UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UN SISTEMA DE SEGURIDAD ELECTRÓNICA SOBRE INFRAESTRUCTURA DE COMUNICACIONES PARA UNA COMPAÑÍA MINERA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

ANTONIO GONZÁLES JÁUREGUI

PROMOCIÓN

2002-II

LIMA-PERU

2009

DISEÑO DE UN SISTEMA DE SEGURIDAD ELECTRÓNICA SOBRE INFRAESTRUCTURA DE COMUNICACIONES PARA UNA COMPAÑÍA MINERA

Mi eterna gratitud a Antonio y Ricardina, mis padres.
A mi Papá por su gran fortaleza y espíritu invencible.
A mi Mamá por su cariño, paciencia y comprensión.
Elementos fundamentales en mi formación

SUMARIO

El presente trabajo describe detalladamente los aspectos que deben tomarse en cuenta para un adecuado diseño de un sistema de seguridad basado en IP.

Hoy en día, la seguridad es un elemento importante dentro de las organizaciones empresariales. En entornos cada vez más competitivos, una de las estrategias para mantener los ingresos y rentabilidad de las compañías, es reducir al mínimo los riesgos que puedan ocasionar perdidas de los activos y/o paralización de las operaciones productivas.

Sucede lo mismo con los gobiernos. Mientras más insegura sea una ciudad o país, este tendrá poco acceso a las inversiones de la empresa privada. Los gobiernos deben brindar un clima de estabilidad y seguridad a los ciudadanos y empresas para que las actividades económicas se lleven a cabo con fluidez.

Para cumplir tales objetivos, los sistemas de seguridad electrónica han sido utilizados durante muchos años como herramientas de prevención e investigación de incidentes delictivos. La tecnología que han utilizado durante mucho tiempo ha sido analógica. Sin embargo, a medida que crecen las necesidades de los usuarios, ya sea porque aumentaron los riesgos o haya un incremento de la actividad económica, es necesario buscar nuevas alternativas que satisfagan estas nuevas necesidades, y eso sólo es posible conseguirlo con los sistemas de seguridad basados en IP, ya que no tienen restricciones en su uso y pueden ser gestionados desde cualquier lugar de la red.

En este informe se exponen los sistemas tradicionales de seguridad y la manera en que han venido evolucionando en los últimos años, se mostrará también la forma en la que una compañía puede migrar de un sistema tradicional a uno basado en IP reutilizando al máximo la inversión existente.

ÍNDICE

INTRODUCCIÓN

Actualmente, uno de los principales desafíos para las compañías es implementar un sistema de seguridad eficiente que le permita reducir al mínimo el riesgo de amenazas y prevenir las pérdidas de activos de la compañía.

Uno de los sectores de la economía que han hecho grandes inversiones en materia de seguridad son las compañías mineras, ya que estas al tener grandes extensiones de terreno y mucho capital invertido en equipamiento y maquinaria repartidos en toda el área de exploración, pueden sufrir y han sufrido perdidas de diversos equipos y materiales de mucho valor.

Los sistemas de seguridad, particularmente el de video vigilancia, no solamente son utilizados para contrarrestar actos delictivos, sino también para ayudar a las áreas de producción a reducir los accidentes causados por las malas prácticas en el trabajo diario, y también para monitorear procesos críticos donde la presencia del hombre es muy riesgosa.

Muchas de las actuales instalaciones de estas compañías utilizan aún tecnología analógica, por lo que se deben tener múltiples centros de control y monitoreo por las limitaciones en la distancia de transmisión que tiene la señal analógica. Y no es posible en muchos de los casos, compartir información de video a otras áreas diferentes del centro de control.

La tendencia hoy en día es que las compañías deben ser cada vez más eficientes en sus procesos productivos, y para ello el uso de la tecnología juega un rol fundamental.

Muchos sistemas de seguridad y video vigilancia están dejando se ser de uso exclusivo del área de seguridad, puesto que pueden ayudar a otras áreas como producción, recurso humanos, marketing, etc. a ser más eficientes.

Pero esto solo es aprovechable con los modernos sistemas basados en IP, ya que son sistemas que pueden agregar inteligencia a su operación, y se pueden acceder a ellos desde cualquier parte de la red corporativa o incluso Internet.

Obviamente, reemplazar todo el equipamiento analógico existente por equipos basados en IP, no es una buena alternativa económica. Dicho cambio debe ser gradual,

aprovechando al máximo la instalación existente, sin paralizar las operaciones de la compañía y acorde con las necesidades del área usuaria.

En este informe, se describe las mejores prácticas para el diseño de un sistema de seguridad basado en IP, aprovechando al máximo los recursos disponibles y cubriendo todos los aspectos relacionados a los sistemas.

Se asumirá en muchos casos, que la infraestructura de red es existente y a lo mucho se deberán hacer algunos tendidos de cableado estructurado horizontal para nuevas ubicaciones. Los conceptos de networking, cableado estructurado y sistemas de protección eléctrica se van a mencionar en diferentes partes de este informe, pero no se ahondarán en ellos, ya que no forman parte del alcance de éste.

La bibliografía utilizada fue obtenida de los fabricantes más importantes de la industria y brinda información actualizada y de gran utilidad para la elaboración de este informe

CAPÍTULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

1.1 Descripción del Problema

Muchas compañías mineras cuentan en la actualidad con sistemas de seguridad electrónica basados en video vigilancia y control de acceso. El primero para monitorear en tiempo real las instalaciones de la planta y/o áreas perimétricas y el segundo, para controlar el ingreso de vehículos y personas a áreas restringidas de la compañía.

Como consecuencia del crecimiento de la demanda de minerales en los últimos años; la mayoría de compañías mineras han tenido que ampliar y/o modernizar sus plantas de producción y en consecuencia, ampliar sus sistemas de seguridad.

Los requerimientos actuales de seguridad han cambiado mucho desde la vez que se implementó el sistema de seguridad basado en tecnología analógica, ya que se ha reducido el presupuesto para los puestos de vigilancia y también, debido a que los conflictos sociales se acrecentaron en la zona.

El sistema de video vigilancia actual no brinda a los operadores las herramientas adecuadas que les permitan actuar oportunamente ante un evento o incidente que ponga en riesgo la operación de la mina, sino que es utilizado básicamente para hacer análisis forense de eventos que ya sucedieron y por consiguiente; generaron pérdidas a la compañía. Así mismo, cuando se revisan los archivos grabados, la calidad de la imagen es mala y no logran identificarse nítidamente a las personas o vehículos que ocasionaron la paralización de la operación o pérdida de objetos valiosos, por poner un ejemplo.

La compañía minera actualmente cuenta con un sistema de CCTV analógico adquirido hace 4 años en una de sus plantas.

Los equipos existentes consisten de: 13 cámaras tipo PTZ modelo Esprit de Pelco, 10 cámaras Domo PTZ con compartimentos presurizados y 16 cámaras fijas. Todas las cámaras están ubicadas estratégicamente en toda la planta de producción.

Debido a las grandes distancias de transmisión, se utiliza fibra óptica multimodo para la transmisión del video analógico, utilizando para ello conversores de cable coaxial a fibra óptica en cada cámara.

En el centro de control, se cuenta con una matriz de video analógico de 48x16 (48 entradas de video y 8 salidas para monitores). Además se tienen 3 grabadores digitales de 16 canales de video y 2 TB de disco duro cada uno.

La operación y mantenimiento de este sistema se ha vuelto cada vez más costoso y ahora que, se va a modernizar la planta se necesita instalar más cámaras y repotenciar el sistema existente.

Así mismo, para complicar más el escenario, la compañía minera se encuentra ubicada en el departamento de Apurimac y está ubicada a una altura promedio de 4300 m.s.n.m. La temperatura ambiente oscila entre - 5 ºC y 16.5 ºC y se tienen fuertes precipitaciones durante 9 meses del año, con presencia de tormentas eléctricas. Deben considerarse todos estos factores al momento de diseñar la solución.

Según el informe del departamento de operaciones, se requiere migrar a un sistema de seguridad moderno, pero es necesario aprovechar al máximo la infraestructura existente y que conviva con el nuevo sistema de manera integrada.

Según el informe, las necesidades de seguridad del área de operaciones para la zona ampliarse incluyen 16 cámaras fijas, 15 cámaras Domo PTZ y un sistema de control de acceso peatonal y vehicular al ingreso de la planta.

Ambos sistemas deben estar integrados. Es decir: se debe guardar un registro de cada persona o vehículo que ingresa a la planta con su correspondiente archivo de video o de imagen.

1.2 Objetivo del Trabajo

Plantear el diseño de un moderno sistema de seguridad integrado para la compañía minera, que pueda ser utilizado como plataforma de gestión de seguridad para todas las sedes de la compañía.

1.3 Evaluación del Problema

Se necesita brindar a las diferentes áreas de la compañía, herramientas tecnológicas confiables para la seguridad que les permita reducir las pérdidas debido a accidentes y/o robos

Es necesario también supervisar las diferentes etapas productivas de la compañía minera. Para facilitar la supervisión de los responsables de la operación, se debe poder acceder al video desde cualquier estación de trabajo de la mina.

Para conocer más de cerca la problemática actual, se tratará a continuación la evolución de los sistemas de seguridad electrónica.

1.3.1 Evolución de los Sistemas de Seguridad Electrónica

Tradicionalmente, los fabricantes de seguridad diseñaron sus sistemas con arquitecturas propietarias, ya que se pensaba que mientras más cerrado era un sistema, más difícil era vulnerarlo.

Eso ha cambiado mucho desde entonces, pero es necesario conocer como han ido evolucionando los sistemas de seguridad para comprender mejor las necesidades y la solución que se plantea en este informe. Los sistemas de seguridad electrónica pueden clasificarse en:

- Sistemas de Circuito Cerrado de Televisión
- Sistemas de Control de Accesos
- Sistemas de Detección de Intrusos
- Sistemas de Alarma Contra Incendios

El presente informe se enfocará únicamente en los sistemas de Circuito Cerrado de Televisión y Control de Accesos, según las necesidades de la minera.

a. Evolución del CCTV

Se empezará describiendo un sistema de CCTV tradicional basado en tecnología analógica, el cual utiliza como medio de transmisión el cable coaxial. En la figura 1.1 se muestra un sistema de CCTV tradicional.

