguras, y registra todos los eventos de control de acceso.</p>
<p>Administrador de LPR</p> 	<p>El Administrador de LPR es una función específica de AutoVu que gestiona y controla patrulleros y unidades fijas de Sharp. El Administrador de LPR gestiona los datos (lecturas y aciertos) recogidos por las unidades de LPR, controla y actualiza la configuración de las unidades móviles (patrulleros) cada vez que comienzan un nuevo turno.</p>
<p>Media Router</p> 	<p>El Media Router es una función específica de Omnicast que asegura que todos los flujos de vídeo utilizan la ruta más óptima para llegar desde su origen hasta su destino, mientras realiza toda transformación necesaria (por ejemplo, de unicast a multicast, o de IPv4 a IPv6).</p>
<p>Zone Manager</p> 	<p>El Zone Manager gestiona zonas y desencadena eventos o relés de salida basado en las entradas configuradas para cada zona. El Zone Manager también registra los eventos de la zona en una base de datos para los informes de actividad de zona.</p>
<p>Health Monitor</p> 	<p>El Health Monitor es la función encargada de monitorear las entidades del sistema, tales como servidores, funciones, unidades y aplicaciones cliente para cuestiones de salud. Los eventos de salud se registran en una base de datos con el propósito de la presentación de informes y análisis estadístico. Los errores de sistema actuales se informan en tiempo real en la bandeja de notificación de la aplicación.</p>
<p>Administrador de Reportes</p> 	<p>El papel del Administrador de Reportes automatiza envío de reporte por email y la impresión, basado en los horarios.</p>

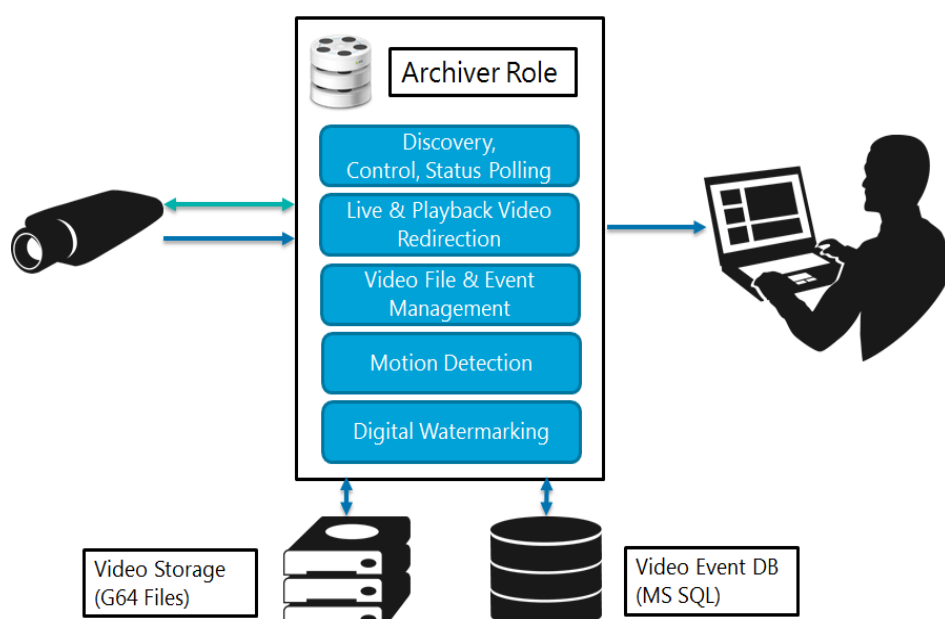
Grabación de la cámara

La pestaña de grabación de la cámara le permite configurar los ajustes de grabación por defecto aplicados a todas las cámaras controladas por el Archiver. Los arreglos por defecto pueden ser reemplazados por los ajustes de grabación de cada cámara.

Archiver

El Archiver es responsable del descubrimiento, el control y el sondeo de estado de unidades de vídeo. Todas las comunicaciones entre las unidades del sistema y de vídeo se establecen a través de este rol realizado por el archiver.

Todos los eventos generados por las unidades (de movimiento, análisis de vídeo) transmitidos por el Archiver a las partes interesadas en el sistema. El Archiver también administra los archivos de vídeo y realiza detección de movimiento en unidades de vídeo que no admiten esta función.



Fuente: www.Genetec.com

Figura N° 21. Función Del Archiver.

Modos de Grabación

El Archiver puede aplicar diferentes modos de grabación en diferentes momentos.

Tabla N° 2. Modos de Grabación

MODO DE GRABACIÓN	DESCRIPCIÓN
APAGADO	Grabación está apagada. Este modo evita que la grabación se lleve a cabo, ni siquiera cuando se activa una alarma.
CONTINUÓ	Graba continuamente. La grabación no puede ser detenida por el usuario.
EN MOVIMIENTO/MANUAL	Graba cuando la grabación se desencadena por una acción (como la grabación en Inicio, Añadir favorito, o una alarma Trigger), a través de la detección de movimiento, o manualmente por el usuario. En este modo, el botón de grabación en la Seguridad Escritorio aparece gris () Cuando el Archiver no está grabando, cuando el rojo que es la grabación, pero puede ser detenido por el usuario, O el rojo con el bloqueo () Cuando se está grabando, pero no puede ser detenido por el usuario (en movimiento o grabación de alarma).

Flujos de Vídeo

Sólo un único flujo de vídeo se activa por defecto (otros pueden ser activadas manualmente) La calidad del video se establecerá en medio de la mayoría de las cámaras. (Algunas unidades tienen una resolución predeterminada superior).

El Flujo de red se establecerá en:

- **Unicast UDP** (Multicast Cuando está disponible)
- **Mejor Disponible** (Cuando Multicast no está disponible)

Unicast.

El método de transmisión de la información lo realiza entre 2 nodos, emisor y receptor, *unicast* se usa actualmente en Internet.²⁴

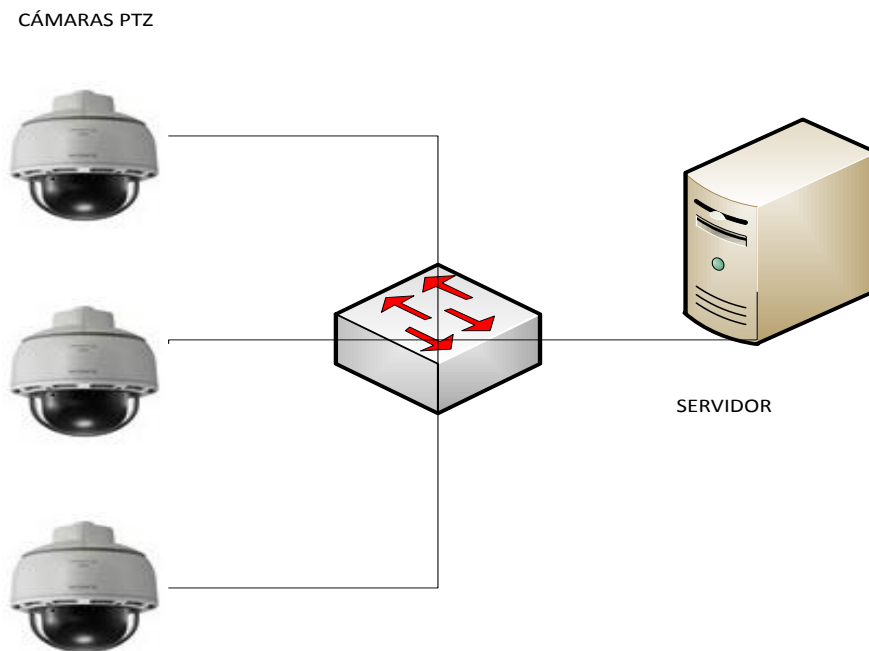


Figura N° 22. Método de Trasmisión Unicast.

Fuente: el autor.

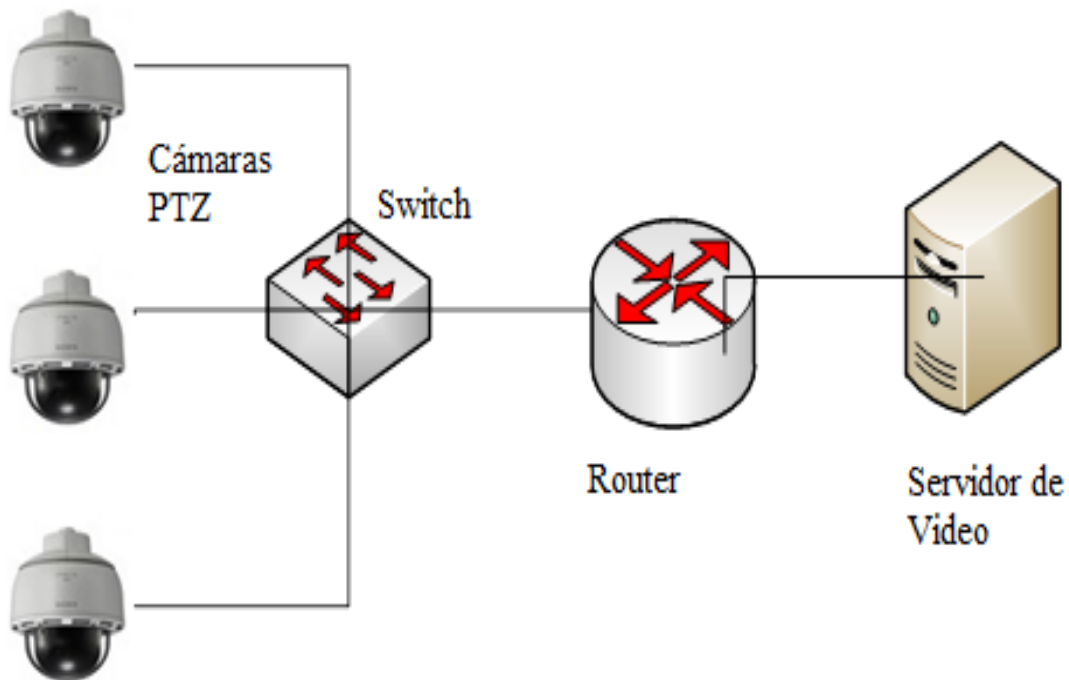
Multicast.

Multicast, tienen como característica el envío de la información de forma simultanea, y sera receptada los paqueres por un grupo determindado de receptores. Ahorra considerablemente el ancho de banda cuando se envia una gran cantidad de datos.

La información se envía desde su origen pasando por la parte central de la red y se multiplica o distribuye hasta llegar a los usuarios finales.²⁵

²⁴ **Unicast.** Recuperado de: <https://es.wikipedia.org/wiki/Unicast>

²⁵ **Multicast.** Recuperado de: <http://www.delfirosales.com/2009/06/metodos-de-transmision-unicast.html>



Fuente: el autor.

Figura N° 23. Método de Trasmisión Multicast

Gestión del control de ancho de banda y almacenamiento

Omnicast soporta las siguientes características para ayudar a reducir las necesidades del tráfico de la red y la capacidad de almacenamiento:

- Transmisión de Multicast
- Redirección de vídeo por los Servidores Genetec (redirectores)
- Formatos de compresión de vídeo (MPEG-4, MJPEG, H.264, etc.)
- Velocidad de cuadros, intervalo de fotograma clave
- Grabación de sólo fotogramas clave
- Opciones de codificador como: Calidad de imagen, modo de filtro de entrada, el modo de compresión, etc.
- Control de la tasa de bits
- Grabación por eventos

- Mejora de calidad por evento / grabación manual
- Uso de la secuencia de vídeo (en vivo, grabación, remota, etc.)
- Cambio automático de flujo

Consideraciones Adicionales del Servidor

Cuando la transmisión de vídeo no está en multicast desde la cámara, el cálculo máximo de rendimiento debe incluir secuencias de cámara siendo redirigidos por el Archiver.

- Un servidor más potente que la especificación de gama alta no necesariamente aumentará la capacidad máxima.
- La misma configuración en una máquina virtual reducirá el desempeño en un 20%.
- Una tarjeta dedicada de red (NIC²⁶) debe ser asignado por cada Archiver al utilizar la virtualización.
- Máquina virtual debe ejecutarse en Windows Server 2008 R2 y con Hardware VMWare Ready.
- No se admite Windows 2003/2008 Server que ejecute un controlador de dominio.

Lista de Comprobación Previa a la Instalación.

Antes de instalar o actualizar Security Center, debe comprobar y realizar lo siguiente:

- Revisar las conexiones de red entre los servidores, estaciones de trabajo y unidades.
- Revisar las conexiones y los ajustes de red unicast y multicast.
- Revisar que los requerimientos mínimos de hardware (servidores y estaciones de

²⁶ NIC. Network Interface Card, NIC

trabajo) así como de software (windows, navegador web, etc) se cumplen.

- Deshabilitar la función de ahorro de energía en sus servidores.
- Revisar que sus servidores no son controladores de dominio.
- Revisar el orden de las tarjetas de interfaz de red (NIC).

Portal de Asistencia Técnica de Genetec - GTAP

GTAP

El GTAP es un área segura donde los usuarios del sistema GENETEC pueden ingresar y leer detenidamente la extensa base de conocimiento y documentación de productos, descargar software, contribuir en el foro de clientes o abrir una solicitud de soporte para acelerar el soporte.

“El acceso de GTAP es GRATIS para todos los clientes y socios de negocios de Genetec. Regístrese ya, y descubra una variedad de recursos para soporte técnico que le ayudarán a instalar, mantener y utilizar todas las soluciones en seguridad innovadoras de Genetec”.

(GTAP , 2016)

ACCESO GTAP.

Contacte al Centro de Asistencia Técnica de Genetec

+1 514.856.7100

De lunes a viernes de 08:00am a 8:00pm EST.

Número telefónico para llamadas gratis

Canadá & EE.UU.

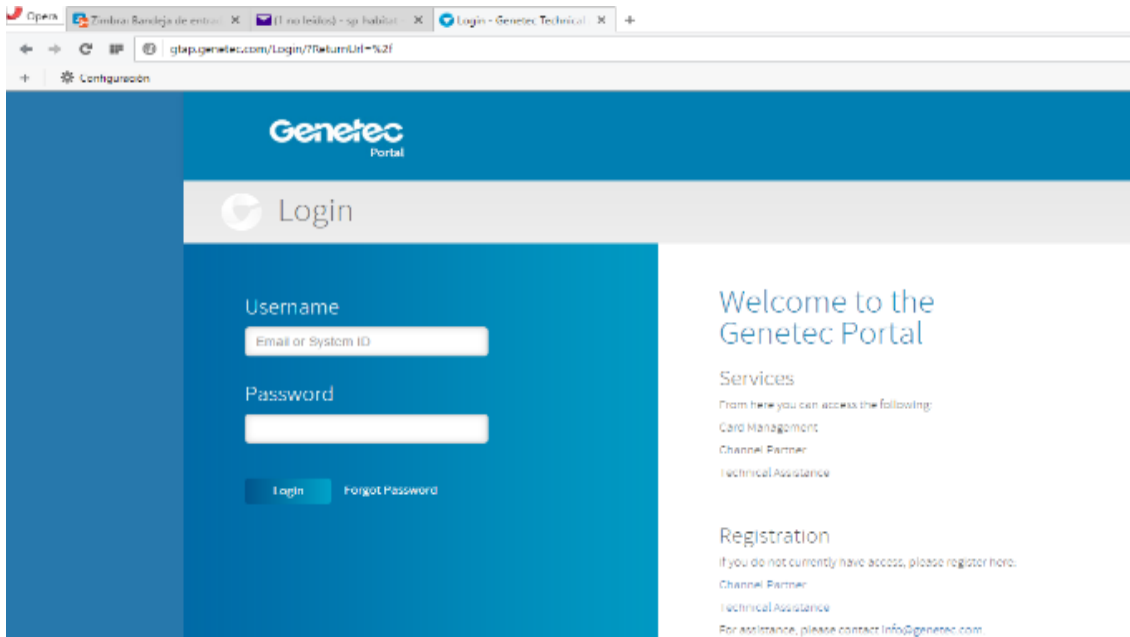
+1 866.338.2988

De lunes a viernes de 08:00am a 8:00pm EST

Europa

+800.100.11111

De lunes a viernes de 09:00am a 6:00pm CET



Fuente: gtap.genetec.com

Figura N° 24. Portal de Asistencia Técnica de Genetec - GTAP.

Centro de Asistencia Técnica de Genetec

El soporte es brindado por un equipo de profesionales altamente dedicados, estarán disponibles para ayudar en cada incidente que el sistema de video vigilancia GENETEC necesite.



Fuente: <https://gtap.genetec.com>

Figura N° 25. Portal de Asistencia Técnica de Genetec - GTAP.

Socios de Cámaras



Fuente: <http://www.genetec.com/es/socios>

Figura N° 26. Socios de Cámaras.

Plataforma Security Center

- Es una sola aplicación para vigilar e investigar su entorno de seguridad.
- Es una única plataforma de seguridad para gestionar dispositivos de seguridad perimétricos.
- Es una única plataforma de seguridad para fusionar la intrusión, y sistemas de terceros.
- Es una única plataforma de seguridad que unifica video vigilancia, control de acceso y sistemas de lectora de tarjetas.

CAPITULO III

3.1. Funciones Tecnicas De Los Sistemas De Video Vigilancia IP.

3.1.1. Comparación Funcional de los Sistemas.

El propósito de este capítulo es proporcionar un análisis comparativo del rendimiento operativo y funcional de los sistemas de video vigilancia que son VDI vs GENETEC, se verificaran requisitos operativos mínimos que el sistema de seguridad debe cumplir: configuración, productos, componentes y materiales que son necesarios para la óptima operatividad y desempeño del sistema de video vigilancia dentro de las instalaciones del Aeropuerto Internacional Mariscal Sucre.

Tabla N° 3. Comparación técnica de los sistemas de video vigilancia.

CARACTERÍSTICAS	COMPATIBILIDAD	XProtect VDI		GENETEC	
	FUNCIONALIDAD	Cumple	No Cumple	Cumple	No Cumple
Instalación y configuración	Detección automática de cámaras para iniciar la configuración dentro del sistema.	OK		OK	
Actualizaciones	La actualización de un reléase nuevo debe ser de forma automática.	OK		OK	
Acceso y Administración	Acceso de remoto con cualquier dispositivo que necesite el usuario, móvil o PC.	OK		OK	

Alquiler de parking (vehículos)	Un software de reconocimiento de placas de vehículos. Es una forma sencilla de identificar y controlar el acceso de vehículos, por ejemplo, para barreras de entrada/salida, aparcamientos y peajes	OK		OK	
Función SDK	Un software / Kits para usar como controladores de dispositivos. Necesario para el desarrollo de drivers o controladores, y unificar varios sistemas incompatibles.	-	-	OK	
Función de Active Directory	La función SDK basado en la web expone los métodos de Security Center y los objetos como servicios Web para apoyar la interoperabilidad entre plataformas.	-	-	OK	
Máquina virtual	Máquina virtual debe ejecutarse en Windows Server 2008 R2 y con Hardware VMWare Ready	OK		OK	
Titulares de Tarjetas, Credenciales, Manejo de Visitantes	Reglas de control de acceso se basan en los titulares de tarjetas, no credenciales	-	-	OK	
Manejo de Eventos	Los tipos de eventos generados por el sistema que varían de una entidad a otra. Por ejemplo: Acceso denegado a un titular de la tarjeta, La señal perdida en una cámara.	-	-	OK	

<p>Manejo de Eventos y Acciones.</p>	<p>Una acción es una función programable por el usuario que puede ser activado como una respuesta automática a un evento (Puerta mantenida abierta por mucho tiempo, o un objeto desatendido) o ejecutado de acuerdo a una tabla de tiempo específico.</p>	-	OK	OK	
<p>Intrusión Role Manager</p>	<p>Eventos de intrusión se registran por el administrador de intrusiones para los informes de actividad de intrusos. Usted puede decidir por cuánto tiempo desea mantener antes de que se purguen de la base de datos Administrador de intrusiones</p>	-	-	OK	
<p>Reportes</p>	<p>Las tareas programadas y el evento automatizado a mecanismo de acción a menudo se utilizan para automatizar el envío de correos electrónicos e informes.</p>	-	OK	OK	
<p>Partes y Repuestos</p>	<p>Es compatible con cualquier fabricante de los dispositivos de comunicación</p>	-	-	OK	

Integración con otros sistemas de seguridad.	Flexibilidad para trabajar de forma integrada con sistemas de seguridad.	OK. Tiene Problemas de lentitud	-	OK	
Misaicos	Permite poner en mosaicos más de 16 cámaras.	OK, Tiene Problemas de lentitud para manipular cámaras	-	OK	
Solución de Problemas y Mantenimiento	La tarea de inventario de hardware genera un informe de las unidades de hardware matriculadas en el sistema (unidades de vídeo, las unidades de control de acceso, unidades LPR, paneles de intrusión).	-	-	OK	
Herramienta de Sustitución de Unidad	La herramienta de sustitución de unidad se utiliza para sustituir un dispositivo de hardware que ha fallado por otro compatible, garantizando que los datos asociados a la antigua unidad se transfieren a la nueva.	-	-	OK	

Una vez realizado el análisis técnico en la anterior Tabla No.3, donde se detalla las principales características y bondades de los sistemas, se ha determinado que el sistema GENETEC brinda todas las garantías técnicas en funcionalidad y operatividad sobre tecnología IP, razón por la cual será el sistema elegido para reemplazar al sistema análogo antiguo.

