UNIVERSIDAD RICARDO PALMA

FACULTAD DE INGENIERÍA

PROGRAMA DE TITULACIÓN POR TESIS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

APLICACIÓN DE LA PLATAFORMA VMS PARA OPTIMIZAR LA SEGURIDAD ELECTRÓNICA DEL CENTRO DE MONITOREO DE LA UNIVERSIDAD RICARDO PALMA, 2019

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO

PRESENTADO POR:

Bach. GONGORA ZALAZAR, FEDERICO AXEL

Bach. NOLASCO ARIAS, RENATO MIGUEL

ASESOR: Ing. CUADRADO LERMA, LUIS ALBERTO

LIMA – PERÚ

2019

DEDICATORIA

Esta tesis está dedicada, en primer lugar, a Dios, seguidamente a nuestros padres quienes con su amor, paciencia y esfuerzo nos han permitido llegar a cumplir hoy un sueño más, gracias por inculcarnos el ejemplo de esfuerzo y valentía. A toda nuestra familia porque con sus oraciones, consejos y palabras de aliento hicieron de cada uno de nosotros una mejor persona y de una u otra forma nos acompañan en todas nuestras metas.

AGRADECIMIENTO

Queremos expresar nuestra gratitud a Dios, quien con su bendición llena siempre mi vida y a nuestras familias por estar siempre presentes. De igual manera nuestros agradecimientos a la Universidad Ricardo Palma, a toda la Facultad de Ingeniería Electrónica, a mis docentes. Finalmente queremos expresar nuestro más grande y sincero agradecimiento al Ing. Luis Alberto Cuadrado Lerma, quien con su dirección, conocimiento, enseñanza y colaboración permitió el desarrollo de este trabajo

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El actual trabajo de investigación de título Aplicación de la Plataforma VMS para optimizar la Seguridad Electrónica del Centro de Monitoreo de la Universidad Ricardo Palma, 2019 tuvo como objetivo la optimización de los sistemas de seguridad electrónica, los cuales se consideran los sistemas de video vigilancia y control de acceso, mediante la aplicación de una plataforma VMS que integra dichos sistemas, a través de la red LAN, en una sola interfaz de gran versatilidad y altas configuraciones de políticas de seguridad modernas. Primeramente, se tuvo que comparar las características fundamentales entre los dispositivos propuestos de cada sistema, con la finalidad de elegir, técnicamente como económicamente, los equipos con mejor compatibilidad entre ellos. Para cumplir los objetivos del presente trabajo de investigación se tuvo que determinar el diseño de topología del sistema para aplicar la plataforma VMS, se estableció la parte de control y configuración de todo el sistema, y se simuló el sistema VMS para obtener pruebas del correcto funcionamiento y alta seguridad perimetral.

Palabras Claves: VMS, seguridad electrónica, video vigilancia, control de acceso, LAN, políticas de seguridad.

ABSTRACT

The current research project entitled Application of the VMS Platform to optimize the Electronic Security of the Monitoring Center of the University Ricardo Palma, 2019 was aimed at optimizing electronic security systems, which are considered video systems surveillance and access control, through the application of a VMS platform that integrates these systems, through the LAN, into a single interface of great versatility and high configurations of modern security policies. First, the fundamental characteristics had to be compared between the proposed devices of each system, in order to choose, technically and economically, the equipment with the best compatibility between them. To meet the objectives of this research work, the system topology design to apply the VMS platform had to be determined, the control and configuration part of the entire system was established, and the VMS system was simulated to obtain proof of proper functioning. and high perimeter security.

Keywords: VMS, Electronic security, video surveillance, access control, LAN, security policies.

INTRODUCCIÓN

Hoy en día la criminalidad y violencia en el Perú está en aumento, se ven en los noticieros locales que diariamente las personas circulan con mayor temor por la inseguridad que se vive actualmente. A esto también está propenso las empresas, negocios, universidades, entre otros, ya que probablemente algunas empresas desconozcan o no cuenten con un sistema de seguridad electrónico sofisticado y seguro con el avance tecnológico que está en constante actualización. En donde en el primer capítulo de esta tesis damos a conocer la problemática de la Universidad Ricardo Palma y cómo puede ser solventada.

Esto ayuda a proteger la seguridad física perimetral y el acceso hacia oficinas dentro de la misma a personales autorizados. Por ello es bueno saber qué o quienes están ingresando y/o saliendo de sus lugares de trabajo dando la certeza de saber si son personales que laboran en la empresa o si es que son usuarios externos. Para esto, en el segundo capítulo abarcamos cuáles son los antecedentes de investigación y bases teóricas para una mayor compresión de esta tesis, así como también para la seguridad electrónica.

Como se menciona anteriormente, la seguridad electrónica es importante, más aún para entidades la cual tienen mucha demanda de personas, como lo es la Universidad Ricardo Palma. Dicha universidad es concurrida por muchas personas entre ellos están: alumnos, docentes, personal administrativo, trabajadores, así como también gente externa, es decir, personas que no cumplen ninguna función en el mismo, pero sin embargo ingresan, por ejemplo: para pedir informes, o son familiares de alumnos, etc.; en la cual hacemos uso de qué tipo y método de estudio está relacionado la investigación, como se menciona en el tercer capítulo.

En el cuarto capítulo se menciona que, para un control de mucha demanda de personas autorizadas y no autorizadas en la URP, se aplicaron las bases teóricas y prácticas del capítulo dos para el diseño este proyecto para dar una mayor seguridad, usando una plataforma unificada que envíe registro de grabación de cámaras de videovigilancia con una buena resolución de video, una plataforma Video Management System. En donde todo este proceso conlleva una inversión para que se pueda dar una muy buena seguridad perimetral, como se referencia en el quinto capítulo.

CAPÍTULO I: PLANTEAMIENTO DEL ESTUDIO

1.1 Descripción y formulación del problema general y específicos

1.1.1 Descripción del problema

La Universidad Ricardo Palma, importante universidad de prestigio, hoy en día cuenta con un centro de monitoreo con un sistema de video-vigilancia conformado por un conjunto de cámaras y grabador central, interconectados a través de la red IP interna, la cual se gestiona por un software de monitoreo y grabación, distribuido en dos operadores, los cuales se encargan de supervisar los sucesos en las puertas de entrada y vehiculares, y en los pasillos del edificio "Aulario". Al realizar un estudio técnico en el centro de monitoreo, se encontraron cámaras inactivas, con baja resolución, mala calibración y lentes con suciedad; la falta de actualización del software existente y de la alta complejidad que demanda la configuración de dicho software.

Con respecto a las cámaras, al tener los problemas mencionados, ello puede implicar en posibles pérdidas de evidencia video gráfica y caídas ocasionales de señal.

Con respecto a la actualización y configuración software, la entidad al solicitar al fabricante del software, personal capacitado para realizar dichas acciones, puede resultar en costos muy elevados.

Analizando el problema, nos percatamos que la entidad no cuenta con un centro de monitoreo actualizado y conforme a las tendencias tecnológicas de la actualidad. Por consiguiente, es necesaria la optimización y renovación del centro de monitoreo, el cual debe brindar la información en tiempo real, fácil manejo para los operadores y permitir comunicación con sistema de control de accesos.

Según los requerimientos observados, se propone aplicar la plataforma VMS junto con un diseño de sistema de video-vigilancia integrado con un sistema de control de accesos, así mismo unificando dentro de la red LAN que tiene la universidad, para que la respuesta del control de monitoreo a través de cámaras y el control de acceso a personas, se de en tiempo real, y poder llevar a cabo una mejor calidad de servicio.

1.1.2 Problema principal

¿Cómo se aplicará la plataforma VMS para optimizar la seguridad electrónica del centro de monitoreo de la Universidad Ricardo Palma, 2019?

1.1.3 Problemas secundarios

a) ¿Cómo será el diseño de la topología del sistema de seguridad aplicando la plataforma VMS en el centro de monitoreo?
b) ¿Cómo será el diseño de la parte control de monitoreo del sistema de seguridad aplicando la plataforma VMS en el centro de monitoreo?
c) ¿Cómo será la simulación del sistema de seguridad aplicando la plataforma VMS en el centro de monitoreo?

2.1 Objetivo general y específicos

2.1.1 Objetivo general

Determinar la aplicación de la plataforma VMS para optimizar la seguridad electrónica en el centro de monitoreo de la Universidad Ricardo Palma.

2.1.2 Objetivos específicos

a) Determinar el diseño de la topología del sistema de seguridad aplicando la plataforma VMS en el centro de monitoreo.
b) Establecer el diseño de la parte de control del sistema de seguridad aplicando la plataforma VMS en el centro de monitoreo.
c) Implementar la simulación del sistema de seguridad aplicando la plataforma VMS en el centro de monitoreo.

2.2 Limitación de la investigación: temporal espacial y temática

Como limitación del estudio se tiene:

Teórica: Bibliografía relacionada con la plataforma y con sistemas unificados de video-vigilancia y control de acceso.

Espacial: El proyecto se realizará en el Centro de monitoreo de la Universidad Ricardo Palma, Distrito de Santiago de Surco, Lima, Perú.

Temporal: Comprende el periodo mayo a noviembre de 2019.

2.3 Justificación e importancia

2.3.1 Justificación

Teórico: Con la aplicación de la plataforma VMS va a ayudar a generar mayor protección y tranquilidad hacia los estudiantes, docentes, personal administrativo, etc. dentro de las instalaciones de la universidad.

Práctico: La aplicación la plataforma VMS nos ayudará a unificar los eventos y sucesos registrados para una mejor comunicación en tiempo real, bajo una red LAN existente, los sistemas de video-vigilancia y control de accesos

2.3.2 Importancia

La importancia de este proyecto de tesis se basa en una oportunidad de optimización y redefinición de parámetros de seguridad electrónica en el centro de monitoreo, mejorando calidad de visualización, con mayor nitidez de la imagen, así como video registros en su base de datos en tiempo real, añadiéndose además eventos de acceso de miembros y visitantes de la universidad por la unificación de sistemas a través de la red LAN existente.

CAPITULO II: MARCO TEÓRICO

2.1 Antecedentes del estudio de investigación

2.1.1 Antecedentes internacionales

Chávez, M (2016), en su tesis sostiene que:

> Se obtiene gran control de acceso y seguridad de cada una de las subestaciones en tiempo real; y de acuerdo a la configuración de stream de video se observó que la transmisión es en tiempo real y el ancho de banda generado no satura el canal de la red de datos. (p.65)

Las conclusiones de esta investigación solo mencionan la aplicación de video vigilancia, mas no mencionan que se haya aplicado la unificación de control de acceso y videovigilancia, como en el caso de nuestra investigación.

Pavón, J (2016), en su tesis nos dice que:

> 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. (p.122)

En esta investigación no se menciona que parámetros de seguridad ni configuraciones se emplea en dicha localidad.

2.1.2 Antecedentes nacionales

Peláez, J. (2013), en demuestra que:

> Con respecto a las Horas-Hombre destinado al control de activos con el sistema actual es de 23.44 hora/soles, en comparación al sistema propuesto que es de 25.00 hora/soles, lo que determina una reducción de horas hombre de 1.56 hora/soles; lo cuál permitirá una reducción de 6.24% para el control de activos. Con respecto al Tiempo de respuesta de consulta en tiempo real con el sistema actual es de 27.26 segundos, en comparación al Sistema propuesto que es de 3.42 segundos, lo que determina una reducción de tiempo de 23.84 segundos; lo cuál permitirá una reducción del 87.45% de las consultas de acceso remoto. (p.154)

En este trabajo de investigación no se registran los hechos delictivos e incidencias en forma de reportes dentro de una base de datos dentro de la plataforma aplicada.

Perez, C. (2016), en su tesis manifiesta que:

> El diseño del sistema para la implementación de un sistema de monitoreo centralizado de seguridad asegura un control adecuado desde un solo punto con todas las señales reunidas en monitores de visualización que podrán reducir hurtos y daños a la propiedad en la instalación minera donde sea instalada. (p.100)

Sin embargo, se debe tener en cuenta la distancia máxima permitida del cable UTP, y los switches a utilizar para no perder la señal de video.

Puse, R; Ruiz, M (2015), en su tesis menciona que:

> El sistema de gestión y monitoreo nos permite contar con un historia de eventos, lo cual sirve al administrador para tomar las medidas respectivas en los mantenimientos preventivos; el sistema de gestión y monitoreo además nos permite la creación de notificaciones, lo cual facilita la visualización de un problema; el sistema de gestión y monitoreo permite el acceso directo a la interfaz web de los dispositivos, logrando así la configuración remota de los mismos; el sistema de gestión y monitoreo

permite el envío de notificaciones vía email, con ello asegurando una mejor administración del sistema. (p.136)

Se concluye que al implementar un sistema de monitoreo y gestión se logra optimizar los recursos humanos empleados en la atención de problemas para la reducción de costos y mejorar los tiempos de respuesta ante averías, sin embargo, se tiene que considerar que dichas funcionalidades y características se encuentren disponibles en la plataforma y el licenciamiento adecuado.

2.2 Bases teóricas vinculadas a las variables de estudio

2.2.1 Plataforma VMS

Son sistemas de información que permiten ejecutarse en todo tipo de hardware, acoger gran cantidad de periféricos y dispositivos IP's o dispositivos analógicos, manejar y gestionar flujos de video y eventos que ingresan al sistema, para poder hacer con ellos, las accione que un administrador u operador dispongan.

Es un aplicativo software que combina funciones de videovigilancia IP, control de acceso y comunicaciones en un aplicativo intuitivo y modular para los usuarios operadores de seguridad, donde se debe cargar en servidores y PCs para obtener mayor libertad y potencia en control de grandes cantidades de cámaras a menor costo (Zeljkovic, 2014, 279). La plataforma que se está proponiendo se divide a nivel software en 3 aplicaciones dependientes entre ellas mismas: Config Tool, Security Desk y Server Admin, las cuales en conjunto permiten la operatividad de la plataforma. (Ver Figura 1)

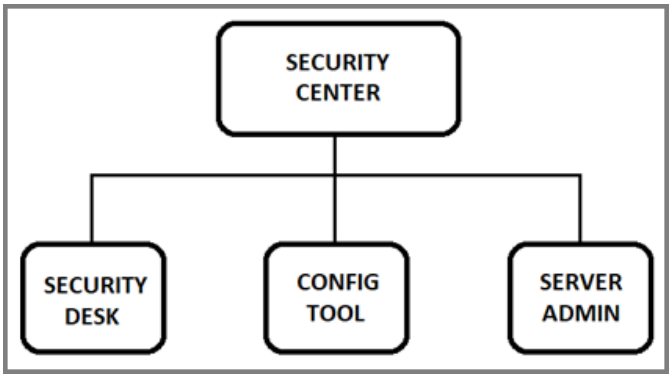


Figura 1: Distribución de las aplicaciones dependientes.

Fuente: Genetec Inc. (2018)

Según Nilsson (2017) existen 3 modelos de arquitectura de plataformas VMS:

1. Gestión de video basado en servidor: consta de un servidor central o grupos de servidores con aplicativo software instalado, los cuales se encargan de gestionar flujos de video de cámaras de seguridad.
2. Gestión de video basado en perímetro: en este modelo, el mismo periférico (cámara) se encarga de gestionar el flujo de video hacia una aplicación cliente, la cual a través de su interface permite al usuario visualizar y manejar las cámaras.
3. Gestión de video basado en la nube: se trata de una aplicación software, ejecutándose en servidores de la nube, que gestiona los flujos de video de las cámaras. (p.44)

La arquitectura de esta plataforma toma como base un modelo de cliente/servidor o WebClient/MainServer, donde todas las funciones del sistema son administradas por un conjunto de computadoras distribuidas a través de una red IP. Cada sistema de la plataforma VMS debe tener su propio grupo de servidores. Su cantidad puede variar desde una sola máquina para un sistema pequeño hasta cientos de máquinas para un sistema a gran escala. (Ver Figura 2)

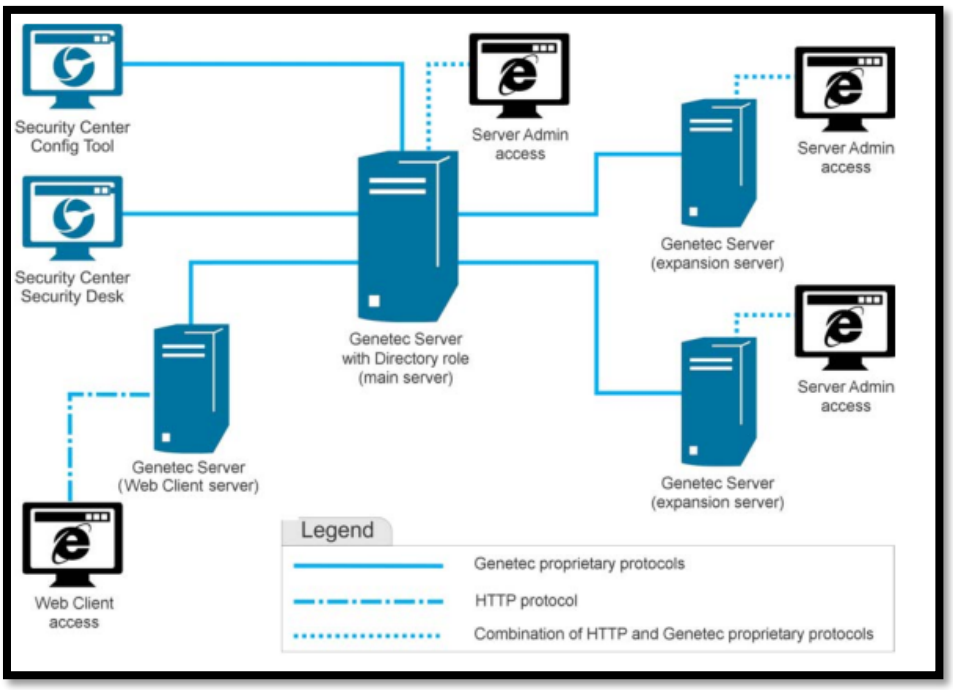


Figura 2: Arquitectura física de la plataforma Security Center

Fuente: Genetec Inc. (2018)

En relación al ente servidor, éste presenta una arquitectura consolidada como un único servicio Windows que puede ser configurado para arrancarse en segundo plano cuando se inicia el sistema operativo del equipo host y que en todos los casos será el mismo como menciona Genetec Inc (2018, p.100), a excepción del servidor de Directorio que será el responsable de mantener la base de datos del sistema. El ente servidor puede implantarse en un mismo servidor físico o en multitud de servidores sin límite alguno, para cubrir las demandas del servicio a explotar. Cada uno de los servidores implantados tendrá el mismo servicio Windows instalado y presentará una arquitectura basada en roles que podrán ser activados o desactivados dinámicamente para proporcionar redundancia, balanceo de carga, tareas de mantenimiento, etc.