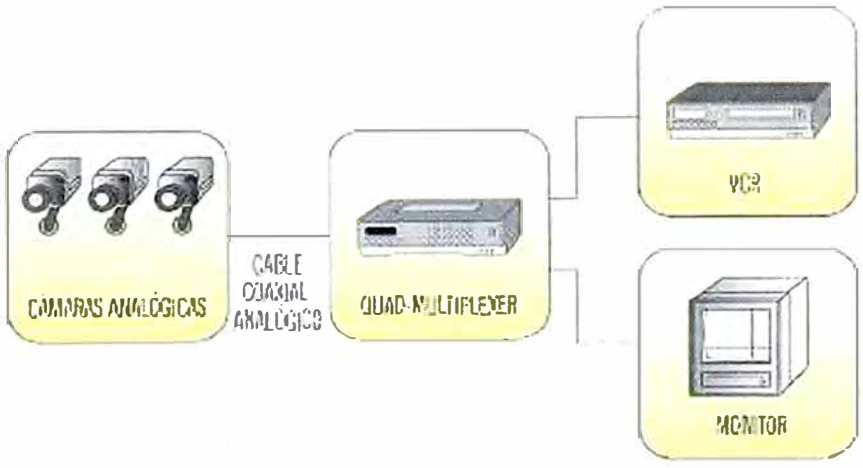


Figura 1.1 Sistema de CCTV Tradicional

En la figura anterior se observa que las cámaras envían el video a un equipo que se encarga de multiplexar las señales de video para mostrarlo en un monitor y son grabados en un VCR (Video Cassete Recorder)

A medida que aumentaba la cantidad de cámaras y necesidades de grabación, debido también al aumento de la capacidad de procesamiento de las computadoras y reducción del costo de los discos duros, los VCR y multiplexores fueron paulatinamente reemplazados por grabadores digitales de video o DVR por sus siglas en ingles (Digital Video Recorder). Ello se muestra en la figura 1.2

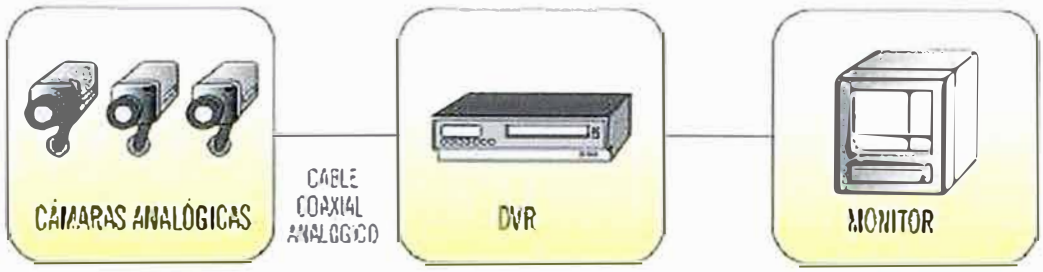


Figura 1.2 Grabadores Digitales de Video o DVR

Una de las consecuencias de la masificación del uso de las redes e Internet, fue que los responsables de seguridad y gerentes de las compañías deseaban poder visualizar el video en vivo o grabado de sus instalaciones en forma remota. Tal es así, que la siguiente generación de DVR contó con capacidad de conexión a redes Ethernet e Internet, donde cualquier usuario de la red puede acceder a los archivos y grabaciones de los DVR. En la figura 1.3 se muestra este tipo de sistema.

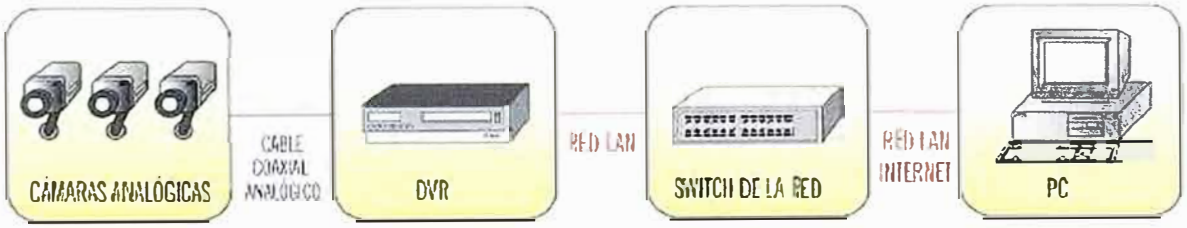


Figura 1.3 Acceso al Video por Red de Datos

Actualmente, los sistemas de CCTV basados en IP están tomando parte importante del mercado, ya que brindan mayores ventajas y beneficios para los usuarios finales, debido a que cada cámara cuenta con un procesador interno, y se puede utilizar esta "inteligencia" para tener sistemas predictivos de video (Video Inteligente). El esquema de funcionamiento es el que se muestra en la figura 1.4.

Al conectarse las cámaras directamente a las redes, los parámetros de diseño cambiaron significativamente, ya que existen elementos intermedios adicionales como: switches, routers y la misma infraestructura física (cableada o inalámbrica). Esto ha

ocasionado que el sector de la industria de seguridad reclute a nuevos profesionales con buena formación técnica en estas áreas.

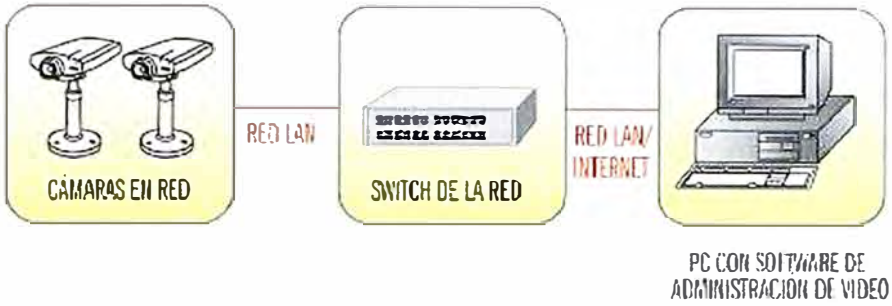


Figura 1.4 Esquema de Funcionamiento

b. Evolución de los Sistemas de Control de Acceso

Respecto a los sistemas de control de acceso e intrusión, estas han evolucionado de manera más lenta que los sistemas de CCTV, donde la principal añadidura está en las interfaces Ethernet que los principales fabricantes han añadido a sus controladores. En la figura 1.5 se puede observar un sistema tradicional de control de acceso.

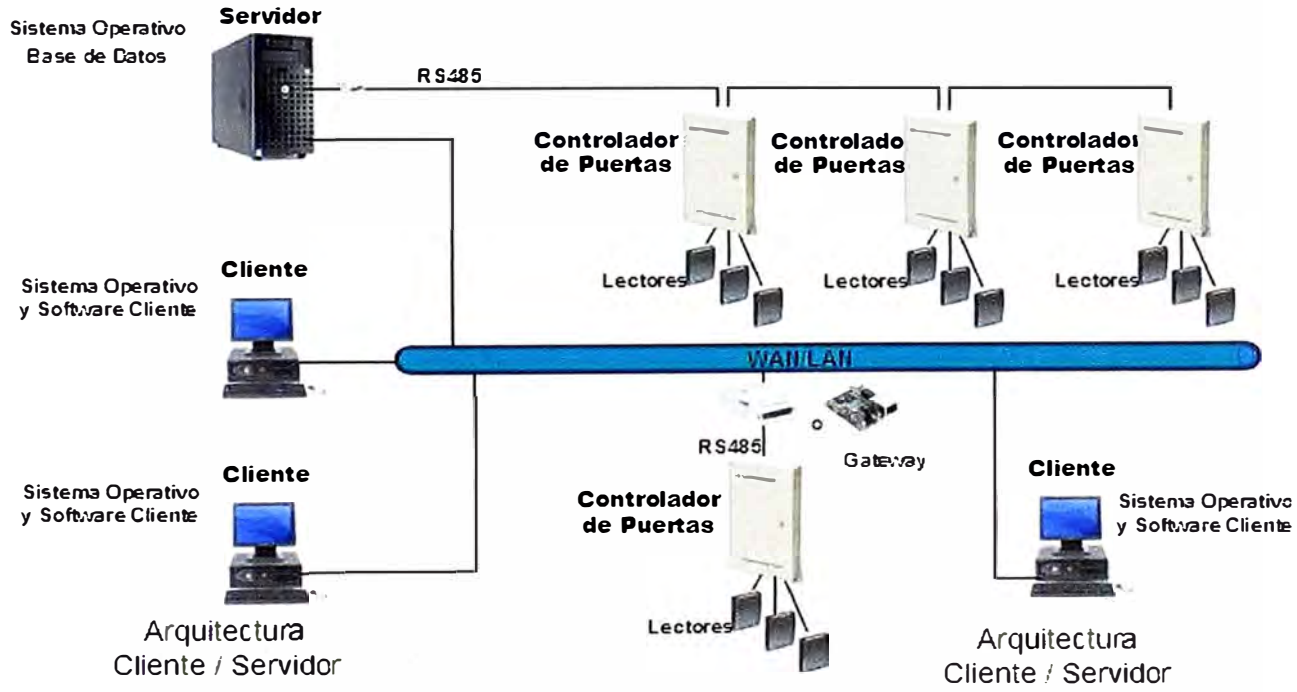


Figura 1.5 Sistema Tradicional de Control de Acceso

1.3.2 Conclusiones

Como se pudo observar, la tendencia del mercado de seguridad va hacia el mundo IP. Ha sido tan importante el crecimiento de esta industria en los últimos años,

que muchas compañías del segmento de TI han incursionado a ella y, se han creado nuevas unidades de negocio dentro de estas compañías, dedicadas solo a seguridad electrónica.

La respuesta al problema de la compañía minera es diseñar una solución de seguridad basada en IP, que utilice protocolos estándares de comunicación y permita convivir tecnología analógica y digital bajo una misma plataforma de gestión, que nos permita optimizar al máximo los puestos de vigilancia para el centro de control (Ya que de mantener sistemas separados se tendría que duplicar el número de operadores)

Así mismo, es importante que se integre el sistema de control de acceso con el de video. Es decir, cuando se active una tranquera vehicular o puerta de ingreso se almacene junto con el registro de la persona que ingreso, un clip de video. Ya que con esto se ahorra mucho tiempo en el análisis forense de eventos pasados.

CAPÍTULO II
MARCO TEÓRICO CONCEPTUAL

2.1 Introducción

En este capítulo se expone los conceptos relacionados a los Sistemas de Video Vigilancia IP, y a los Sistemas de Control de Acceso

2.2 Sistemas de Video Vigilancia IP

En esta sección se describen los siguientes elementos:

- Fuentes de Video IP
- Calidad de Imagen
- Compresión de Video
- Métodos de Transmisión
- Software de Gestión de Video
- Almacenamiento

2.2.1 Fuentes de Video IP

Las fuentes de video son las cámaras IP y los Codificadores de Video o también llamados video Server. Se explican cada uno de ellos en los siguientes párrafos:

a. Cámaras IP

La cámara IP es el elemento que captura la imagen, la digitaliza y transmite directamente a una red IP. Las cámaras IP cuentan con una dirección IP. Existen cámaras IP fijas y cámaras IP del tipo PTZ (Pan / Tilt / Zoom), es decir, que cuentan con movimiento horizontal, vertical y acercamiento de lente. Los componentes de la cámara IP se muestran en la figura 2.1.

Como se puede observar, la cámara cuenta con diferentes componentes comunes a todos los fabricantes, los cuales se describirán brevemente en las siguientes páginas, y están relacionados a la óptica de la cámara. Estos son:

- La lente,
- el filtro IR y
- el sensor de imagen.