3.2. Elección de Tecnología entre VDI vs GENETEC.

GENETEC, es la arquitectura elegida para la implementación dentro de las instalaciones del Aeropuerto. Esta basada en tecnología IP, cumple con todas las características técnicas que la seguridad aeroportuaria necesita *“El Security Center es la plataforma unificada de GENETEC, combina de manera transparente sistemas de control de accesos basadas en IP dentro de una única interfaz intuitiva para simplificar sus operaciones”*²⁷. GENETEC está afiliada a muchas asociaciones internacionales industriales, donde las soluciones satisfacen las exigencias y requerimientos empresariales.

GENETEC, tiene una vinculación con las asociaciones más importantes de seguridad aeroportuarias, esto hace que brinde un soporte dentro de la seguridad aeroportuaria.

- Asociación Americana Para Los Ejecutivos De Aeropuertos (American Association Of Airport Executives (Aaae).
- Asociación Americana de Autoridades Portuarias (American Association of Port Authorities (AAPA).
- Consejo de Consultores Aeroportuarios (Airport Consultants Council (ACC).

3.2.1. Sistema de Gestión Monitoreo GENETEC.

GENETEC, es una arquitectura Cliente/Servidor debido a la centralización de la información procesada por los diferentes módulos que brinda. El cliente realiza peticiones al servidor, el servidor es quien da respuesta a la petición del cliente.

Características Técnicas de GENETEC.

²⁷ <http://www.genetec.com/es/acerca/noticias/centro-de-prensa/notas-de-prensa/genetec-presenta-la-nueva-versión-de-su-security-center>

- **Herramientas y Componentes de Security Center**

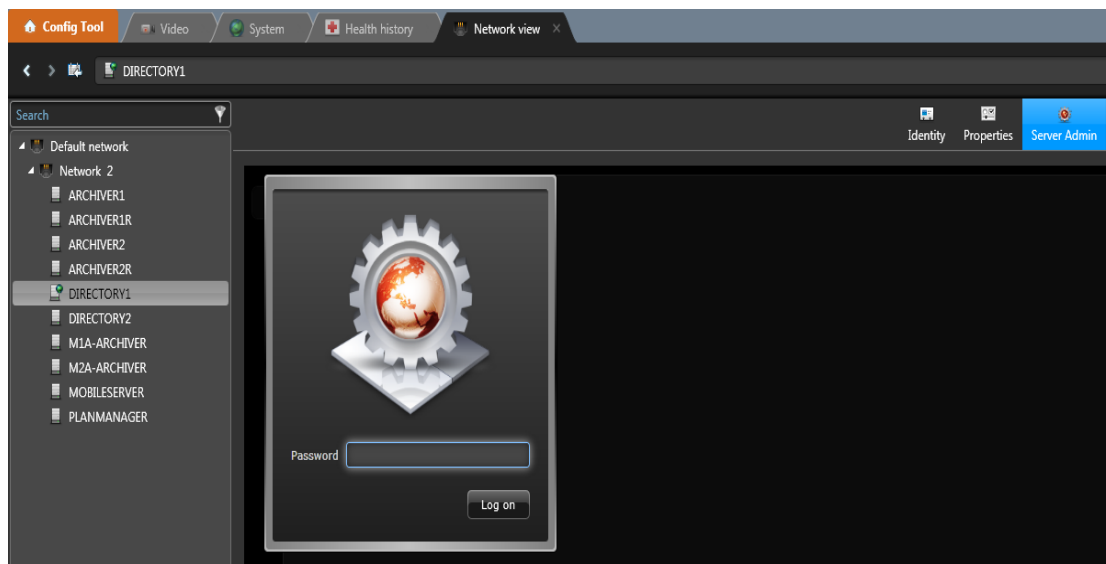


Fuente: el autor

Figura N° 27. Herramientas y Componentes de Security Center.

- **Aplicaciones Config Tool.**

Es la principal herramienta utilizada para la configuración y la administración avanzada del sistema y solución de problemas.

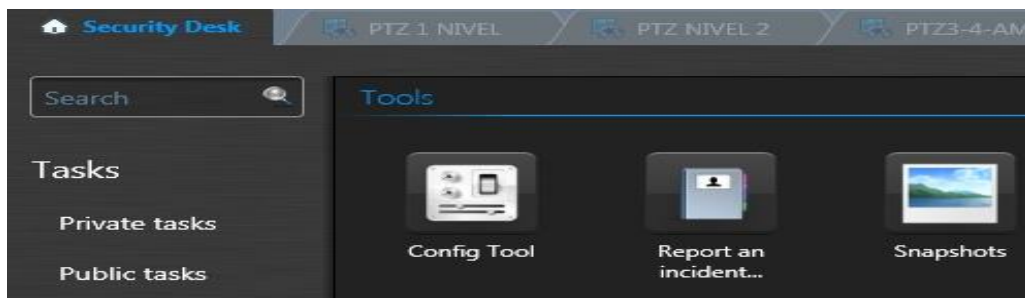


Fuente: el autor

Figura N° 28. Acceso como Administrador de GENETEC.

- **Security Desk**

El software que utiliza el sistema de video vigilancia como cliente es “Security Desk”, utiliza principalmente para los usuarios finales (monitoreo, investigación, informes, etc). Cuando el usuario ingresa al sistema, la barra de herramienta muestra de color azul las letras como se muestra en la Figura No. 29.

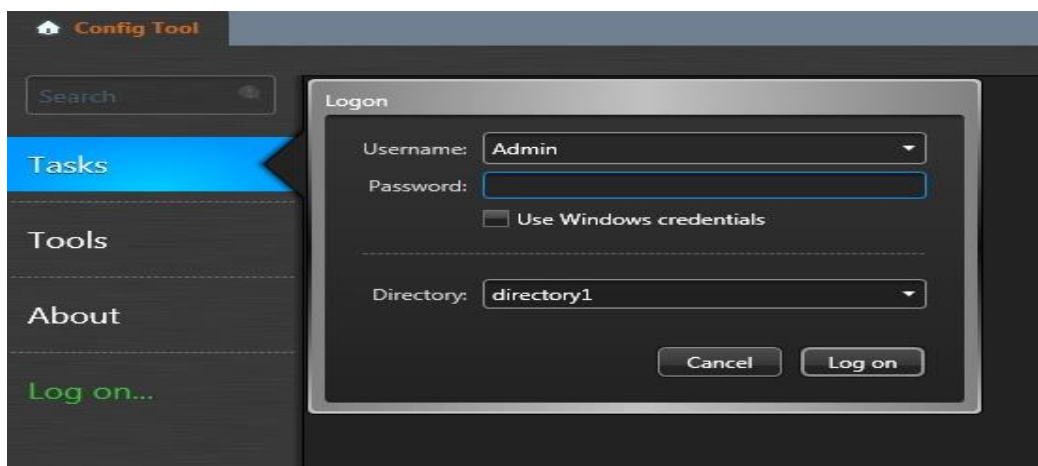


Fuente: el autor

Figura N° 29. Herramienta Security Desk del Cliente.

- **Servers**
 - **Server Admin.**

El servidor de Genetec Server puede ser instalado en Windows server 2008R1/2012R2 y sus bases de datos en SQL Server 2008 R2 Express/Standard/Enterprise. Cuando el usuario Administrador ingresa al sistema, la barra de herramienta muestra de color tomate las letras como se muestra en la Figura No. 30.

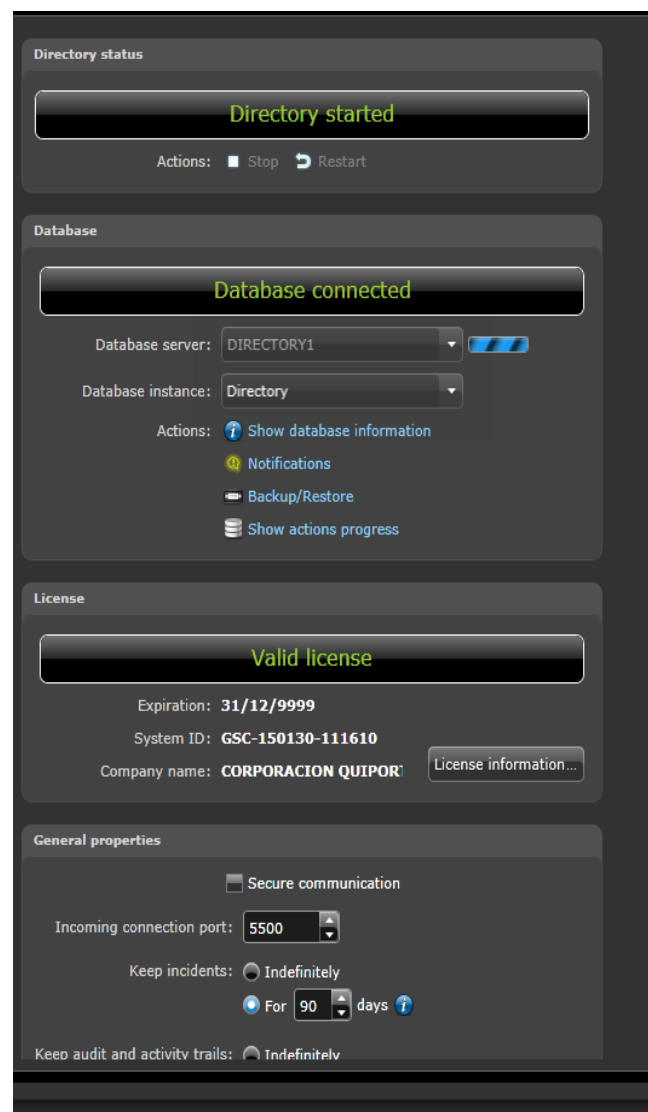


Fuente: el autor

Figura N° 30. Herramienta Config Tool.

- **Servidor Principal (Main Server)**

El servidor principal es el único servidor en el sistema que aloja la función del Directorio. El Directorio es el papel que le da a su sistema su identidad. Todos los otros servidores en el sistema deben conectar con el servidor principal a fin de ser parte del mismo sistema.



Fuente: el autor

Figura N° 31. Herramienta del Servidor Principal²⁸

Se puede tener sólo un servidor principal en todo el sistema de Security Center.

²⁸ **Figura N° 31.** Herramienta del Servidor Principal. Elaborado por: El Investigador (2016).

Roles del servidor.

	<p>REPORT MANAGER.</p> <p>Monitorea el estado de las entidades del sistema para registrarlo en una base de datos de salud.</p>
	<p>ACCESS MANAGER.</p> <p>Gestiona unidades de video y graba archivos de video</p>
	<p>ZONA MANAGER.</p> <p>Gestiona zonas, grupos de entradas</p>
	<p>MEDIA ROUTER.</p> <p>Gestiona controladores de puertas y graba los eventos de las puertas en una base de datos.</p>
	<p>LPR MANAGER.</p> <p>Gestiona la configuración del sistema y acepta conexiones del cliente.</p>
	<p>DIRECTORY.</p> <p>Gestiona y ejecuta la autorización de informes</p>
	<p>HEALTH MONITOR.</p> <p>Entiende, la topología de red para dirigir paquetes de video, ruta del origen al destino.</p>
	<p>ARCHIVER.</p> <p>Gestiona cámaras y Patrones de móviles.</p>

Fuente: el autor

Figura N° 32. Funciones Del Servidor Genetec.

- **Qué es una Función o Rol.**

Una Función (Rol) es un módulo de software que realiza un trabajo específico en Security Center. Por ejemplo, puede asignar funciones para el guardado de vídeo, para el control de un grupo de unidades, o para la sincronización de los usuarios de Security Center con su servicio de active directory de empleados de la empresa.

- **Servidor de expansión (Expansion Server)**

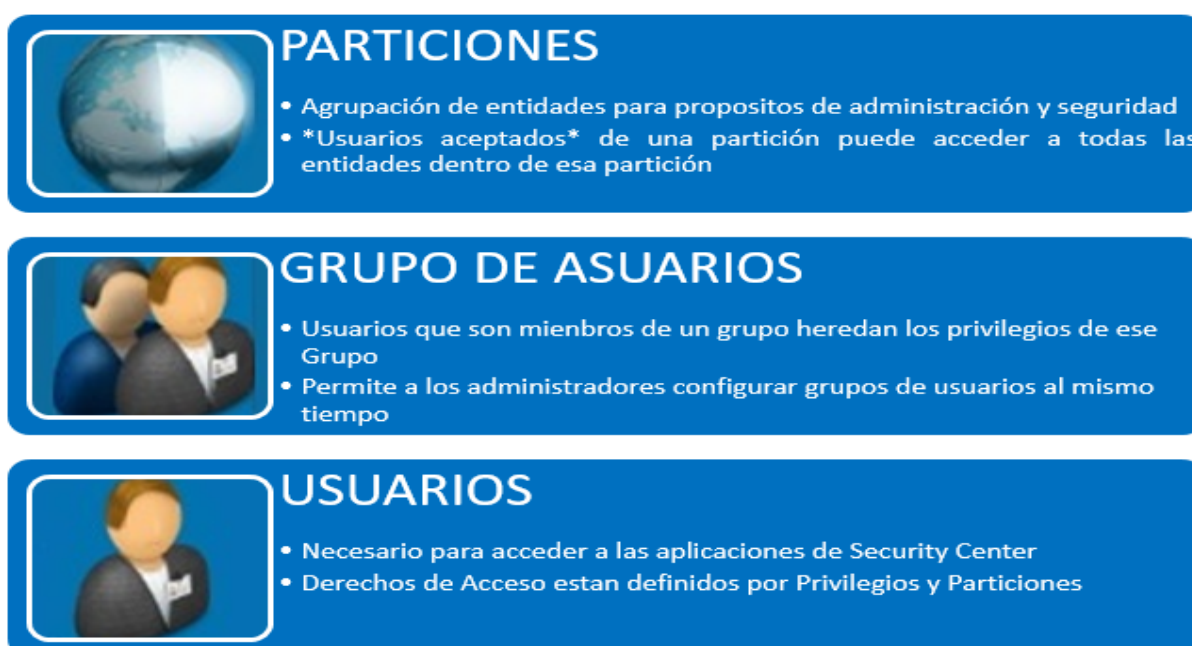
El servidor de expansión es cualquier equipo que no sea el servidor principal que se agrega a su sistema para aumentar su potencia total de computación. Un servidor de expansión debe conectarse al servidor principal y puede albergar cualquier función en Security Center, excepto la función de Directorio.

Se puede agregar servidores de expansión en cualquier momento y dependiendo del requerimiento de ampliación del sistema de video vigilancia IP.

- **Secuencia De Configuración Recomendada de Usuarios.**

- 1. Definición de las particiones.**

Identificar las partes del sistema que son relativamente independientes entre sí, y crear un perfil de usuarios con atributos de administradores y operadores del sistema que no tienen mayor privilegio para realizar modificaciones dentro del sistema.



Fuente: el autor

Figura N° 33. Particiones de Usuarios

2. Definir grupos de usuarios.

Identificar los grupos de usuarios que comparten las mismas funciones y responsabilidades, y crear un grupo de usuarios para cada uno. Por ejemplo, todos los operadores de seguridad pueden formar un grupo, y todos los investigadores pueden formar otro grupo.

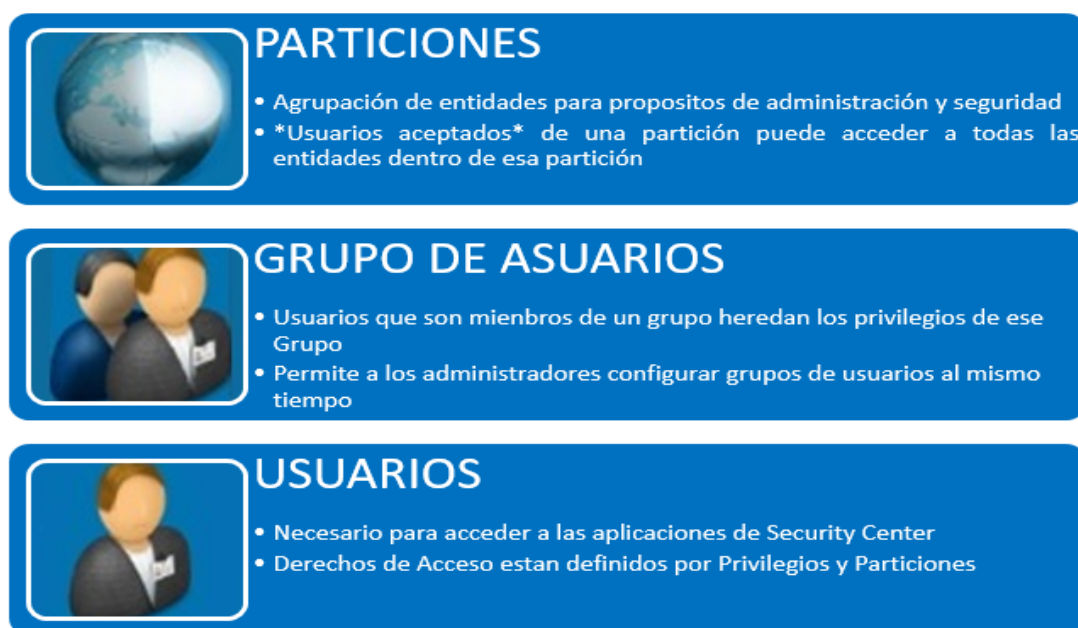


Fuente: el autor

Figura N° 34. Grupos de Usuarios.

3. Definir Usuarios.

Define los usuarios individuales y añadirlos como miembros de los grupos de usuarios ya creados, tratando de agregarlos como miembros del grupo más pequeño. Un usuario puede pertenecer a varios grupos de usuarios. Cada entidad de usuario hereda todo, desde el grupo de usuarios de los padres, puede recurrir a configuraciones individuales sólo para las excepciones.



PARTICIONES

- Agrupación de entidades para propósitos de administración y seguridad
- *Usuarios aceptados* de una partición puede acceder a todas las entidades dentro de esa partición

GRUPO DE ASUARIOS

- Usuarios que son miembros de un grupo heredan los privilegios de ese Grupo
- Permite a los administradores configurar grupos de usuarios al mismo tiempo

USUARIOS

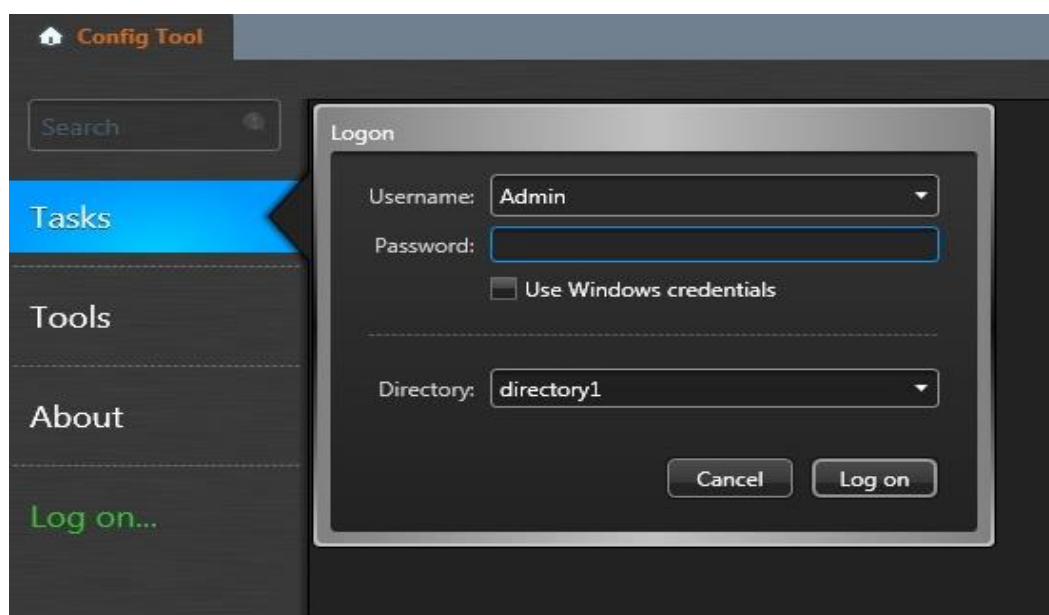
- Necesario para acceder a las aplicaciones de Security Center
- Derechos de Acceso estan definidos por Privilegios y Particiones

Fuente: el autor.

Figura N° 35. Roles y Usuarios.

- **Gestión de los privilegios y derechos de acceso.**

Hay cientos de posibles privilegios de usuario. Para una gestión más fácil, en sistemas más grandes, los privilegios de un usuario tienden a definirse en su nivel de grupo de usuarios más que el nivel de usuario individual.