Los diseños de VMS basado en servidores son fácilmente escalables, dado que tanto los dispositivos hardware como licencias software pueden expandirse o mejorar para cumplir con requisitos de mayor rendimiento. Además, son adecuados para escenarios donde se requieren grandes cantidades de cámaras o en caso de que las áreas de tecnología se encuentran bajo especificaciones estandarizadas.

La plataforma VMS propuesta opera varios subsistemas, entre los cuales se tiene el módulo de videovigilancia IP Omnicast y el módulo de control de Acceso Synergis, entre otros (Genetec Inc., 2018, p.3).

2.2.2 Seguridad Electrónica

Sadowsky (2003), dice que:

> La seguridad electrónica es cualquier herramienta, técnica o proceso utilizado para proteger los activos de información de un sistema. Los componentes de la infraestructura de software son las políticas, procesos, protocolos y directrices que protegen el sistema y los datos del compromiso. (p.86)

La seguridad electrónica para este proyecto se basa en un sistema de distintos dispositivos electrónicos, que se mencionarán a continuación:

2.2.2.1 Videovigilancia IP

La videovigilancia IP es una tecnología que trabaja a través del Protocolo de Internet (IP) para la transmisión y recepción de audio y video de la cámara de videovigilancia la cual trabaja bajo una red, como en la mayoría de este tipo de tecnologías. Además de ello, hay dispositivo que usan red IP la cual alimentan eléctricamente a otros dispositivos como por ejemplo cámaras de red, telefonía por IP, etc.; esto se da mediante el uso de la tecnología PoE (Power over Ethernet). Una arquitectura básica con un sistema de video vigilancia a través del protocolo IP, hace referencia a los elementos que mencionaremos a continuación:

- Cámaras de red IP
- Servidores de video
- Servidor de almacenamiento/gestión de video
- Puntos finales de monitorización
- Elementos de redes de datos (cableado estructurado, routers, switches, etc.) (García, 2010, p.17)

2.2.2.2 Cámara de red

La cámara de red o cámaras IP, se define como una cámara digitalizada en conjunto con un dispositivo que usa una dirección lógica (IP), como por ejemplo una computadora, laptop, etc. Por lo que captura y envía imágenes y videos en tiempo real a través de una red IP. Esto hace que los administradores y/o usuarios autorizados puedan ver, almacenar y administrar el video/imagen de manera local y/o remota mediante una infraestructura de red basad en IP. La cámara de red o IP ofrece variedades de funcionabilidades para cualquier sistema de video vigilancia. Por el avance tecnológico, estas se caracterizan por tener una mejor calidad de imagen, una mayor resolución, mayor almacenamiento y demás incorporaciones inteligentes que se le pueda adaptar (Nilsson, 2017, p.20).

Los componentes básicos que tiene una cámara de red o cámara IP, tal y como se muestra en la Figura 3

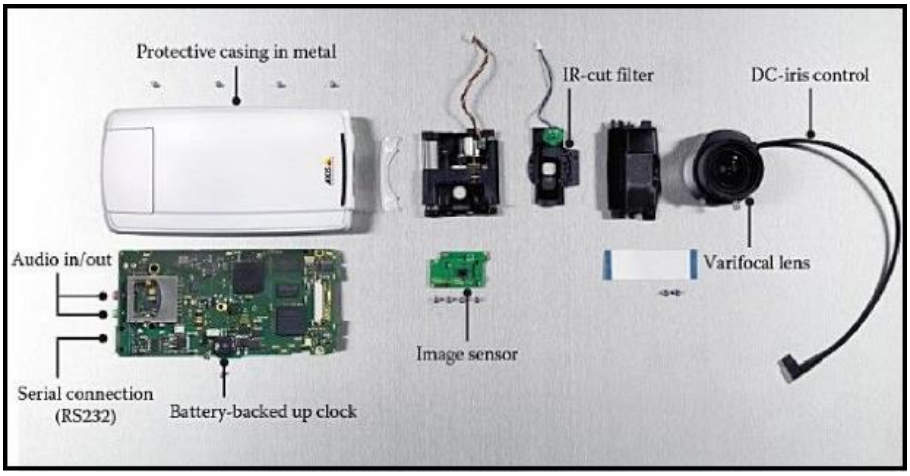


Figura 3: Componentes de una cámara de red

Fuente: Nilsson, F. (2017)

- Lente para enfocar la imagen en el sensor de imagen.
- Sensor de imagen, ya sea un dispositivo de carga acoplado o un semiconductor.
- Procesador, uno o varios, para procesamiento de imágenes, compresión, análisis de video y funcionalidad de redes.
- Memoria flash para almacenar el código de firmware de la cámara.
- Memoria de acceso y/o tarjeta SD para grabación local de videoclips y eventos.

2.2.2.2.1 Resolución de grabación

La resolución de grabación de una cámara de video vigilancia es la cantidad de pixeles de imagen que se pueden visualizar desde un monitor o pantalla. En donde para García (2010), afirma que:

> La resolución de pantalla es el número de píxeles que se muestran en nuestra televisión o en nuestra pantalla, manifestada a través de la multiplicación de los píxeles horizontales y los verticales. El píxel es la unidad mínima de cualquier imagen digital, es decir, cada uno de los diminutos cuadrados que se unen para componer cualquier elemento que se muestre en nuestra pantalla. (p.69).

Dependiendo de los recursos o tarjeta gráfica de la pantalla de visualización, se puede encontrar sistemas de televisión analógica, televisión digital y monitores informáticos, donde este último es que se aplicará en nuestra tesis y se encuentra ligado a fabricantes, siendo estos de sistemas cerrados.

A continuación, se muestran las resoluciones en monitores informáticos en la Tabla 1.

Tabla 1: Resoluciones en monitores informáticos

Estándar	Resolución	Número de Pixeles
CGA	320x200	64 K
QVGA	320x240	77 K
B&W Macintosh/Macintosh LC	512x384	197 K
EGA	640x350	224 K
MCGA	640x480	307 K
HGC	720x348	251 K
MDA	720x350	252 K
Apple Lisa	720x360	259 K
SVGA	800x600	480 K
WVGA	850x480	409 K
XGA	1024x768	786 K
XGA+	1152x864	995 K
WXGA	1280x768	983 K
WXGA	1360x768[1]	1020 K
WXGA+	1280x800	1 M
SXGA	1280x1024	1'3 M
WSXGA o WXGA+	1440x900	1'4 M
SXGA+	1400x1050	1'5 M
WSXGA	1600x1024	1'6 M
WSXGA+	1680x1050	1'8 M
UXGA	1600x1200	1'9 M
WUXGA	1920x1200	2'3 M
QWXGA	2048x1152	2'35 M
QXGA	2048x1536	3'1 M
WQXGA	2560x1600	4'1 M
QSXGA	2560x2048	5'2 M
WQSXGA	3200x2048	6'6 M
QUXGA	3200x2400	7'7 M
WQUXGA	3840x2400	9'2 M
HSXGA	5120x4096	21 M
WHSXGA	6400x4096	16 M
HUXGA	6400x4800	31 M
WHUXGA	7680x4800	35 M

Fuente: García, 2010

2.2.2.2.2 Compresión de video

Para poder grabar grandes secuencias de video, es necesario disminuir el "peso" o tamaño del archivo a través de las técnicas de compresión. Así mismo Musburger & Ogden (2014), menciona que:

> Su señal de video analógica original se muestrea y cuantifica, lo que requiere hasta 300 MB por segundo de programa grabado, en comparación con menos de 100 K por segundo para audio digital. La información de la cámara se comprime para reducir la velocidad de datos y ajustarla al medio de grabación: en el mundo del video digital, la compensación es la velocidad, el tamaño y la calidad: ¡elija dos! El acto de malabarismo de todos los formatos de codificación de video digital es cómo reducir el tamaño de los datos de la imagen manteniendo simultáneamente la mayor calidad posible. Si comprime demasiado, la calidad de la imagen se ve afectada. Si no comprime lo suficiente, los archivos son demasiado grandes y lentos para trabajar. (p.40).

Para aligerar el peso del archivo es necesario sacrificar la velocidad de carga del archivo, para así tener mayor cantidad de días de grabación.
El último estándar de compresión de video es el H.265, el cual permite mayores velocidades de transmisión de video, trabajar con mayores resoluciones y admitir procesamiento en paralelo a comparación de H.264.

> H-265 es un estándar de compresión de video nuevo, avanzado y con pérdida para la grabación, compresión y distribución de video de alta definición y ultra alta definición. H.265 es el sucesor del estándar H.264 Advanced Video Compression. H.265 también se conoce como el estándar de codificación de video de alta eficiencia. El estándar de video H.265 ofrece el doble de la relación de compresión de la

> codificación de video basada en H.264. El video H.265 requiere solo la mitad de la velocidad de transmisión de datos para entregar un video de tamaño y calidad similares a uno codificado por H.264. H.265 puede admitir video con resoluciones de hasta 8192 píxeles por 4320 píxeles. H.265 también se puede utilizar para comprimir imágenes fijas. La codificación y decodificación de video H.265 es computacionalmente intensiva y requiere el uso de códecs basados en hardware o potentes microprocesadores genéricos. El estándar H.265 admite el uso de procesamiento paralelo, que puede usarse para reducir el tiempo necesario para codificar o decodificar un video. (Gilling, 2017, p.80).

2.2.2.3 Control de acceso

El control de acceso es un término que abarca una gran variedad de definiciones para el ámbito de seguridad, ya que, por ejemplo, puede apuntar a la tecnología de video vigilancia y/o CCTV, así como también para la ciberseguridad, seguridad de la información y afines.

HID Global Protection (2019) menciona que:

"Los sistemas de control de acceso confiables protegen sus entornos físicos y digitales." (p.1)

La forma en la que trabaja el control de acceso electrónico, normalmente, Honey (2004) refiere que:

> Hay disponible una buena selección de perímetro que se puede adaptar para disuadir y físicamente restringir el acceso no autorizado a una zona, pero este siempre se puede complementar con detección electrónica de integrar con el sistema de control de acceso. (p.131)

A continuación, en la Figura 4 se puede visualizar una muestra de ejemplo deun control de acceso electrónico.

Figura 4: Control de acceso electrónico

Fuente: https://calidad.steren.cr/control-de-acceso-rfid-y-teclado-numerico.html

2.2.2.4 RFID

RFID (Radio Frequency Identification) conocido en el habla hispana como Identificación por Radiofrecuencia, es una tecnología usada para que automáticamente capture e identifique la información que contienen los tags (etiquetas o transpondedores), donde Portillo (2008) menciona que:

> Es un método de almacenamiento y recuperación remota de datos, basado en el empleo de etiquetas o "tags" en las que reside la información. RFID se basa en un concepto similar al del sistema de código de barras; la principal diferencia entre ambos reside en que el segundo utiliza señales ópticas para transmitir los datos entre la etiqueta y el lector, y RFID, en cambio, emplea señales de radiofrecuencia (en diferentes bandas dependiendo del tipo de sistema, típicamente 125 KHz, 13,56 MHz, 433-860-960 MHz y 2,45 GHz). (p.31)

A continuación, visualizar en la Figura 5 se muestra un ejemplo de tarjeta RFID.

Figura 5: Tarjetas RFID

Fuente: https://www.nova.com.bo/tarjetas-rfid-1356mhz.html

2.2.2.5 Interfaz RS-485

JM Industrial (2006) menciona que:

> La interfaz RS485 ha sido desarrollada - analógicamente a la interfaz RS422 - para la transmisión en serie de datos de alta velocidad a grandes distancias y encuentra creciente aplicación en el sector industrial. Pero mientras que la RS422 sólo permite la conexión unidireccional de hasta 10 receptores en un transmisor, la RS485 está concebida como sistema Bus bidireccional con hasta 32 participantes. Físicamente las dos interfaces sólo se diferencian mínimamente. El Bus RS485 puede instalarse tanto como sistema de 2 hilos o de 4 hilos. (p.1)

Así mismo Lyon (2002) sostiene que:

- **Modo Half Duplex**

El término Half Duplex en un sistema de comunicación se refiere, a que solamente en un tiempo determinado, el sistema puede transmitir o recibir información, sin embargo no lo puede hacer al mismo tiempo. En muchos enlaces del tipo RS-485 se comparte el BUS. Como se puede observar existe una línea de control, la cual habilita a los controladores en un solo sentido. Por lo tanto, se debe tener cuidado de no transmitir y recibir al mismo tiempo, ya que se podría crear una superposición de información. (p.5)

A continuación, lo descrito anteriormente se muestra en la Figura 6:

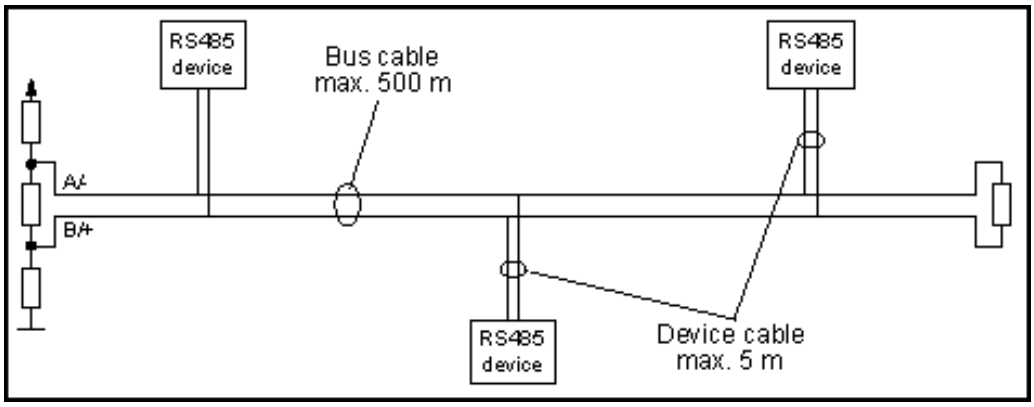


Figura 6: Distribución de bus de 2 hilos

Fuente: https://www.wut.de/e-6wwww-11-apes-000.php

En donde también para JM Industrial (2006):

- **Modo Full Duplex**

La técnica de 4 hilos usada p. ej. por el bus de medición DIN (DIN 66 348) sólo puede ser usada por aplicaciones Master/Slave. Conforme al bosquejo se cablea aquí la salida de datos del Maestro a las entradas de datos de todos los Servidores. Las salidas de datos de los Servidores están concebidas conjuntamente en la entrada de datos del Maestro. (p.1)

A continuación, se lo descrito anteriormente se muestra en la Figura 7:

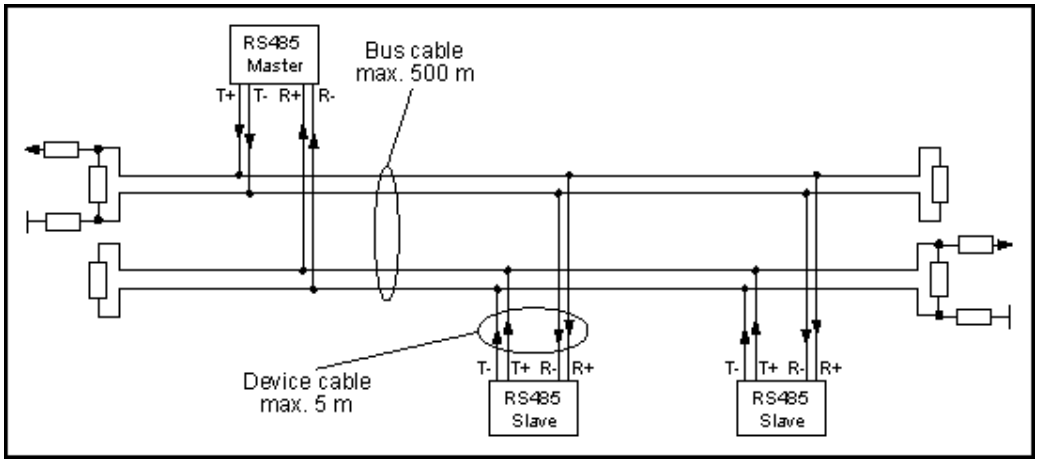


Figura 7: Distribución de bus de 4 hilos

Fuente: https://www.wut.de/e-6wwww-11-apes-000.php

- Características Mecánicas

Para las Forero (2012) menciona que:

> En la comunicación de la norma RS-485 se tiene que el emisor opera el "1" lógico a un voltaje de -1.5 a -5 Volt. el "0" lógico a la entrada del receptor en el rango de +0.2 a +12 Volt y la máxima tensión aplicada a la línea de salida es de -7 a +12 Volt. El alcance de la transmisión está dado por la relación existente entre el volumen de los datos a transferir y el tiempo de la señal en la portadora determinado por la velocidad de transferencia de donde se obtiene que la longitud máxima del cable es de 1.200 m y la velocidad máxima de 10 Mbps que se obtiene en una distancia de 12 m. (p.91)

A continuación, en la Figura 8 se muestra la relación de distancias y velocidades.