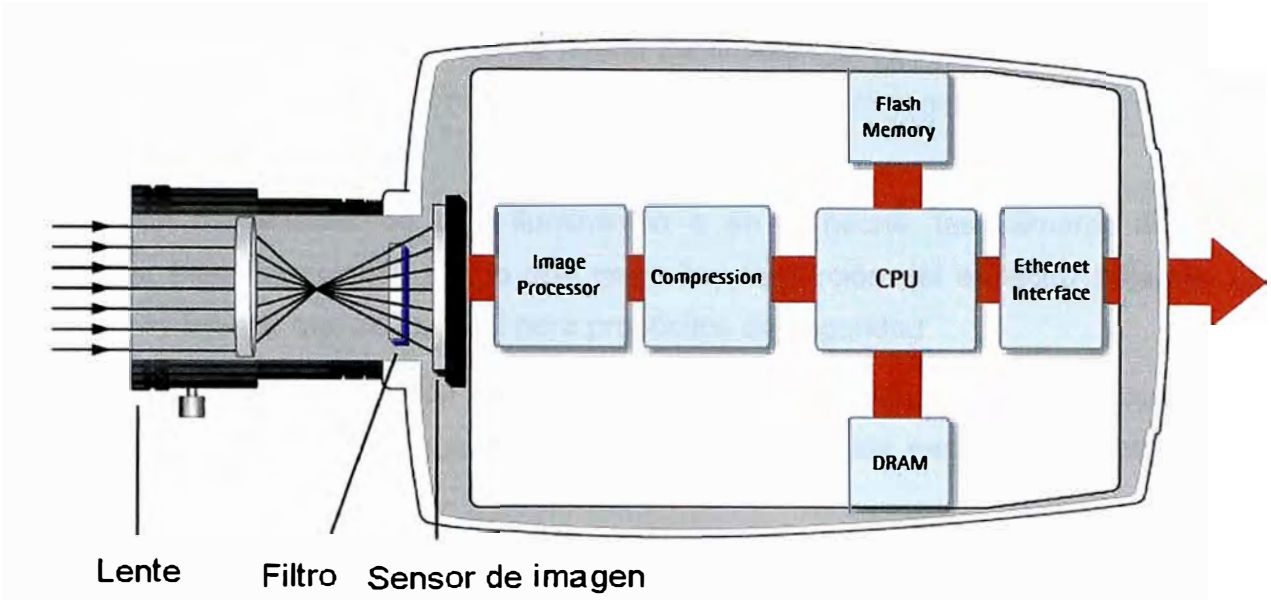


Figura 2.1 Componentes de Cámara IP

a.1 Lentes

Un lente es un dispositivo óptico para lograr el enfoque de la imagen. Los dos parámetros más importantes para seleccionar las lentes son por su longitud focal y el tipo de iris. Por tanto, Basado en su longitud focal se clasifican en:

- Lentes Monofocales
- Lentes Varifocales: Permite diferentes distancias focales
- Lentes Zoom

Basado en el tipo de iris:

- Lentes de iris fijo
- Lentes iris manual
- Lentes Autoiris
  - Autoiris tipo DC: El circuito de control está en la cámara
  - Autoiris de video: El circuito de control está en la lente

Los elementos constructivos de la lente se muestran en la figura 2.2

a.2 Filtro IR

Este elemento está relacionado al tipo de luz que ingresa al sensor de imagen. El filtro se encuentra entre el lente y el sensor de imagen. Para entender el funcionamiento del filtro es necesario explicar un poco del comportamiento de la luz.

Si se observa el espectro radioeléctrico. Las ondas de luz visible por el hombre tienen longitudes de onda entre 400 y 750 nm aproximadamente. Las cámaras captan todo el espectro de luz, incluido el infrarrojo.

En condiciones donde existe buena iluminación en la escena o existe luz diurna, las cámaras filtran la porción del espectro infrarrojo para tener una mejor calidad de imagen.

En condiciones de baja iluminación o en la noche, las cámaras no pueden distinguir bien los colores, por lo que necesitan la porción del espectro infrarrojo para obtener imágenes que sean útiles para propósitos de seguridad.

Cuando la iluminación es muy baja o no hay iluminación, algunas aplicaciones requieren que se instalen iluminadores infrarrojos externos para obtener imágenes en blanco y negro.

El tipo de luz que ingresa al sensor de imagen se muestra en la figura 2.3

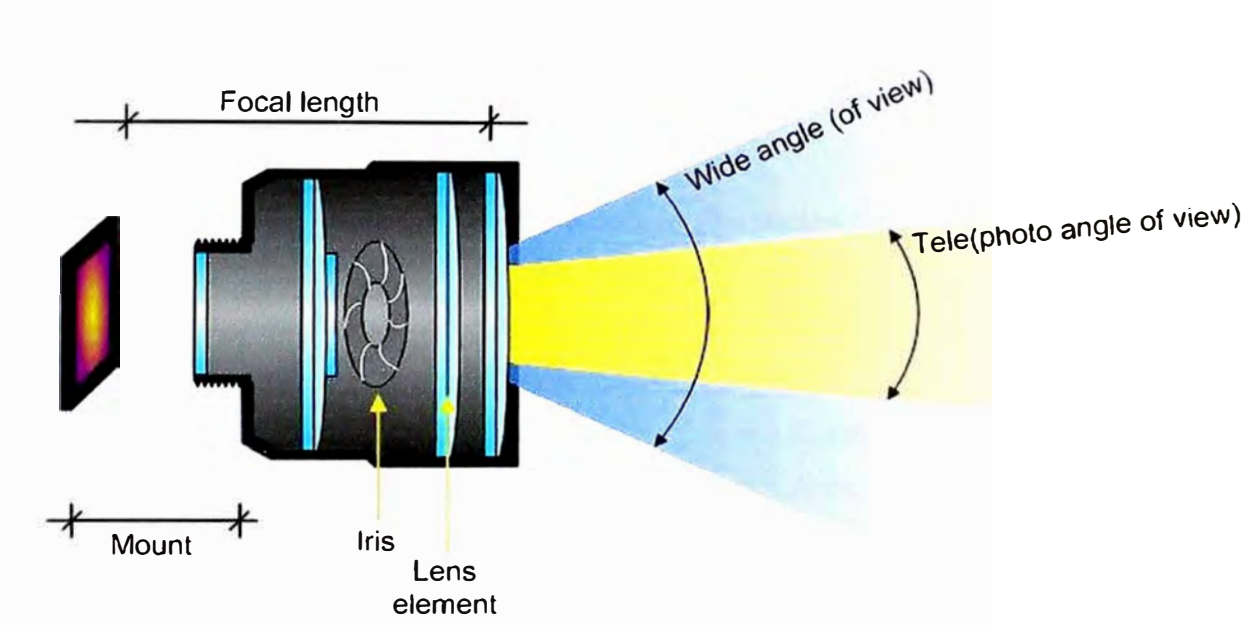


Figura 2.2 Elementos Constructivos de la Lente

a.3 Sensor de Imagen:

Es el elemento que capta la imagen de la escena. Este dispositivo convierte la luz en voltaje (fotones → electrones → señal de voltaje) utilizando el efecto fotovoltaico. Existen dos clases de elementos sensores:

CCD (Charged Coupled Device)

CMOS (Complementary Metal Oxide Semiconductor)

Las ventajas y desventajas entre cada uno de ellos se muestran en la tabla 2.1.

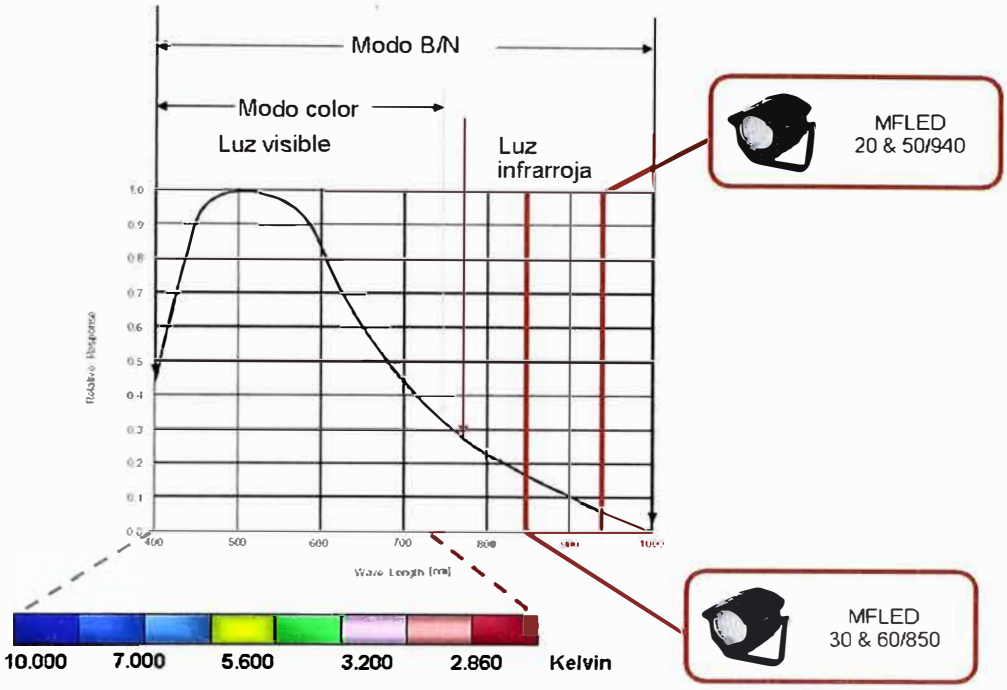


Figura 2.3 Tipo de Luz que Ingresa al Sensor de Imagen

Tabla 2.1 Comparación de Elementos Sensores

CCD	CMOS
PROS	**PROS**
+ Buena dinámica (sensibilidad luminica)	+ Coste de fabricación
+ **Bajo ruido**	+ Ahorro de espacio
CONTRAS	+ Posibilidad de utilización de múltiples partes del sensor (Windowing)
- Coste de fabricación	**CONTRAS**
- Construcción compleja	- Sensibilidad lumínica

b. Codificadores de Video

Los codificadores de video digitalizan las fuentes de video analógico, transformando una cámara analógica en una cámara IP. Esto las hace ideales para integrarlas a un sistema CCTV analógico. Un codificador de video puede incluir una o más entradas de video, un digitalizador y compresor de imagen, un servidor de Internet y un puerto de red Ethernet. En la figura 2.4 se muestra el uso común de los codificadores de video.