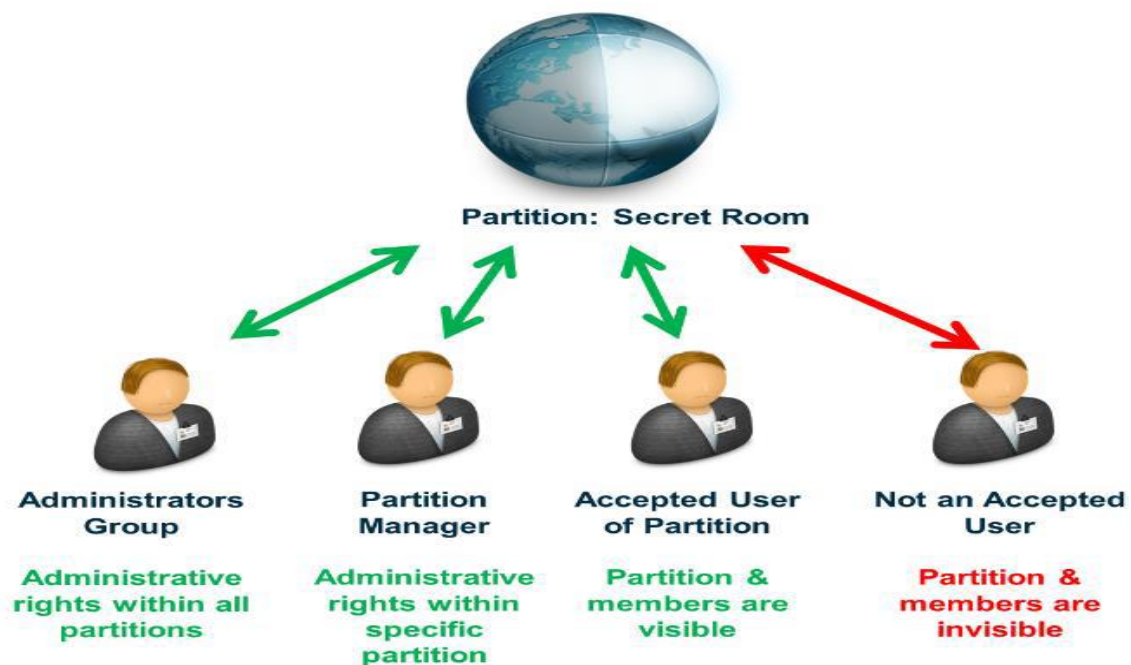
Fuente: el autor.

Figura N° 36. Privilegio de Usuarios GENETEC.

- **Particiones**

Las particiones se utilizan para dividir un gran sistema en subsistemas más pequeños. Esto tiene dos ventajas:

Reduce el alcance del trabajo de un usuario para que sea más manejable. Si un usuario sólo tiene que ver con una parte del sistema (un sitio en un sistema multi-site), es mejor para el operador por las entidades que no tienen nada que ver.



Fuente: www.genetec.com

Figura N° 37. Roles y Usuarios.

- **Selección de red del cliente.**

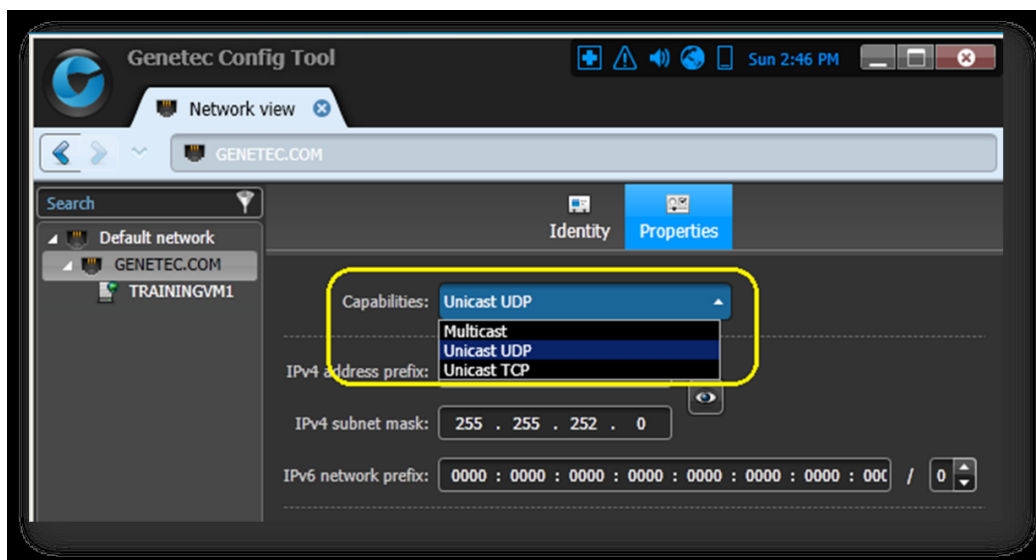
Mientras que Security Desk y Config Tool utilizan una función de "*Detección Automática*" para determinar en qué red se encuentra la estación de trabajo, puede forzar su estación de trabajo en una red específica utilizando el menú opciones de la aplicación cliente.



Fuente: el autor.

Figura N° 38. Autodetección de IP dentro de la Red LAN.

- **Capacidades de Red Multicast/Unicast**



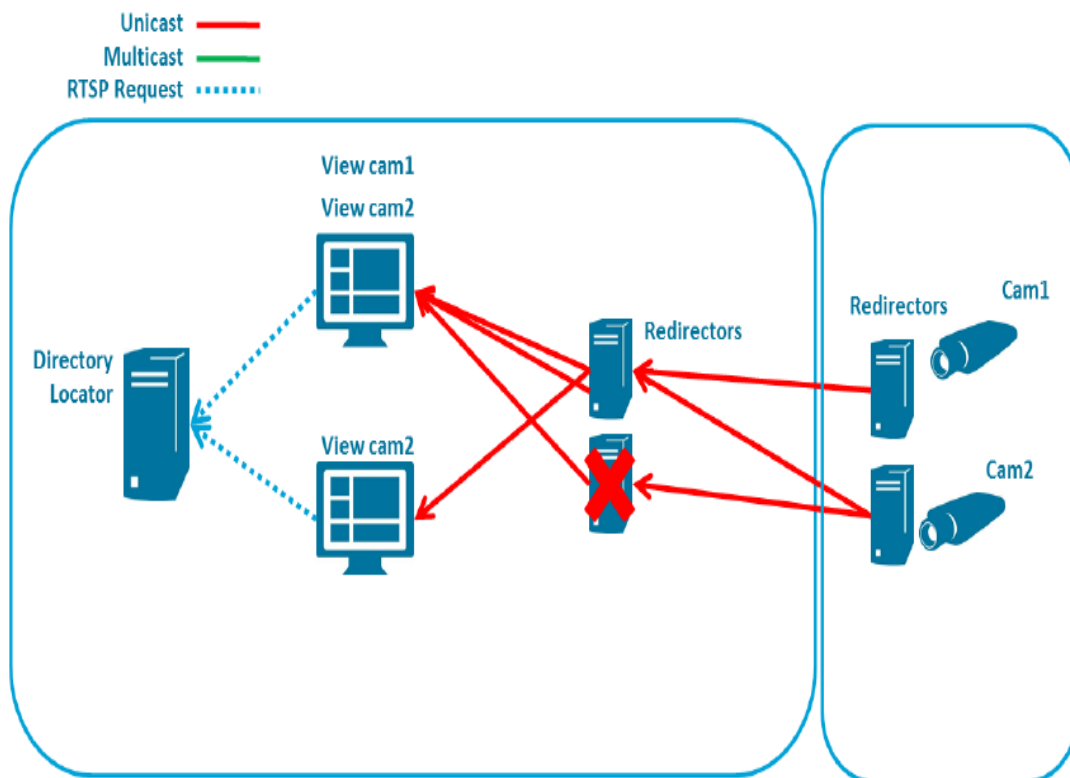
Fuente: el autor.

Figura N° 39. Capacidad de la Red LAN.

- **Multicast:** Cuando se envía grandes cantidades de datos el método multicast ahorra considerablemente el ancho de banda en la red, debido a que la mayor parte de los datos se envían solo una vez.
- **Unicast:** Método de transmisión sencillo, lo realiza entre 2 nodos (emisor y receptor)

- **Failover Redirector**

Si un redirector se desconecta, el cliente solicitará la secuencia de vídeo y la obtendrá de un redirector disponible.



Fuente: el autor.

Figura N° 40. Failover Ridirector.

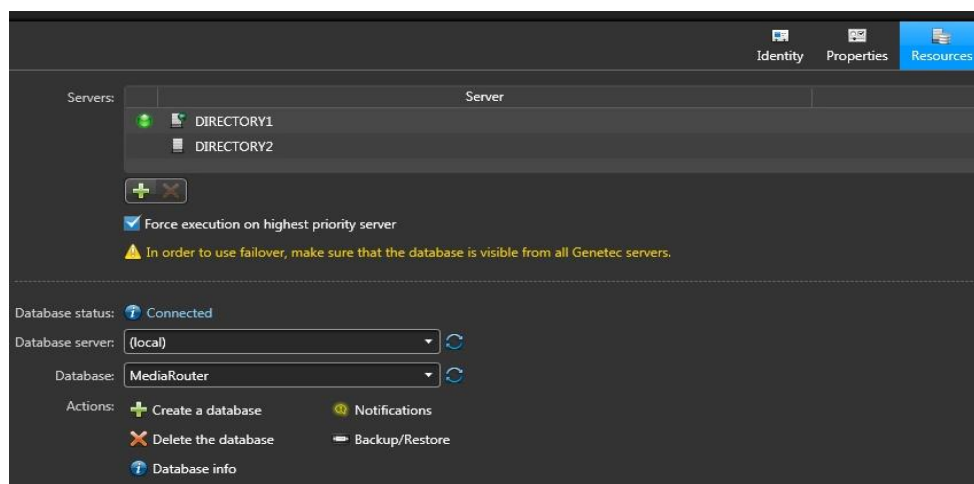
- **Opciones de Failover**

Para asegurarse de que hay un acceso ininterrumpido y protección de datos para el sistema, Security Center ofrece las siguientes características de alta disponibilidad:

- **Failover de Directory.** Se asegura de que la función Directory está disponible si su servidor principal falla. La función Directory se encarga del failover para todos las demás funciones, así que es importante que la función Directory esté disponible en todo momento.
- **Balanceo de carga Directory.** Un beneficio del failover del Directory. El Directorio se

puede ejecutar simultáneamente en un máximo de 5 servidores para compartir la carga de trabajo de la función Directory. Todos los servidores que están configurados para failover del Directorio se utilizan automáticamente para el equilibrio de carga.

- **Failover de Base de datos (Sólo para la función Directory).** Protege la base de datos del directorio, usando uno de los siguientes métodos:
 - **Copia de seguridad y restauración.** Realiza una copia de seguridad de su base de datos, y se restaura si se produce el failover.
 - **Microsoft SQL Server Database Mirroring.** Las instancias de base de datos se mantienen en sintonía con Microsoft SQL Server.
- **Failover Archiver.** Se asegura de que la función de Archiver y los archivos de vídeo están todavía disponibles si el servidor principal del Archiver falla. Failover de otras funciones. Se asegura de que las otras funciones en el sistema están todavía disponibles si falla su servidor primario.

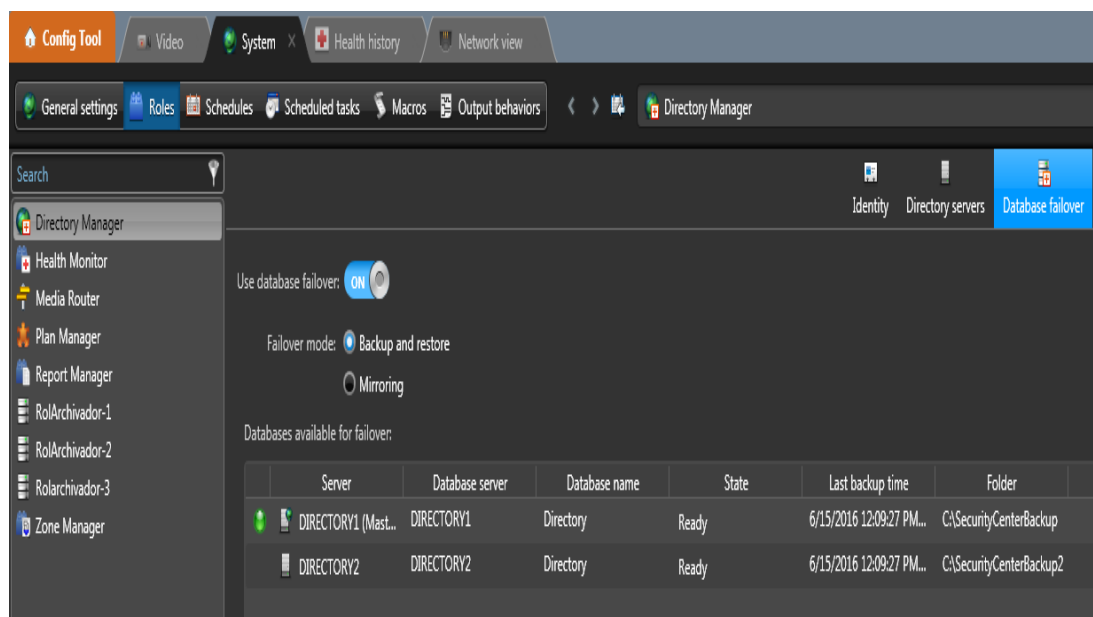


Fuente: el autor.

Figura N° 41. Configuración del Failover del Servidor Principal de GENETEC.

El orden de aparición de los servidores de la lista corresponde al orden en el que se recogen si se produce failover. Cuando falla el servidor principal, la función cambia automáticamente al siguiente servidor de la lista.

Después de que se produce el failover, si se desea que el servidor principal vuelva a tomar el control de la función una vez que se restaura, seleccionariaos la ejecución de tareas sobre la opción de más alta prioridad del servidor. Por defecto, la función permanece en el servidor secundario después se produce una conmutación por error para minimizar las interrupciones del sistema.

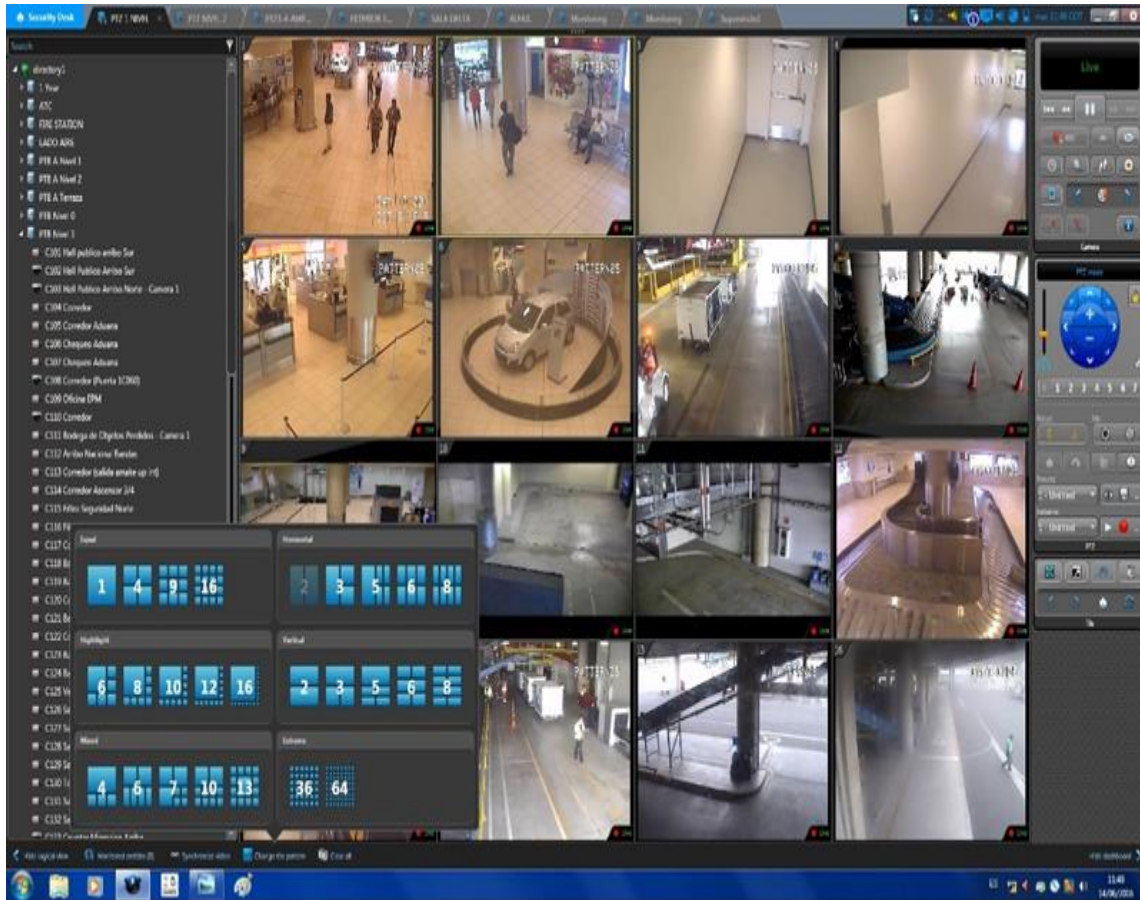


Fuente: el autor.

Figura N° 42. Configuración del Failover del Servidor Principal de GENDETEC.

- **Lienzo y Mosaicos**

Con el lienzo se puede ver y controlar entidades, como videos, módulos de ampliación de mosaico, etc. El lienzo solo aparece en algunas tareas y se puede mostrar en varias opciones como se puede observar en la Figura N° 43.



Fuente: el autor.

Figura N° 43. Mozaicos de la Herramienta Security Desk.

- **Cómo funcionan los mosaicos**

El lienzo contiene mosaicos que pueden mostrar:

- Entidades
- Información del evento
- Video en vivo y reproducido
- Imágenes de video
- Fotografías e información del tarjetahabiente o del visitante
- Módulos de ampliación de mosaico

Los mosaicos de Security Desk tienen una memoria de mosaico, lo que significa que Security Desk recuerda las últimas 8 entidades que se mostraron en cada mosaico.

- **Reproductores**

Los reproductores son grupos de botones ubicados en el tablero de control que el operador puede usar para controlar entidades en el lienzo. Los reproductores que se muestran dependen del tipo de entidad en el mosaico seleccionado.

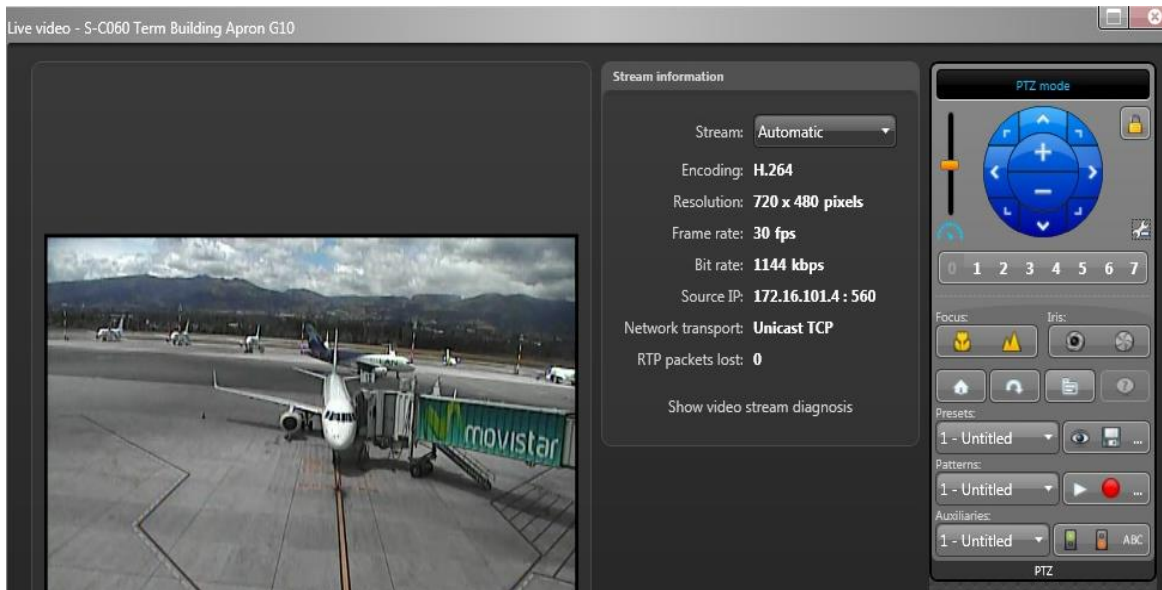


Fuente: el autor.

Figura N° 44. Reproductores de la Herramienta Security Desk

- **Diagnóstico de video**

Tanto Security Desk como Config Tool ofrecen una herramienta de diagnóstico de vídeo. Esta herramienta va a describir la ruta de red utilizada por los paquetes de vídeo para ir desde el origen al destino. Se utiliza generalmente para diagnosticar por qué el vídeo no llega a un determinado destino.



Fuente: el autor.

Figura N° 45. Información del Video

El reproductor de la cámara aparece en el tablero de control cuando el mosaico actualmente seleccionado está mostrando una cámara.

Los botones que se muestran en el reproductor de la cámara cambian de acuerdo a la tarea que se realiza y el tipo de cámara que está reproduciendo una grabación, algunos botones cambian. Si la cámara admite audio, aparecen botones de audio; de otro modo, permanecen atenuados.