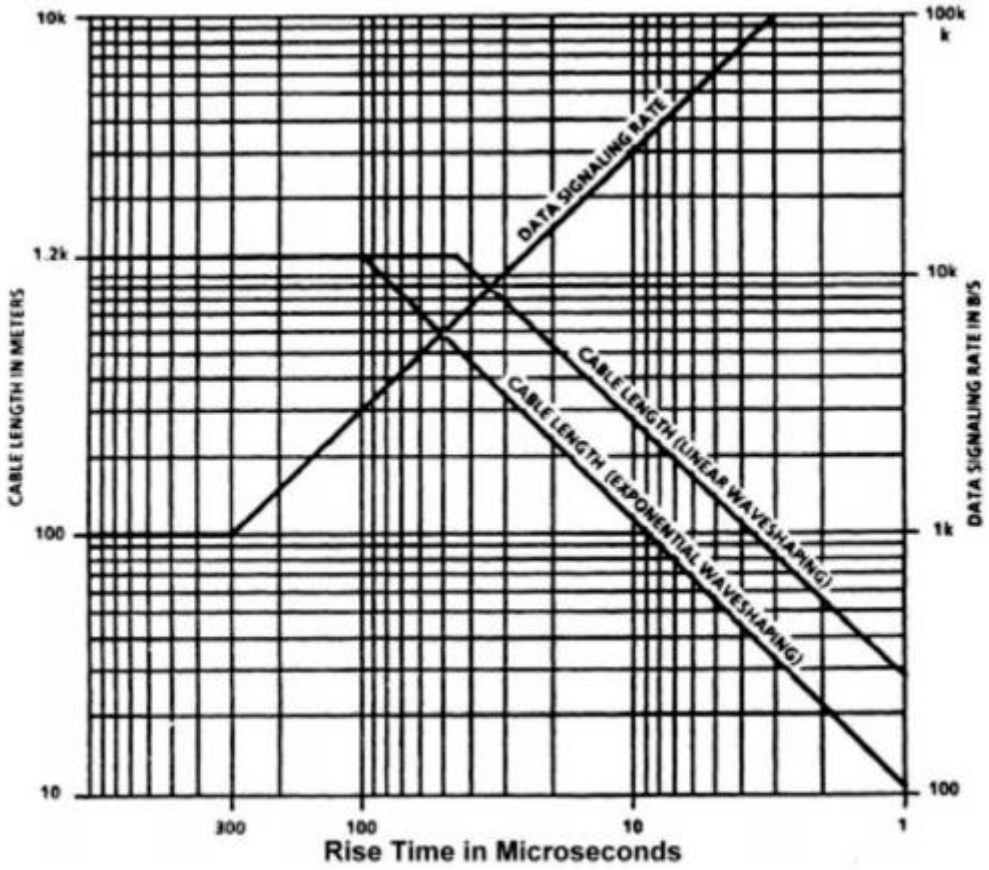


Figura 8: Tasa de Transferencia en Cable para la Norma RS422

Fuente: Forero (2012)

- Características Eléctricas

Para las Forero (2012) menciona que:

> El estándar define conexiones con cable de par de cobre trenzado y terminales RJ11por lo cual existe mayor resistencia a la interferencia electromagnética y mayor velocidad de transmisión que con la norma RS232. Permite la conexión de hasta 32 emisores con 32 receptores en transmisión doble simultánea full dúplex capaz de enlazar procesadores de comunicación principal (master) con procesadores subordinados (slaves) cuyo funcionamiento (acceso priorizado) esta definido por los mismos arreglos topológicos de las redes de datos. (p.91)

A continuación, en la Figura 9 se muestra una interfaz RS485 de 16 puertos:

Figura 9: Interfaz RS485 de 16 Puertos de Alto Rendimiento PCI Express

Fuente: Forero (2012)

2.2.2.6 Protocolo Wiegand

Según DSX Access Systems (2011), el protocolo Wiegand:

> El protocolo Wiegand es un código de bits estándar (típicamente 26 bits) que comprende un bit de paridad, 8 bits de código de instalación, 16 bits de código de identificación y un bit final para un total de 26 bits. El protocolo Wiegand puede lograr muchas permutaciones, incluidos muchos patrones de bits especializados, proporcionando una tarjeta única para cada instalación individual. (p.67)

A continuación lo descrito anteriormente se muestra en la Figura 10:

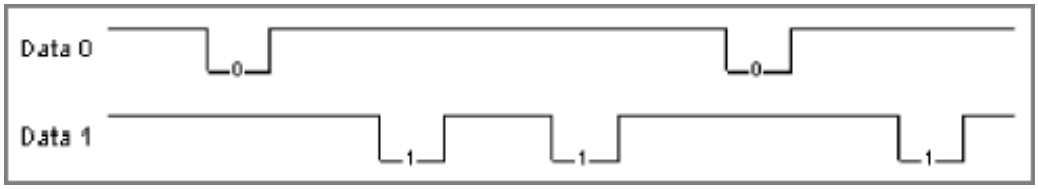


Figura 10: Flujo de datos del Protocolo Wiegand

Fuente: DSX Access Systems, Inc. (2011)

2.2.2.7 Servidor de video

Servidor de video es un dispositivo que almacenamiento la cual tienen una cierta cantidad de discos mediante una interfaz ATA, para recopilar información que recibe de otros dispositivos ayudando así a que no se saturen dichos dispositivos. (García, 2010, p.162)

En la Figura 11 se muestra un tipo de servidor de video de marca Streamvault.

Figura 11: Servidor de video Streamvault

Fuente: https://www.genetec.com/solutions/all-products/streamvault-turnkey-security-infrastructure-solutions/1000-series

2.2.2.8 Modelo OSI

Según ISO/EIC 9646-2:1994 (2019), el término OSI (Open System Interconection) califica los estándares para el intercambio de información entre sistemas que están "abiertos" entre sí para este propósito en virtud de su uso mutuo de los estándares aplicables.

A continuación, se lo descrito anteriormente se muestra en la Figura 12:

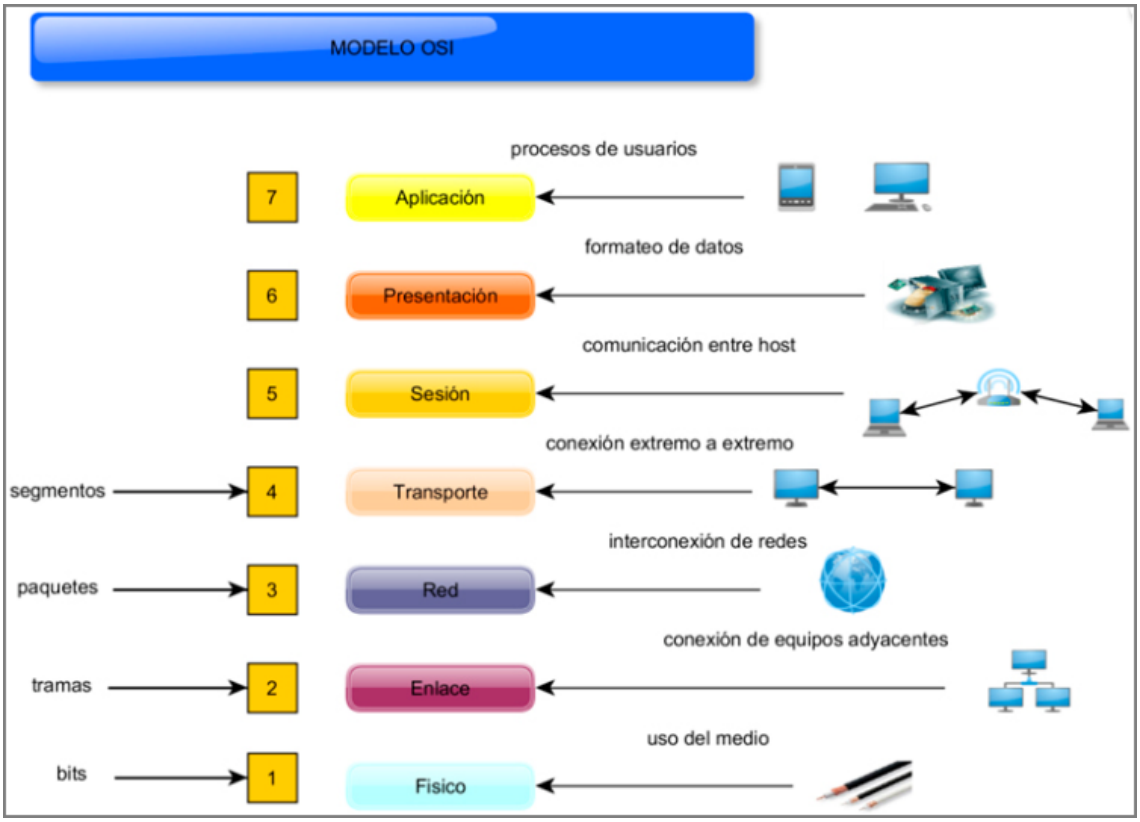


Figura 12: Niveles del Modelo OSI

Fuente: https://www.uaeh.edu.mx/scige/boletin/huejutla/n10/r1.html

A continuación, se describe las 7 capas, como menciona The Cisco Learning Network (2017):

- La **capa física** describe las propiedades físicas de los distintos medios de comunicación, así como las propiedades eléctricas y la interpretación de las señales intercambiadas. Ej: esta capa define el tamaño del cable coaxial Ethernet, el tipo de conector BNC utilizado y el método de terminación. Esto incluye el diseño de pines, voltajes, impedancia de línea, especificaciones de cable, temporización de señal, concentradores, repetidores, adaptadores de red, adaptadores de bus host. Por lo tanto, los conectores físicos se encuentran en la capa 1, llamada capa física.

- La **capa de enlace de datos** describe la organización lógica de los bits de datos transmitidos en un medio particular. Ej: esta capa define el encuadre, el direccionamiento y la suma de verificación de los paquetes de Ethernet. Capa de enlace de datos dividida en dos subcapas: -Capa de control de acceso a medios (MAC): responsable de controlar cómo las computadoras en la red obtienen acceso a los datos y permiso para transmitirlos. Capa de control de enlace lógico (LLC): controla la comprobación de errores y la sincronización de paquetes. El Protocolo punto a punto (PPP) es un ejemplo de una capa de enlace de datos en la pila de protocolos TCP / IP.

- La **capa de red** describe cómo una serie de intercambios a través de varios enlaces de datos pueden entregar datos entre dos nodos en una red. Ej: esta capa define la estructura de direccionamiento y enrutamiento de Internet. La información de enrutamiento está en la capa 3, los protocolos de enrutamiento como RIP, IGRP, EIGRP, OSPF son protocolos de capa 3.

- La **capa de transporte** describe la calidad y la naturaleza de la entrega de datos. Ej: esta capa define si y cómo se utilizarán las retransmisiones para garantizar la entrega de datos.

- La **capa de sesión** describe la organización de secuencias de datos más grandes que los paquetes manejados por capas inferiores. Ej: esta capa describe cómo se emparejan los paquetes de solicitud y respuesta en una llamada a procedimiento remoto o puede decir que La capa de sesión controla los diálogos (conexiones) entre computadoras. Establece, gestiona y finaliza las conexiones entre la aplicación local y la remota. El modelo OSI hizo que esta capa sea responsable del cierre elegante de las sesiones, que es una propiedad del Protocolo de Control de Transmisión, y también de los puntos de comprobación y recuperación de la sesión, que generalmente no es utilizado en Internet Protocol Suite.

- La **capa de presentación** describe la sintaxis de los datos que se transfieren. Ej: esta capa describe cómo los números de coma flotante pueden intercambiarse entre hosts con diferentes formatos matemáticos. La capa de

presentación establece el contexto entre las entidades de la capa de aplicación, en el que las entidades de la capa de aplicación pueden usar diferentes sintaxis y semántica si el servicio de presentación proporciona un mapeo entre ellas. Si hay una asignación disponible, las unidades de datos del servicio de presentación se encapsulan en unidades de datos del protocolo de sesión y se transmiten a la pila TCP / IP. Esta capa proporciona independencia de la representación de datos (p. Ej., Cifrado) al traducir entre los formatos de aplicación y de red. La capa de presentación transforma los datos en la forma que acepta la aplicación. Esta capa formatea y cifra los datos que se enviarán a través de una red. A veces se llama la capa de sintaxis.

- La **capa de aplicación** describe cómo se hace realmente el trabajo real. Ej: esta capa implementaría operaciones del sistema de archivos. Esta capa interactúa con aplicaciones de software que implementan un componente de comunicación. Dichos programas de aplicación quedan fuera del alcance del modelo OSI. Las funciones de la capa de aplicación generalmente incluyen identificar socios de comunicación, determinar la disponibilidad de recursos y sincronizar la comunicación. Al identificar socios de comunicación, la capa de aplicación determina la identidad y disponibilidad de socios de comunicación para una aplicación con datos para transmitir. Al determinar la disponibilidad de recursos, la capa de aplicación debe decidir si existe suficiente red o la comunicación solicitada. Al sincronizar la comunicación, toda comunicación entre aplicaciones requiere cooperación gestionada por la capa de aplicación.

2.2.2.9 Modelo TCP/IP

El modelo TCP/IP conocido como Transmission Control Protocol / Internet Protocol, similar al modelo OSI, es un conjunto de protocolos que permite la correcta comunicación. Este modelo está dividido por 4 capas o niveles: acceso a red, Internet, transporte y aplicación. (USERS, 2011, p.222)

A continuación, se presenta el diagrama del Modelo TCP/IP en la Figura 13:

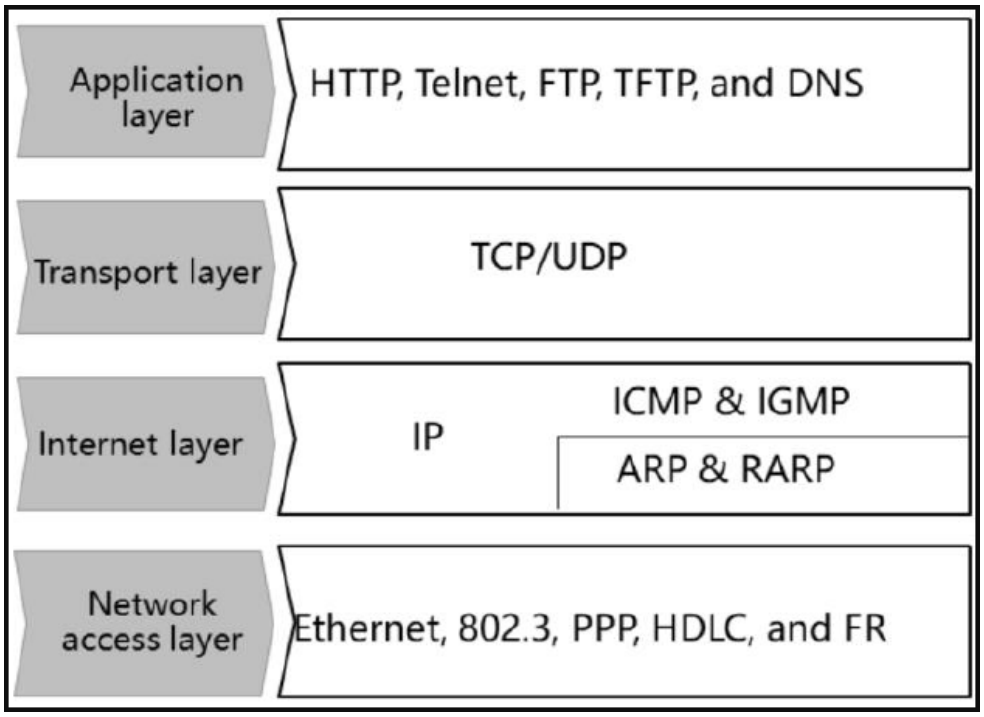


Figura 13: Capas del Modelo TCP/IP

Fuente: https://forum.huawei.com/enterprise/es/aportaci%C3%B3n-principales-protocolos-del-modelo-tcp-ip/thread/550505-100235

Así mismo Cisco System (2019) describe las siguientes capas del dicho modelo:

- Capa de Acceso a Red: El diseño de TCP / IP oculta la función de esta capa a los usuarios: se trata de obtener datos a través de un tipo específico de red física (como Ethernet, Token Ring, etc.). Este diseño reduce la necesidad de reescribir niveles más altos de una pila TCP / IP cuando se introducen nuevas tecnologías de red física (como ATM y Frame Relay). Las funciones realizadas en este nivel incluyen encapsular los datagramas IP en tramas que son transmitidas por la red. También asigna las direcciones IP a las direcciones físicas utilizadas por la red. Una de las fortalezas de TCP / IP es su esquema de direccionamiento, que identifica de manera única cada computadora en la red. Esta dirección IP debe convertirse a cualquier dirección que sea apropiada para la red física a través de la cual se transmite el datagrama.

- Capa de Internet: El protocolo TCP / IP más conocido en la capa entre redes es el Protocolo de Internet (IP), que proporciona el servicio básico de entrega de paquetes para todas las redes TCP / IP. Además de las direcciones físicas de nodo utilizadas en la capa de acceso a la red, el protocolo IP implementa un sistema de direcciones lógicas de host llamadas direcciones IP. Las direcciones IP son utilizadas por la red interna y las capas superiores para identificar dispositivos y realizar el enrutamiento entre redes. El Protocolo de resolución de direcciones (ARP) permite a IP identificar la dirección física que coincide con una dirección IP dada. Todos los protocolos utilizan IP en las capas superiores e inferiores para entregar datos, lo que significa que todos los datos TCP / IP fluyen a través de IP cuando se envían y reciben, independientemente de su destino final.

- Capa de Transporte: La capa de protocolo justo encima de la capa entre redes es la capa de host a host. Es responsable de la integridad de los datos de extremo a extremo. Los dos protocolos más importantes empleados en esta capa son el Protocolo de control de transmisión (TCP) y el Protocolo de datagramas de usuario (UDP). TCP proporciona conexiones confiables de dúplex completo y un servicio confiable al garantizar que los datos se vuelvan a enviar cuando la transmisión genera un error (detección y corrección de errores de extremo a extremo). Además, TCP permite a los hosts mantener múltiples conexiones simultáneas. Cuando no se requiere corrección de errores, UDP proporciona un servicio de datagramas poco confiable (sin conexión) que mejora el rendimiento de la red en la capa de transporte de host a host. Ambos protocolos entregan datos entre la capa de aplicación y la capa entre redes. Los programadores de aplicaciones pueden elegir el servicio más apropiado para sus aplicaciones específicas.