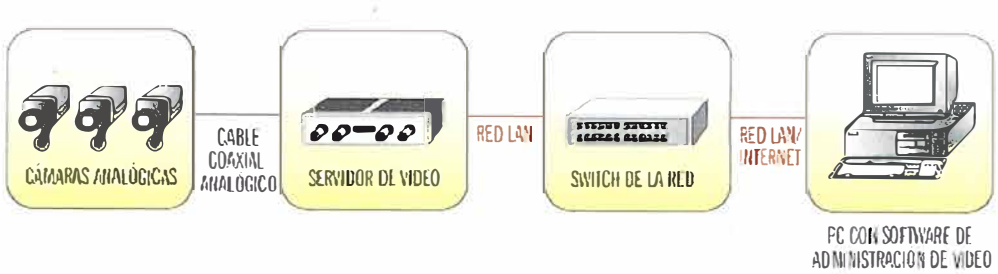


Figura 2.4 Uso Común de los Codificadores de Video

2.2.2 Calidad de Imagen

La calidad de imagen en las cámaras y codificadores IP se miden bajo dos parámetros: Resolución y cuadros por segundo.

a. Resolución y Cuadros por Segundo

La resolución en el mundo analógico o digital es similar, pero hay algunas importantes diferencias en cómo ésta es definida. En el mundo analógico, la resolución está definida por las líneas de TV horizontal y es derivada de la industria de TV. En un sistema digital, la resolución está definida en píxeles.

En el Perú, el sistema de Televisión utilizado es el NTSC, el cual consta de 30 cuadros por segundo o fps por sus siglas en ingles, y 480 TVL.

Cuando esta señal es digitalizada, la máxima cantidad de píxeles está basada en el número de líneas de TV disponibles en ser digitalizados. El máximo tamaño de una imagen digitalizada es típicamente D1 (720x480 píxeles) y más comúnmente 4CIF (704X480 píxeles). Ver Figura 2.5.

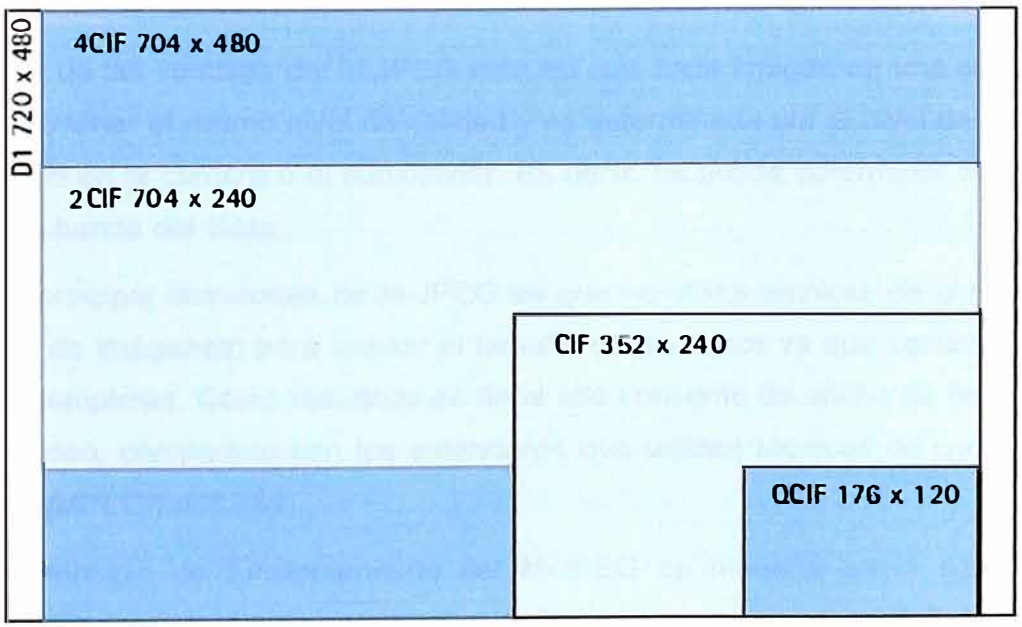


Figura 2.5 Tamaños de Imagen digitalizada

b. Resolución Megapíxel

Una cámara IP que ofrece una resolución megapíxel, utiliza un sensor de imagen megapíxel que genera una imagen de un millón o más píxeles. Esto permite tener imágenes de mayor calidad y mejores detalles (ideales para identificación de personas y objetos. Las diferentes resoluciones disponibles en el mercado se muestran en la tabla 2.2.

Tabla 2.2 Resoluciones Disponibles en el Mercado

Display format	No. of megapixels	Pixels
SXGA	1.3 megapixels	1280x1024
SXGA+ (EXGA)	1.4 megapixels	1400x1050
UXGA	1.9 megapixels	1600x1200
WUXGA	2.3 megapixels	1920x1200
QXGA	3.1 megapixels	2048x1536
WQXGA	4.1 megapixels	2560x1600
QSXGA	5.2 megapixels	2560x2048

2.2.3 Compresión de Video

Se muestra en esta sección aspectos relacionados a los métodos de compresión de video: M-JPEG, MPEG4, H.264.

a. M-JPEG

Motion JPEG o M-JPEG es una secuencia de video digital hecho de una serie de imágenes JPEG individuales. Cuando son mostradas 16 o más imágenes por segundo, se percibe como video en movimiento. Si se transmite los 30 cuadros en NTSC se dice que es video en tiempo real.

Una de las ventajas del M-JPEG está en que cada imagen en una secuencia de video puede tener el mismo nivel de calidad y es determinada por el nivel de compresión seleccionado en la cámara o el codificador. Es decir, se puede determinar con exactitud el ancho de banda del video.

La principal desventaja de M-JPEG es que no utiliza técnicas de compresión de video (solo de imágenes) para reducir el tamaño de los datos ya que continua enviando imágenes completas. Como resultado se tiene alto consumo de ancho de banda para el envío de video, comparado con los estándares que utilizan técnicas de compresión de video como MPEG4 o H.264.

El principio de funcionamiento del M-JPEG se muestra en la figura 2.6. Se observa que a pesar que solo una porción de la imagen cambia, el total de la imagen es transmitida.

Figura 2.6 Principio de Funcionamiento del M-JPEG

b. MPEG4

Cuando MPEG4 se menciona en aplicaciones de video vigilancia, usualmente hacen referencia a MPEG-4 part 2, también conocido como MPEG-4 Visual.

Tal como todos los demás MPEG estándares (Moving Pictures Experts Group) es un estándar licenciado, es decir, los usuarios deben pagar una licencia adicional por cada estación de monitoreo. MPEG-4 soporta aplicaciones que requieren alta calidad de imagen y bajo consumo de ancho de banda.

A diferencia de M-JPEG, MPEG-4 utiliza un método predictivo para reducir los datos de video entre una serie de cuadros, esto implica hacer una comparación de cada cuadro con un cuadro de referencia y únicamente los píxeles que han cambiado con respecto al cuadro de referencia son codificados y enviados. En la figura 2.7 se muestra el funcionamiento de MPEG-4.

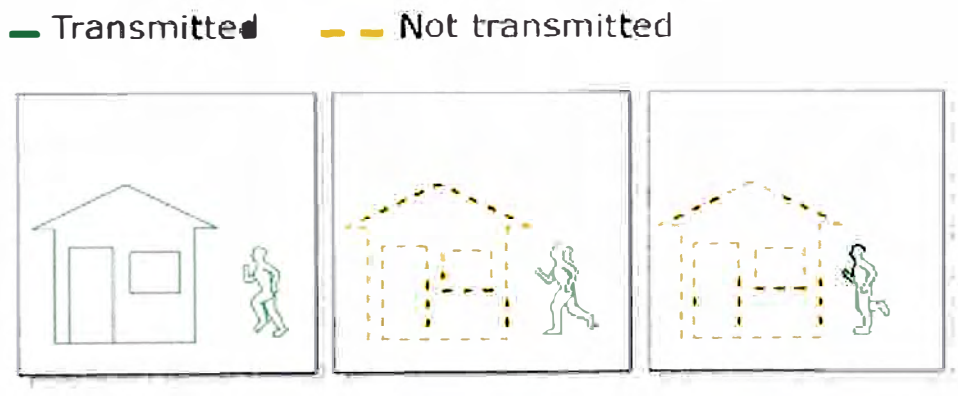


Figura 2.7 Funcionamiento de MPEG-4

c. H.264

H.264 es conocido como MPEG-4 Part 10 / AVC (Codificación Avanzada de Video) y es el último estándar de codificación de video y se espera que sea el estándar a elegir en los próximos años por los diferentes fabricantes de cámaras de video. Esto porque H.264 puede, sin comprometer la calidad de la imagen, reducir el tamaño de los datos de video hasta un 80% comparado con el M-JPEG y alrededor de 50% más que el M-PEG4.

La mejora se ve reflejada por el menor consumo de ancho de banda y capacidad de discos duros para almacenamiento. En la figura 2.8 se muestra la comparación entre los tres estándares de compresión revisados.

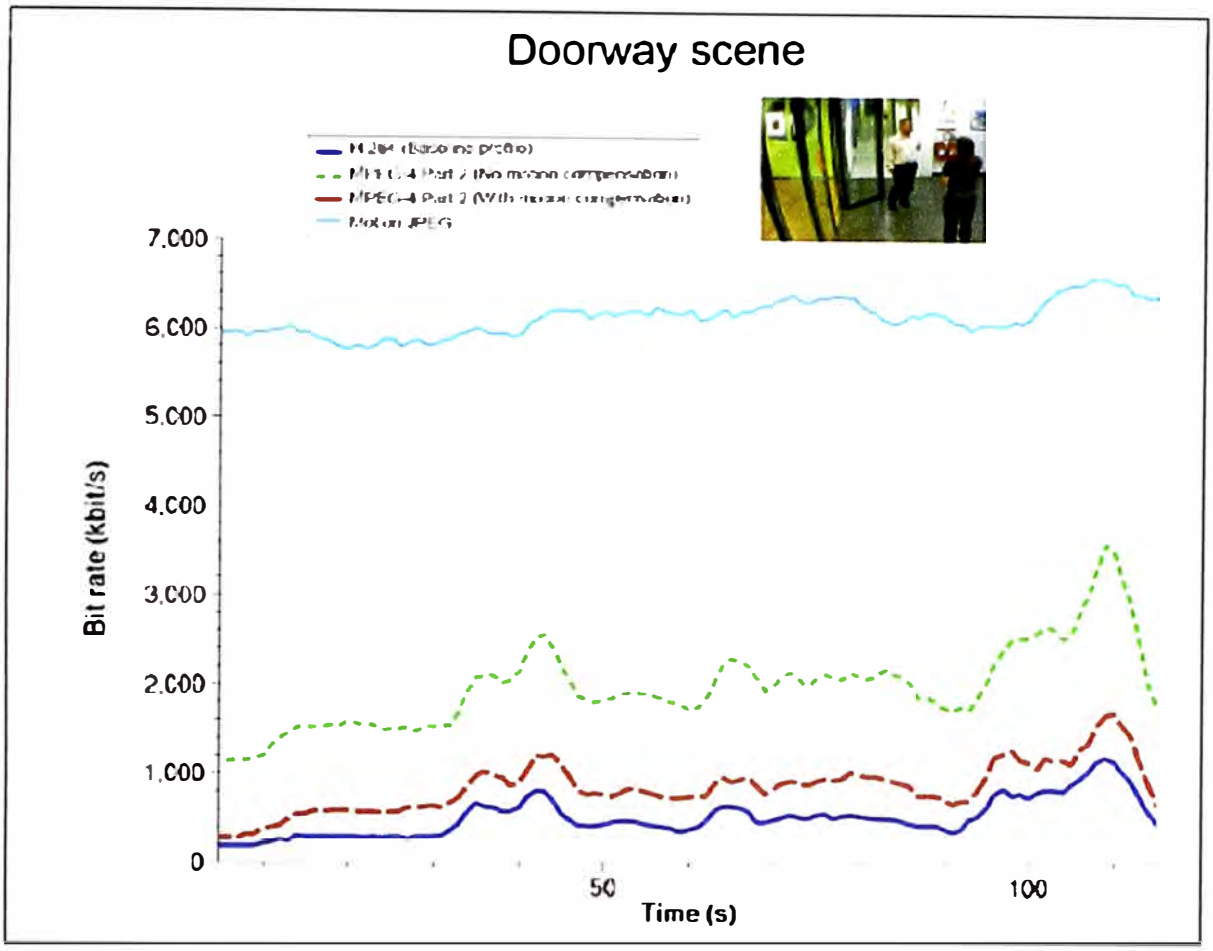


Figura 2.8 Comparación de los Tres Estándares

2.2.4 Métodos de Transmisión.

Los métodos de transmisión a describir son: Unicast y Multicast.

a. Unicast.