Video en vivo/sin audio:

Video en reproducción con audio:



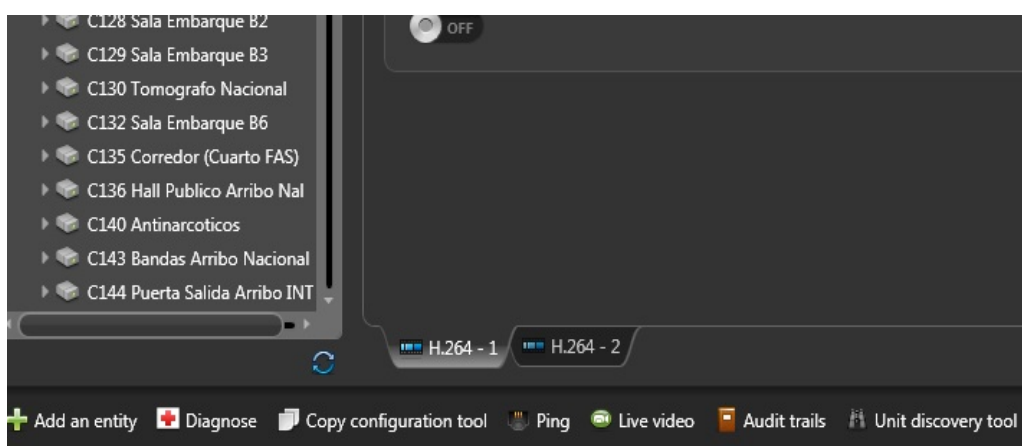
Fuente: el autor.

Figura N° 46. Botones de Control del Video

3.2.2. Sistema de Codificación/Grabación/Transmisión

- **Codificación en el sistema GENETEC.**

El sistema Genetec tiene como características brindar una gama de codificaciones para la seguridad de compresión de video digital, la compresión de vídeo digital que utiliza es H.264, ofrece una mayor resolución y calidad de vídeo que MJPEG o MPEG-4 a la misma velocidad de bits y el mismo ancho de banda.²⁹

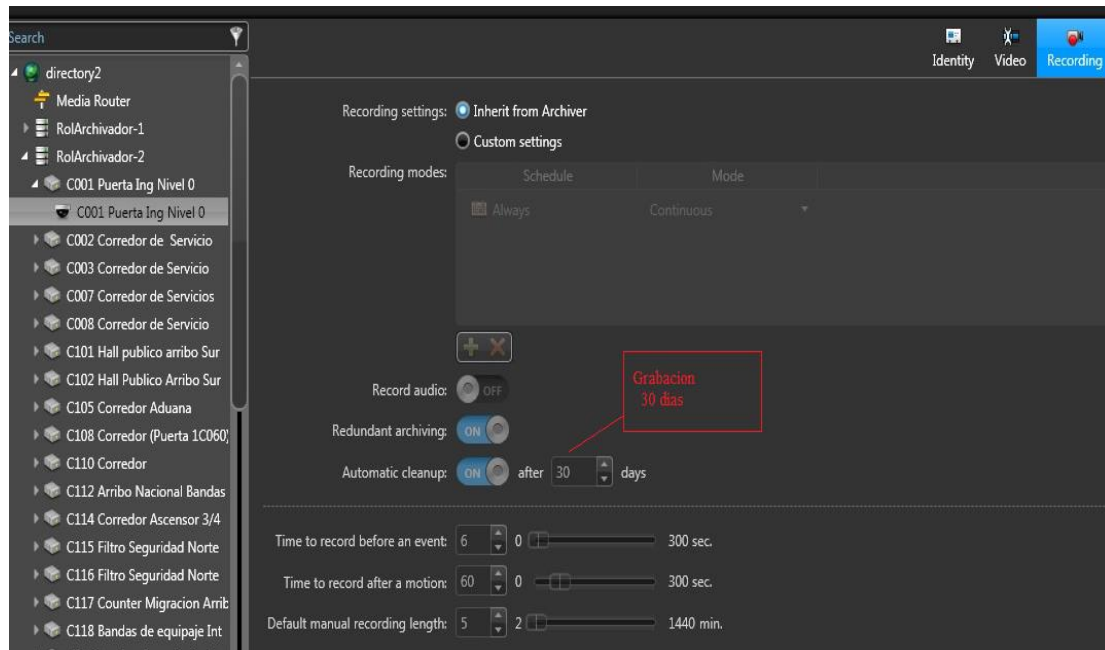


Fuente: el autor.

Figura N° 47. Esquema de codificación H.264

- **Grabación.** La grabación de la información realiza de forma continua y de acuerdo a los parámetros establecidos por la empresa para su almacenamiento.
- **Tareas programadas.** Tareas preconfiguradas por el operador del sistema para que realice grabación de videos en una determinada área.
- **Grabación por eventos.** Únicamente graba en los momentos de detección de movimientos.

²⁹ <https://riunet.upv.es/bitstream/handle/10251/34082/memoria.pdf?sequence=1>.



Fuente: el autor.

Figura N° 48. Configuración Del Grabador.

El servidor de video se encarga de almacenar la información de las cámaras por un periodo de 30 dias, luego de este tiempo la información se sobrescribira. Las imágenes y video serán vizualizados y analizados durante el tiempo antes detallado. Los servidores están preconfigurados para determinadas cámaras el almacenamiento de 1 año.



Figura N° 49. NVR Sistema GENETEC.

- **Transmisión**, la información que envía la cámara a los monitores o Video Walls para ser visualizadas operador. Esta señal debe llegar en óptimas condiciones.

Las cámaras analógicas tienen una resolución ineficiente lo cual significa que en muchos de los casos no se puede identificar claramente el rostro de las personas.



Figura N° 50. Cámara Analógica.

Fuente: el autor.

Usualmente el método de transmisión es el cable *UTP*³⁰ Cat6, Cat6 A, usado en las modernas redes de video vigilancia IP.



Figura N° 51. Cámara Analógica en la pista del AIMS.

Fuente: el autor.

³⁰ <https://www.google.com/search?client=opera&q=que+es+unicast&sourceid=opera&ie=UTF-8&oe=UTF-8#q=CABLE+UTP>.

Los monitores o video walls que tiene instalado el centro de control del AIMS permite monitorizar las señales de vídeo en vivo. A diferencia de un televisor los monitores de vídeo no incluyen sintonizador de televisión ni suelen tener altavoces.



Fuente: el autor.

Figura N° 52. Sistema de Gestión CCTV del AIMS.

El Aeropuerto Internacional Mariscal Sucre, hace uso de video walls para realizar un control de video vigilancia, y para preservar la seguridad de las personas y los bienes de los edificios.



Fuente: el autor.

Figura N° 53. Fotografía la Pista del AIMS.

3.2.3. Sistema de Grabación.

BCDVideo.

El Aeropuerto utiliza como servidores de video Serie BCDVideo, es fabricado específicamente para aplicaciones de vigilancia de vídeo IP para empresas, estadios, calles principales de las grandes ciudades, aeropuertos.

BCDVideo, es un fabricante mundial de grabadores de vídeo IP, es socio OEM global de HP para IP Video Security y sobresale en soluciones de redes inteligentes de almacenamiento y seguridad IP.



Fuente: <http://www.bcdvideo.com>

Figura N° 54. BCDVideo PART NUMBER—BCD360V8-M-MP-C.

Son sistemas de la plataforma de gestión de 1U se construyen específicamente para las aplicaciones de vídeo. El BCD360 puede ser utilizado como un servidor de administración o como un servidor de grabación de vídeo donde el almacenamiento durante el periodo de 30 días. Luego de pasar los 30 días la información se iniciará a sobreponer.³¹



Fuente: el autor.

Figura N° 55. BCDVideo PART NUMBER—BCD360V8-M-MP-C.

³¹ <https://www.bcdvideo.com/news/bcdvideo-genetec-partnership/>.

3.3. Cámaras de seguridad FIJAS y PTZ.

El Aeropuerto Internacional Mariscal Sucre tiene como exigencia mantener un óptimo monitoreo de las áreas como: lado aire, torre de control, salas de preembarque, área pública, bandas de equipaje, por esta razón existen cámaras PTZ giratorias haciendo un barrido del área en los 360° de forma inteligente y haga un zoom a un determinado punto. Las cámaras Fijas tienen un enfoque fijo hacia un determinado lugar.

3.3.1. Tipos de Cámaras.

Las cámaras que están instaladas en el Aeropuerto Internacional Mariscal Sucre, son marca Axis con bondades diferentes, fijas y PTZ. El funcionamiento diurno y nocturno de las cámaras permite la vigilancia tanto con luz diurna como de noche o en condiciones de luz escasa.



Figura N° 56. Cámara AXIS P3215-VE Network Camera.

Fuente: el autor.

Las cámaras disponen de una ranura integrada para tarjetas de memoria que permite el almacenamiento local de vídeo.

El funcionamiento diurno y nocturno de las cámaras permite la vigilancia tanto con luz diurna como de noche o en condiciones de luz escasa.



Fuente: el autor.

Figura N° 57. AXIS P3215-VE - Para Exteriores.

3.1.5.1. Historia de Construcción del Aeropuerto.

La planificación de la construcción de un nuevo aeropuerto en Quito empezó en los años 60. Debido al crecimiento acelerado de la ciudad los alrededores del antiguo aeropuerto de Quito fueron poblados, urbanizaciones, edificios, casas, avenidas; por lo que el aeropuerto de Quito terminó representando un peligro para los habitantes de la ciudad, después de varios accidentes la Dirección de Aviación Civil recomendó la edificación del nuevo terminal en la meseta de Oyambaro-Puembo, en las parroquias de Tababela-Yaruquí, debido a que consideró que la ubicación geográfica de la meseta dentro del distrito metropolitano era la más propicia para reubicar el aeropuerto, porque es una zona menos poblada, plana y está ubicada a menor altitud, fuera de los límites urbanos de la ciudad.



Fuente: el autor.

Figura N° 58. Toma Aerea de la Superficie en Costruccion Del Aeropuerto.

El nuevo Aeropuerto Internacional Mariscal Sucre de Quito se encuentra localizado en la Parroquia Tababela, a unos 25 kilometros al este de la ciudad de Quito. Este aeropuerto sustituye al antiguo Aeropuerto de Quito que se encontraba ubicado dentro del casco urbano de la ciudad capital. (Aeropuerto Internacional Marisacal Sucre, 2016).

Se tiene previsto construir una segunda pista, para cubrir la demanda futura. En una segunda etapa, prevista para el 2023, se ampliará el terminal en 20 mil metros cuadrados más.

El Aeropuerto Internacional Mariscal Sucre es el aeropuerto con mayor movimiento de pasajeros del país y está concesionado hasta el 2041 por la empresa concesionaria Quiport. Por el largo de su pista, puede recibir a los aviones más grandes de la actualidad, como el Boeing 747 o el Airbus A380. La superficie del Aeropuerto es de 1500 hectáreas, el área construida es de 70 hectáreas, el terminal de pasajeros tiene 38 mil metros cuadrados de superficie, y se estima que más de cinco millones de personas lo usarán al año.



Fuente: el autor.

Figura N° 59 Toma Satelital Del Aeropuerto.

La construcción inicial del Aeropuerto Internacional Mariscal Sucre de Quito, ubicado en la Parroquia de Tababela y se construyó inicialmente 10 edificios indispensables para dar inicio sus operaciones, la obra se entregó por el concesionario Quiport el 11 de octubre del 2012.

Los edificios entregados fueron:

1. Edificio principal de pasajeros
2. Torre de control
3. Edificio de carga internacional
4. Edificio de carga nacional
5. Edificio para el Catering (2)
6. Edificio para servicios en Tierra
7. Edificio de bomberos y de mantenimiento

8. Edificio para la Dirección de Aviación Civil – DAC.
9. Edificio para la Policía Nacional.
10. Edificio para el Nodo de comunicaciones CNT.

A continuación se detalla varias áreas y edificios principales que están habilitados dentro del aeropuerto, para lo cual se incluye tomas fotografías de la realidad que reflejan en la actualidad.

3.1.5.2 Terminal de Pasajeros.

El terminal de pasajeros principal tiene 38.000 metros cuadrados, existe una proyección de crecimiento según las operaciones aumenten y exista la necesidad de más espacio.



Fuente: el autor.

Figura N° 60. Toma Fotografía desde la Torre de Control.

El edificio principal del aeropuerto maneja vuelos nacionales e internacionales, la salida del país se realiza por el segundo nivel y la llegada es por el primer nivel, que lleva directamente al espacio de estacionamientos.³²

³² <http://aeropuertoquito.com/aeropuerto-mariscal-sucre/infraestructura/>.



Figura N° 61. Tomas Fotograficas de los diferentes areas del AIMS.

3.1.5.3 Edificio Del Nodo De Comunicaciones De CNT.

El nodo de comunicaciones de CNT, tiene como objetivo principal brindar el servicio de telefonía y servicio de internet por medio de fibra óptica.

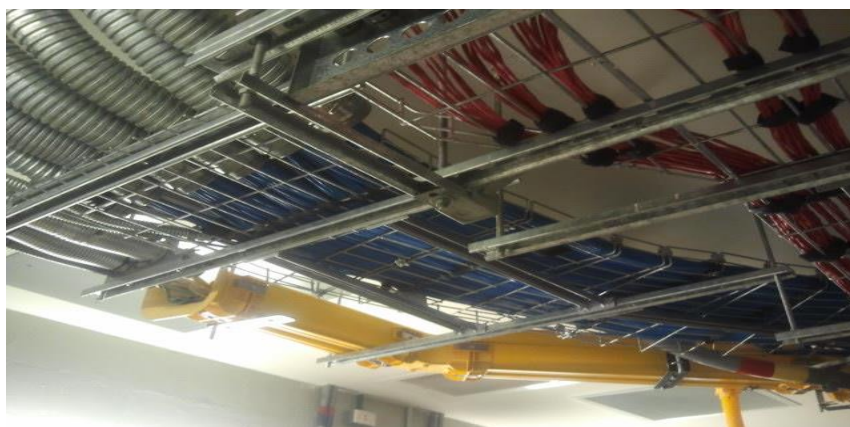


Figura N° 62. Tomas Fotograficas Del Nodo de Comunicaciones de CNT.

Fuente: el autor.

3.1.5.4 Estacionamientos.

Para lo vehículos públicos, el aeropuerto tienen una aproximación de 600 estacionamientos. La Figura N° 63 muestra como están habilitadas las plazas de parqueo.



Fuente: el autor.

Figura N° 63. Tomas Fotograficas Parqueaderos del AIMS.

Las oficinas de las aerolíneas están habilitadas en el nivel tres del edificio principal del aeropuerto.

3.1.5.5 Lineas Aereas.



Fuente: el autor.

Figura N° 64. Tomas fotograficas de las oficinas de las lineas Aereas del AIMS.

3.1.5.6 Terraza.



Fuente: el autor.

Figura N° 65. Tomas Fotograficas de la Terraza del AIMS

3.1.5.7 Corredor de mangas.

El aeropuerto tiene habilitado en la actualidad 8 mangas que se tienen el objetivo de acoplarse a los aviones para el embarque y desembarque de los pasajeros.



Fuente: el autor.

Figura N° 66. Tomas Fotograficas Del Corredor de Mangas del AIMS.

3.1.5.8 Torre de Control.

La torre de control es considerada como un icono del aeropuerto, posee una altura de 41 metros de altura y esta considerada como la más alta de Latinoamérica. El objetivo de la torre de control es controlar el tráfico aéreo como: despegues, aterrizajes y rutas de aproximación. Los controladores están en contacto permanente con las aeronaves y es el vínculo con tierra en casos de emergencia.

*“Permite una visibilidad a 37,7 metros de altura y de 360 grados y está a cargo de la Dirección General de Aviación Civil”.*³³



Fuente: el autor.

Figura N° 67. Tomas Fotograficas de la torre de Control AIMS.

³³ <http://aeropuertoquito.com/aeropuerto-mariscal-sucre/infraestructura/>.

3.1.6 Distribución de las Cámaras en cada nivel del Aeropuerto.

La instalación de todos los componentes del sistema de video vigilancia como las cámaras están instaladas y distribuidas dentro de todos los niveles del AIMS que son: 0, 1, 2, 3, 4. Estas cámaras están operando dentro del sistema de video vigilancia y de control de accesos en todo el edificio del Aeropuerto Internacional Mariscal Sucre.

El sistemas de seguridad aeroportuario actualmente tiene un despliegue importante de una infraestructura tecnológica de punta, comprende principalmente de un centro de monitoreo (CCTV), cableado estructurado, servidores de vídeo, bases de datos, fibra óptica por las largas distancias que hay que instalar los dispositivos y componentes del sistema integrado de seguridad, este conjunto de infraestructura tecnológica permite que sistema actualmente opere como un solo sistema central integrado.

Cámaras Operativas Dentro Del Sistema De Seguridad AIMS.

Tabla N° 4. Cámaras Operativas Dentro Del AIMS.

PTB PRINCIPAL			
UBICACIÓN	FIJA	PTZ	TOTAL
Nivel 0	6	2	8
Nivel 1	71	17	88
Nivel 2	73	16	89
Nivel 3	3	1	4
Nivel 4	0	6	6
Tower	2	1	3
Fire Station	2	0	2
TOTAL	157	43	200

3.1.6.2 Niveles 0, 1, 2, 4 del Aeropuerto (Cámaras DOMOS PTZ).

Los domos PTZ están instalados de manera estratégica en las diferentes áreas del Aeropuerto Internacional Mariscal Sucre, están instaladas con el objetivo de hacer un barrido de 360°, las cámaras AXIS tienen funciones de protección climática, como el control de temperatura, para entornos extremadamente fríos. En la actualidad el AIMS tiene 43 cámaras PTZ giratorias.

Tabla N° 5. Camaras Domoz PTZ (Cámaras Instaladas)

No	Nivel	Camera id	Ubicación de la Cámara	Tipo
1	0	C001	Puerta ingreso Nivel 0	PTZ
2	0	C002	Corredor de servicio	PTZ
3	1	C102	Hall publico arribo Sur	PTZ
4	1	C103	Hall publico arribo Norte	PTZ
5	1	C108	Corredor	PTZ
6	1	C110	Corredor	PTZ
7	1	C133	Counter Migracion Arribo	PTZ
8	1	C138	Hall Publico Arribo Nal	PTZ
9	1	C151	Make up INT	PTZ
10	1	C152	Make up INT	PTZ
11	1	C160	Bandas equipaje/Counters migracion	PTZ
12	1	C165	Make up Nal	PTZ
13	1	C166	Make up Nal	PTZ
14	1	C168	Bandas equipaje Nal	PTZ
15	1	C171	Gradas electricas arribo Nal	PTZ
16	1	C176	Make up INT	PTZ
17	1	C177	Make up INT	PTZ
18	1	C185	Make up INT	PTZ
19	1	C188	Exterior Lado Aire	PTZ
20	2	C201	Hall Publico Salidas N	PTZ
21	2	C202	Hall Publico Salidas S	PTZ
22	2	C203	Corredor Sur	PTZ
23	2	C210	Corredor Sur	PTZ
24	2	C211	Filtro Seguridad	PTZ
25	2	C215	Inspección de Seguridad	PTZ
26	2	C217	Hall Emigración	PTZ
27	2	C221	Corredor Norte	PTZ

28	2	C224	Sala Embarque A10-A11	PTZ
29	2	C236	Sala Embarque A7	PTZ
30	2	C252	Cheque Nacional Sur	PTZ
31	2	C257	Cheque Nacional Sur	PTZ
32	2	C262	Chequeo Counters B/C	PTZ
33	2	C267	Chequeo Internacional	PTZ
34	2	C271	Corredor Sur	PTZ
35	2	C278	Corredor Central (Dutty)	PTZ
36	3	C301	Corredor	PTZ
37	4. Terraza	C401	Terraza	PTZ
38	4. Terraza	C402	Terraza	PTZ
39	4. Terraza	C403	Terraza	PTZ
40	4. Terraza	C404	Terraza	PTZ
41	4. Terraza	C405	Terraza	PTZ
42	4. Terraza	C406	Terraza	PTZ
43	TOWER	T-C102A	West Building Wall	PTZ

3.1.6.3 Niveles 0, 1 ,2 ,3 ,4 Cámaras FIJAS

Una vez que las cámaras IP fijas son instaladas, su enfoque o visualización es fija, el zoom de es manual, a diferencia de las PTZ que son pre configurados los patrones de monitoreo y zoom. Dentro de las diferentes áreas del Aeropuerto Internacional Mariscal Sucre, están distribuidas diferentes cámaras con enfoques fijos a los counter's, salas de preembarque y ambientes públicos. En la actualidad el AIMS tiene 147 camaras fijas que se detallan a continuación.