- Capa de Aplicación: Los protocolos de capa de aplicación TCP / IP más conocidos e implementados se enumeran a continuación:

• Protocolo de transferencia de archivos (FTP). Realiza transferencias básicas de archivos interactivos entre hosts.
• Telnet. Permite a los usuarios ejecutar sesiones de terminal con hosts remotos.
• Protocolo simple de transferencia de correo (SMTP). Admite servicios básicos de entrega de mensajes.
• Protocolo de transferencia de hipertexto (HTTP). Admite el transporte de archivos de bajo costo que consiste en una mezcla de texto y gráficos. Utiliza una conexión sin estado, y protocolo orientado a objetos con comandos simples que admiten la selección y el transporte de objetos entre el cliente y el servidor. Además de los protocolos ampliamente conocidos, la capa de aplicación incluye lo siguiente protocolos:
• Servicio de nombres de dominio (DNS). También llamado servicio de nombres; Esta aplicación asigna direcciones IP a los nombres asignados a los dispositivos de red.
• Protocolo de información de enrutamiento (RIP). El enrutamiento es fundamental para la forma en que funciona TCP / IP. Los dispositivos de red utilizan RIP para intercambiar información de enrutamiento.
• Protocolo simple de administración de red (SNMP). Un protocolo que se utiliza para recopilar información de gestión de dispositivos de red.
• Sistema de archivos de red (NFS). Un sistema desarrollado por Sun Microsystems que permite a las computadoras montar unidades en hosts remotos y operarlas como si fueran unidades locales.

Algunos protocolos, como Telnet y FTP, solo se pueden usar si el usuario tiene algún conocimiento de la red. Otros protocolos, como RIP, se ejecutan sin que el usuario sepa que existen.

2.2.2.10 Switch

El Switch o conmutador, es un dispositivo que realiza la conectividad entre otros dispositivos que trabajan bajo la misma red. Este a su vez puede funcionar a través de VLAN para mantener aislado una red de otra para tener una mayor seguridad. También Huidobro (2008, p.254) menciona que, se comporta como un gestionador de ancho de banda. (Ver Figura 14)

Figura 14: Switch de 50 puertos

Fuente: http://redestelematicas.com/wp-content/uploads/2013/11/02-HP-Procurve-2650.jpg

2.3 Definición de términos básicos

Security Desk: "Es la interfaz gráfica unificada Security Center para el usuario. Ofrece un flujo entre los operadores de los sistemas de Security Center, Omnicast, Synergis y AutoVu. El diseño gráfico de Security Desk permite a los operadores o administradores controlar y monitorear aplicaciones de seguridad y protección pública" (Genetec, 2018, p.1241).

Config Tool: "Esta aplicación se usa para gestionar a todos los usuarios de Security Center y configurar todas las categorías de Security Center como, por ejemplo: áreas, cámaras, puertas, horarios, tarjetahabientes, unidades de Patroller/LPR y dispositivos de hardware" (Genetec, 2018, p.1208).

Server Admin: "Aplicación web que se ejecuta en todos los servidores de Security Center que permite configurar los ajustes del Servidor Genetec." (Genetec, 2018, p.1241)

Centro de Monitoreo: "Es un sistema de red que utiliza tecnología moderna de comunicación e informática para el monitoreo y control remoto de equipos de subestaciones en operación." (Li, 2018, p.110)

Transpondedor*:* "Donde se incorpora un chip electrónico con la información del producto para poder identificarlo." (Perdiguero, 2017, p.76).

CAPITULO III: METODOLOGÍA DEL ESTUDIO

3.1 Tipo y método de investigación

3.1.1 Tipo de investigación

La investigación aplicada según Hernández (2014), nos dice que:
"Tiene como justificación adelantos y productos tecnológicos." (p.42)

Por lo tanto, la presente investigación es de tipo aplicada, debido a que se manipulará la variable Plataforma VMS para analizar sus efectos en la seguridad electrónica de la Universidad Ricardo Palma.

3.1.2 Metodología de investigación

Hernández (2014) menciona que:
"La investigación correlacional tiene, en alguna medida, un valor explicativo, aunque parcial, ya que el hecho de saber que dos conceptos o variables se relacionan aporta cierta información explicativa." (p.94)

El método de investigación es correlacional, ya que se medirá el grado de relación entre las variables. Es decir, en esta investigación se aplica una plataforma VMS (variable independiente) que ayuda y aporta con una mejor y mayor tecnología a la seguridad electrónica (variable dependiente) en el ambiente del centro de monitoreo de la Universidad Ricardo Palma.

Finalmente, se observa cómo influye, aporta y/o hay relación entre la variable dependiente y la variable independiente, apoyando el método de investigación que se aplica para esta tesis.

3.2 Relación entre variables

Las variables de esta investigación están determinadas por el título del proyecto las cuales comprometen al diseño de la investigación.
Variable 1: Plataforma VMS (Variable Independiente)
Variable 2: Seguridad electrónica (Variable Dependiente)

La presente investigación determinará la relación entre ambas variables.

Como se menciona en el punto 3.1.2, hay una relación tanto de la variable dependiente como la variable independiente.

CAPITULO IV: DISEÑO DE INGENIERÍA

4.1 Etapas de diseño de la topología del sistema de seguridad aplicando la plataforma VMS en el centro de monitoreo

4.1.1 Etapas del estudio y evaluación del ambiente

En el transcurso del año 2018, a requerimiento de la U.R.P., se realizó una visita técnica dentro de las instalaciones del local, primordialmente el perímetro, donde se encuentran instaladas las cámaras de seguridad, y la sala de monitoreo, donde se encuentran los operadores de video vigilancia.

Para ello, en primer lugar, se solicitó el plano de ubicación referencial de cámaras, el cual se presenta a continuación en la Figura 15:

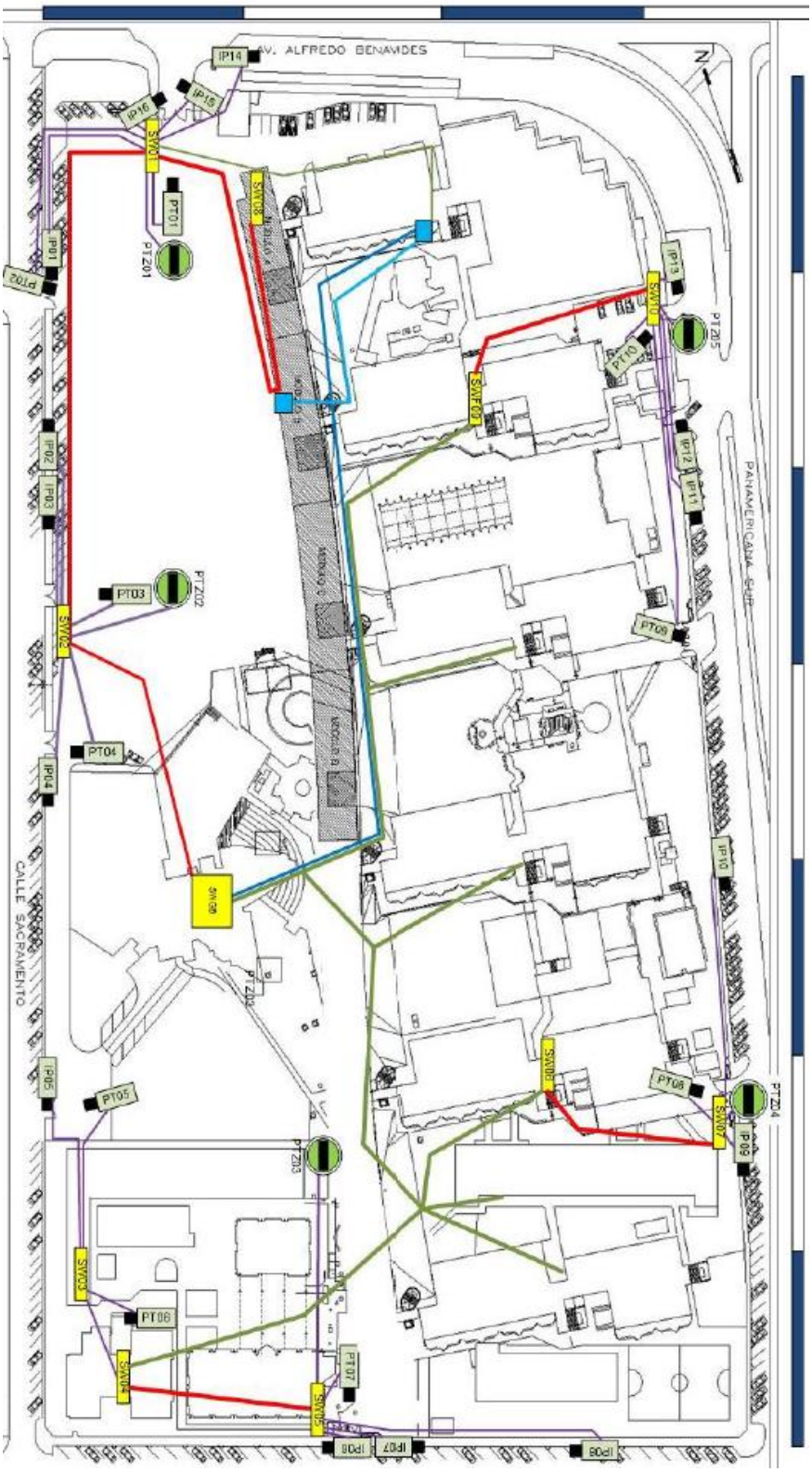


Figura 15: Plano de ubicación actual de cámaras de video vigilancia

Fuente: Universidad Ricardo Palma

A continuación, se detalla la información recolectada de cada cámara que abarca desde la Figura 16 a la Figura 45.

Cámara N°1: IP01, IP 192.90.0.105

(a) (b)

Figura 16: (a) Ubicación física y (b) Visualización

Fuente: Propia

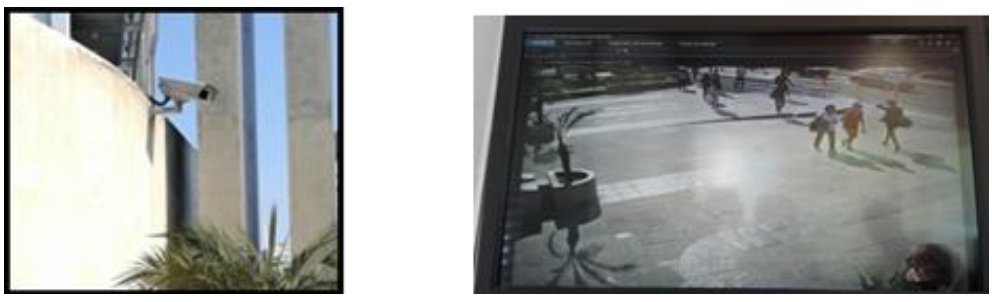
Cámara N°2: IP14, IP 192.90.0.99

(a) (b)

Figura 17: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°3: IP15, IP 192.90.0.100

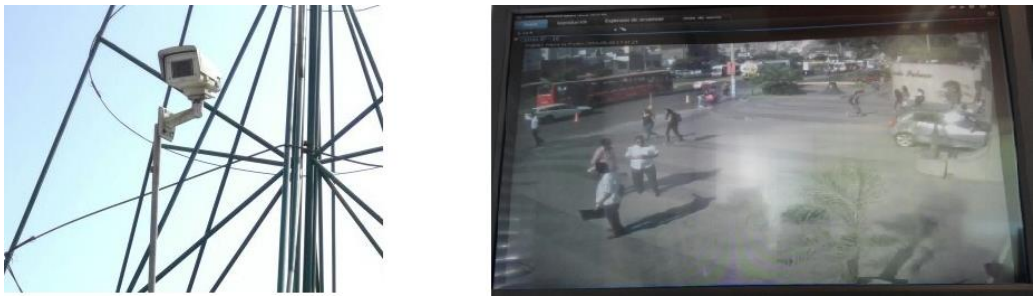


(a) (b)

Figura 18: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°4: IP16, IP 192.90.0.101

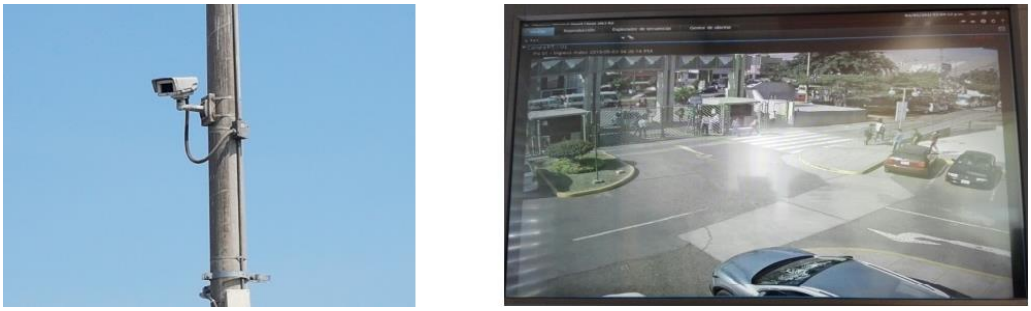


(a) (b)

Figura 19: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°5: PT01, IP 192.90.0.108



(a) (b)

Figura 20: (a) Ubicación física y (b) Visualización

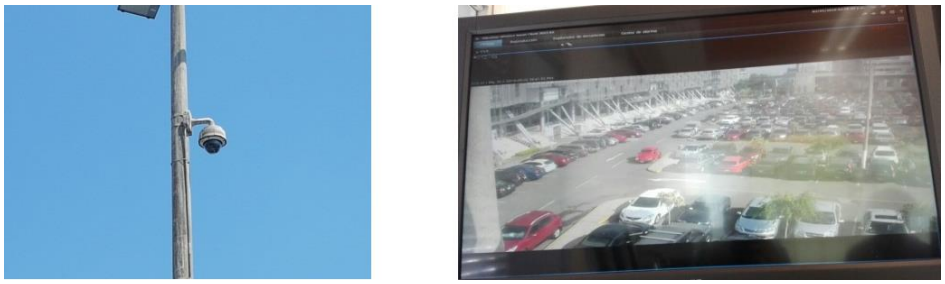
Fuente: Propia

Cámara N°6: PT02, IP 192.90.0.103

Figura 21: (a) Ubicación física

Fuente: Propia

Cámara N°7: PTZ01, IP 192.90.0.129



(a) (b)

Figura 22: (a) Ubicación física y (b) Visualización

Fuente: Propia

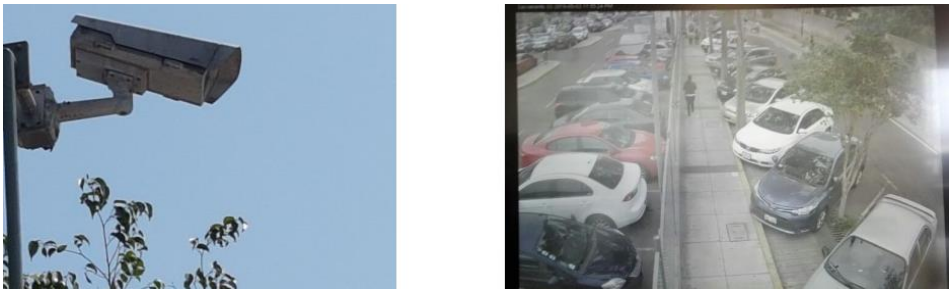
Cámara N°8: IP02, IP 192.90.0.102

(a) (b)

Figura 23: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°9: IP03, IP 192.90.0.104

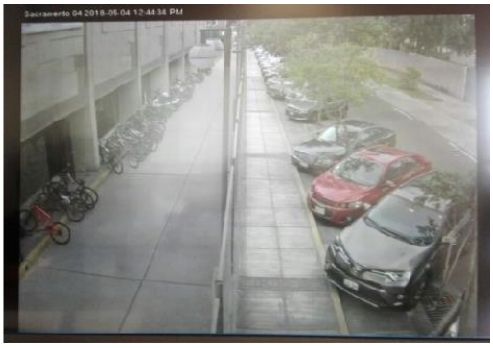


(a) (b)

Figura 24: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°10: IP04, IP 192.90.0.106



(a) (b)

Figura 25: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°11: PT03, IP 192.90.0.109

(a) (b)

Figura 26: (a) Ubicación física y (b) Visualización

Fuente: Propia

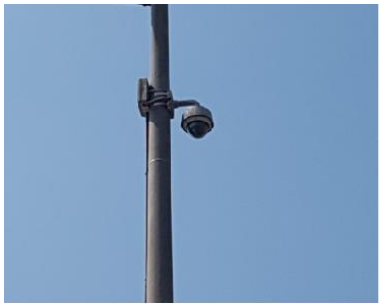
Cámara N°12: PT04, IP 192.90.0.107

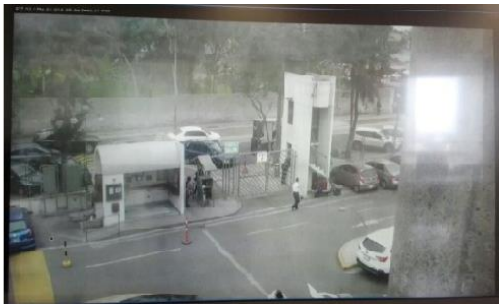
(a) (b)

Figura 27: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°13: PTZ02, IP 192.90.0.121





(a) (b)

Figura 28: (a) Ubicación física y (b) Visualización

Fuente: Propia

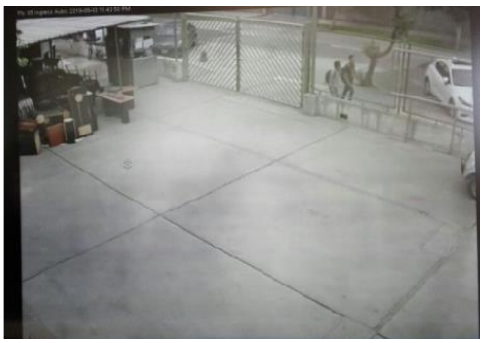
Cámara N°14: IP05, IP 192.90.0.115

(a) (b)

Figura 29: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°15: PT05, IP 192.90.0.113



(a) (b)

Figura 30: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°16: PT06, IP 192.90.0.114

(a) (b)

Figura 31: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°17: IP06, IP 192.90.0.116

(a) (b)

Figura 32: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°18: IP07, IP 192.90.0.118

(a) (b)