El Unicast es un método de transmisión utilizado para transmitir video de un único emisor (cámara) a un único receptor.

La desventaja de este método de transmisión es que si una cámara quiere ser vista por más de un usuario, esta generara tantos streams de video como usuarios conectados, reduciendo considerablemente el ancho de banda disponible para las demás aplicaciones diferentes de video.

b. Multicast.

El método utilizado para reducir el consumo de ancho de banda en la red, es utilizando transmisiones Multicast, donde un único stream de video es enviado a un grupo de usuarios simultáneamente.

La desventaja de este método, es que no todas las redes soportan Multicast, ya que todos los elementos de red como switches y routers deben estar configurados para soportarlo.

2.2.5 Software de Gestión de Video

Un importante aspecto de un sistema de video vigilancia es el software de gestión de video para monitoreo en tiempo real, grabación, reproducción y almacenamiento del video.

En la actualidad existen diferentes sistemas de gestión de video para uso en diferentes sistemas operativos y segmentos del mercado. Dentro de las consideraciones de selección del software están la plataforma de hardware (basado en PC o grabador de video en red de fabricación específica), características del sistema como instalación y configuración, manejo de eventos, video inteligente, seguridad y posibilidades de integración con otros sistemas como el control de acceso.

2.2.6 Almacenamiento

En aplicaciones de video vigilancia, es necesario que el video recibido de las cámaras sea almacenado en discos duros. Los factores a tener en cuenta para el cálculo de disco duro son las siguientes:

- Número de cámaras
- Grabación continua o por eventos
- Números de hora por día que se requiere grabar el video
- Cuadros por segundo
- Resolución
- Formato de compresión: M-JPEG, MPEG-4 o H.264
- Escenario, complejidad de la imagen por Ej.: vía pública u oficina, condiciones de iluminación y porcentaje de movimiento.
- Cuánto tiempo se desea almacenar el video

2.3 Sistemas de Control de Acceso

Los sistemas de control de acceso han sido tradicionalmente utilizados para autenticar el ingreso de las personas a una edificación.

Los ingresos peatonales y vehiculares de la mayoría de edificios modernos cuentan con sistemas de bloqueo tales como: puertas, barreras, molinetes, tranqueras, etc., los cuales son controlados electrónicamente por los sistemas de control de acceso.

Si un usuario con cuenta con los permisos para ingresar a la edificación, podrá autenticarse en el sistema y liberar las cerraduras de puertas o barreras que impiden el ingreso.

Existen diversos elementos utilizados para la autenticación, desde simples claves numéricas, tarjetas de banda magnética, código de barras, proximidad y sistemas que utilizan información biométrica del hombre, como la huella digital, palma de la mano y reconocimiento de iris. El presente informe se basará en los sistemas que utilizan tarjetas de proximidad, ya que son los más utilizados del mercado.

En las siguientes secciones se detallarán cada uno de los componentes de un sistema de control de acceso. Estos son las tarjetas de proximidad, los lectores, el controlador.

2.3.1 Tarjetas de Proximidad

La tarjeta funciona como una llave de ingreso a una edificación, esta cuenta con un código de identificación única en el sistema y este esta asociado a cada persona con permisos de ingreso.

Las tarjetas no se alimentan de corriente por sí mismas, sino que utilizan la señal de radiofrecuencia enviada por el lector para energizar los componentes internos. Esta energía se usa entonces para enviar la información de vuelta al lector.

Las frecuencias más utilizadas para las tarjetas de proximidad son de 125 Khz. y 13,6 MHz. En la figura 2.9 se ve el principio de funcionamiento de una tarjeta de control de acceso.

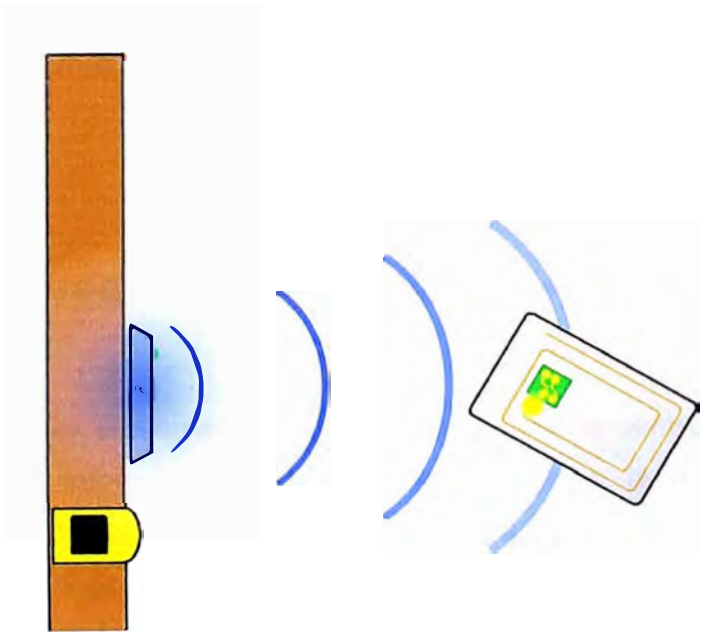


Figura 2.9 Principio de Funcionamiento de una Tarjeta de Control

2.3.2 Lectores

El lector es el portero del control de acceso físico. El lector es el que le proporciona la energía a la tarjeta, recibe la información binaria que transmite la tarjeta, convierte la información y la envía al controlador

El alcance de lectura depende del tamaño de la tarjeta y del lector. Los lectores y las tarjetas de mayor tamaño tienen mayor alcance de lectura que sus contrapartes de menor tamaño.

La comunicación entre una tarjeta y un lector comienza con una señal de baja frecuencia que el lector envía constantemente. Esta frecuencia es una señal simétrica que se envía desde el frente y la parte posterior del dispositivo. La señal de radiofrecuencia "llama" constantemente a las tarjetas que se encuentren dentro de su campo de alcance. La señal se envía a una de las frecuencias mencionadas arriba con un pulso que se repite 10 veces por segundo. En la figura 2.10 se observa que una vez que es presentada la tarjeta al lector, este se energiza y envía su información al lector el cual lo codifica en formato wiegand y envía al controlador.

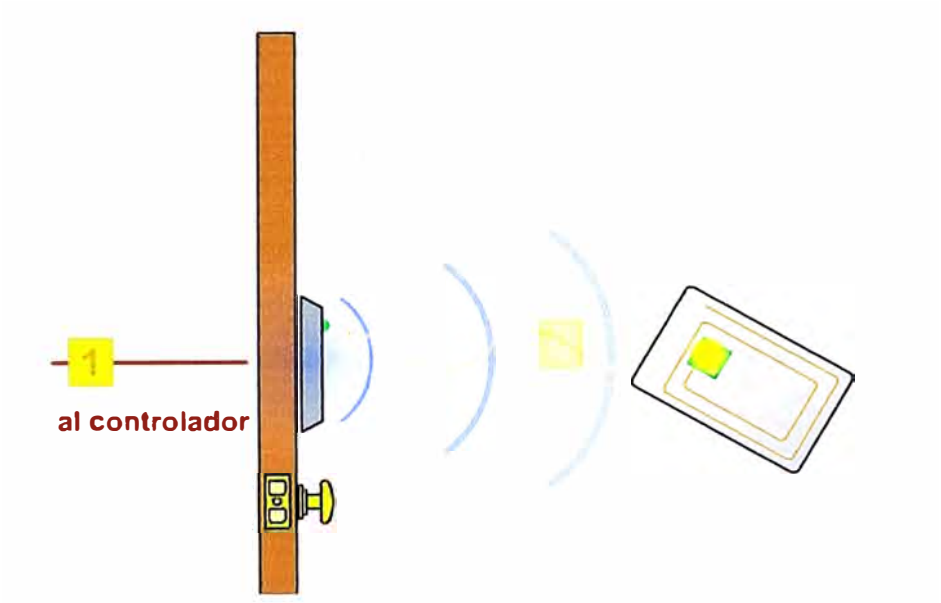


Figura 2.10 Comunicación del Lector con los otros dispositivos.

2.3.3 Controlador

El controlador es el elemento principal del sistema de control de acceso, en el se registra y mantiene la información de las tarjetas habilitadas, así como a que puertas o zonas tiene autorización de acceso el propietario de la tarjeta. El controlador también se encarga de almacenar todos los eventos asociados a los usuarios. Al controlador están conectados físicamente el lector, la cerradura eléctrica o electromagnética, el pulsador de salida y el contacto magnético de supervisión de estado de puerta.

Los controladores cuentan con interfaces físicas para conectar los lectores, entradas y salidas de alarma por contacto seco y a su vez, este está conectado a un puerto Ethernet para comunicarse con otros controladores y el software. En la figura 2.11 se muestra una puerta típica con un sistema de control de acceso.