Tabla N° 6. Cámaras Fijas

Numeración MAPA	NIVEL	CAMERA ID	Ubicación de la Cámara	TIPO
1	0	C003	Corredor de servicio	Fija
2	0	C004	Filtro Seguridad	Fija
3	0	C005	Corredor de seguridad	Fija
4	0	C006	Corredor de servicio	Fija
5	0	C007	Corredor de servicio	Fija
6	0	C008	Corredor de servicio	Fija
7	1	C101	Hall publico arribo Sur	Fija
8	1	C104	Corredor	Fija

9	1	C105	Corredor Aduana	Fija
10	1	C106	Chequeo Aduana	Fija
11	1	C107	Chequeo Aduana	Fija
12	1	C109	Oficina EPM	Fija
13	1	C111	Bodega de Objetos perdidos	Fija
14	1	C112	Arribo Nacional Bandas	Fija
15	1	C113	Corredor	Fija
16	1	C114	Corredor Ascensor ¾	Fija
17	1	C115	Filtro Seguridad Norte	Fija
18	1	C116	Filtro Seguridad Norte	Fija
19	1	C117	Counter Migracion Arribo	Fija
20	1	C118	Bandas de equipaje Int	Fija
21	1	C119	Bandas de equipaje Int	Fija
22	1	C120	Counter Migracion Arribo	Fija
23	1	C121	Bandas de equipaje Int	Fija
24	1	C122	Counter Migracion Arribo	Fija
25	1	C123	Bandas de equipaje Int	Fija
26	1	C124	Bandas de equipaje Nac	Fija
27	1	C125	Vestibulo	Fija
28	1	C126	Sala Embarque B1	Fija
29	1	C127	Sala Embarque B1	Fija
30	1	C128	Sala Embarque B2	Fija
31	1	C129	Sala Embarque B3	Fija
32	1	C130	Tomografo Nacional	Fija
33	1	C131	Sala Embarque B5	Fija
34	1	C132	Sala Embarque B6	Fija
35	1	C134	Arribo Internacional	Fija
36	1	C135	Corredor (Cuarto FAS)	Fija
37	1	C136	Hall Publico Arribo Nal	Fija
38	1	C137	Hall Publico Arribo Nal	Fija
39	1	C139	Oficina EPM	Fija
40	1	C140	Antinarcoicos	Fija
41	1	C141	Bandas arribo Nacional	Fija
42	1	C142	Bandas arribo Nacional	Fija
43	1	C143	Bandas arribo Nacional	Fija
44	1	C144	Puerta Salida Arribo INT	Fija
45	1	C145	Hall Publico Arribo Norte	Fija
46	1	C146	Hall Publico Arribo Norte	Fija
47	1	C147	Exteriores Arribo Sur	Fija
48	1	C148	Exteriores Arribo Sur	Fija

49	1	C149	Exteriores Arribo Norte	Fija
50	1	C150	Corredor Norte	Fija
51	1	C153	Make up INT	Fija
52	1	C154	Make up INT	Fija
53	1	C159	Bandas equipaje Int	Fija
54	1	C161	Bandas de equipaje INT	Fija
55	1	C162	Bandas de equipaje INT	Fija
56	1	C164	Corredor	Fija
57	1	C167	Tomografo Nacional	Fija
58	1	C169	Bandas equipaje Nal	Fija
59	1	C170	Salas Embarque B	Fija
60	1	C172	Sala Embarque B2	Fija
61	1	C173	Sala Embarque B3	Fija
62	1	C174	Filtro Seguridad Norte	Fija
63	1	C175	Tomografo Internacional	Fija
64	1	C178	Tomografo Internacional	Fija
65	1	C179	Filtro Seguridad Sur	Fija
66	1	C180	Exterior B1	Fija
67	1	C181	Exterior B3	Fija
68	1	C182	Exterior B4	Fija
69	1	C183	Exterior B6	Fija
70	1	C184	Exterior Arribo	Fija
71	1	C186	Exterior Lado Aire	Fija
72	1	C187	Exterior Lado Aire	Fija
73	1	C189	Oficina Antinarcocticos	Fija
74	1	C190	Make up Nal	Fija
75	1	C191	Make up Nal	Fija
76	1	C192	Sala Embarque B4	Fija
77	1	C193	Bandas equipaje INT	Fija
78	1	C194	Bandas equipaje INT	Fija
79	2	C204	Escalera de servicio 6	Fija
80	2	C205	Elevador 6	Fija
81	2	C206	Equipaje Sobredimensionado N	Fija
82	2	C207	Cuarto chequeo Nacional	Fija
83	2	C208	Filtro Seguridad	Fija
84	2	C209	Filtro Seguridad	Fija
85	2	C212	Filtro Seguridad	Fija
86	2	C213	Filtro Seguridad	Fija
87	2	C214	Cuarto chequeo INT	Fija
88	2	C216	Hall Emigración	Fija
89	2	C218	Hall Emigración	Fija

90	2	C219	Elevador 5	Fija
91	2	C220	Equipaje Sobredimensionado INT	Fija
92	2	C222	Sala Embarque A11	Fija
93	2	C223	Exterior Salida Int	Fija
94	2	C225	Equipaje sobredimensionado INT	Fija
95	2	C226	Sala Transito Norte	Fija
96	2	C227	Corredor Esteril N	Fija
97	2	C228	Sala Embarque A9	Fija
98	2	C229	Corredor de Mangas A8	Fija
99	2	C230	Sala Embarque A8	Fija
100	2	C231	Corredor Esteril Sur	Fija
101	2	C232	Filtro Transito Sur	Fija
102	2	C233	Filtro Transito Sur	Fija
103	2	C234	Manga 11	Fija
104	2	C235	Corredor Mangas A7	Fija
105	2	C237	Sala Embarque A6	Fija
106	2	C238	Sala Embarque A5	Fija
107	2	C239	Corredor Mangas A5/A6	Fija
108	2	C240	Manga puente móvil 10	Fija
109	2	C241	Ingreso Manga 10	Fija
110	2	C242	Manga 12	Fija
111	2	C243	Manga 13	Fija
112	2	C244	Corredor Mangas A9	Fija
113	2	C245	Manga 14	Fija
114	2	C246	Ingreso Manga 15	Fija
115	2	C247	Puente Movil Manga 15	Fija
116	2	C248	Exteriores Nacional	Fija
117	2	C249	Exteriores Nacional	Fija
118	2	C250	Hall Publica Salidas Sur	Fija
119	2	C253	Cheque Nacional Sur	Fija
120	2	C254	Cheque Nacional Sur	Fija
121	2	C255	Cheque Nacional Sur	Fija
122	2	C256	Cheque Nacional Sur	Fija
123	2	C258	Cheque Nacional	Fija
124	2	C259	Cheque Nacional	Fija
125	2	C260	Cheque Nacional	Fija
126	2	C261	Cheque Nacional	Fija
127	2	C263	Chequeo Internacional	Fija
128	2	C264	Chequeo Internacional	Fija
129	2	C265	Chequeo Internacional	Fija
130	2	C266	Chequeo Internacional	Fija
131	2	C269	Hall Publica Salidas Sur	Fija
132	2	C270	Hall Publica Salidas Norte	Fija
133	2	C272	Counters en transito	Fija

134	2	C273	Filtro Seguridad	Fija
135	2	C274	Filtro Seguridad	Fija
136	2	C275	Filtro Seguridad	Fija
137	2	C276	Filtro Transito INT	Fija
138	2	C277	Escaleras publicas 8	Fija
139	2	C279	Escaleras publicas	Fija
140	2	C280	Corredor Mangas A10/A11	Fija
141	2	C281	Sala Embarque A7	Fija
142	2	C282	Sala Embarque A10	Fija
143	2	C283	Corredor de Mangas A6/a7	Fija
144	2	C284	Corredor de Mangas A7/A8	Fija
145	2	C285	Corredor de Mangas A8	Fija
146	2	C286	Corredor de Mangas A8/A9	Fija
147	2	C287	Corredor de Mangas A10/A11	Fija
148	2	C288	Filtro Seguridad	Fija
149	2	C289	Casilleros EPMSA	Fija
150	2	C290	Casilleros EPMSA	Fija
151	3	C302	Elevador ¾	Fija
152	3	C303	Entrada Oficina ADC	Fija
153	3	C304	Corredor	Fija
154	Torre de Control	T-C101A	Ingreso DGAC	Fija
155	Torre de Control	T-C500A	PTB Apron	Fija
156	FIRE	F-C100F	Filtro Seguridad Ingreso SSEI	Fija
157	FIRE	F-C101F	Bodega General	Fija

CAPÍTULO IV

4.1. Requerimientos tecnológicos del sistema de video vigilancia.

4.1.1 Descripción Técnica Del Equipos de Red.

La infraestructura tecnológica de red de comunicaciones del Aeropuerto Internacional Mariscal Sucre, amerita de nuevos equipos, componentes y servidores para la implementación del nuevo sistema de video vigilancia que esta basado en tecnología de punta IP, para lo cual es importante mencionar los equipos de networking con que cuentan las instalaciones del AIMS³⁴.

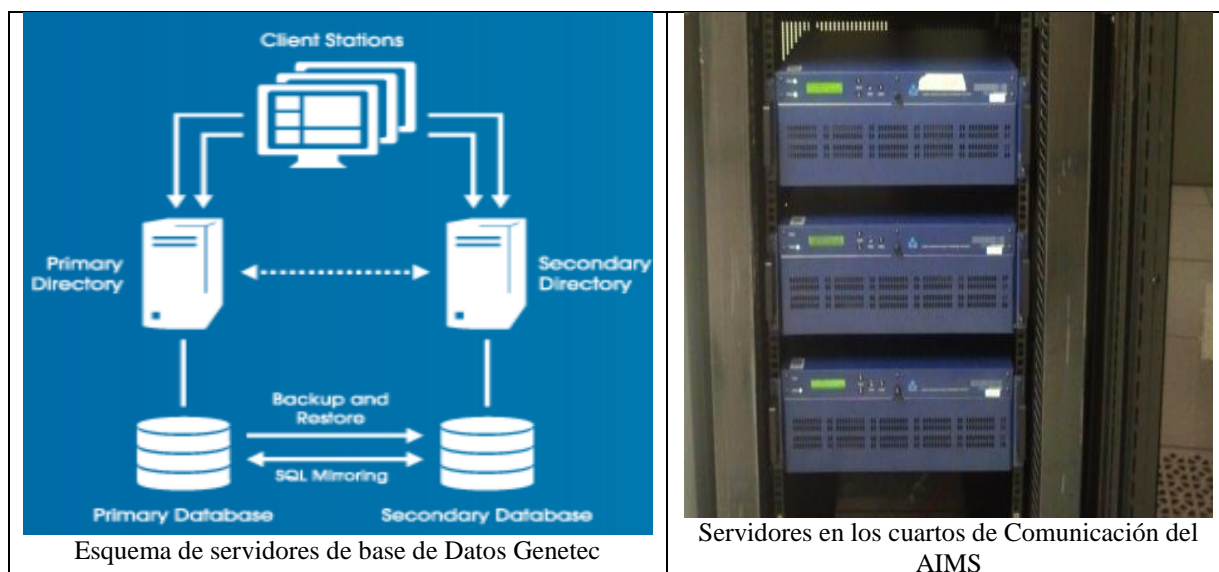
4.1.2 Servidores de bases de datos.

El Aeropuerto Internacional Mariscal sucre tiene como requerimiento almacenar el video dentro del sistema durante 30 días, para lo cual el servidor de base de datos debe proporciona múltiples mecanismos para garantizar que el sistema esté funcionando todo el tiempo, y que la información este consistente con la integridad, disponibilidad y confidencialidad.

Dentro del análisis técnico realizado por la parte técnica del Aeropuerto Internacional Mariscal Sucre, se ha determinado que la plataforma más efectiva que cumple con el requerimiento que necesita la seguridad aeroportuaria es: GENETEC Security Center.

Esta arquitectura esta basada en módulos, garantiza una alta disponibilidad al permitir que cada rol o modulo esté alimentado por múltiples servidores, reduciendo así, el riesgo de una falla puntual.

³⁴ AIMS. Aeropuerto Internacional Mariscal Sucre.



Fuente: el autor.

Figura N° 68. Servidores de Bases de datos GENETEC security Center

La tarea o Rol del Directorio es manejar las conexiones de los usuarios o clientes. Brinda el estricto cumplimiento de las políticas de seguridad, al tomar en mayor parte las decisiones en el sistema como: flujos de trabajo, almacenamiento de las configuraciones del sistema.

4.1.3 Equipos de Comunicaciones Switchs Core.

La infraestructura tecnológica de networking del Aeropuerto Internacional Mariscal Sucre operan sobre equipos de marca Cisco Core modelo Catalyst series 4503-E. Estos Switches brindan servicio de convergencia, seguridad y facilidad de gestión y administración.

Los clientes pueden converger y controlar más fácilmente los datos del Protocolo de Internet (IP), streaming video, telefonía y aplicaciones basadas en Internet para una rentabilidad y productividad mejorada dentro del desarrollo corporativo aeroportuario.

Permiten un ahorro de seguridad, movilidad, rendimiento de las aplicaciones, video y energía a lo largo de una infraestructura que apoya la resistencia, la virtualización y la automatización

CISCO Catalyst 4503-E - WS-C4503-E.



Fuente: el autor.

Figura N° 69. Cisco Core Catalyst 4503-E - WS-C4503-E.

La siguiente tabla presenta la comparación de tecnologías de los equipos de networking para ser utilizados en los cuartos de comunicaciones del AIMS.

Tabla N° 7. El Cisco Catalyst 4500 y Series y Modelos de Switch Catalyst.

Cisco Catalyst 4500 Series Switching Modules	Number of Interfaces Supported per Line Card	Cisco Catalyst 4503-E	Cisco Catalyst 4506-E	Cisco Catalyst 4507R+E	Cisco Catalyst 4510R+E
Switched 10/100 Fast Ethernet (RJ-45)	48	96 OK	240	240	384
Switched 10/100 Fast Ethernet (RJ+45) with IEEE 802.3af at Power over Ethernet (PoE/PoE+)	48	96	240	240	384
Switched 100 FX Fast Ethernet (MT-RJ)	48	96	240	240	384

Switched 1000BASE-X (fiber)	6, 18, or 48	100	244	244	388
Switched 10/100/1000BASE-T Gigabit Ethernet	48	96	240	240	384
Switched 10/100/1000BASE-T Gigabit Ethernet with IEEE 802.3af at PoE/PoE+	48	96	240	240	384
Switched 10/100/1000BASE-T Gigabit Ethernet with UPOE	48	96	240	240	384
Switched 10 Gigabit Ethernet	6 or 12	32	68	68 ⁶	104

4.1.4 Switchs de Distribución.

Los switches de la capa de distribución con lo que actualmente el AIMS cuenta son Cisco, son dispositivos de networking que presentan disponibilidad y alta redundancia para asegurar la fiabilidad en las comunicaciones, para lo cual el aeropuerto tiene 2 cuartos de comunicaciones denominados MRC1, y MCR2.

CUARTOS DE COMUNICACIONES MCR1.

- Existe 2 filas de 5 armarios de comunicaciones.
- Existe 1 fila de 4 armarios de comunicaciones
- Total 14 ARMARIOS.



Fuente: el autor.

Figura N° 70. Cuarto de Comunicaciones MCR1 del AIMS.

4.1.4.1 Capa de acceso.

El objetivo fundamental de la capa de acceso es brindar un medio de conexión principal a los dispositivos de red, y controlar los componentes finales como: puertas, intercomunicadores, cámaras, teléfonos, que forman parte del sistema de seguridad integrado aeroportuario.



Fuente: el autor.

Figura N° 71. Cableado Estructurado CAT6A del AIMS

4.1.5 Detalle de Vlans y Direccionamiento IP.

La infraestructura de red LAN del aeropuerto tienen ejecutandose varios sistemas y servicios que están haciendo uso de la misma infraestructura de red para brindar un eficaz servicio de voz, datos, e internet a las diferentes empresas que operan, para lo cual se ha segmentado la red en diferentes VLAN's. Están creadas para brindar un óptimo funcionamiento de red como: servidores, intercomunicadores, estaciones de trabajo. La subdivisión de la red LAN en VLAN's, ha permitido designar diferentes directivas de seguridad a los grupos de trabajo.

Tabla N° 8. Detalle de Vlans y direccionamiento IP.

LISTADO DE VLAN DEL SISTEMA – AIMS		
Vlan	Asignado a	Segmento de direcciones ip
101	CCTV	172.16.101.1 - 172.16.101.255
113	IP Anterior VLAN 113	172.16.113.1 - 172.16.113.255
104	Servidores.	172.16.104.1 - 172.16.104.255
105	Intercomunicadores/ Control de accesos.	172.16.105.1 - 172.16.105.255
115	Estaciones De Trabajo	172.16.115.1 - 172.16.115.255

Los servicios que se ejecutan por la red LAN del aeropuerto están configurados actualmente para dar prioridad a los sistemas mediante QoS. En general, las aplicaciones que se ejecutan en tiempo real tales como aplicaciones de video y voz tienen distintas necesidades que una aplicación de datos regular.

El sistema integrado de seguridad aeroportuario está configurado para cumplir con las mejores prácticas comunes de la industria.

4.1.6 QoS o Calidad de Servicio.

El Aeropuerto Mariscal Sucre, tiene una infraestructura de red compartida con varios sistemas de seguridad que fueron detallados con anterioridad. Para lo cual se toma en consideración varios aspectos muy importantes como: ruido, atenuación, eco, pérdida de paquetes, todos estos aspectos pueden afectar el rendimiento de los servicios de comunicaciones que se brinda a las diferentes empresas y aerolíneas.

La red LAN aeroportuaria garantiza un cierto nivel de calidad de servicio para un nivel de tráfico que sigue un conjunto específico de parámetros. Las políticas de calidad fueron implementadas según los requerimientos principales de la red que detalla la tabla N° 9.

La aplicación de QoS es un requisito básico para poder implantar servicios interactivos (Ejemplo voip).³⁵

Tabla N° 9. Prioridad de tráfico QoS.

PRIORIDAD	TIPO DE TRÁFICO
1	Voice
2	IP Video
3	Priority Data
4	Best Effort Data

4.1.7 Ancho De Banda.

El ancho de banda aproximado que utiliza una cámara configurada dentro del sistema de seguridad CCTV-EPMSA, utiliza aproximadamente de 2 a 3 Mbit/s del ancho de banda disponible de la red.

La estimación del ancho de banda se realiza mediante el análisis de varios factores, entre los

³⁵ <https://sites.google.com/site/redessconvergentes/unidad-ii/1-introduccion-qos>.

cuales se detalla a continuación.

- Códec de compresión de vídeo. (H.264)
- Resolución de Imagen
- Velocidad binaria aprox.
- Imágenes por segundo (frames por segundo)
- Horas de funcionamiento (24hrs)
- Días de almacenamiento.

Proyectos	Nombre	Modelo	Tipo	Nº	Escenario	Perfil	Ancho de ...	Almacen...
AIMS-TABABELA	AIMS	AXIS M3204-V	Cámara	200	Patio de colegio	Personalizado	135 MBit/s	8.15 TB

Nombre	Modelo	Cantidad	Escenario
AIMS	AXIS M3204-V	200	Patio de colegio

Perfil	Personalizado ...
--------	-------------------

<input checked="" type="checkbox"/> Visualización	<input checked="" type="checkbox"/> Grabación continua	<input checked="" type="checkbox"/> Grabación de eventos
Velocidad de imagen: 6	1	30
Resolución: VGA	VGA	VGA
Codificación de vídeo: H.264	H.264	H.264
Compresión: 30	30	30
Audio: Desactivado	Desactivado	Desactivado
Grabación	24 h	20%
Ancho de banda: 133 KBit/s	29.4 KBit/s	511 KBit/s

Resumen	Configuración
---------	---------------

Ver: 26.6 MBit/s
 Grabar: 5.89 MBit/s
 Evento: 102 MBit/s
 Total: 135 MBit/s
 Almacenamiento: 8.15 TB

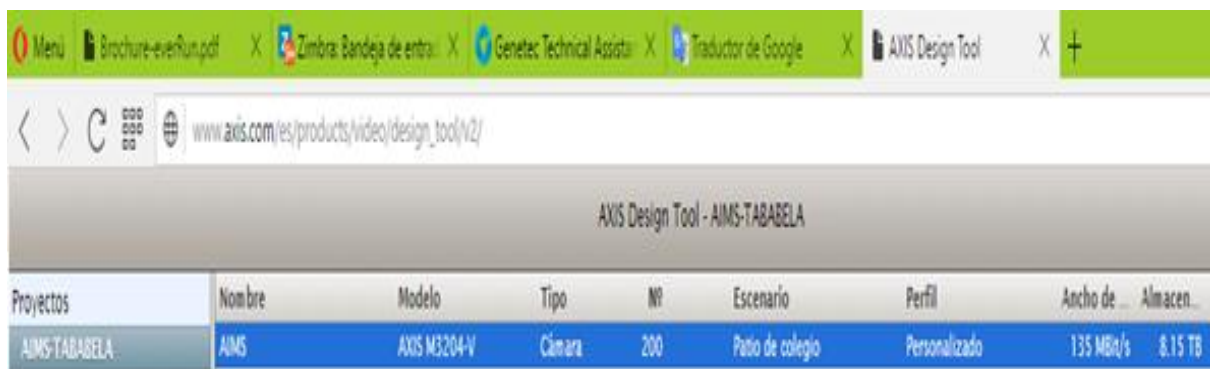
Fuente: el autor.

Figura N° 72. Calculo del Ancho de Banda.

El sistema de video vigilancia del Aeropuerto Internaciona Marsical Sucre se compone de 200 cámaras, considerando un eventual incremento de cámaras, y la carga de la red con respecto a la velocidad de transmisión.