Figura 33: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°19: IP08, IP 192.90.0.117

(a) (b)

Figura 34: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°20: PT07, IP 192.90.0.119

(a) (b)

Figura 35: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°21: PTZ03, IP 192.90.0.120

Figura 36: (a) Ubicación física

Fuente: propia

Cámara N°22: IP09, IP 192.90.0.110

(a) (b)

Figura 37: (a) Ubicación física y (b) Visualización

Fuente: Propia

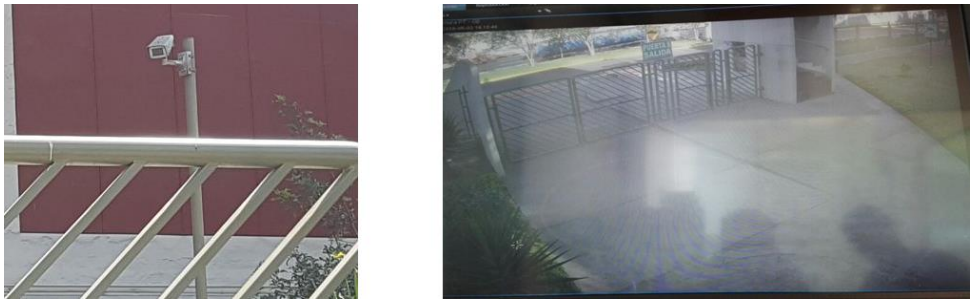
Cámara N°23: IP10, IP 192.90.0.112

(a) (b)

Figura 38: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°24: PT08, IP 192.90.0.111



(a) (b)

Figura 39: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°25: PTZ04, IP 192.90.0.122

(a) (b)

Figura 40: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°26: IP11, IP 192.90.0.126

(a) (b)

Figura 41: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°27: IP12, IP 192.90.0.127

(a) (b)

Figura 42: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°28: IP13, IP 192.90.0.125

(a) (b)

Figura 43: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°29: PT09, IP 192.90.0.124

(a) (b)

Figura 44: (a) Ubicación física y (b) Visualización

Fuente: Propia

Cámara N°31: PTZ05, IP 192.90.0.128

(a) (b)

Figura 45: (a) Ubicación física y (b) Visualización

Fuente: Propia

4.1.2 Diseño del sistema CCTV

Según el diseño inicial, se mantiene la cantidad de cámaras, modificando el modelo de cámara, donde se presenta en la Tabla 2 las características mínimas para nuestra solución y una comparación de cámaras en la Tabla 3:

Tabla 2: Características mínimas de cámaras

CARACTERÍSTICAS	**DATOS**
Resolución de grabación	2 MP
Compresión de video	H.265
Infra rojo	Si
Control de apagado/encendido de IR	Automático
Número de canales	3
ONVIF	SI

Fuente: Propia

Tabla 3: Comparación de cámaras

CARACTERÍSTICAS	**IPC-HFW4231E-S**	**Q1785-LE**	**SNO-L6013R**
Resolución de grabación	2 MP	2 MP	2 MP
Compresión de video	H.265	H.264	H.264
Infra Rojo	Si	SI	SI
Control de apagado/encendido de IR	Automático	Automático	Automático
Número de canales	3	2	3
ONVIF	SI	SI	SI

Fuente: Propia.

De la tabla 3, el modelo de las cámaras que cumple con las características mínimas sugeridas es el IPC-HFW4231E-S, y es el que se propuso a utilizar.

Para nuestro proyecto usaremos un programa, llamado BCDVideo, que realiza cálculos automáticos de ancho de banda y almacenamiento de un servidor, la cual parten de las características que usaremos, tales como: resolución, compresión, tamaño de trama, FPS, días de almacenamiento, cantidad de cámaras, entre otros, como se muestra en la Figura 46.

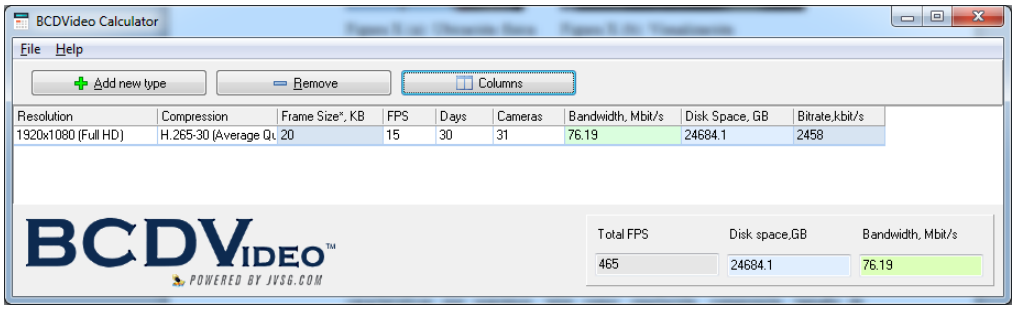


Figura 46: Cálculo de ancho de banda y almacenamiento del servidor.

Fuente: Propia

Teniendo así 24 TB como mínimo para el almacenamiento de 31 cámaras a 2MP con 15 FPS para 30 días (1 mes) de almacenamiento.

4.1.3 Diseño del sistema de Control de Acceso

El diseño para este planteamiento de proyecto de tesis se basa con los componentes RFID, Protocolo RS485, laptop o PC, sirena, botón de salida, etc., como se puede observar en la Figura 47.

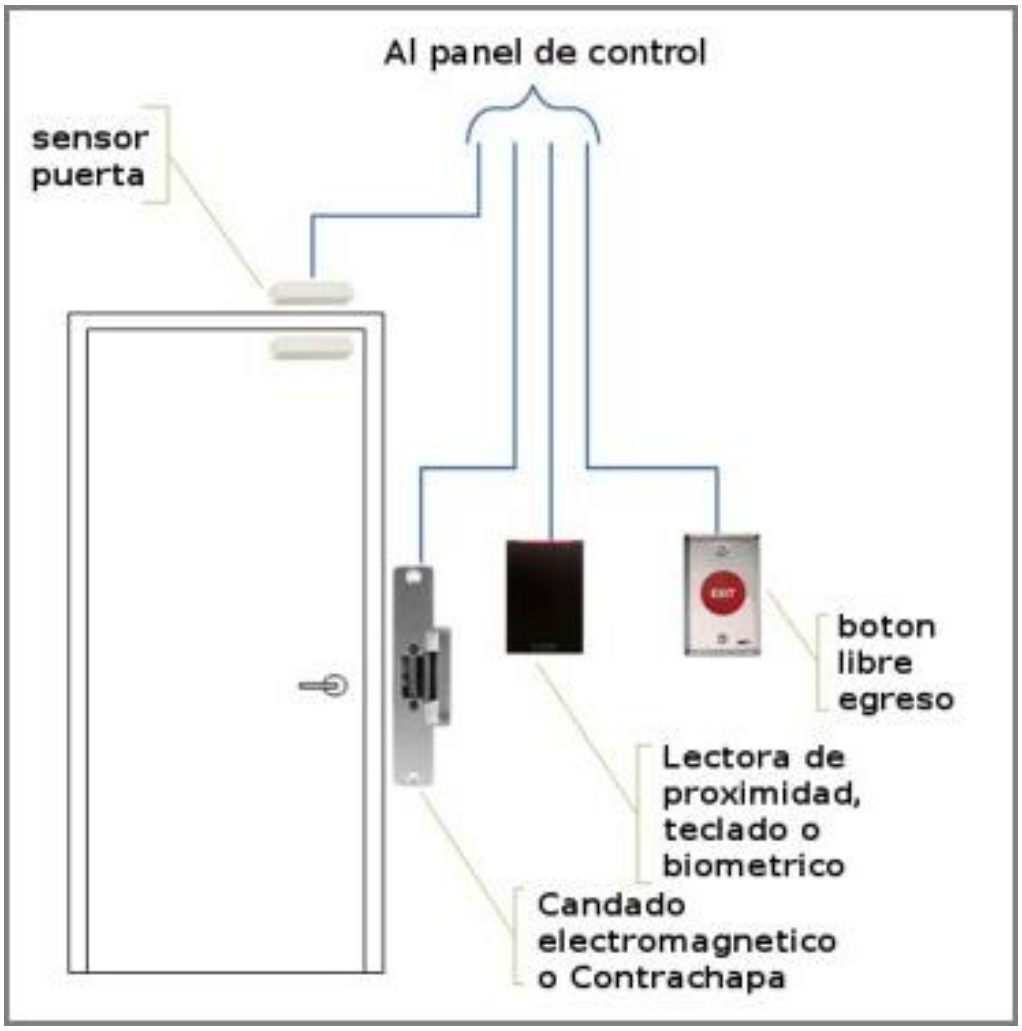


Figura 47: Sistema de control de acceso

Fuente: http://00de0d9.netsolhost.com/control.htm

4.1.4 Arquitectura de la red LAN

Para realizar el diseño de la topología física de los equipos de red LAN, en cuanto a la distribución de las cámaras en la Universidad Ricardo Palma, se recreó, con respecto al punto 3.1.1 Plano de ubicación actual de cámaras de video vigilancia, una simulación general de dicha distribución; ya que se cómo se nombra en el punto 3.1.1, se tiene una cantidad total de 31 cámaras desplazadas en el perímetro de la Universidad Ricardo Palma. (Ver Figura 48)

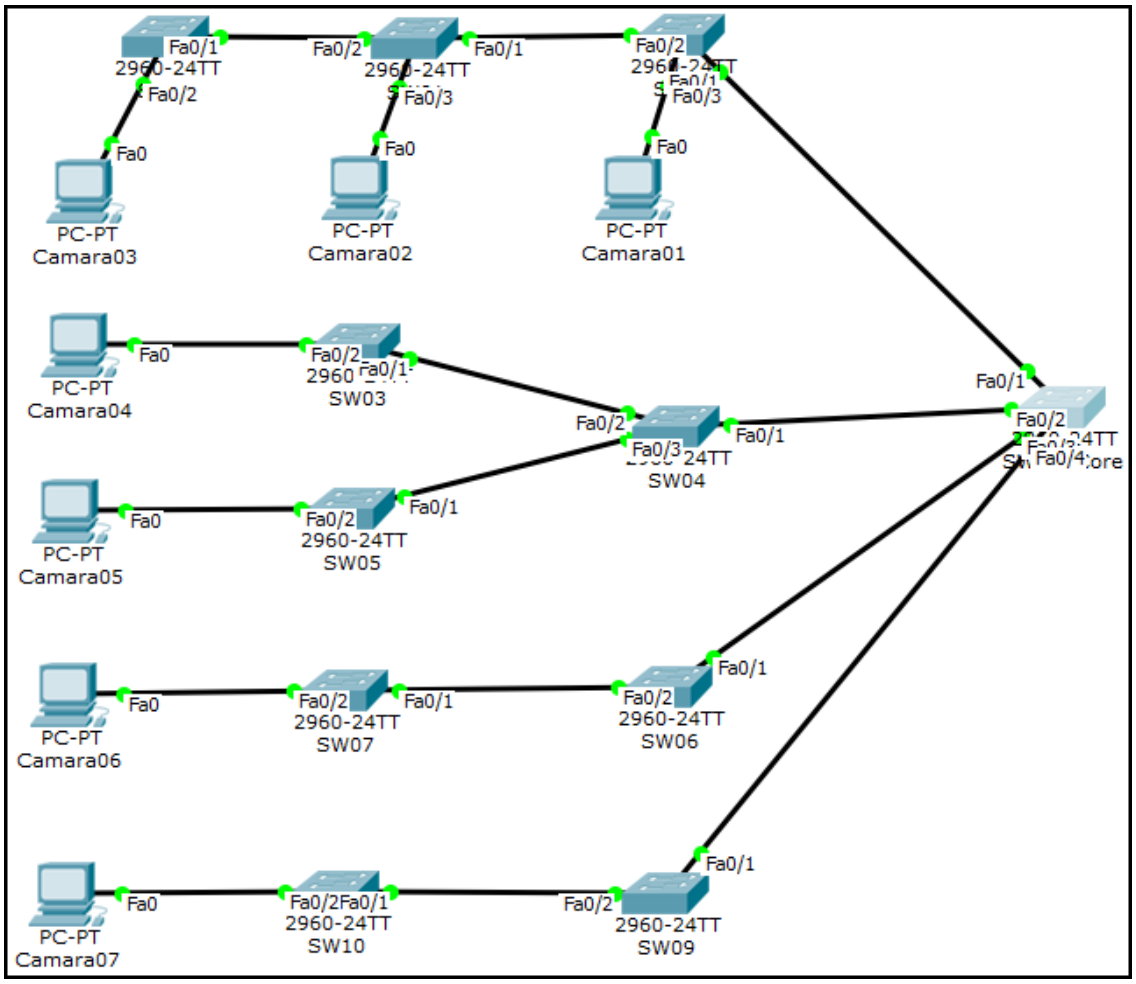


Figura 48: Distribución general de red LAN.

Fuente: Universidad Ricardo Palma

4.1.5 Diseño de la plataforma VMS

Luego de tener diseñado los subsistemas anteriores mencionados, estos se unificaran, a traves de la red LAN por medio de los switches, dentro del servidor con los aplicativos instalados, como se observa en la Figura 49 y se procederán a configurar en el siguiente capítulo.

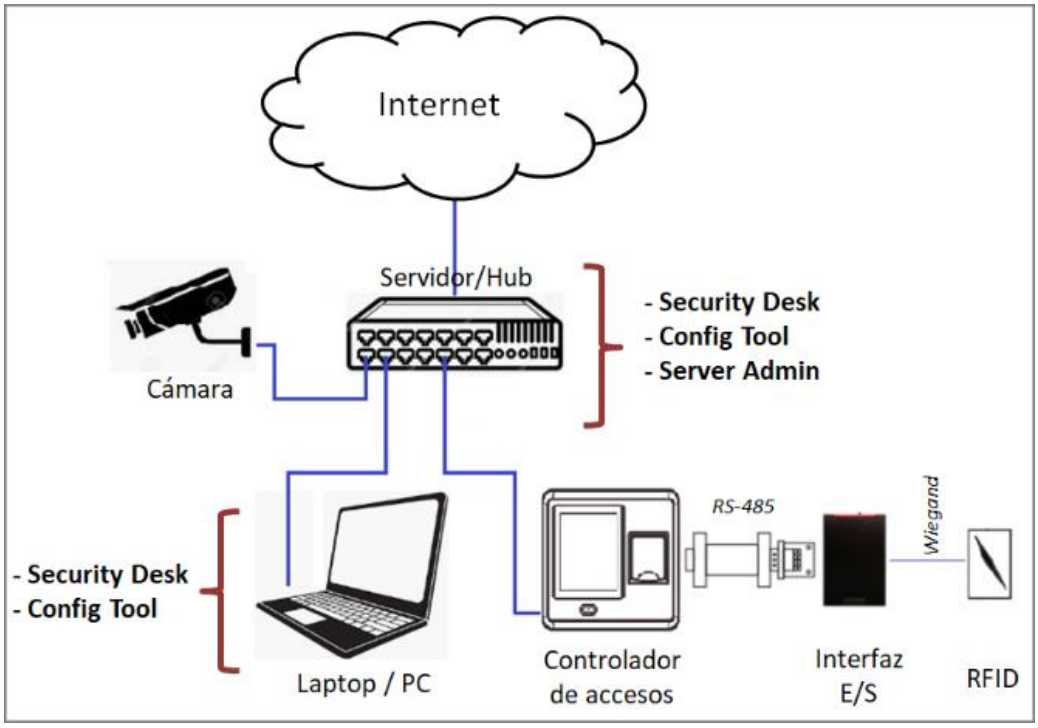


Figura 49: Sistema de la plataforma Video Management System

Fuente: Propia

Las características mínimas que debe tener el servidor se presentan en la siguiente Tabla 4, y en la Tabla 5 se hace una comparación de servidores:

Tabla 4: Características mínimas de servidor

Características	**Datos**
Capacidad máxima de almacenamiento	40 TB
Procesador	Intel® Core™ i5 3.00 GHz
Memoria RAM	16 GB
Puertos Ethernet	1 x 1 GB

Fuente: Propia.

Tabla 5: Comparación de servidores

CARACTERÍSTICAS	SV-300E-T4-30T-10-I5	X3250 M5	BL460c Gen10
Capacidad máxima de almacenamiento	40 TB	8 TB	2 TB
Procesador	Intel® Core™ i5 3.00 GHz	Intel Xeon 4C E3-1230 v3	Chipset Intel 612
Memoria RAM	16 GB	8 GB	8 GB
Puertos Ethernet	1 x 1 GB	4 x 1GB	2 x 10GB

Fuente: Propia.

El servidor debe ser de la marca Genetec y debe tener 30 TB de capacidad de almacenaje y soportar procesamiento de 77Mbp/s, el cual el número de parte es SV-300E-T4-30T-10-I5, el cual posee 3 bahías de discos duros, cada uno de 10 TB (especificaciones en Anexo 5).

4.2 Parte de control del sistema de seguridad aplicando la plataforma VMS en el centro de monitoreo

4.2.1 Configuración de parámetros de red

Para la configuración de los parámetros de red de las cámaras es necesario, primeramente, colocar la IP predeterminada de la marca en el explorador web (es necesario que la PC también se configure dentro de la misma LAN), luego de ingresar, dentro de parámetros de red, se coloca la IP a asignar, como en la Figura 50.

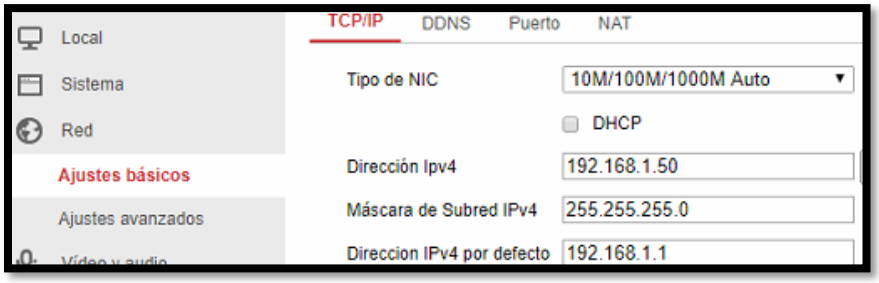


Figura 50: Configuración de parámetro de red de cámara

Fuente: Propia

Una vez configurada las cámaras, se procede a activar el servidor con los aplicativos instalados, para lo cual se accede al aplicativo Server Admin, y dentro de la sección de red, se coloca la IP, como se muestra en la Figura 51.