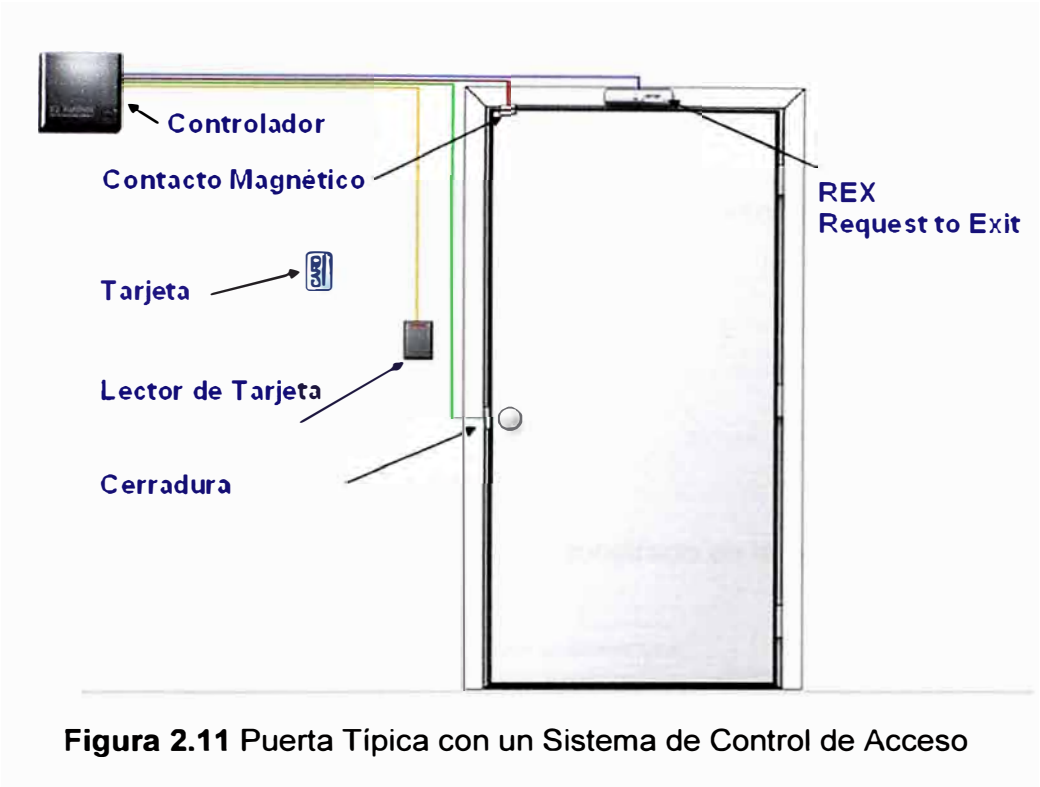


Figura 2.11 Puerta Típica con un Sistema de Control de Acceso

Cuando un usuario autorizado presenta su tarjeta al lector, este último envía el código al controlador quien valida si el usuario cuenta con los permisos de acceso. Si la validación es correcta, el controlador envía un pulso eléctrico para liberar la cerradura de la puerta.

La función del contacto magnético es supervisar el estado de la puerta, es decir si esta se encuentra abierta, cuánto tiempo se encuentra abierta, si está cerrada o si es vulnerada (abierta sin que se haya presentado una tarjeta valida). En este último caso, el controlador genera una alarma en el sistema.

El dispositivo REX (por sus siglas en ingles) o dispositivo de solicitud de salida es utilizado generalmente al interior del área protegida, este puede ser un pulsador o un detector de movimiento, que al ser activado libera la cerradura de la puerta. Algunas aplicaciones utilizan también un lector a la salida para esto.

En este punto, se debe seguir las recomendaciones de defensa civil para la seguridad humana, principalmente si esa puerta es una vía de evacuación masiva en casos de emergencia.

Es norma que los sistemas de control de acceso estén integrados a los sistemas de alarma contra incendio, ya que al generarse un incendio en una edificación, se debe liberar todas las puertas para facilitar la evacuación de las personas.

2.3.4 Software de Control de Acceso

El software de control de acceso sirve de interfaz con el administrador del sistema para la configuración, la operación diaria y la realización de auditorias al sistema. En él se realizan las siguientes funciones:

- Configuración de los controladores: entradas, salidas, lectores, etc.
- Creación y alta de usuarios
- Asignación de Permisos
- Creación de Layouts del edificio
- Alarmas
- Integración con Video, etc.

La interfaz de configuración es similar al mostrado en la figura 2.12

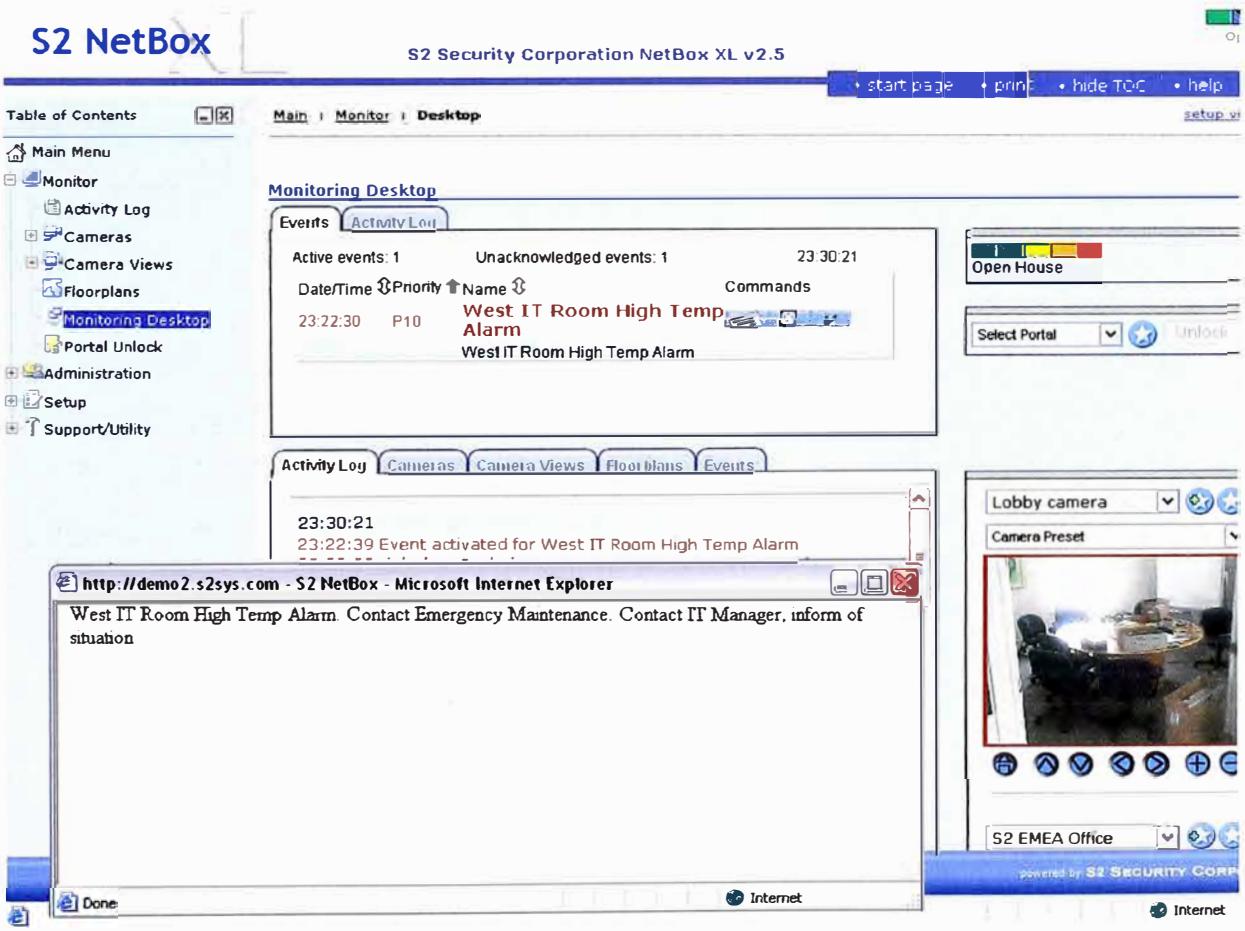


Figura 2.12 Ejemplo de Interfaz de Configuración

2.3.5 Integración de los Sistemas

Para la mayoría de aplicaciones en edificios modernos, los sistemas de control de acceso están integrados al video ya que, además de mantener un registro histórico de las personas que ingresaron a un ambiente en el último mes, se guarda junto con el registro un archivo de video o una imagen de la persona al momento de atravesar la puerta. Para ello, se debe tener una cámara enfocando el ingreso, o en su defecto, ante la solicitud de ingreso de un usuario, el sistema de control de acceso le indica a una cámara móvil que apunte hacia la puerta en mención. En los sistemas basados en IP, esta integración es hecha a través de software y no se requieren conexiones físicas adicionales.

Los sistemas de alarma contra incendio también requieren de un nivel de integración, pero este es logrado a través de hardware ya que es necesaria una conexión física entre el panel de incendios principal y el controlador principal de acceso.

Cuando ocurre una alarma de incendio, las puertas de la edificación deberán liberarse para una rápida evacuación. En el próximo capítulo se diseña una solución de un sistema de seguridad para una refinería de petróleo.

CAPÍTULO III
DISEÑO DEL SISTEMA DE SEGURIDAD

3.1 Introducción

En este capítulo, se utilizarán los principales conceptos descritos en las páginas anteriores. Para este caso de estudio se tomará el caso más general donde se pueda aplicar todos los conceptos aprendidos que se pueden encontrar con facilidad en un escenario real.

Según se vio en el capítulo I. El equipamiento actual de la minera es el siguiente:

13 cámaras tipo PTZ modelo Esprit, marca Pelco,
10 cámaras Domo PTZ con cobertores presurizados marca Pelco
16 cámaras fijas marca Pelco.

Todas las cámaras están ubicadas estratégicamente en toda la planta de producción.

Debido a las grandes distancias de transmisión, se utiliza fibra óptica multimodo para la transmisión del video analógico, utilizando para ello conversores de cable coaxial a fibra óptica en cada cámara.

En el centro de control, se cuenta con una matriz de video analógico de 48x16 (48 entradas de video y 8 salidas para monitores) y tres grabadores digitales de 16 canales de video con 2 TB de disco duro cada uno. Ambos sistemas deben estar integrados a través de software, es decir: no se requiere cableados adicionales al Ethernet.

El requerimiento actual consta de:

16 cámaras fijas
15 cámaras Domo PTZ
Un sistema de control de acceso peatonal y vehicular de ingreso de la planta y oficinas administrativas.

3.2 Diseño del Sistema de Video Vigilancia

El sistema existente cuenta con 48 cámaras de video analógicas y todas deben reutilizarse para la ampliación del sistema.

La ampliación del sistema estará basada en tecnología IP. Las nuevas cámaras serán IP, pero es necesario convertir las cámaras existentes a IP para ser controladas en el nuevo sistema.

Lo primero que se debe hacer en la etapa de ingeniería es recabar toda la información disponible de la instalación existente.

En la figura 3.1 se muestra el diagrama topológico de la solución existente.