Datos del Proyecto del sistema de video vigilancia:

- **Proyecto:** AIMS- TABABELA
- **Nombre:** AXIS Modelo: AXIS M3204-V
- **Tipo:** Cámara No.: 200
- **Perfil:** Personalizado
- **Ancho de Banda:** 135Mbit/s
- **Almacenamiento:** 8.15TB



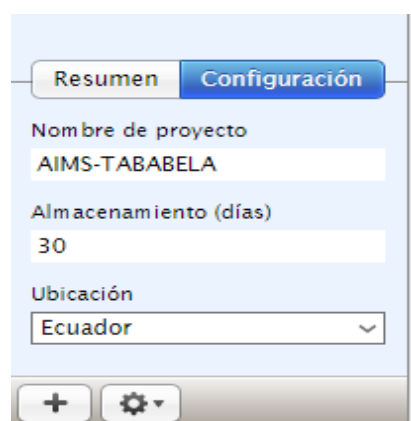
The screenshot shows a web browser window with the URL www.axis.com/es/products/video/design_tool/v2/. The page title is "AXIS Design Tool - AIMS-TABABELA". Below the title is a table with the following data:

Proyectos	Nombre	Modelo	Tipo	Nº	Escenario	Perfil	Ancho de ...	Almacen...
AIMS-TABABELA	AIMS	AXIS M3204-V	Cámara	200	Patio de colegio	Personalizado	135 Mbit/s	8.15 TB

Fuente: el autor.

Figura N° 73. Calculo del Ancho de Banda y Almacenamiento.

- **Configuracion del almacenamiento.**



The screenshot shows the "Configuración" (Configuration) tab of the storage settings. The fields are as follows:

- Nombre de proyecto:** AIMS-TABABELA
- Almacenamiento (días):** 30
- Ubicación:** Ecuador

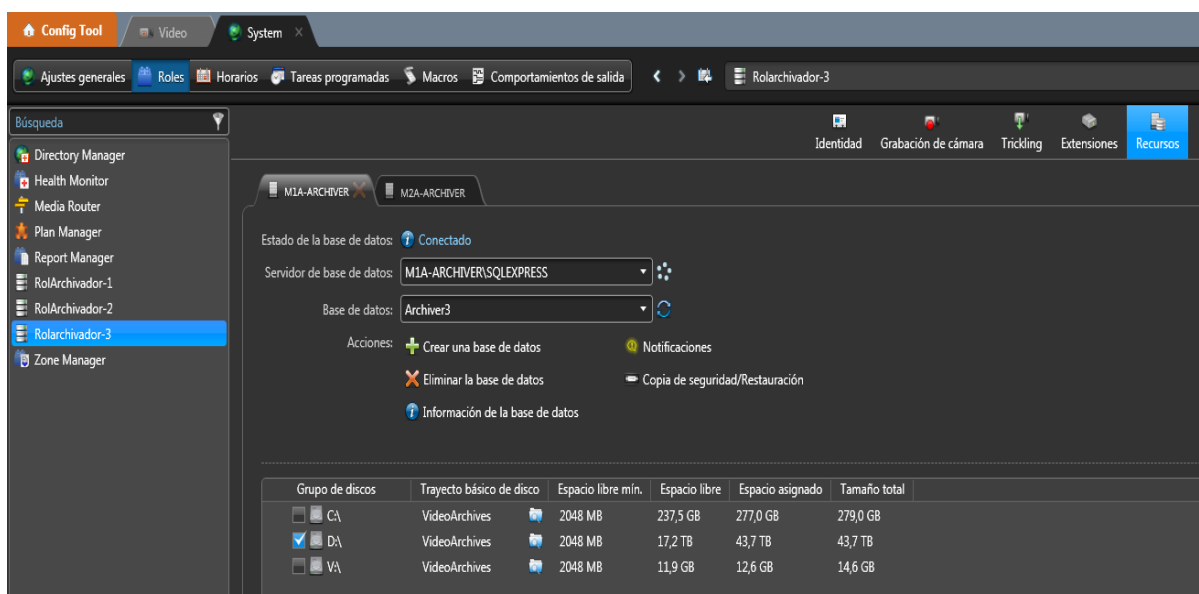
At the bottom, there are two buttons: a plus sign (+) and a gear icon (⚙️).

Fuente: el autor.

Figura N° 74. Calculo del Almacenamiento.

Para realizar el cálculo efectivo del consumo del ancho de banda de las 200 cámaras se lo hizo con la ayuda de la herramienta de AXIS.

Los servidores de video vigilancia se deben adaptar al entorno de seguridad que requiere el Aeropuerto Internacional Sucre, el tiempo de almacenamiento de los video es de 30 dias, pasado este tiempo los video se remplazaran automáticamente.



Fuente: el autor.

Figura N° 75. Almacenamiento de la Información en los servidores

4.1.8 Sistemas de redundancia y alta disponibilidad.

El AIMS tiene 2 cuartos de comunicaciones denominados MCR1 como primario ubicado en el edificio principal del Aeropuerto, el MCR2 esta ubicado en el edificio de bomberos con 1 kilometro de distancia denominado cuarto redundante.



Fuente: el autor.

Figura N° 76. Cuarto de Comunicaciones del MCR1.

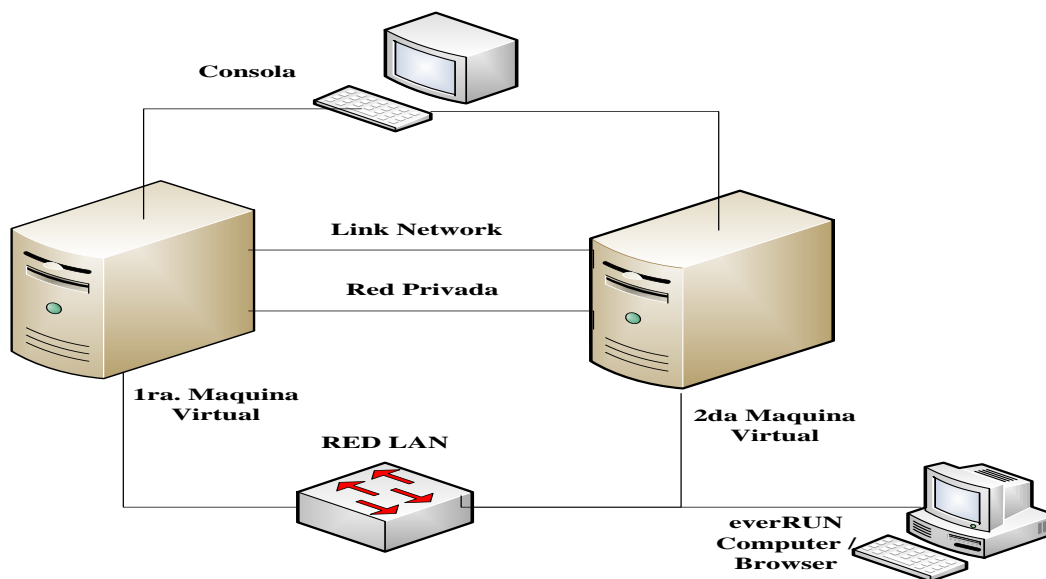
El sistemas de video vigilancia debe estar disponible y operativo las 24 horas del día, y los 365 días al año, minimiza los fallos que puedan afectar al funcionamiento normal del sistema, razón por la cual el Aeropuerto Internacional Mariscal Sucre utiliza aplicaciones redundantes mediante el uso de software de alta disponibilidad y tolerancia a fallos llamado everRun, que permite mantener una alta disponibilidad dentro de los servicios de comunicaciones en el AIMS.

everRun

El software everRun Enterprise es una herramienta que mantiene en ejecución sus aplicaciones ya sean Windows o Linux. Previene tiempos de inactividad, asegurando la continuidad del servicio de red este siempre operativo.

Beneficios:

- Es compatible con entornos Windows, servidores basados en Intel®.
- Incluye una interfaz de gestión basada en navegador la administración del sistema.



Fuente: el autor.

Figura N° 77. Sistemas de Redundancia en Redes LAN

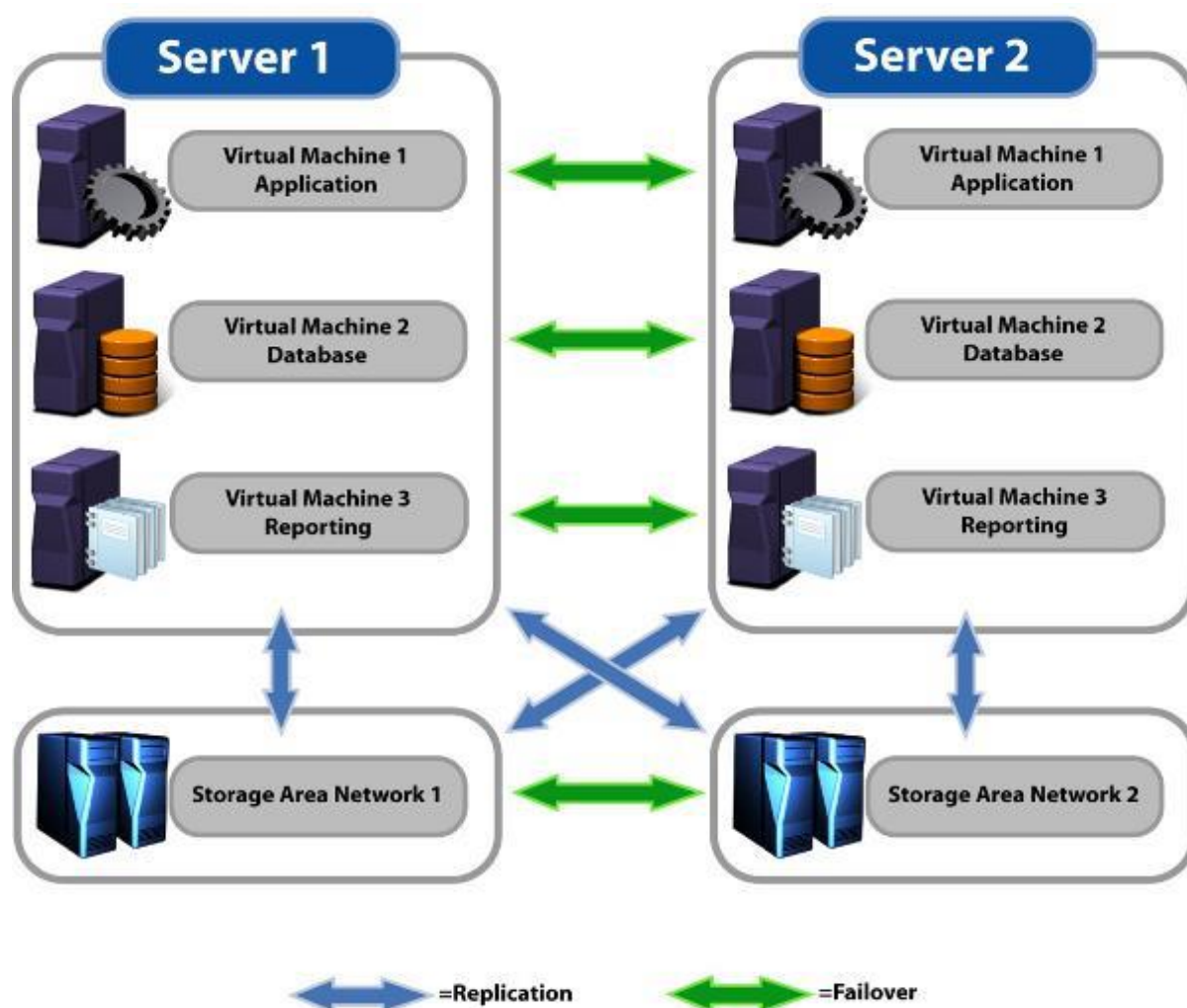
Beneficios de everrun:

- **Protección máxima según la criticidad del sistema:** protección ante fallos de hardware en modo FT (Faul Tolerance: sin paso por cero) o en modo HA (High Availability: existe un tiempo "x" de recuperación).
- **Continuidad de negocio:** everRun permite cumplir con requisitos elevados de continuidad de negocio y cumplimiento de normativas y SLAs.
- **Sin pérdida de datos:** con everRun puede asegurar que las aplicaciones funcionarán en modo continuo, sin interrupciones y sin pérdida de datos.
- **Protección ante desastres:** everRun permite el despliegue “*de tus soluciones*” en servidores ubicados en edificios distintos (en modo Split Site) o en ubicaciones geográficas distintas (en modo Disaster Recovery).
- **Flexibilidad en la elección del hardware:** Permite el uso de servidores tradicionales.
- **Facilidad y rapidez:** la instalación de everRun es fácil y rápida sin necesidad de conocimiento avanzado de informática.
- Previene tiempos de inactividad a nivel local o cross-campus
- Asegura las operaciones sin interrupciones y previene la pérdida de datos
- Proporciona recuperación ante desastres – Data Recovery – integrada
- Funciona con servidores estándar
- Fácil instalación sin necesidad de personal IT altamente especializado
- No es necesario modificar sus aplicaciones.
- Funciona en entornos físicos, virtuales o en la nube
- Protege un servidor completo o datos específicos
- Al ser escalable, se adapta fácilmente a los cambiantes requerimientos del negocio
- Proporciona protección en configuración HA (Alta Disponibilidad) o en FT

(Tolerante a Fallos) para cargas de trabajo en procesadores simétricos (SMP) y de múltiples núcleos.

- Capacidad de enviar alertas vía SNMP en caso de fallos de componentes.

En cada máquina física se asigna dos puertos de red, uno como el privado (Priv0), y el otro puerto de red como la administración red (Ibiz0). Se puede utilizar puertos de red de (1 Gb, o 10 Gb) para la administración y servicio de redundancia, puede utilizar los siguientes medios de transmisión según la TIA/EIA: CAT6, CAT6A, o CAT7 cables para toda red. La siguiente ilustración muestra un como el modelo de everRun. (everRun, 2016)



Fuente: el autor.

Figura N° 78. Diagrama de Red y redundancia.

4.1.9 Especificaciones Técnicas de las cámaras IP.

4.1.9.1 Cámaras fijas.

Las cámaras de red fijas, una vez que son empotradas en el lugar donde esta designada, tiene un enfoque fijo a un bjetivo. Si la cámara tiene un requerimiento de cambiar el enfoque, se tiene que haer de forma manual. Ejemplo: puertas de las mangas, bandas de equipajes como muestra la Figura N° 79.



Fuente: el autor.

Figura N° 79. Cámaras ubicadas en arribos Internacional

El diseño de la camara es discreto y disimula muy bien, tiene una carcasa curva que cubre por completo a la cámara y su ventaja es de proteger de cualquier tipo de manipulación al desenfoco de visión.

4.1.9.2 Cámaras móviles. (PTZ Giratoria)

Las cámaras PTZ pueden rotar alrededor de dos ejes, uno horizontal y otro vertical, así como acercarse o alejarse (zoom) para enfocar un área u objeto de forma manual o automática. Dicho de otra forma, este tipo de cámaras es capaz de rotar en un plano vertical (tilt en inglés) y en un plano horizontal (panning), además de acercarse o alejarse de forma manual o automática.



Cámaras PTZ / Ubicada en Pasillos

Toma fotográfica desde la Cámara

Fuente: el autor.

Figura N° 80. Cámaras ubicadas los Corredores.

4.1.9.3 Equipo de administración y grabación digital.

El sistema de administración de videos en redes esta basado en tecnología IP, proporciona la habilidad de instalar un sistema de video vigilancia que realmente se adapte a las necesidades y exigencias cambiantes de seguridad del Aeropuerto Internacional Mariscal Sucre.

4.1.9.4 Servidores de Grabaciones.

Los servidores de video vigilancia se deben adaptar al entorno de seguridad que requiere el Aeropuerto Internacional Sucre, el tiempo de almacenamiento de los videos sera de 30 dias, pasado este tiempo los videos se remplazaran automáticamente.

Las configuraciones del sistema y de todas las entidades como: reportes, historia de alarmas, y de todas las incidencias están contenidas dentro de la base de datos.

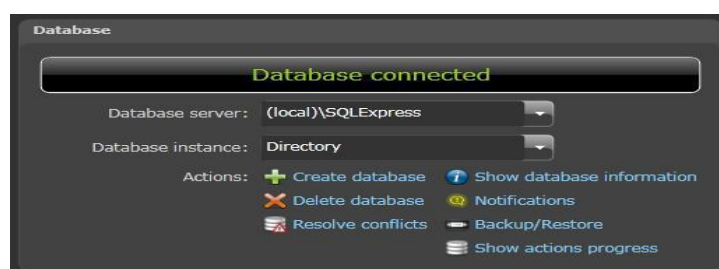
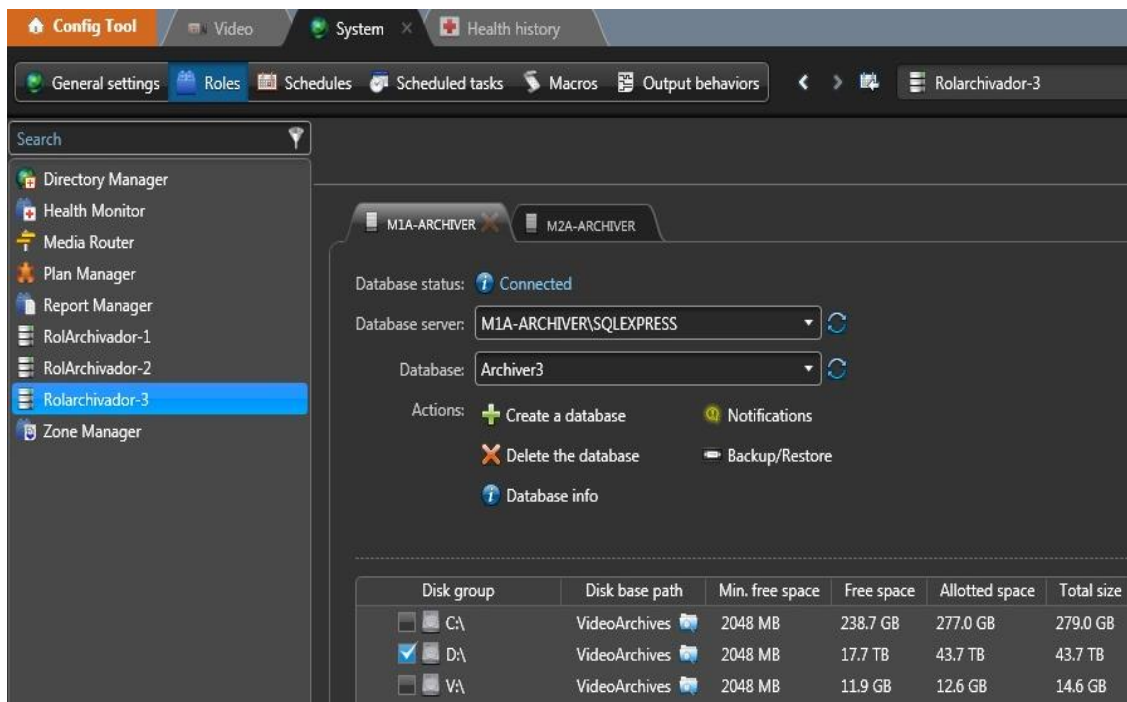


Figura N° 81. Base de datos del sistema GENETEC.

Fuente: el autor.

Los servidores tienen una capacidad de almacenamiento de 43.7 TB como muestra la Figura No. 80, la arquitectura flexible y abierta asegura la integridad, disponibilidad e integridad de la información, se puede adaptar a la evolución y crecimiento del sistemas de video vigilancia.



Fuente: el autor.

Figura N° 82. Espacio de Almacenamiento de los Servidores de video.

4.1.10 Equipos de cómputo para el centro de control y monitoreo CCTV.

El Centro de Control y Monitoreo es el punto central y principal del sistema de monitoreo, esto sin restar importancia a los equipos de vigilancia como los paneles de alarma y las cámaras de vigilancia que son parte fundamental del sistema de vigilancia aeroportuario.

El correcto diseño del Centro de Control y Monitoreo es muy importante ya que es el punto central donde se va a recibir toda la información proveniente de las áreas vigiladas y monitoreadas, lugar donde se van a realizar la toma de decisiones de acuerdo a lo que ocurra en el Aeropuerto. Los aspectos a tomar en cuenta en el proceso de diseño del Centro de Control y Monitoreo son:

- Número de equipos de monitoreo a utilizar.
- Características técnicas necesarias de los equipos de monitoreo.
- Protección de los equipos de monitoreo.
- Diseño del sistema de respaldo de información.
- Brindar seguridad al mismo Centro de Control y Monitoreo.

4.1.10.1 Estaciones de Trabajo para los Operadores.

Las estaciones de trabajo garatinzan una velocidad eficiente y optima dentro de las operaciones ejecutadas por el operador dentro del sistema de seguridad, las estaciones de trabajo habilitadas para el centro de control CCTV están prendidas todo el tiempo 24/ y los 265 días del año. Razón por la cual hace que el requerimiento tecnológico del equipo sea de tomado en consideración. Actualmente los equipos instalados son modelo: HP Workstation HP Z440.

- Rendimiento optimo para la reproducción de videos y fotografías almacenados.
- Respaldo de videos solicitados por los entes públicos (Fiscalia, Ministerio del Interior.