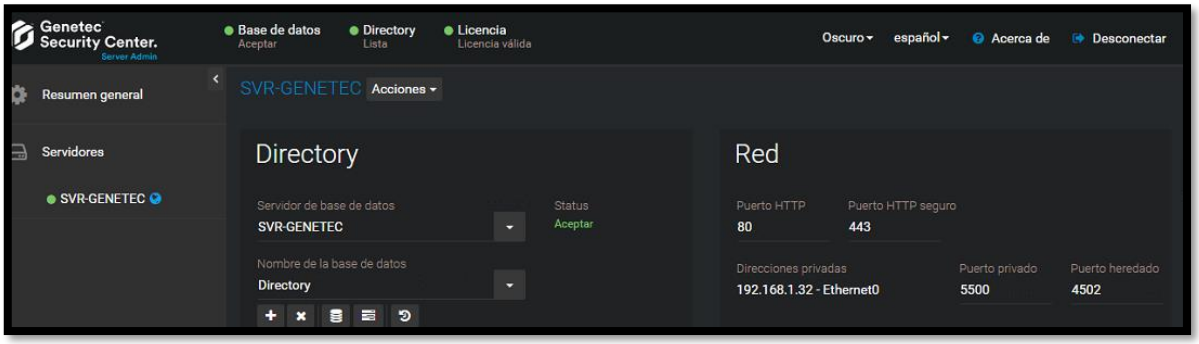


Figura 51: Parámetros de red de plataforma

Fuente: Propia

4.2.2 Configuración de la plataforma VMS

Una vez configurado los parámetros de red de los equipos, se debe preparar el servidor central con los aplicativos instalados (Server Admin, Config Tool y Security Center), el cual necesita de licencia brindado por fabricante, instalar y activar la base de datos central, llamado Directorio, a través del aplicativo “Server Admin”, y dentro de esta base de datos central, se genera una sección dedicada a video llamada “Archiver”, la cual almacenará el flujo de video y eventos de todas las cámaras configuradas dentro del sistema y de los discos duros (30 TB); mientras que el control de acceso se encuentra dentro de “Access Control”, sección dedicada dentro de Directorio.

Como se aprecia en la Figura 52**,** se muestra el icono del Directorio como primero en la jerarquía, luego el icono de Archiver como el abarcador de todas las cámaras, y finalmente el icono de cada cámara, la cual es similar a un NVR convencional, debido a las políticas de configuración interna del servidor, dado que las cámaras actuales son del fabricante Dahua.

Figura 52: Organigrama de icono de sección de video

Fuente: Propia

Luego se configura el Archiver con los siguientes parámetros:

Resolución: Alta, la cual permite a las cámaras grabar en resoluciones mayores a 1MP automáticamente.

Cuadros por segundo: 15 FPS

Modos de grabación: En movimiento/ Manual, donde la cámara graba el ambiente a muy baja resolución, y cuando se presenta movimiento, dentro del campo de visión, se empieza a almacenar el evento.

Limpieza automática: Encendida, después de 30 días, la cual borra los registros de video, pasados los 30 días, del día 1 y así sucesivamente reemplazando cada día que pase.

Esta configuración de Archiver ayuda para que todas las cámaras que se encuentren dentro de este, y tengan las mismas configuraciones, la cual brinda facilidad y rapidez en configuraciones, como se aprecia en la Figura 53.

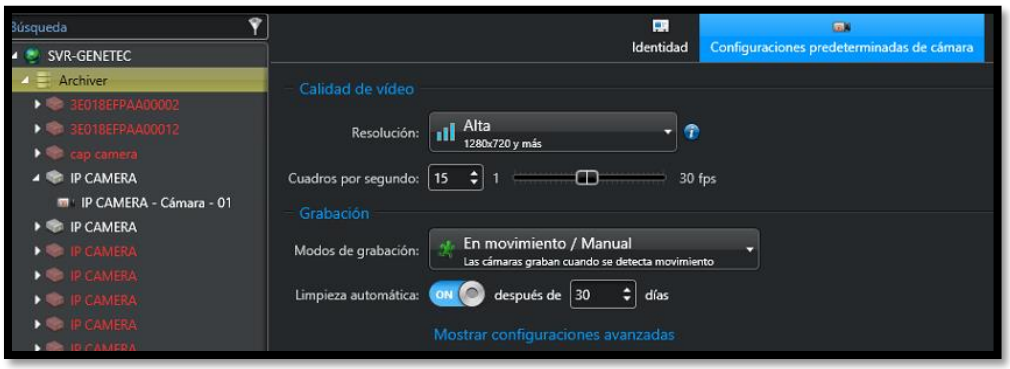


Figura 53: Configuración de Archiver

Fuente: Propia

Para tener una visión de todo el escenario, se cargó el plano de distribución de la URP en el software, en la sección de “Diseñador de mapas” y se colocó los iconos de cámaras en los sectores donde se ubican actualmente, tal como se ilustra en la Figura 54. Estos iconos tienen la función de acceso directo de visualización del entorno desde la cámara a través de plano.

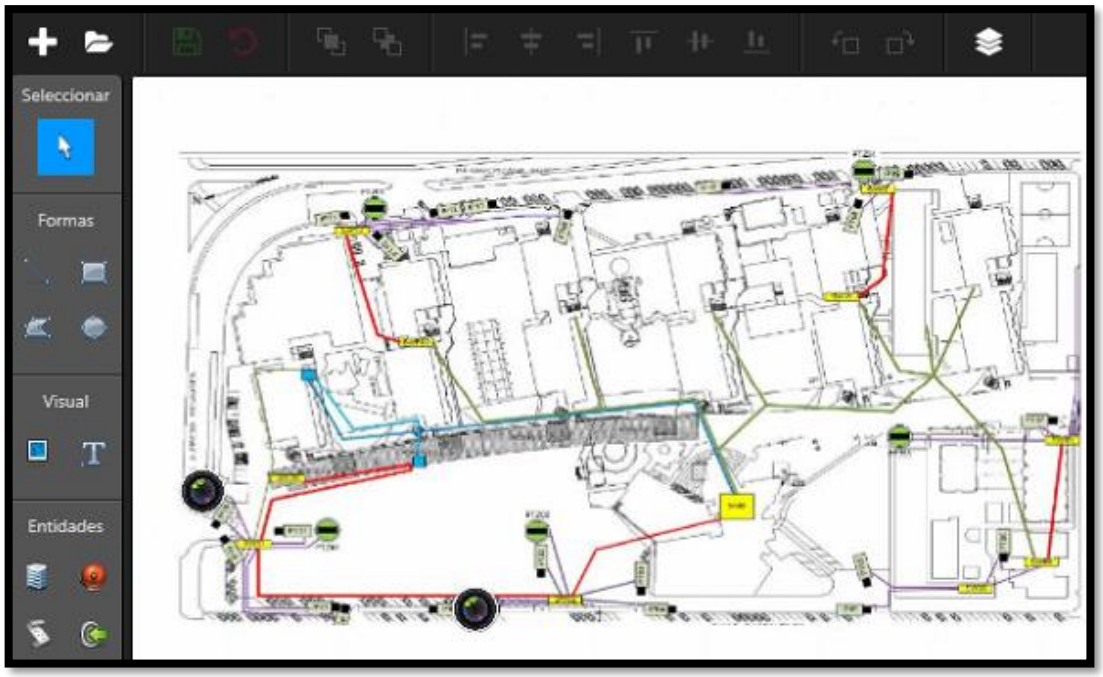


Figura 54: Plano referencial dentro de plataforma

Fuente: Propia

Para la sección de Access Control, se tienen los dispositivos Synergis Cloudlink, Vertx V100 y lectora RFID configurados jerárquicamente, como en el caso de la sección de video. Como se aprecia en la Figura 55, la lectora puede conectarse a entradas (sensores de estado) y salidas (alarmas, botón de salida) de una puerta.

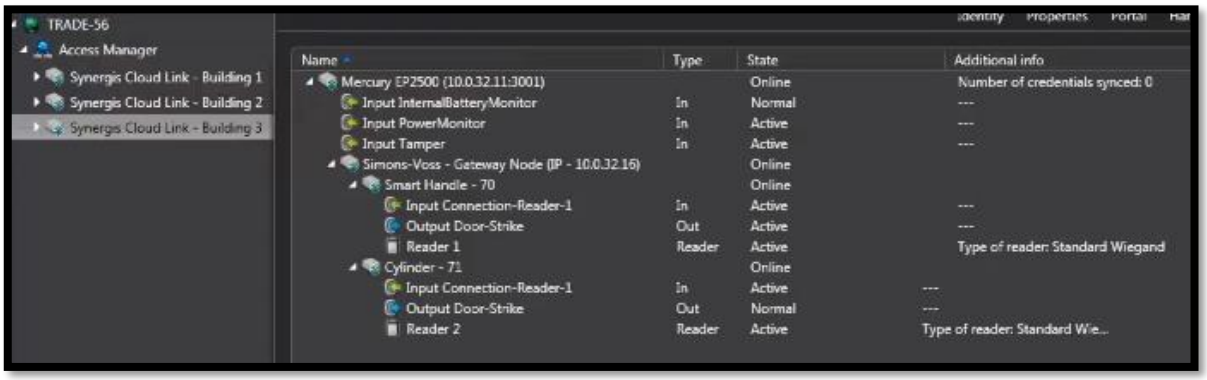


Figura 55: Organigrama de íconos del control de acceso

Fuente: Propia

Luego, se configuró una puerta virtual y se asoció la lectora a esta, tal como se aprecia en la Figura 56, para tener dinamismo y fácil operatividad dentro del sistema.

Figura 56: Puerta en plataforma

Fuente: Propia

En la Figura 57, se aprecia la puerta configurada dentro del plano de ubicaciones de la sede.

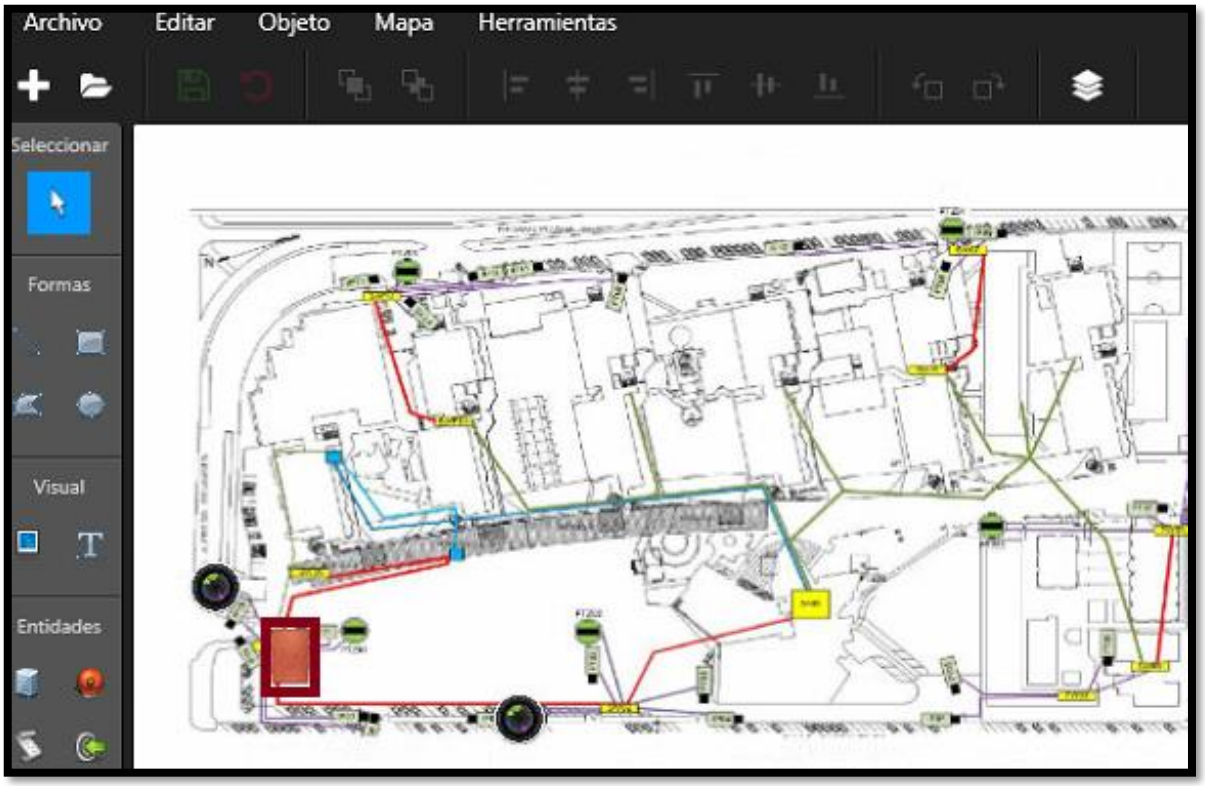


Figura 57: Puerta en plano

Fuente: Propia

Dentro del control de acceso, se generaron “políticas” o “reglas de acceso”, dentro del cual primero se creó un horario, el cual representa las horas en que está disponible la URP para los alumnos, como se muestra en la Figura 58.

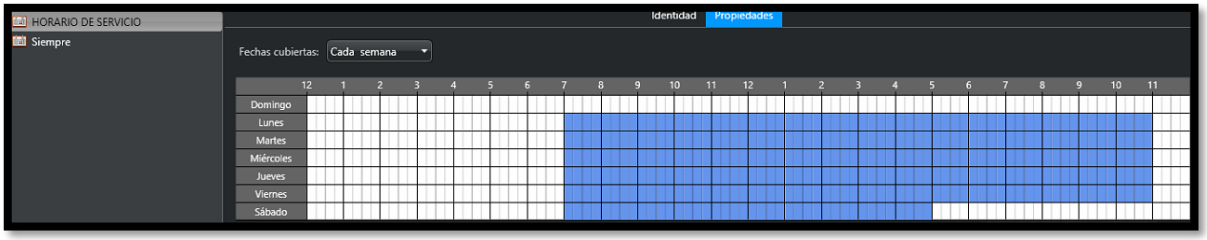


Figura 58: Horario de servicio para alumnos de la URP

Fuente: Propia

Como siguiente paso, se creó un grupo de usuarios con tarjetas RFID asociadas (credenciales), como se muestra en la Figura 59, para así tener acceso dentro de las instalaciones de la URP.

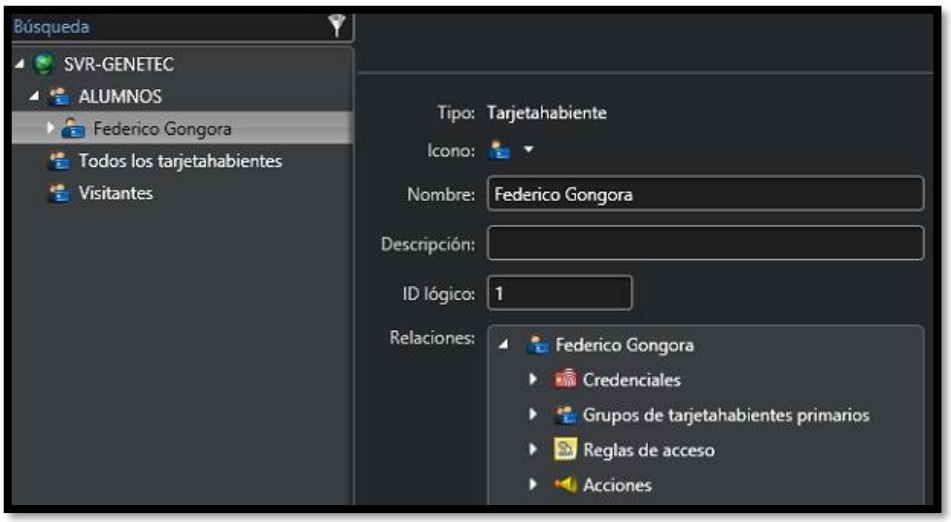


Figura 59: Grupo de usuarios en la plataforma

Fuente: Propia

Luego de crear un horario y grupo de usuarios, estos se asocian a una regla o política de acceso, como se visualiza en la Figura 60, la cual tiene soberanía sobre las lectoras de acceso configuradas dentro del sistema.

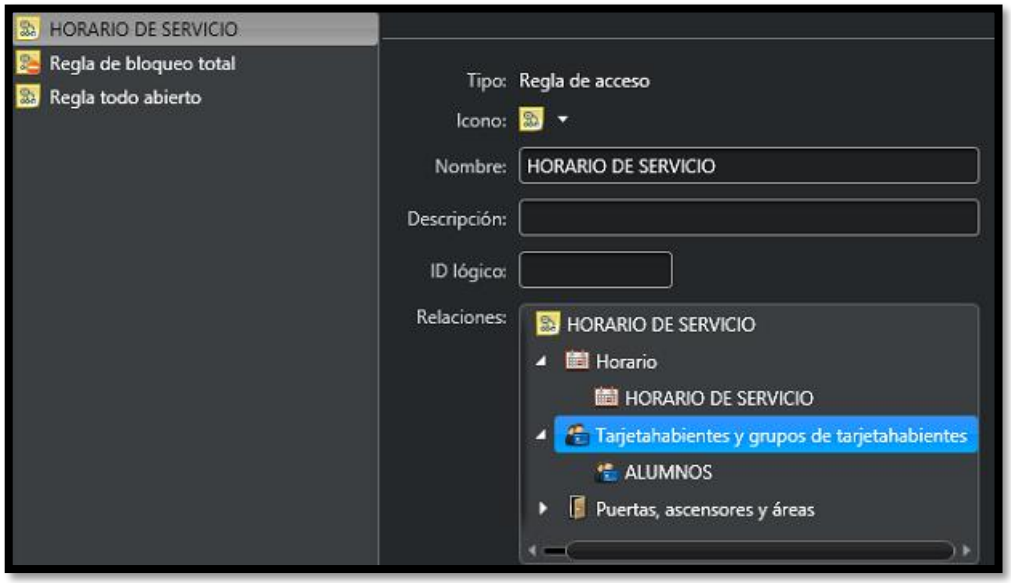


Figura 60: Regla de acceso en plataforma

Fuente: Propia

Para la creación de eventos especiales, como en este caso, el ingreso de una persona por la puerta será grabado, tendrá su propio evento. Esto requiere primeramente de la Asociación de una cámara a una puerta virtual, como se presenta en la Figura 61.