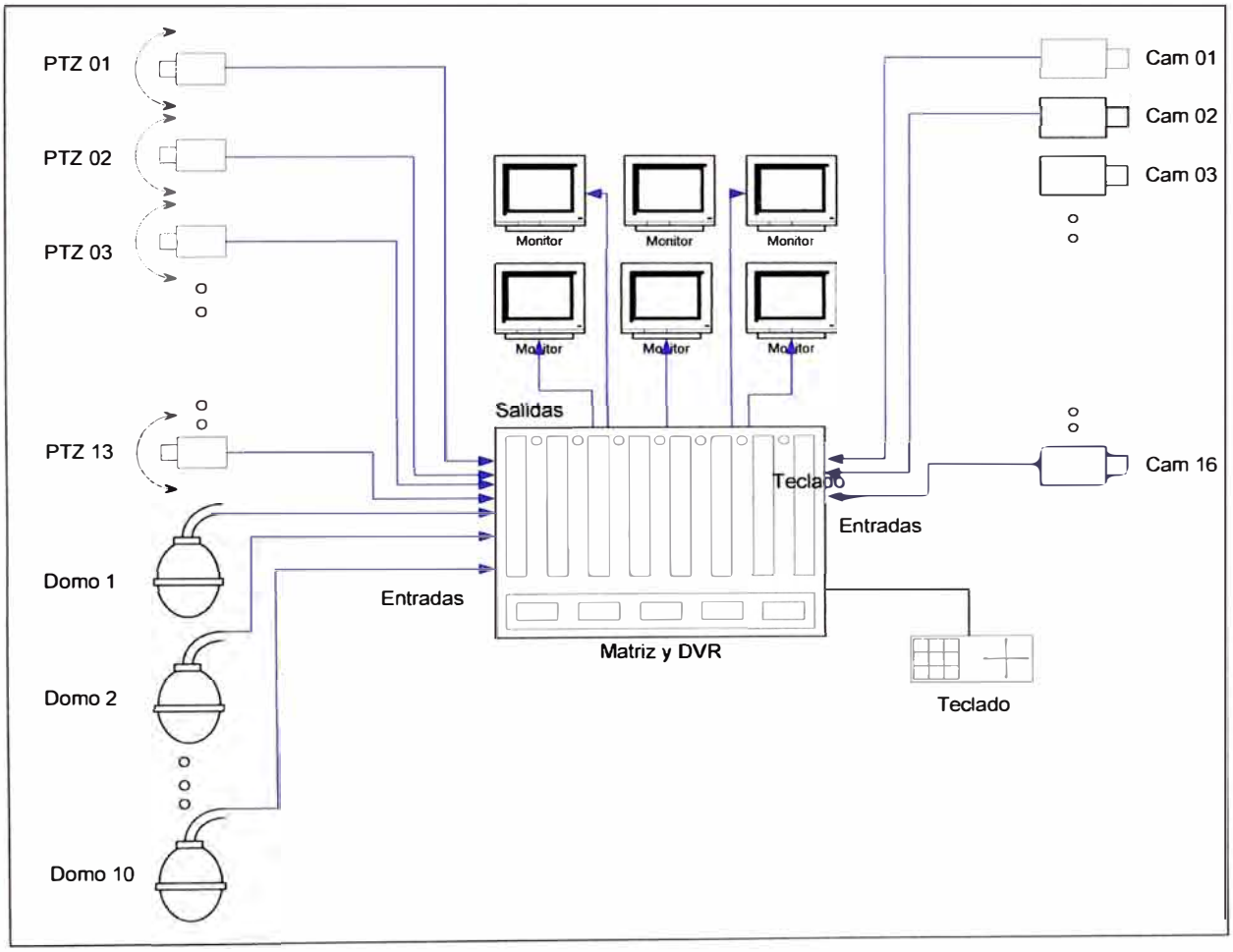


Figura 3.1 Diagrama Topológico

En la tabla 3.1 (página siguiente) se muestra la relación completa de componentes.

Tabla 3.1 Relación de Componentes.

MODELO	FABRICANTE	DESCRIPCION	CANTIDAD
CAMARAS			
ES30PCBW24-5N	PELCO	Cámara PTZ Esprit, 24X zoom, NTSC, cobertor presurizado, montaje en poste. 230 VAC	13
SD435-PRME0	PELCO	Cámara Domo modelo Spectra IV, 35X zoom óptico, NTSC, housing presurizado, salida de fibra óptica multimodo. 24VAC	10
IWM-24GY	PELCO	Adaptador de montaje para pared. Fuente 230 VAC	10
PA402	PELCO	Adaptador para montaje en poste	10
CCC1390H-6	PELCO	Cámara Día/Noche. WDR, alta resolución, 1/3 CCD. NTSC	16
13VDIR2.8-11	PELCO	Lente 1/3 CCD, varifocal 2,8-11 mm, filtro infrarrojo	16
EH3508-3	PELCO	Housing para cámaras fijas, incluye calefactor, desempañador. 230 VAC	16
EM1450	PELCO	Adaptador de montaje para pared. Fuente 230 VAC	16
EM1109	PELCO	Adaptador para montaje en poste	16
MATRIZ DE VIDEO			
CM6800E-48X8	PELCO	Switcher/controller, 48 video inputs, 8 video outputs, NTSC, 120/230 VAC, 50/60 Hz	1
CM9760-CDU-T	PELCO	Code distribution unit; 16-channel RS-422 transmit only (2 data wires and ground) distributor. Primarily used for wiring up to 16 pan/tilt/zoom receivers in a "star" configuration.	1
KBD960	PELCO	Full-function desktop variable-speed keyboard; white finish; 100-240 VAC, 50/60 Hz.	1
DVR			
DX4616	PELCO	Grabador Digital de 16 canales. DVD-RW, 3TB HHDD	3
MONITORES			
PMCS19A	PELCO	Monitor de 19" CRT. NTSC	6

3.2.1 Criterios de Selección para los Codificadores de Video Analógico a IP

Teniendo toda la información de la instalación existente disponible. Es hora de iniciar con el diseño utilizando los conceptos aprendidos en los capítulos anteriores.

Los criterios más importantes para seleccionar el equipo más adecuado son la cantidad de cámaras, el protocolo serial de las cámaras PTZ y/o Domo, la resolución de cada canal de video y el formato de compresión. Como existen 39 cámaras; se propondrán 39 codificadores de video IP para convertir las señales de las 39 cámaras existentes a IP.

Es importante mencionar, que de acuerdo al plano esquemático de instalación, las señales que controlan el movimiento de las cámaras PTZ y Domo han sido llevadas a través de un cableado paralelo al coaxial y pueden conectarse directamente al puerto serial de los codificadores. Las cámaras Pelco utilizan protocolo Pelco P o D a través de una interfaz serial RS-422/485.

Un punto a tener en cuenta es la disposición física que tendrán estos equipos en el centro de control, ya que la instalación de 39 equipos de manera individual es complicada debido a que se debe energizar cada uno de ellos y conectar a una interfaz Ethernet de manera independiente. Por tanto se debe tener en mente poder seleccionar un equipo que pueda instalarse en un rack de comunicaciones y permita centralizar la energía eléctrica de cada uno de los codificadores.

Como segundo punto está la resolución de la imagen. Cada canal de video debe poder manejar una resolución de 4CIF (704x480 píxeles) a 30 fps. Esto garantizara que las imágenes grabadas puedan reproducirse a la mayor calidad de imagen y sea útil en los procesos de investigación.

Como tercer punto, el formato de compresión a utilizar debe ser aquel que me permita el mayor ahorro en los recursos de red (ancho de banda) y capacidad de almacenamiento. El H.264 es el método de compresión más eficiente a la fecha y es el recomendado para utilizar. Existen hoy en día, pocos fabricantes que tiene soluciones de este tipo, dentro de los más reconocidos se encuentran AXIS, Sony y BOSCH.

Se tomarán los modelos de AXIS como referencia, pero puede utilizarse cualquier fabricante de video que cumpla con las especificaciones técnicas mínimas recomendadas. En la figura 3.2 se muestra las características físicas del equipo Q7406 de AXIS. Este posee 6 canales de video y utiliza H.264 como método de compresión.

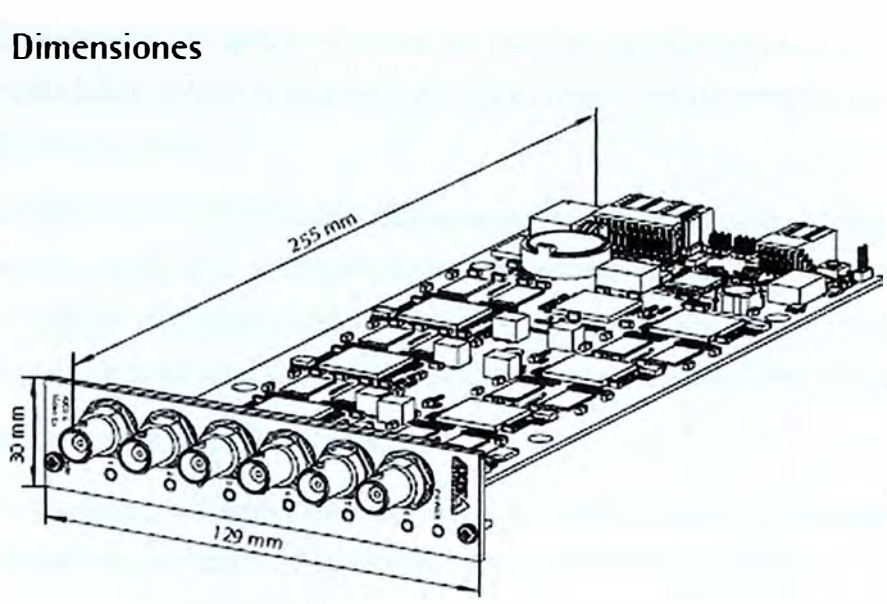


Figura 3.2 Equipo Q7406 de AXIS

Como puede verse, esta tarjeta cuenta con 6 conectores BNC a donde va conectada cada cámara. Para albergar los codificadores, se debe agregar el bastidor donde se instale cada una de las tarjetas de los codificadores.

El AXIS Q7900 tiene 14 bahías, y puede soportar hasta 14 AXIS Q7406 dando un total de 84 entradas de video. Para el proyecto se necesitarían 7 AXIS Q7406 lo que da una capacidad de 42 canales de video y 01 bastidor Q7900. En la figura 3.3 se muestra las características físicas de este equipo.

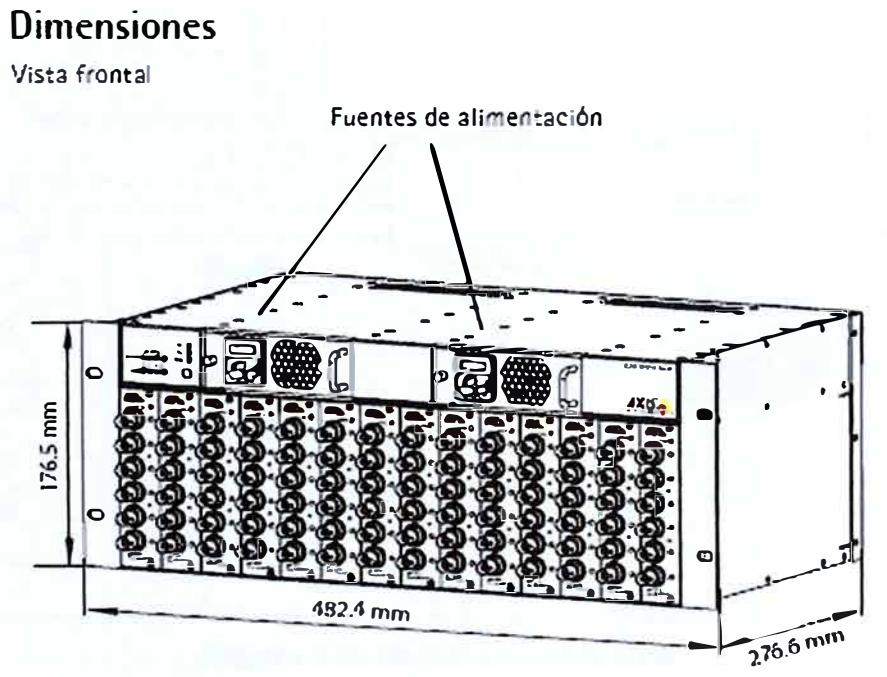


Figura 3.3 Bastidor Q7900.