Fuente: el autor.

Figura N° 83. Estaciones de Trabajo.

4.1.10.2 Especificaciones Generales.

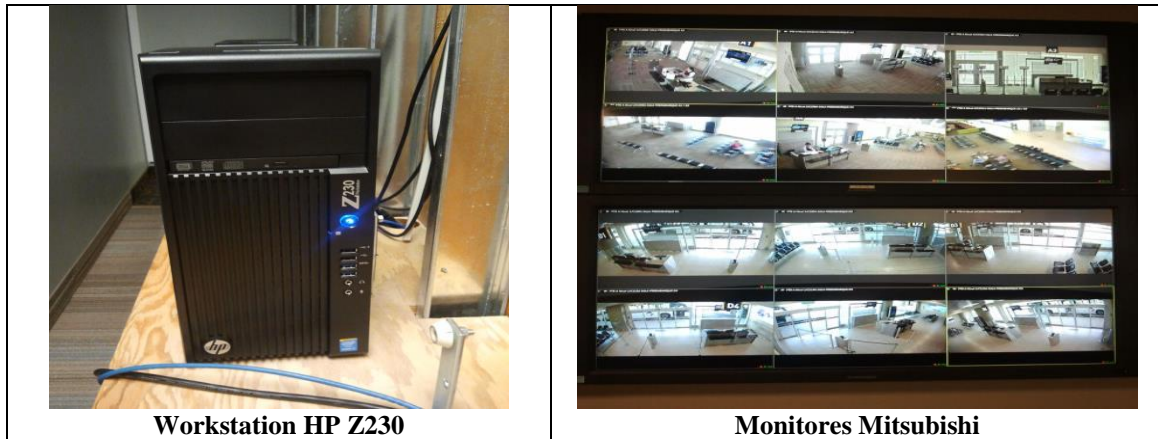
- **Sistema Operativo**
 - Windows 8.1 Pro 64.
 - Windows 7 Professional 64 (disponible mediante derechos de desactualización de Windows 8.1 Pro 64).
 - HP Installer Kit para Linux.
- **Familia de Procesadores.**
 - Procesador Intel® Xeon® E5 1600 v3.
 - Procesador Intel® Xeon® E5 2600 v3
- **Memoria**
 - Memoria Máxima.
 - 128 GB de SDRAM registrada DDR4-2133 ECC SDRAM de registro ECC DDR4-2133 (Velocidades de transferencia de hasta 2133 MT/s. Solo se admite memoria registrada.)
 - Ranuras de memoria
 - 8 DIMM
- **Almacenamiento**
 - Unidad Interna.
 - 500 GB SED SATA (7200 rpm)
- **Garantía**
 - Protección de Servicios HP, incluye una garantía estándar limitada de 3 años para piezas, 3 años para mano de obra y 3 años para servicio in situ (3/3/3).

4.1.10.3 Estaciones de Trabajo para el sistema Video Wall.

Actualmente los equipos que están operando como Video Wall dentro del centro de control y monitoreo CCTV son equipos HP modelo Z230, para lo cual se detallan las características.

- **Estación de trabajo HP Z230**

Brinda un ambiente de trabajo totalmente eficiente, ya que el Centro de Control y monitoreo del AIMS exige confiabilidad y rendimiento dentro del sistema de seguridad y monitoreo de video vigilancia.



Fuente: el autor.

Figura N° 84. Video Wall Operativos dentro del Centro de Control del AIMS

4.1.10.4 Pantallas para el Video Walls.

El Aeropuerto Internacional Marsical Sucre tiene en la actualidad 10 video walls operativos dentro del CCTV para monitoreo y vigilancia de las áreas pública y restringidas.

Actualmente los monitores que están operando como Video Wall dentro del centro de control y monitoreo CCTV son equipos Mitushubishi modelo LDT421V2, para lo cual se detallan las características.

- **Especificación general:**
 - **Model:** LDT421V2
 - **Monitor características:** Display Type 42" WXGA-Wide LCD Display
 - **Área visible:** 42" (106.7 cm) diagonal.
- Tiene un excelente brillo y contraste, la pantalla brinda imágenes de vídeo de buena resolución HD.



Fuente: el autor.

Figura N° 85. Pantalla de 42" Operativas dentro Del CCTV AIMS.

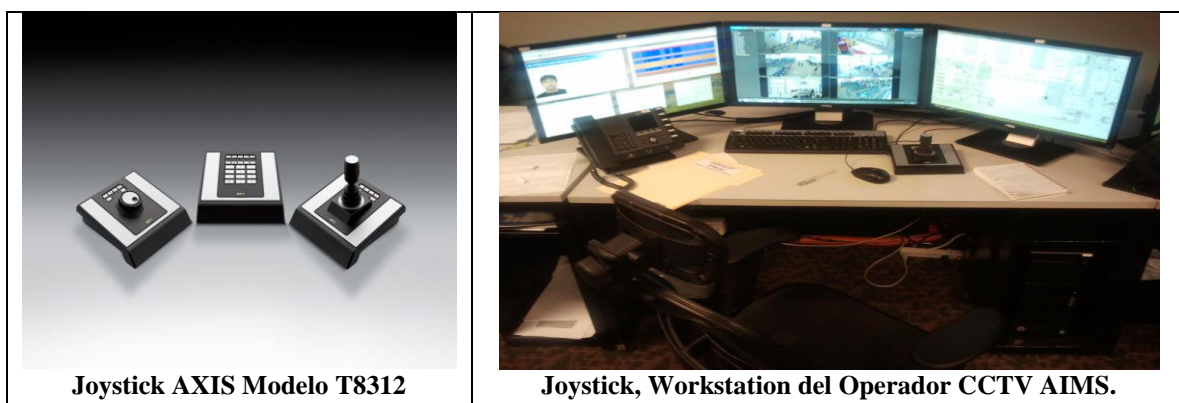
4.1.10.5 Monitor.

El centro de control y monitoreo CCTV tiene como exigencia monitorear y vigilar las diferentes ambientes, para lo cual necesitan un monitor de muy buena resolución y nitidez.

4.1.10.6 Joystick.

Las estaciones de trabajo de los operadores del centro de control y monitoreo CCTV tienen la necesidad de utilizar joystick de videovigilancia marca AXIS T8312, que permite un control eficaz y preciso de todas las cámaras de red PTZ (Giratorias).

El operador se desplaza rápidamente entre los espacios de trabajo con las bondades que brinda el joystick.



Joystick AXIS Modelo T8312

Joystick, Workstation del Operador CCTV AIMS.

Fuente: el autor.

Figura N° 86. Fotografía de los Equipos del Centro de Control CCTV

4.1.11 Diagrama de red de las Cámaras IP.

- **ANEXO 1**, MAPA DE CÁMARAS INSTALADAS EN EL NIVEL 0
- **ANEXO 2**, MAPA DE CÁMARAS INSTALADAS EN EL NIVEL 1
- **ANEXO 3**, MAPA DE CÁMARAS INSTALADAS EN EL NIVEL 2
- **ANEXO 4**, MAPA DE CÁMARAS INSTALADAS EN EL NIVEL 3
- **ANEXO 5**, MAPA DE CÁMARAS INSTALADAS EN EL NIVEL 4 (TERRAZA).

4.1.12 Diagrama de RED LAN DEL AIMS.

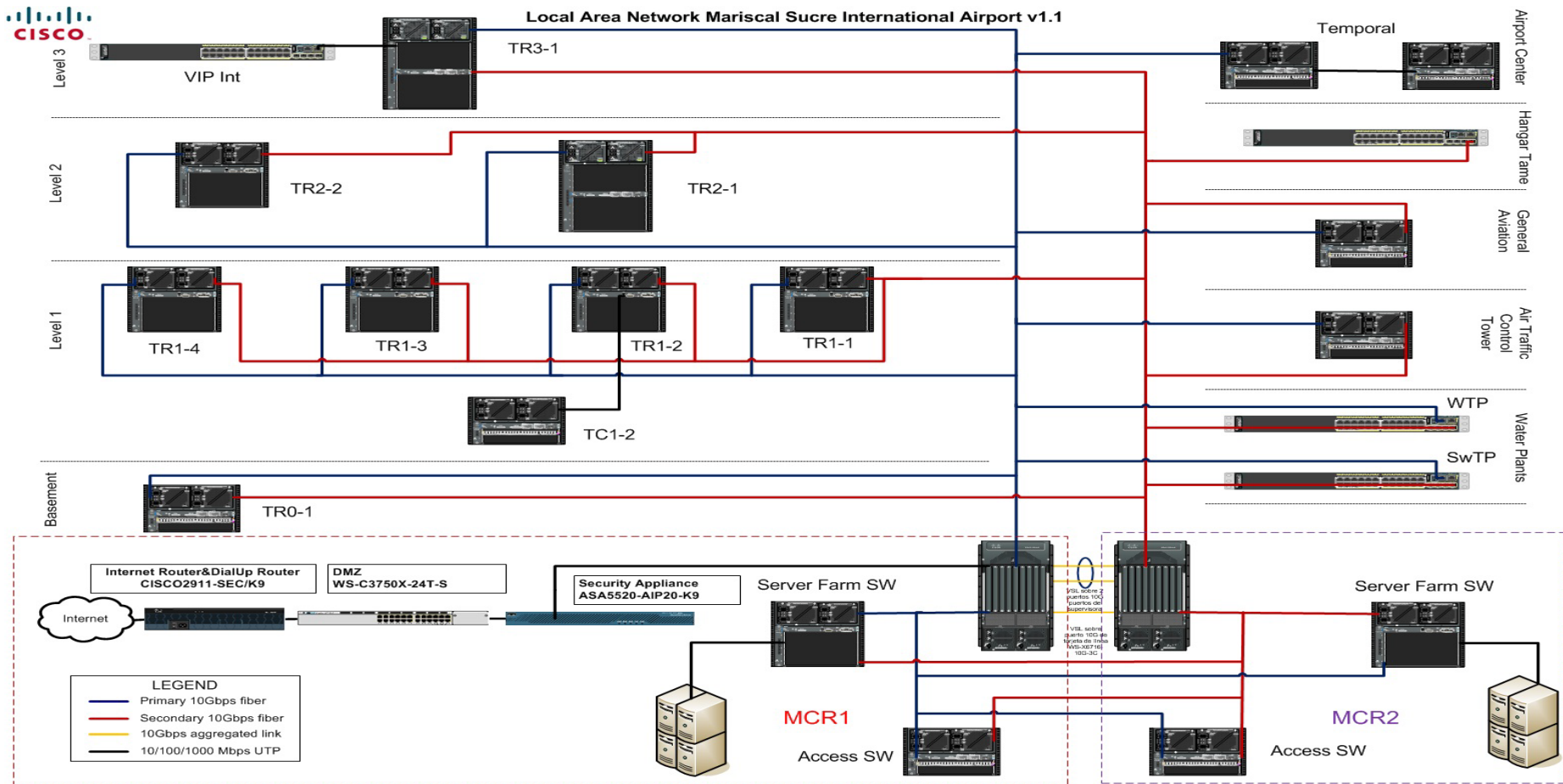


Figura N° 87. Diagrama de la Red Lan del AIMS.

CAPÍTULO V

5.1. Estudio Económico.

El proyecto del sistema de video vigilancia es vital para la seguridad del Aeropuerto Internacional Mariscal Sucre, la tendencia creciente del auge delictivo en esta zona es muy alta, razón por la cual es muy importante la implementación de un sistema de video vigilancia automatizado con tecnología de punta basado en IP.

Licencias en estudio de factibilidad para la implementación del sistema de video vigilancia.

Tabla N° 10. Licencias y Software GENETEC.

LICENCIAS Y SOFTWARE			
No.	Descripción	Cantidad	Valor Total
1	Cctv Software License For Monitors	4	44.000
2	DVSS License Key	1	25.000
3	Sofmonitor License	1	22.000
4	Map Navigation Software License	4	20.000
5	License To Record One Camera	1	8.000
6	License To View On Live Camera Feed	1	8.000
7	Management Console For Vmware	1	8.000
8	Mapping Server Software	1	8.000
9	Backup Software	1	6.600
10	Alarm Management Software License	4	6.400
11	DMS License	1	6.000
12	Host For Vmware Management Console	1	6.000
13	IMS License	1	6.000
14	Virtual Machine Software	1	6.000
15	VMS License	1	6.000
16	Intercom Desktop Software License	1	4.000
17	Windows Server 2008 R2 64-Bit Standard	5	3.000
18	Badge Image Designer	1	2.995
19	Microsoft 64-Bit Sql 2008 R2	2	2.400
20	Licencia LK – Substation	1	2.000
21	Licencia De Puertas	1	1.400
22	Windows Server 2008 R2 64-Bit	1	1.340
23	3C Server License	1	900
24	Microsoft 64-bit SQL 2005 Sp1	1	600
25	Windows Server 2003 R2 64-Bit Standard	1	600

26	License Plugin	1	80
27	Canon License Plugin	1	60
TOTAL			205.375

Red LAN (Cableado & Networking)

Cableado.

Tabla N° 11. Cableado Estructurado.

DESCRIPCIÓN	VALOR TOTAL
Material de Ducteria y Canalización Horizontal.	171.503
Materiales de Cableado Estructurado Horizontal de Cobre.	853.695
Material de Cableado BACKBONE de Fibra Optica.	1.036.261
Material de Aterrizamiento Telecomunicaciones.	11.845
Instalación de Canaletas y Ducterías Metalicas.	25.725
Instalación de Cableado Estructurado de Cobre.	184.995
Instalación de Cableado de Fibra Optica.	191.424
TOTAL DEL CABLEADO	2.475.443

Networking.

Descripción de la tabla de los cuartos de comunicaciones operativos en los diferentes niveles del Aeropuerto.

PTB: Passenguer Building Terminal

NIVEL: EL Aeropuerto tiene varios pisos o niveles.

MCR1: Cuarto de Comunicaciones Principal

TR: Cuartos de Comunicaciones ubicados dentro del mismo nivel.

Tabla No. 12 Cuartos de Comunicaciones y Networking.

DESCRIPCIÓN	VALOR TOTAL
PTB – NIVEL 0 MCR1	440.394
PTB – NIVEL 0 TR0-1	21.480
PTB – NIVEL 1 TR1-1	38.975
PTB – NIVEL 1 TR1-2	44.470
PTB – NIVEL 1 TR1-3	38.975
PTB – NIVEL 1 TR1-4	38.975
PTB – NIVEL 1 TC1-2	21.480
PTB – NIVEL 2 TR2-1	191.933
PTB – NIVEL 2 TR2-2	141.669

PTB – NIVEL 3 TR3-1	130.797
EDIFICIOS EXTERNOS	132.936
FSMB-NIVEL 1 –MCR2	506.460
ACCESS POINT RED WI-FI	7.772
TOTAL DE EQUIPOS	1.756.316
TOTAL INSTALACIÓN Y CONFIGURACIÓN	263.447
TOTAL	2.019.763

Valores torales:

Tabla N° 13. Costo Total de Red LAN del AIMS.

TOTAL DE VALORES EN CABLEADO	2.475.443
TOTAL DE VALORES EN CABLEADO	2.019.763
RED LAN TOTAL	4.495.206

Hardware

El Aeropuerto Internacional Mariscal Sucre al ser una institución de servicio de transporte aereo requiere de una optima seguridad operacional, por lo cual cuenta con la siguiente lista de equipos tecnológicos que brindarán el apoyo necesario para operar el Sistema de video vigilancia aeroportuario.

Tabla No. 14 Equipos tecnologicos Del CCTV.

#	Marca	Modelo	Cant.	Descripción	Nombre del equipo	Vlan	Dirección ip	Ubicación
1	HP	DL360e	1	eth3 - Local Area Connection	P2000SERVER	104	172.16.104.2	MCR1
2	HP	DL360e	1	eth3 - Local Area Connection	P2000SERVER	104	172.16.104.2	MCR2
3	HP	DL360e	1	Directorio 1 CCTV MCR-1	DIRECTORY1	101	172.16.101.3	MCR1
4	HP	DL380e	1	Archivador 1 CCTV MCR-1	ARCHIVER1	101	172.16.101.4	MCR1
5	HP	DL380e	1	Archivador 2 CCTV MCR-1	ARCHIVER2	101	172.16.101.5	MCR1
6	Veracity	Coldstore	1	Coldstore-1 MCR1	COLDSTORE1	101	172.16.101.6	MCR1
7	Veracity	Coldstore	1	Coldstore-2 MCR1	COLDSTORE2	101	172.16.101.7	MCR1
8	Veracity	Coldstore	1	Coldstore-3 MCR1	COLDSTORE3	101	172.16.101.8	MCR1
9	HP	DL360e	1	Directorio 2 CCTV MCR-2	DIRECTORY2	101	172.16.101.10	MCR2
10	HP	DL380e	1	Archivador 1R CCTV MCR-2	ARCHIVER1R	101	172.16.101.11	MCR2
11	HP	DL380e	1	Archivador 2R CCTV MCR-2	ARCHIVER2R	101	172.16.101.12	MCR2
12	Veracity	Coldstore	1	Coldstore-1R MCR-2	COLDSTORE1R	101	172.16.101.13	MCR2
13	Veracity	Coldstore	1	Coldstore-2R MCR-2	COLDSTORE2R	101	172.16.101.14	MCR2
14	Veracity	Coldstore	1	Coldstore-3R MCR-2	COLDSTORE3R	101	172.16.101.15	MCR2
15	HP	DL320e	1	Mobiler-server CCTV MCR-1	MobileServer	101	172.16.101.16	PTB
16	HP	Z820	1	WORKSTATION LAB	Video-HP	104	172.16.104.5	LAB
17	HP	Z440	1	Estacion trabajo operador 1 COCC	EPM-Op1	115	172.16.115.41	COCC - EPM
18	HP	Z440	1	Estacion trabajo operador 2 COCC	EPM-Op2	115	172.16.115.42	COCC - EPM
19	HP	Z440	1	Estacion trabajo operador 3 COCC	EPM-Op3	115	172.16.115.43	COCC - EPM
20	HP	Z440	1	Estacion trabajo Supervisor COCC	EPM-Supervisor	115	172.16.115.44	COCC - EPM
21	HP	Z440	1	Estacion trabajo operador ADC-COCC	ADC-COCC	115	172.16.115.45	PTE UBICACIÓN FINAL
22	HP	Z440	1	Estacion trabajo operador ADC-COE	ADC-COE	115	172.16.115.46	PTE UBICACIÓN FINAL
23	HP	Z440	1	Estacion trabajo de Torre de control	DGAC-TWR	115	172.16.115.47	PTE UBICACIÓN FINAL
24	HP	Z440	1	Estacion trabajo de Bomberos	ADC-Bomberos	115	172.16.115.48	PTE UBICACIÓN FINAL
25	HP	Z440	1	Estacion trabajo de gerencia	EPM-Gerencia	115	172.16.115.49	OF. DIR. SEGURIDAD - EPM
26	HP	Z230	1	Estacion de visualizacion en video Wall	EPM-Monitor1-2	115	172.16.115.50	COCC - EPM
27	HP	Z230	1	Estacion de visualizacion en video Wall	EPM-Monitor3-4	115	172.16.115.51	COCC - EPM

28	HP	Z230	1	Estacion de visualizacion en video Wall	EPM-Monitor5-6	115	172.16.115.52	COCC - EPM
29	HP	Z230	1	Estacion de visualizacion en video Wall	COCC-Monitor1-2	115	172.16.115.53	PTE UBICACIÓN FINAL
30	HP	Z230	1	Estacion de visualizacion en video Wall	COCC-Monitor3-4	115	172.16.115.54	PTE UBICACIÓN FINAL
31	HP	Z230	1	Estacion de visualizacion en video Wall	COCC-Monitor5-6	115	172.16.115.55	PTE UBICACIÓN FINAL
32	HP	Z440	1	Estacion de Carnetizacion – EPM	EPM-TCA	115	172.16.115.56	OF. TCA - EPM
33	HP	Z440	1	Estacion de Carnetizacion – EPM	EPM-1TCA	115	172.16.115.57	OF. TCA - EPM
34	HP	Z230	1	Estacion de visualizacion en video Wall	EPM-Monitor-ACC2	115	172.16.115.58	COCC

CAPITULO VI

6.1. CONCLUSIONES

Para la implementación del nuevo sistema de video vigilancia Genetec, se realizó un análisis técnico del nivel de desempeño de los sistemas de seguridad que existían al momento en actividad, para lo cual se hizo un análisis de: infraestructura de red LAN, sistema contra incendios, botones de pánico, intercomunicadores, control de accesos, y CCTV, la integración de todos los sistema antes mencionados forman el sistema de seguridad integrado del aeropuerto y los resultados obtenidos durante el presente estudio se resumen a continuación:

- La infraestructura de red, del aeropuerto tienen una escalabilidad de crecimiento aceptable para futuras ampliaciones del sistema, cuenta con Switches marca cisco, modelo Catalyst 4503-E - WS-C4503-E, tienen la capacidad de 96 puertos 10/100 Fast Ethernet (RJ-45), la ubicación de los cuartos de comunicación y racks están distribuidos de manera estratégica en los diferentes niveles que permite brindar un servicio de red a todos los ambientes del aeropuerto. El cuarto de comunicaciones secundario denominado redundante está instalado fuera del edificio principal y actualmente se conecta con fibra optica monomodo.
- Se realice un análisis técnico sobre el direccionamiento IP de la red LAN, y se determino que hay que reestructurar la red, para lo cual se considero crear VLAN's para los servidores, CCTV, equipos de trabajo, control de accesos, y la configuración de políticas del calidad de servicio QoS.
- **Conectividad:** La red troncal de fibra óptica, se encuentra disponible y es administrado y mantenido por Quiport. También el cableado horizontal de cobre CAT6A es administrado por Quiport. Si existe la necesidad incrementar puntos de

red y cualquier otro requerimiento que exija el servicio de red, será gestionado y direccionado a Quiport.