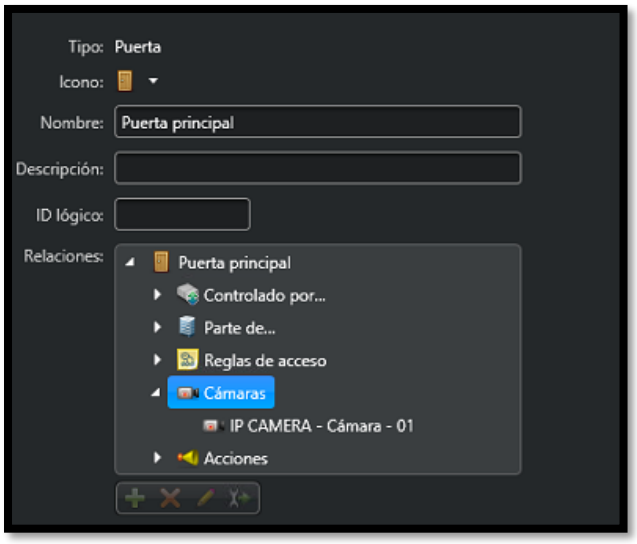


Figura 61: Asociación de cámara con puerta virtual.

Fuente: Propia

Luego de esto, se genera evento a acción, tal como se muestra en la Figura 62, donde al presentarse una persona con su tarjeta RFID al lector y reconocerlo dentro de los registros, accionará la grabación inmediata por un periodo de 5 segundos.

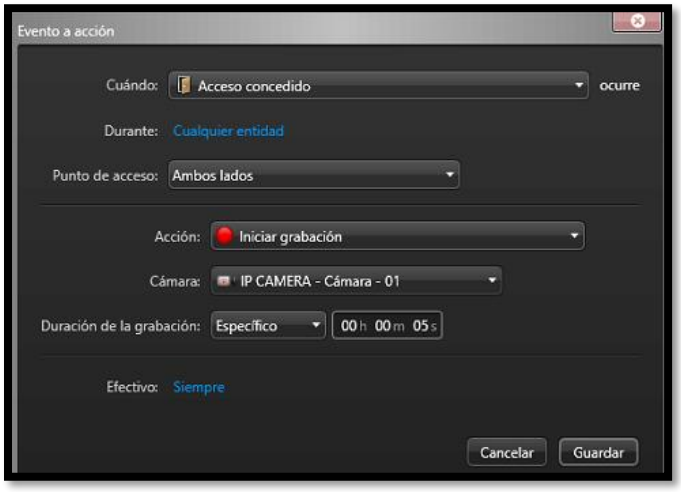


Figura 62: Configuración de eventos de puerta virtual

Fuente: Propia

Para resguardar y asegurar la información, tanto en grabaciones, configuraciones realizadas a la plataforma VMS, eventos, credenciales, etc.; se consideró la configuración de respaldo de la plataforma VMS o “Back-up”, la cual consiste en hacer copias de seguridad y almacenarlas en otro computador/servidor dentro de la red LAN periódicamente. Se inicia con el respaldo de la base de datos “Directory”, el cual se ingresó al aplicativo “Server Admin”, dentro de la sección base de datos, y se configuró la copia de seguridad, donde el archivo se redireccionó a otro computador, como en la Figura 63.

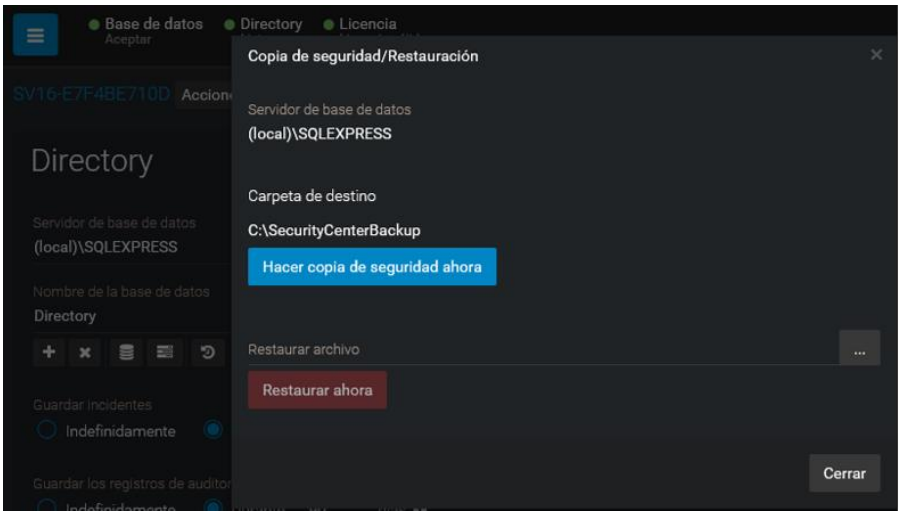


Figura 63: Configuración de respaldo de Directory.

Fuente: Propia.

Los archivos generados se comprimieron y se guardaron con un formato especial propio de la plataforma, como se muestra en la Figura 64.

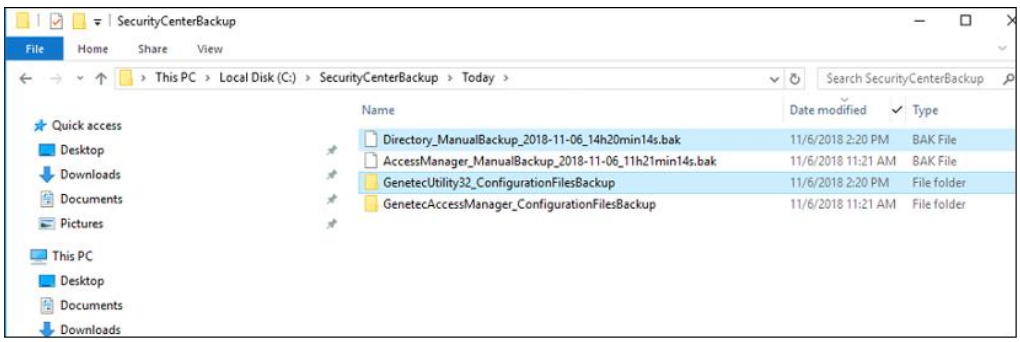


Figura 64: Archivos de respaldo de Directory

Fuente: Propia

Una vez se finalizó con el respaldo de la base de datos principal, corresponde a la sección “Archiver” y “Access Manager”, los cuales tuvieron un proceso similar, en el cual, dentro del aplicativo “Config Tool”, en las secciones Sistema, Roles, se configuró la copia de seguridad, como en la Figura 65.

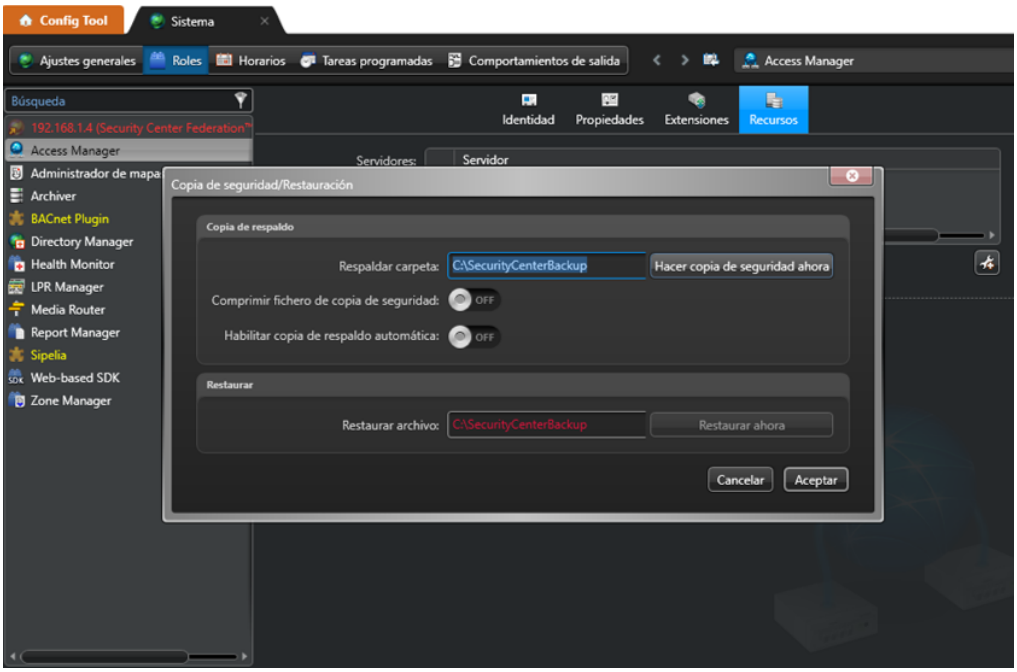


Figura 65: Configuración de respaldo de Access Manager

Fuente: Propia

4.3 Simulación del sistema de seguridad aplicando la plataforma VMS en el centro de monitoreo

4.3.1 Validación de comunicaciones entre dispositivos de red

Dentro del aplicativo Security Center, para verificar si un dispositivo está fuera de red, se visualiza el color del icono, en el caso que este se encuentre desconectado, aparecerá de color rojo, como se aprecia en la Figura 66,

Figura 66: Estado de dispositivos dentro de Security Center

Fuente: Propia

4.3.2 Evaluación de funcionamiento de plataforma VMS

Al acceder en la aplicación Security Center, en la Figura 67, se muestra como quedó la configuración realizada en Config Tool, y tiene la facilidad de manejo en llegar a todas las cámaras con pocos movimientos.

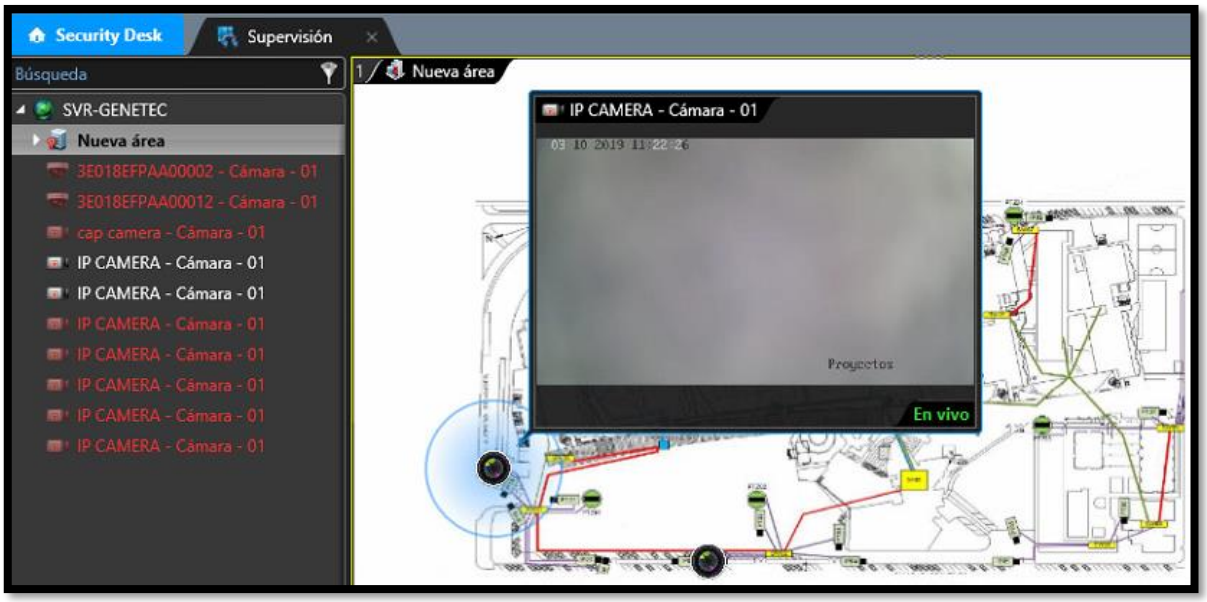


Figura 67: Visualización de cámaras en plano

Fuente: Propia

CAPITULO V: COSTOS

Aquí nos enfocamos en el presupuesto económico que costaría implementar el proyecto en el futuro. Para ello se tiene que tomar en cuenta los siguientes puntos a continuación.

5.1 Inversión CAPEX

A continuación, se verá la tabla de costos de inversión inicial de todos los dispositivos y equipamiento involucrado para la implementación del proyecto.

A continuación, se comparte la Tabla 6 de costos de inversión inicial de todos los dispositivos y equipamiento involucrado para la implementación del proyecto.

Tabla 6: Presupuesto de inversión por equipamiento y software

N°	Descripción	Cantidad	P. Unit $ (sin IGV)	P. Total $ (sin IGV)
Hardware				
1	Cámara IP HFW4231E-S	31	$ 200.00	$ 6,200.00
2	Servidor SV-300E-T4-30T-10-I5	1	$ 4,000.00	$ 4,000.00
3	Controlador de acceso Cloudlink	1	$ 1,500.00	$ 1,500.00
4	Interfaz Vertx V100	2	$ 200.00	$ 400.00
5	Lectora RFID R10 HID	7	$ 150.00	$ 1,050.00
Sub-Total sin IGV				$ 13,150.00
Software				
1	Licencia por cámara	31	$ 100.00	$ 3,100.00
2	Licencia por servidor	1	$ 250.00	$ 250.00
3	licencia por módulo de control de acceso	1	$ 500.00	$ 500.00
Sub-Total sin IGV				$ 3,850.00
Total Capex sin IGV				$ 17,000.00

Fuente: Propia

5.2 Inversión OPEX

En esta sección se presentan los costos de operación del proyecto, que involucran implementación, configuración y soporte.

A continuación, en la Tabla 7 se presenta los costos operativos para el funcionamiento del proyecto.

Tabla 7: Costos operacionales del proyecto

N°	Descripción	Cantidad	P. Unit $ (sin IGV)	P. Total $ (sin IGV)
1	Técnico de instalación de equipos	2	$ 1,000.00	$ 2,000.00
2	Supervisor	1	$ 1,500.00	$ 1,500.00
3	Jefe de proyecto	2	$ 3,000.00	$ 6,000.00
4	Ingenieros de soporte	2	$ 1,000.00	$ 2,000.00
5	soporte por 1 año	1	$ 2,000.00	$ 2,000.00
Total Opex sin IGV				$ 13,500.00

Fuente: propia

CONCLUSIONES

1) En base a la teoría recopilada y la experiencia en el rubro de seguridad electrónica obtenida, se logró determinar la aplicación de la plataforma VMS Security Center en el centro de Monitoreo de la Universidad Ricardo Palma, con el fin de optimizar los procesos internos y tecnología de este.

2) Los niveles de seguridad física perimetral, aplicando políticas de seguridad configuradas dentro de la plataforma, aumentan significativamente, brindando mayores alertas e indicadores a los operadores de seguridad.

3) Las simulaciones de la plataforma VMS nos demuestra lo fácil y amigable que es utilizar los sistemas, mediante la combinación y unificación de los sistemas de video vigilancia y control de acceso en una sola interfaz.

RECOMENDACIONES

1) Es recomendable tener todas las licencias y configuraciones recopiladas en un informe, el cual se debe ir actualizando cada vez que ocurran modificaciones dentro del sistema.

2) No se consideró renovar el cableado interno, debido que las cámaras actuales que se encontraron en la URP no muestran problemas de conectividad.

3) Se recomienda que el soporte operacional esté a cargo de personal certificado de la marca de fabricante, dado que estos tienen garantía sujeta al personal correspondiente.

4) Se debe tener en cuenta que, en caso de instalados los sistemas, estos requerirán periódicamente de mantenimiento preventivo, con el fin de asegurar el tiempo de vida de todos los equipos involucrados.

REFERENCIAS BIBLIOGRÁFICAS

Chávez, M. (2016). Diseño e Implementación del Sistema de Video Vigilancia de las Subestaciones de la Empresa Eléctrica Quito (Tesis de Pregrado). Universidad Tecnológica Israel, Quito-Ecuador.

Cisco (2019). Cisco Systems (2019). Understanding TCP/IP. Apéndice A, 6-8.

Davies A. C. & Velastin S. (2005). A Progress Review of Intelligent CCTV Surveillance Systems. *ResearchGate*, 1-6. Recuperado de: https://www.researchgate.net/publication/44113794_A_Progress_Review_of_Intelligent_CCTV_Surveillance_Systems

Derek, R. (1 de diciembre de 2016). The New Frontier For Video Management Systems. Security Distributing & Marketing, p.1-4. Recuperado de: http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=0&sid=052faa7e-c3ae-4b30-bf79-51819bdb9cf4%40sdc-v-sessmgr03

DSX Access System, Inc. (2011). What is Wiegand. DSX Access System. Recuperado 30 de setiembre de 2019 de: https://www.dsxinc.com/designguide2/docs2/whatiswiegand.pdf

Forero, N. (2012). Normas de Comunicación en Serie: RS-232, RS-422 y RS-485. Revista de la facultad de ingeniería de la universidad libre. p.86-94. Recuperado de: http://www.unilibre.edu.co/revistaingeniolibre/revista-11/art13.pdf

García, F. (2010) Videovigilancia: CCTV usando vídeos IP. [libro en línea] España: Vertice. [Consultado 23 mayo, 2019] Disponible en: https://books.google.com.pe/books?id=xb3mzBE-yIoC&printsec=frontcover&hl=es#v=onepage&q&f=false

Genetec Inc. (2018). Guía para el Administrador de Security Center 5.7. Genetec Security Center, 3,1200-1251.

Gil, P. (2009). Estudio, diseño y optimización de técnicas de visión artificial para su aplicación a los sistemas de videovigilancia (Tesis de Doctorado). Universidad de Alcalá, Madrid-España.