- Para la implementación del nuevo sistema de video vigilancia Genetec, se realizó un plan estratégico y un cronograma de tiempos estimados, y así para proceder a instalar el nuevo sistema de video vigilancia en la cual se detalla a continuación el proceso:
 - Una vez realizada el análisis de la infraestructura de red, se procedió a instalar los equipos con el nuevo sistema de seguridad GENETEC. La migración de las cámaras al nuevo sistema se realizo de manera paulatina, todo esto dependiendo del área de vulnerabilidad y flujo de pasajeros.
 - Dentro del centro de control y monitoreo CCTV se puso a un ingeniero de soporte, para poder trabajar en conjunto con las personas encargadas de la integración. El sistema fue instalado de forma paralela al sistema antiguo.
 - Finalizado la migración de todos los componentes en un plazo de 2 meses trabajando en turnos de día y noche, se iniciaron con las pruebas de rigor de funcionamiento, afinamiento en cuanto a las configuraciones, y salir en vivo con todos los sistemas que integran el sistema aeroportuario.
- En la actualidad dentro de las redes convergentes se busca dar un servicio de comunicaciones eficientes y eficaces, sin embargo en una red homogénea y unificada como la del Aeropuerto Mariscal Sucre requiere de la configuración de calidad de servicios (QoS).
- El sistema de video vigilancia Genetec tiene como característica ser una plataforma modular y multiusuario. Combina de manera transparente los sistemas de seguridad implementados en el Aeropuerto, está basada en tecnología IP y brinda al operador del Centro de Control CCTV una interfaz intuitiva y amigable simplificando de manera eficiente el monitoreo en todas las operaciones de seguridad.

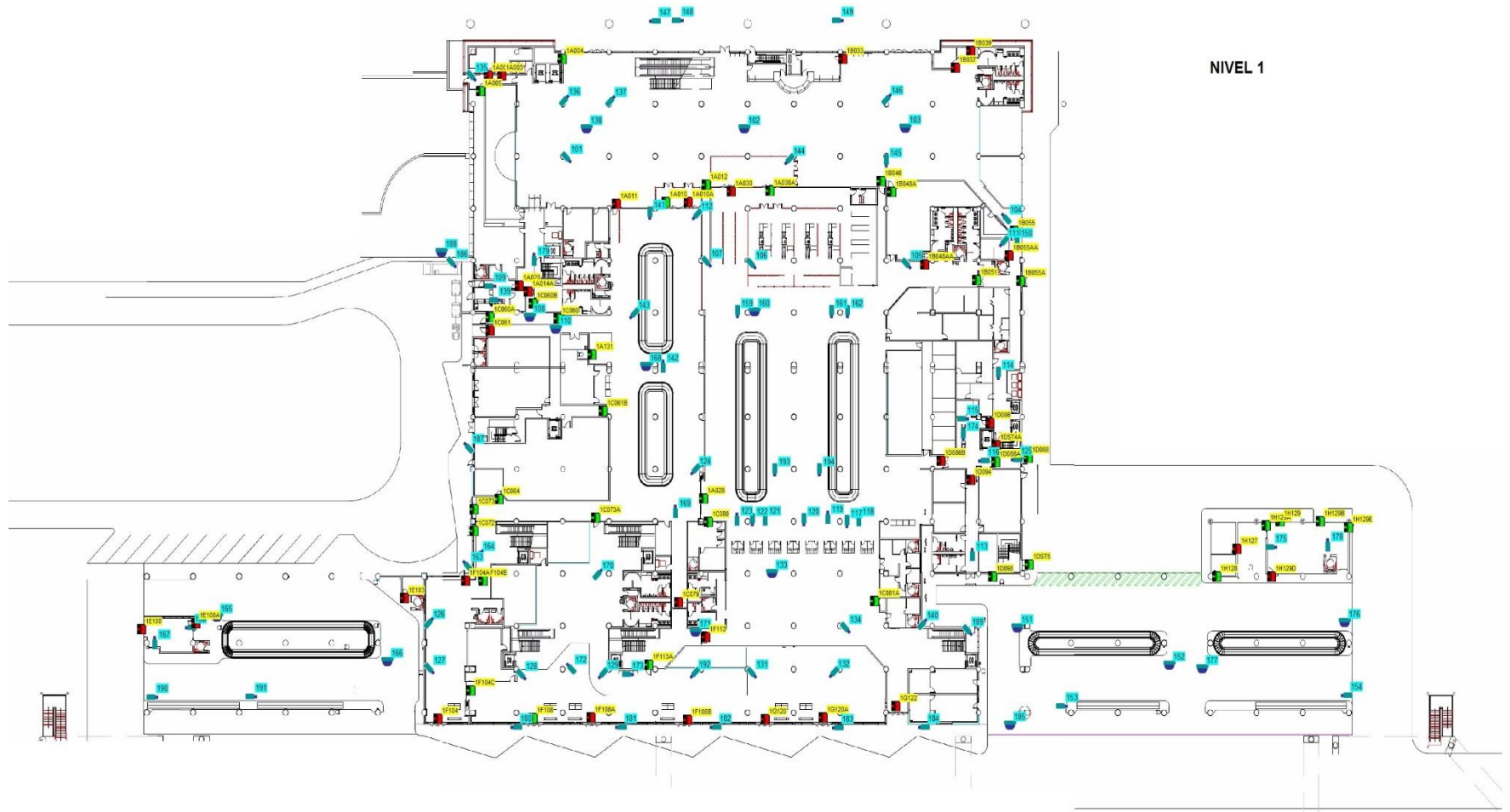
6.2. RECOMENDACIONES

- Mantener actualizado el sistema GENETEC con sus últimas versiones, esto permite que los dispositivos de Red (cámaras), operen de manera eficiente y no tengan problemas con los demás sistemas de seguridad. El sistema tiene como característica un monitoreo del estado del sistema presentándole al operador del sistema su rendimiento de funcionalidad.
- El sistema de video vigilancia implementado en el Aeropuerto Internacional Mariscal Sucre, al ser un sistema de comunicaciones unificadas y estar integrado con varios sistemas de seguridad tiene un constante monitoreo y mantenimiento preventivo en todo sus componentes y dispositivos. La información recopilada por el sistema de videos e imágenes está procesada y almacenada en servidores propios del fabricante GENETEC.
- El avance tecnológico de los sistemas de video vigilancia IP, hace que los equipos de diferentes fabricantes se acoplen de manera eficiente, las integración de cámaras con diferentes característica son administradas por el sistema GENETEC, esto hace que las cámaras instaladas en las diferentes áreas brinden un monitoreo óptimo y eficiente.
- El sistema de video vigilancia está basado en tecnología de comunicaciones unificadas, la implementación del sistema de video vigilancia IP tiene como característica ser parte de varios sistemas como: sistema control de accesos, sistema de botones de pánico, sistemas contra incendios, la integración de estos sistemas hace el aeropuerto tenga un sistema central integrado de seguridad y requiere de un constante mantenimiento preventivo.

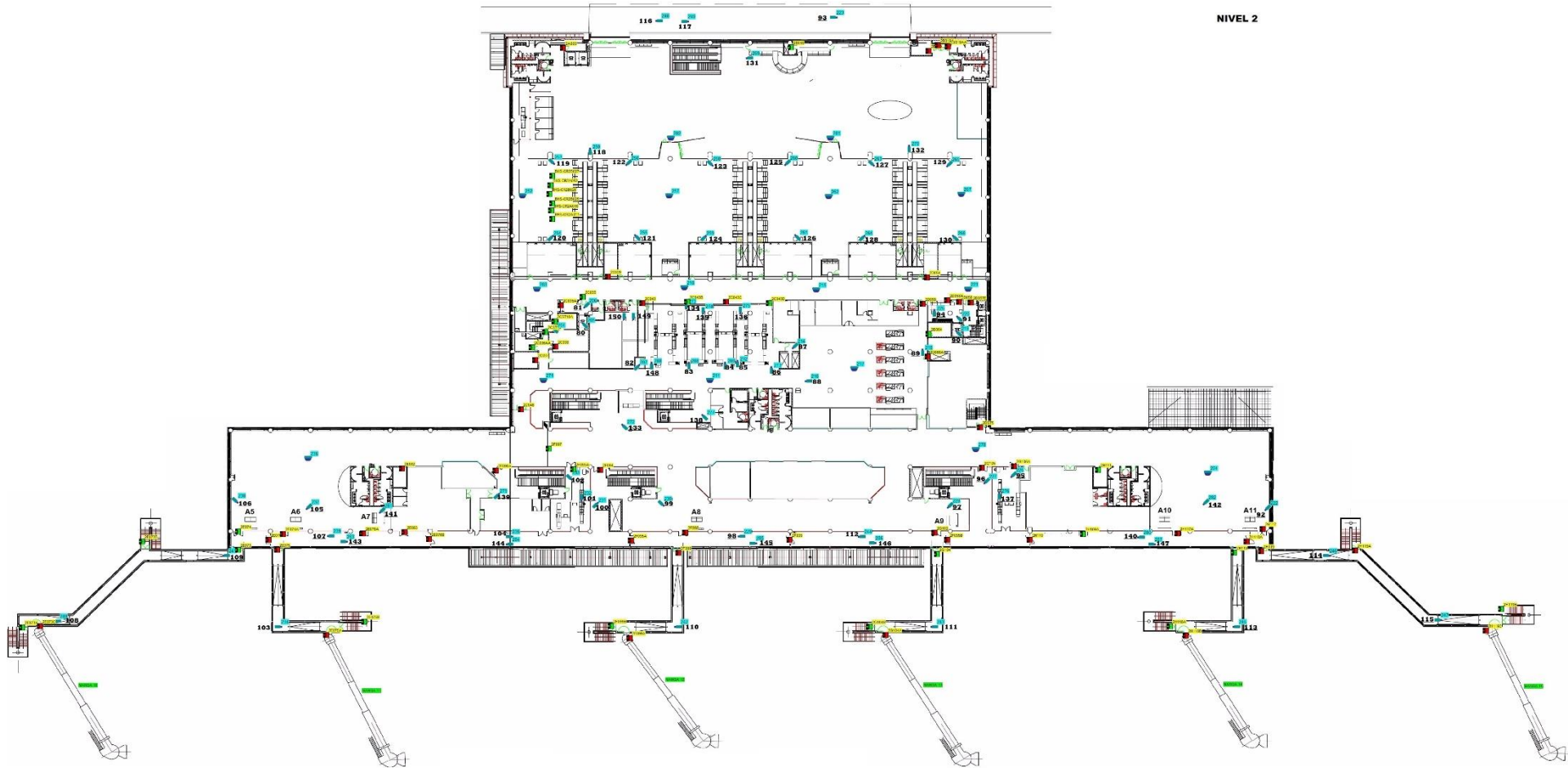
BIBLIOGRAFÍA.

- [1]. CCTV. Recuperado de:
https://es.wikipedia.org/wiki/Circuito_cerrado_de_televisión.
- [2]. http://www2.congreso.gob.pe/Sicr/TraDocEstProc/Contdoc03_2011.nsf/
- [3]. [http://seguridadig.com/historia-del-circuito-cerrado-de-television-cctv/\(2016\)](http://seguridadig.com/historia-del-circuito-cerrado-de-television-cctv/(2016)).
- [4] [http://camarasdeseguridad.jimdo.com/historia-e-información-del-sistema-dvr/\(2016\)](http://camarasdeseguridad.jimdo.com/historia-e-información-del-sistema-dvr/(2016)).
- [5] http://www.novenca.com/site/index.php?option=com_content&view=article&id=257&Itemid=159 (2016).
- [6] http://www.novenca.com/site/index.php?option=com_content&view=article&id=257&Itemid=159.
- [7] La tercera generación del CCTV:http://www.seguridad-online.com.ar/index.php?mod=Home&ac=verNota&id_notas=435&id_seccion=149.
- [8] https://es.wikipedia.org/wiki/Joint_Photosharing_Group.
- [9] Morion. MPEG. Recuperado de: <http://www.axis.com/ve/es/learning/web-articles/technical-guide-to-network-video/compression-formats>.
- [10] Formato H.264. Recuperado de: [https://es.wikipedia.org/wiki/H.264/MPEG-](https://es.wikipedia.org/wiki/H.264/MPEG-4)
- [11] H.264 o MPEG-4 es una norma que define un códec de vídeo de alta compresión desarrollada por la ITU-T.
- [12] Grabador de video digital. Recuperado de:
https://es.wikipedia.org/wiki/Grabador_de_video_digital.
- [13] NVR (Network Video Recorder). Recuperado de: Grabador de Video en Red.
- [14] POE. Recuperado de: https://es.wikipedia.org/wiki/Power_over_Ethernet.
- [15] http://www.axis.com/files/whitepaper/wp_encoders_34384_es_0902_lo.pdf.
- [16] Ventas de servidores en red. Recuperado de: <http://www.dointech.com.co/video-vigilancia-ip.html>.
- [17] AIMS. (Aeropuerto Internacional Mariscal Sucre).
- [18] USAP. (Programa de auditoría de la seguridad universal).
- [19] OACI. (Organización de la Aviación Civil Internacional).

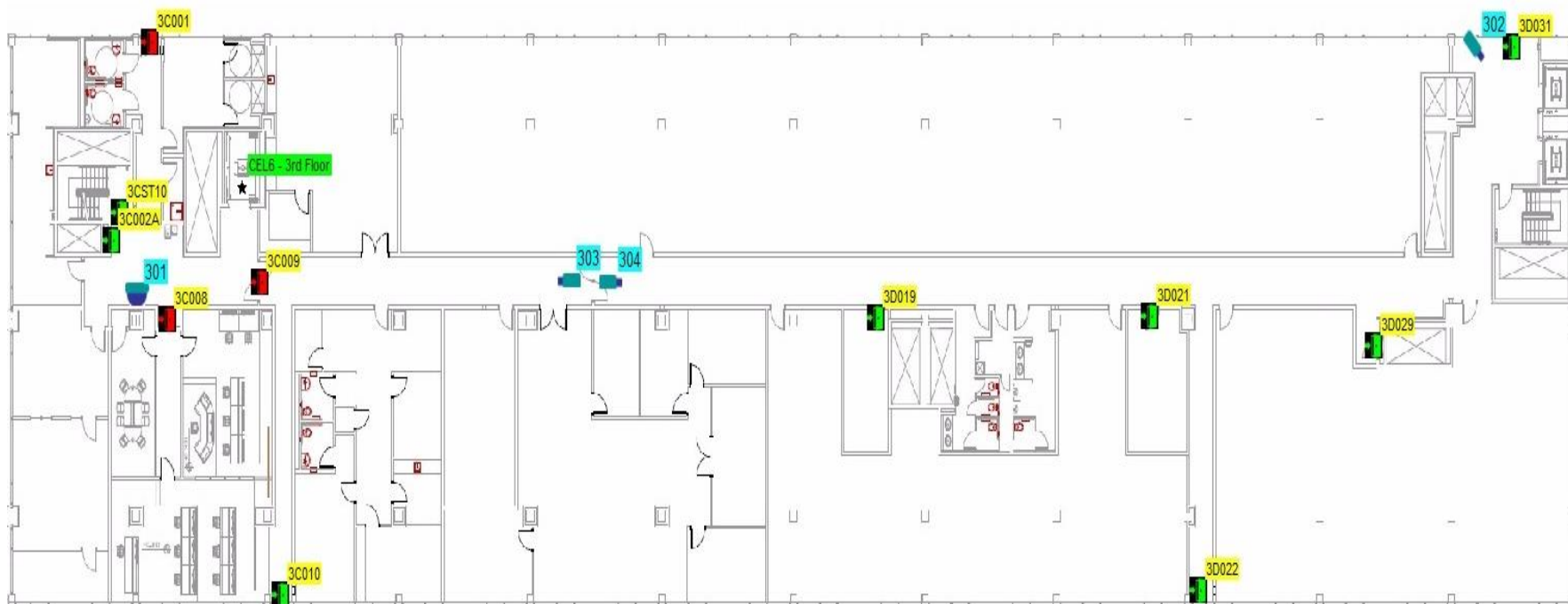
- [20] Toma Satelital del Aeropuerto Internacional Mariscal Sucre. Recuperada de: <https://www.google.com/maps/place/Aeropuerto+Internacional+Mariscal+Sucre/@-0.131836,-78.357239,12560m/data=!3m1!1e3!4m2!3m1!1s0x91d58db4352baa87:0x2f9f7623e0894b8b!6m1!1e1?hl=es>.
- [21] <https://www.milestonesys.com/es/productos/video-management-software/xprotect-professional/>.
- [22] <https://www.milestonesys.com/es/productos/video-management-software/xprotect-professional/>.
- [23] <https://www.genetec.com/es/soluciones/productos/security-center>.
- [24] <https://www.genetec.com/es/soluciones/productos/security-center>.
- [25] Unicast. Recuperado de: <https://es.wikipedia.org/wiki/Unicast>.
- [26] Multicast. Recuperado de: <http://www.delfirosales.com/2009/06/metodos-de-transmision-unicast.html>.
- [27] NIC. Network Interface Card.
- [28] <http://www.genetec.com/es/acerca/noticias/centro-de-prensa/notas-de-prensa/genetec-presenta-la-nueva-versi3n-de-su-security-center>.
- [30] <https://riunet.upv.es/bitstream/handle/10251/34082/memoria.pdf?sequence=1>.
- [31] <https://www.google.com/search?client=opera&q=que+es+unicast&sourceid=opera&ie=UTF-8&oe=UTF-8#q=CABLE+UTP>.
- [32] <http://aeropuertoquito.com/aeropuerto-mariscal-sucre/infraestructura/>.
- [33] <http://aeropuertoquito.com/aeropuerto-mariscal-sucre/infraestructura/>.
- [34] AIMS. Aeropuerto Internacional Mariscal Sucre.
- [35] <https://sites.google.com/site/redessconvergentes/unidad-ii/1-introduccion-qos>.



-
-
- ANEXO 3, MAPA DE CÁMARAS INSTALADAS EN EL NIVEL 2

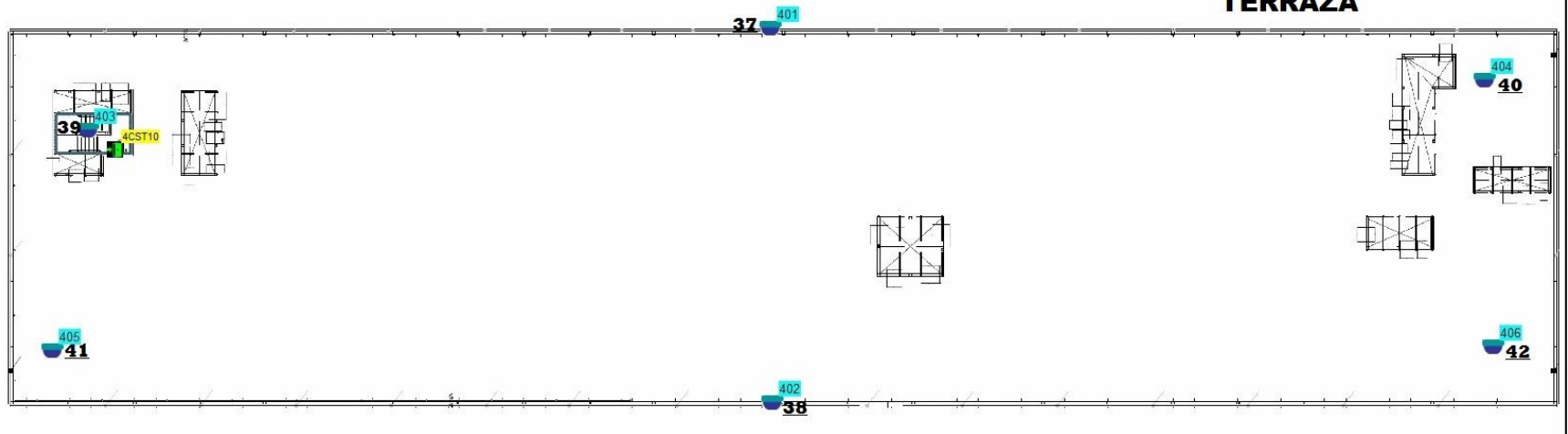


- ANEXO 4, MAPA DE CÁMERAS INSTALADAS EN EL NIVEL 3

NIVEL 3

- **ANEXO 5, MAPA DE CÁMARAS INSTALADAS EN EL NIVEL 4 (Terraza)**

**NIVEL 4
TERRAZA**



ANEXO NO. 6. Manual De Usuario Del Sistema De Seguridad Genetec