Gilling, T. (2017). The STREAM TONE: The Future of Personal Computing?. Inglaterra: Troubador Publishing Ltd. [Consultado 7 de setiembre, 2019] Disponible en: https://books.google.com.pe/books?id=K55wCQAAQBAJ&dq=H.264+H.265&source=gbs_navlinks_s

GRUPO EULEN (4 de junio de 2019). CENTRO DE CONTROL DE SEGURIDAD. Grupo Eulen. Recuperado de: https://www.eulen.com/es/seguridad/centro-de-control-de-seguridad/

Hernández, R y otros (2014). Metodología de la investigación. 6ta Ed. México D.F.: McGRAW-HILL/INTERAMERICANA

HID Global Corporation (14 de junio de 2019). Control de acceso. HID Global. Recuperado en: https://www.hidglobal.mx/access-control

Honey, G. (2004). ELECTRONIC ACCESS CONTROL. [Libro en línea] Oxford: Elseiver Inc. [Consultado 18 de julio, 2019] Disponible en: https://books.google.com.pe/books?id=UIlg6kdz1skC&printsec=frontcover#v=onepage&q&f=false

Huidobro, J. entre otros (2008). Redes de Área Local. 2da Ed. [libro en línea] España: Parainfo. [Consultado 14 de agosto, 2019] Disponible en: https://books.google.com.pe/books?id=V2xogIe99B8C&printsec=frontcover#v=onepage&q&f=false

ISO/EIC 9646-2:1994 (2019). Information Technology - Open System Interconnection - Conformance testing methodology and framework - Part2: Abstract Test Suite specification. [Consultado 01 de octubre, 2019] Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:7498:-1:ed-1:v2:en

JM Industrial (2006). RS-485. JM industrial Technology S.A. de C.V., 1-2.

Kruegle, H. (2011). CCTV Surveillance: Video Practices and Technology. 2nd ed. [Libro en línea] Oxford: Elseiver Inc. [Consultado 23 de mayo, 2019] Disponible en: https://books.google.com.pe/books?id=DaQY8CrmqFcC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Kumar, S. & others. (2018). *Internet of Things Security: Fundamentals, Techniques and Applocations*. [libro en línea] Holanda: River Publishers [Consultado el 26 de junio, 2019] Disponible en: https://books.google.com.pe/books?id=OxhwDwAAQBAJ&printsec=frontcover#v=onepage&q&f=false

Li, J. (2018). Measurement and Analysis of Overvoltages in Power Systems. 1ra Ed. [libro en línea] China:The Atrium [Consultado 06 de agosto, 2019] Disponible en: https://books.google.com.pe/books?id=mKJiDwAAQBAJ&printsec=frontcover#v=onepage&q&f=false

Longdin, A. (2014). The history of CCTV – from 1942 to present. Recuperado 15 de mayo de 2019, en https://pcr-online.biz/2014/09/02/the-history-of-cctv-from-1942-to-present/

López, E. (2008). INGENIERIA EN MICROCONTROLADORES. Protocolo RS-485. Recuperado 04 de noviembre de 2019 de https://www.jmi.com.mx/documento_literatura/RS485.pdf

Lyon D. (2002). Surveillance Studies: Understanding visibility, mobility and the phenetic fix. Surveillance & Society 1(1), 1-7. Recuperado de https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3390/3353

Manuales USERS (2011). MICROCONTROLADORES. 1ra Ed. [libro en línea] Buenos Aires: Fox Andina [Consultado 12 de agosto, 2019] Disponible en: https://books.google.com.pe/books?id=V1wLsfO1114C&printsec=frontcover#v=onepage&q&f=false

Mercado, R. (2017). Diseño de un sistema de videovigilancia para una empresa del sector alimenticio que permita el monitoreo local y remoto de sus instalaciones (Tesis de Pregrado). Universidad Autónoma de Occidente, Cali-Colombia.

Meurant, G. (2013). CCTV Surveillance: Video Practices and Technology. 1ra ed. [Libro en línea]. Washington: British Library. [Consultado 23 de mayo, 2019] Disponible en: https://books.google.com.pe/books?id=Ek0vBQAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

MJ Security Systems Limited (2014). History of the CCTV camera. MJ Security Systems Limited. Recuperado de: https://www.mjsecurity.co.uk/history-cctv.html

Musburger, R. y Ogden, M. (2014). Single-Camera Video Production. New York y Londres: CRC Press. [Consultado 07 de agosto, 2019] Disponible en: https://books.google.com.pe/books?id=tqPcAwAAQBAJ&dq=codec+video+H.265&hl=es&source=gbs_navlinks_s

Nilsson, F. (2017). Intelligent Network Video. Understanding Modern Video Surveillance Systems. 13.1 Video management architectures. 2da ed. [libro en línea] Florida: Taylor & Francis Group. [Consultado 06 de junio, 2019] Disponible en: https://books.google.com.pe/books?id=y6WiDQAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Pavón, J. (2016). Análisis técnico de la implementación de un sistema de seguridad de video vigilancia, caso de estudio Aeropuerto Internacional Mariscal Sucre del Ecuador (Tesis de Maestría). Pontificia Universidad Católica del Ecuador, Quito-Ecuador.

Peláez, S. (2013). Diseño de un Sistema de Video Vigilancia IP para la Corte Superior de Justicia - La Libertad (Tesis de Pregrado). Universidad Privada del Norte, Trujillo-Perú.

Perdiguero, M. (2017). UF0926: Diseño y organización del alamacén. 7.6. Sistemas de radiofrecuencia: los tag y las etiquetas. 1ra ed. [libro en línea] Málaga: IC Editorial. [Consultado 06 de agosto, 2019] Disponible en: https://books.google.com.pe/books?id=QbhdDwAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false

Perez, C. (2016). Diseño de un sistema de seguridad electrónica con monitoreo centralizado para protección de una instalación minera (Tesis de Pregrado). Pontificia Universidad Católica del Perú, Lima-Perú.

Portillo, J. y otros autores. Tecnología de identificación por radiofrecuencia (RFID): aplicaciones en el ámbito de la salud. España, Madrid: Fundación Madrid para el Conocimiento Velázquez.

Puse, R, & Ruiz, M. (2015). Diseño e implementación de un sistema de monitoreo y gestión, mediante el uso de vpns, para optimizar el servicio de soporte en los sistemas de video vigilancia implementados por la empresa netkrom technologies (Tesis de Pregrado). Universidad Nacional Pedro Ruiz Gallo, Lambayeque-Perú.

Rodríguez, D. (2019). Investigación aplicada: características, definición, ejemplos. Recuperado 27 de junio de 2019, en https://www.lifeder.com/investigacion-aplicada/

Sadowsky, G. & others. 2003. INFORMATION TECHNOLOGY SECURITY HANDBOOK. Washington D.C.: The World Bank.

SecureComm Technologies (21 de junio de 2019). The Evolution of Access Control Systems. Recuperado de https://securecomminc.com/2014/06/19/the-evolution-of-access-control-systems/

The Cisco Learning Network. (2017) Open Systems Inteconnectioncmodel (OSI). [Consultado 01 de octubre, 2019] Disponible en: https://learningnetwork.cisco.com/docs/DOC-31934

W&T conecta. (2006). Sistemas de bus RS485. Recuperado 30 de setiembre de 2019, en https://www.wut.de/e-6wwww-11-apes-000.php

Zeljkovic, V. (2014). Video Surveillance Tchniques and Technologies. [libro en línea] EE.UU.: IGI Global [Consultado 05 de agosto, 2019] Disponible en: https://books.google.com.pe/books?id=XFwrAgAAQBAJ&printsec=frontcover#v=onepage&q&f=false

ANEXOS

ANEXO 1: Modelo de cámara DH-IPC-HFW4231E-S

Eco Savvy 3.0 | DH-IPC-HFW4231E-S

DH-IPC-HFW4231E-S

2MP WDR IR Mini Bullet Network Camera

- 1/2.8" 2Megapixel progressive scan STARVIS™ CMOS
- H. 265&H.264 triple-stream encoding
- 50/60fps@1080P(1920×1080)
- Smart Detection supported
- WDR(120dB), Day/Night(ICR), 3DNR, AWB, AGC, BLC
- Multiple network monitoring: Web viewer, CMS(DSS/PSS) & DMSS
- 3.6mm fixed lens (6mm optional)
- Max. IR LEDs Length 40m
- Micro SD Memory,IP67, PoE

System Overview

Eco-savvy products by upgrading H.265 encoding technology, bringing high efficient video compression. It saves bandwidth and storage , energy-saving design to enhance the monitoring system . Meanwhile, the series offers features such as starlight , Smart IR technology , intelligent image analysis techniques. It provides excellent image quality and intelligent and efficient event reminders . This series provides IP67 weatherproof and IK10 vandal-proof protection feature. Give customers more value

Functions

Starlight Technology
Featuring Dahua's Starlight Technology, this camera is ideal for applications with challenging lighting conditions. Its low-light performance delivers usable video with minimal ambient light. Even in extreme low-light conditions, Starlight Technology is capable of delivering color images in near complete darkness (0.009 lux).

Wide Dynamic Range
Embeded with industry leading wide dynamic range (WDR) technology, vivid picutures are achieved even in the most intense contrast lighting conditions. For applications with both bright and low lighting conditions that change quickly, True WDR (120dB) optimizes both the bright and dark areas of a scene at the same time to provide usable video.

Intelligent Video System (IVS)
With built-in intelligent video analytics, the camera has the ability to detect and analyze moving objects for improved video surveillance. The camera provides optional standard intelliegence at the edge allowing detection of multiple object behaviors such as abandoned or missing objects. IVS also supports Tripwire analytics, allowing the camera to detect when a pre-determined line has been crossed, ideal for business intelligence, and Facial Detection, for searching or identification of individuals.

Environmental
With a temperature range of-30 °C to +60 °C (-22°F to +140 °F), the camera is designed for extreme temperature environments. Subjected and certified to rigorous dust and water immersion tests, the IP67 rating makes it suitable for demanding outdoor applications. For enviorments with rain, sleet, snow and fog, an integrated wiper provides users with clear visibility at all times.

Protection
Supporting ±30% input voltage tolerance, this camera suits even the most unstable conditions for outdoor applications. Its 4KV lightning rating provides protectection against the camera and its structure from the effects of lightning.

Smart H.265+
Deliver high quality video without straining the network, Smart H.265+ is the optimized implementation of H.265. The Smart H.265+ encoding technology includes a scene adaptive encoding strategy, dynamic GOP, dynamic ROI, flexible multi-frame reference structure and intelligent noise reduction, providing saving of up to 70% of bandwidth and storage when compared with standard H.265.

HEVC (H.265)
H.265 ITU-T VCEG is a new video coding standard. H.265 Following standard developed around the existing video coding standard H.264 , some retain the original technology , while some of the relevant technology to improve the new technology uses advanced technology to improve the relationship between the code stream , encoding quality , and the delay between algorithm complexity , optimize settings specific contents include : Improve compression efficiency , improve the robustness and error recovery capabilities, real-time to reduce the delay, reduce channel acquisition time and a random access delay , reduce complexity , etc

ANEXO 2: Precio de cámara HFW4231E-S

Fuente: https://articulo.mercadolibre.com.pe/MPE-436385965-camara-bullet-ip-dahua-2mp-savvy-serie-ipc-hfw4231e-se-_JM

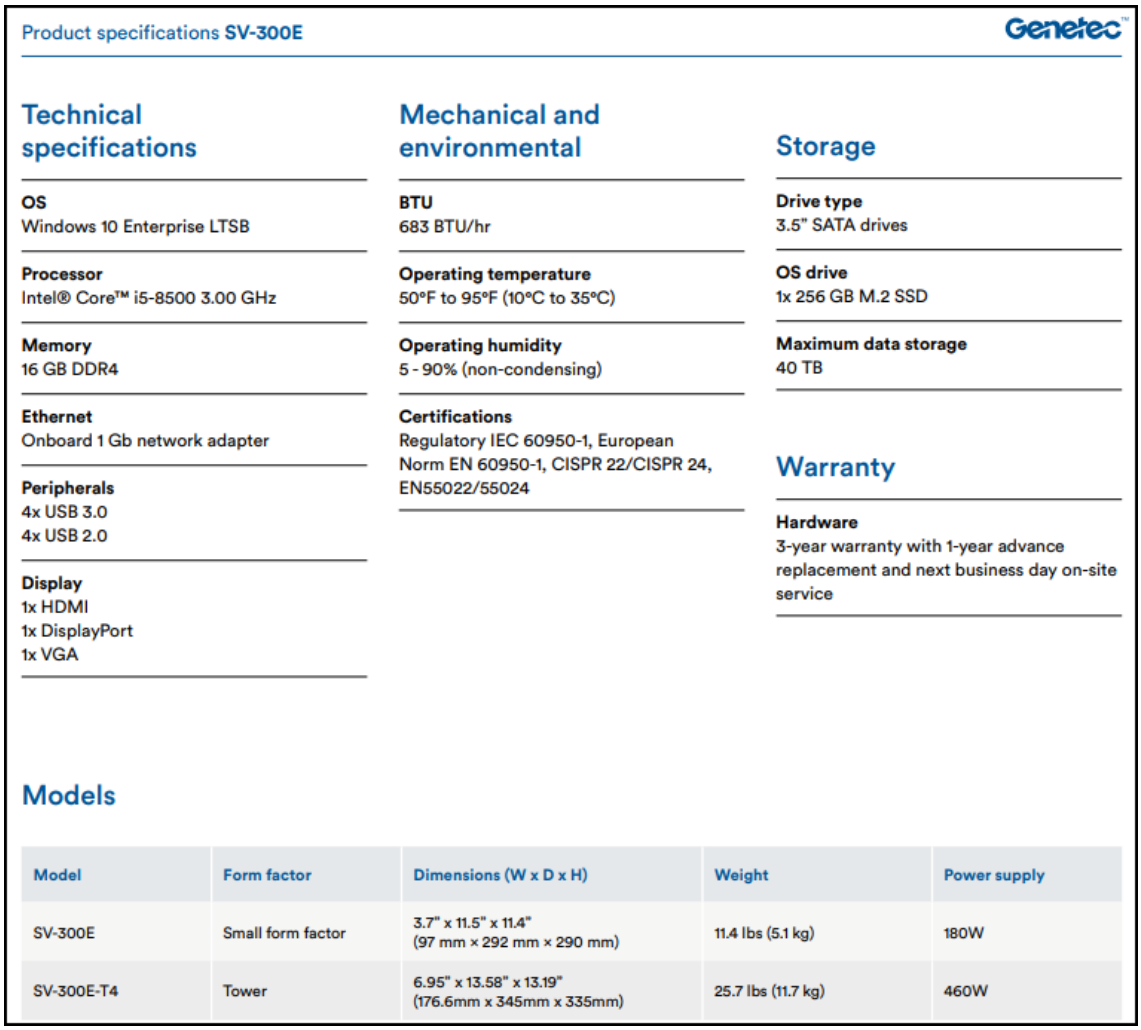
ANEXO 3: Precio de cámara Q1785-LE

Fuente: https://www.amazon.com/Axis-Communications-01161-001-Q1785-LE-Network/dp/B07K7X3JKW

ANEXO 4: Precio de cámara SNO-L6013R

Fuente: https://www.amazon.com/Samsung-SNO-L6013R-Network-Bullet-Camera/dp/B00X8JTAH4

ANEXO 5: Datasheet de servidor SV-300E-T4-30T-10-I5



Product specifications **SV-300E**

Genetec

Technical specifications

OS
Windows 10 Enterprise LTSB

Processor
Intel® Core™ i5-8500 3.00 GHz

Memory
16 GB DDR4

Ethernet
Onboard 1 Gb network adapter

Peripherals
4x USB 3.0
4x USB 2.0

Display
1x HDMI
1x DisplayPort
1x VGA

Mechanical and environmental

BTU
683 BTU/hr

Operating temperature
50°F to 95°F (10°C to 35°C)

Operating humidity
5 - 90% (non-condensing)

Certifications
Regulatory IEC 60950-1, European Norm EN 60950-1, CISPR 22/CISPR 24, EN55022/55024

Storage

Drive type
3.5" SATA drives

OS drive
1x 256 GB M.2 SSD

Maximum data storage
40 TB

Warranty

Hardware
3-year warranty with 1-year advance replacement and next business day on-site service

Models

Model	Form factor	Dimensions (W x D x H)	Weight	Power supply
SV-300E	Small form factor	3.7" x 11.5" x 11.4" (97 mm x 292 mm x 290 mm)	11.4 lbs (5.1 kg)	180W
SV-300E-T4	Tower	6.95" x 13.58" x 13.19" (176.6mm x 345mm x 335mm)	25.7 lbs (11.7 kg)	460W

Fuente: https://resources.genetec.com/en-datasheets/streamvault-sv-300e-datasheet

ANEXO 6: Matriz de consistencia

PROBLEMA GENERAL	OBJETIVO GENERAL	VARIABLES	DIMENSIÓN
¿Cómo se aplicará la plataforma VMS para optimizar el diseño del sistema de seguridad electrónica en el centro de monitoreo de la Universidad Ricardo Palma, 2019?	Determinar la aplicación de la plataforma VMS para optimizar el diseño del sistema de seguridad electrónica en el centro de monitoreo de la Universidad Ricardo Palma.	Plataforma VMS	Configuración
PROBLEMAS ESPECÍFICOS	**OBJETIVOS ESPECÍFICOS**		
1. ¿Cómo será el diseño de la topología del sistema de seguridad aplicando la plataforma VMS en el centro de monitoreo? 2. ¿Cómo será el diseño de la parte de control del sistema de seguridad aplicando la plataforma VMS en el centro de monitoreo? 3. ¿Cómo será la simulación del sistema de seguridad aplicando la plataforma VMS en el centro de monitoreo?	1. Determinar el diseño de la topología del sistema de seguridad aplicando la plataforma VMS en el centro de monitoreo. 2. Establecer el diseño de la parte de control del sistema de seguridad aplicando la plataforma VMS en el centro de monitoreo. 3. Implementar la simulación del sistema de seguridad aplicando la plataforma VMS en el centro de monitoreo-	SISTEMA DE SEGURIDAD ELECTRONICA	Topología Parte de control

Fuente: Propia