Con la inclusión de estos equipos se reduce significativamente los costos de instalación y materiales debido a que solo se utiliza una toma de energía para el bastidor y 2 puertos Ethernet de 1Gb.

Es recomendable que este tipo de equipos posea fuentes de poder redundantes con capacidad de poder ser intercambiadas en plena operación (intercambiables en caliente). El bastidor completo, reemplazaría a la matriz de video y los grabadores digitales, por lo que el diagrama del sistema sería como se muestra en la figura 3.4.

3.2.2 Criterios de Selección de Cámaras

Las necesidades de seguridad del área de operaciones y del departamento de seguridad de la minera, incluyen 16 cámaras fijas y 15 tipos Domo PTZ.

Las ubicaciones de cada cámara están definidas en los planos de planta, y junto con la obra civil para la nueva planta, se incluye un backbone de fibra óptica que cubre la mayor parte del área que se desea monitorear.

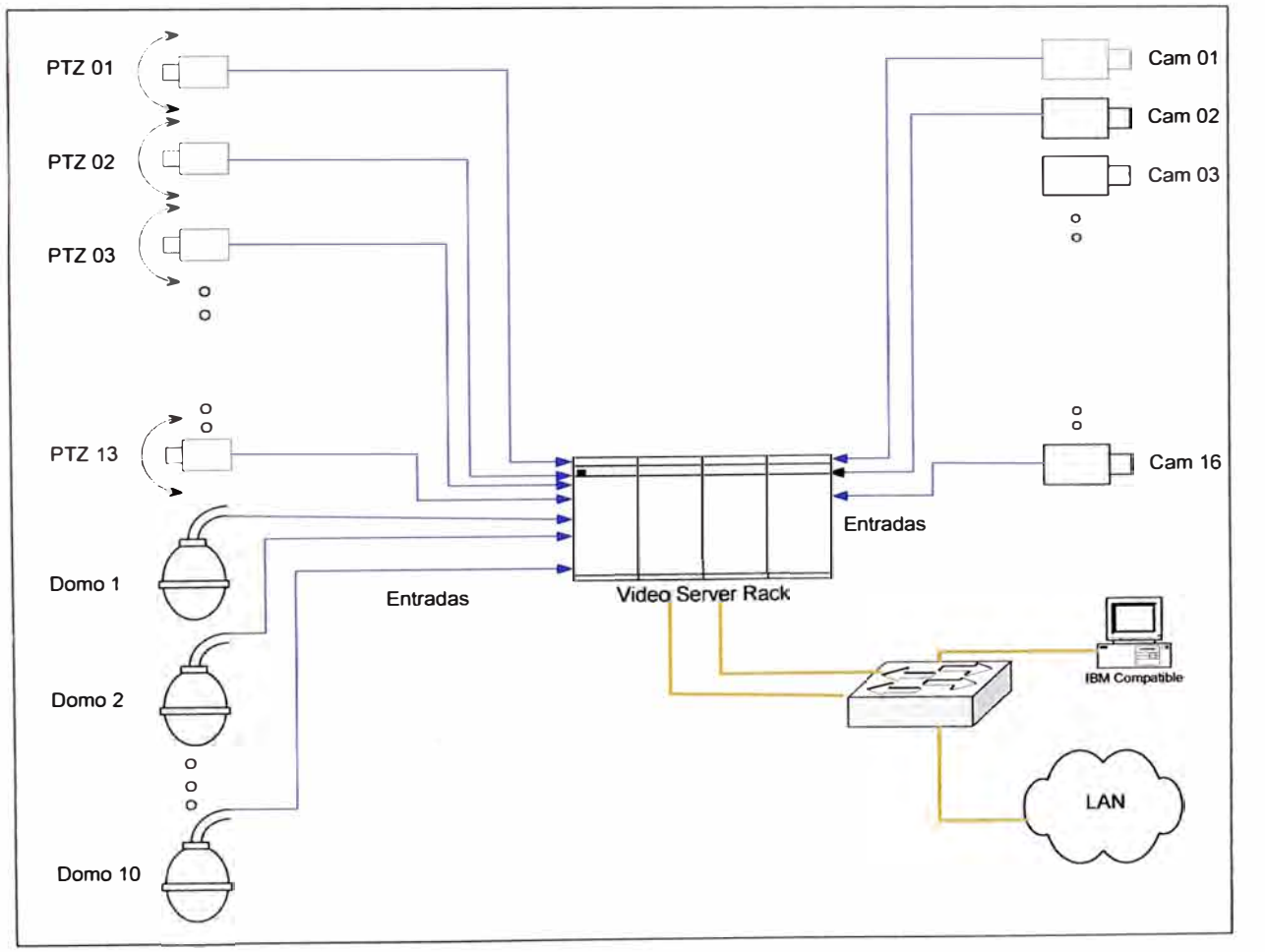


Figura 3.4 Diagrama del Sistema

La descripción y diseño del backbone de comunicaciones está fuera del alcance de este informe. Para la etapa de ingeniería del sistema de video, solo se debe

considerar que existe un gabinete de comunicaciones a menos de 100 metros de cada punto donde se desea instalar una cámara.

Los principales criterios de selección de una cámara está en función a los factores Ambientales y los factores tecnológicos.

a. Factores Ambientales

Lo primero que se debe tener en cuenta al momento de seleccionar una cámara es identificar las condiciones ambientales a las que estará expuesta. Aquí se puede identificar 2 parámetros fundamentales: La iluminación y el grado de protección del medio ambiente

a.1 Iluminación

El primer factor ambiental a tener en cuenta es la iluminación de la zona a proteger. Como las cámaras serán instaladas en la intemperie, la iluminación va cambiando conforme avanza el día.

En las mañanas y parte de la tarde hay buena iluminación natural y a medida que avanza la tarde la iluminación natural se reduce y solo existe iluminación artificial pero es insuficiente para capturar buenas imágenes como en el día.

Las cámaras en blanco y negro necesitan menos iluminación para capturar imágenes en la noche, pero en el día, los detalles se aprecian mejor con una cámara a color. Por ello es que es necesario que las cámaras tengan una función llamada Día/Noche, lo que hace que se comporte como una cámara a color en el día y en modo blanco y negro en la noche.

También es importante que la cámara regule la intensidad de luz que ingresa al elemento sensor. Es por ello que la cámara seleccionada debe ser del tipo autoiris.

El segundo factor a considerar en la selección de la cámara es el soporte a la intemperie y a elementos como el agua, el polvo y temperaturas extremas a las que estará expuesto.

a.2 Grado de Protección al Medio Ambiente:

Para que una cámara pueda ser instalada en ambientes como el de nuestro caso, se debe añadir a la cámara un protector especial, que le brinde a la cámara condiciones especiales para su correcto funcionamiento.

Para ambientes mineros se deberá seleccionar cobertores que tengan un grado de protección IP 66 como mínimo, esto nos garantiza que el equipo estará protegido completamente contra el polvo y chorros directos de agua en todas las direcciones.

Para proteger a la cámara contra los efectos de las temperaturas extrema, el cobertor debe incluir accesorios adicionales como un calefactor, ventilador y desempañador. En algunas zonas muy hostiles, se instalan cobertores presurizados para proteger las cámaras.

a.3 Área a Proteger

Es importante conocer el área que se desea vigilar para seleccionar la cámara apropiada.

Si la zona está confinada a un área pequeña. Es suficiente que la cámara sea fija (no cuente con movimiento), la única preocupación reside en que el lente permita enfocar manualmente una escena. Este tipo de lentes se llaman varifocales, ya que permite ajustar manualmente la longitud focal del lente para visualizar un área determinada. Para obtener más información de las lentes se puede consultar la sección 2.2.1.

Por el contrario, si el objetivo es el de vigilar un área extensa, se recomienda utilizar cámaras que tengan movimiento horizontal, vertical y zoom (PTZ: Pan / Tilt / Zoom por sus siglas en inglés)

Como estas cámaras generalmente van instaladas en postes de relativa altura, y el viento ocasiona que tengan un pequeño desfase de la vertical, una de las características imprescindibles en este tipo de cámara es la estabilización electrónica de la imagen.

b. Factores tecnológicos

Definitivamente, la tecnología a utilizar para la transmisión del video está basada en IP. Por ello las cámaras a escoger deben ser IP nativas ya que por defecto están diseñadas para operar de manera satisfactoria en un entorno de red. Las características mas importantes debe tener una cámara IP son:

b.1 Método de Compresión

H.264 o MPEG-4 como mínimo

b.2 Resolución

4CIF a 30 fps

b.3 Protocolos:

Los más importantes son: TCP, IP v4/v6, IGMP, UDP, SNMP, RTSP, RTP, RTCP, HTTP, HTTPS, DHCP y FTP.

De ellos, el IGMP es para enviar trafico multicast. Típico de entornos con más de una persona (estación de trabajo) observando una secuencia de video. Los protocolos utilizados para transmitir video y/o multimedia en tiempo real como las aplicaciones de video vigilancia son:

RTSP (Real Time Streaming Protocol)

RTP (Real-time Transport Protocol) y

RTCP (Real Time Control Protocol)

Los demás protocolos mencionados son muy conocidos para los profesionales de comunicaciones. Más información acerca de ellos en el glosario de términos.

3.2.3 Especificaciones Técnicas Mínimas

Estas se dividen tanto para las cámaras fijas como para las PTZ.

a. Cámaras fijas:

IP Nativa

Día / Noche

Iluminación mínima: 0.1 Lux

- Autoiris DC

Lente varifocal: 3.5 – 8 mm

Housing de protección IP 66, se incluye calefactor y ventilador.

Soporte para montaje en poste

Certificación de calidad de una entidad independiente como UL o ETL

b. Cámaras Domo PTZ:

IP nativa

Día / Noche

Iluminación mínima: 0.1 Lux

- Autoiris y Auto foco

Lente zoom: 3,4 -100 mm como mínimo

Estabilización electrónica de imágenes

Housing de protección IP 66 presurizado, debe incluir calefactor y ventilador

Soporte para montaje en poste

Certificación de calidad de una entidad independiente como UL o ETL

3.2.4 Cámaras IP Seleccionadas

Existen diversos fabricantes líderes de la industria que cumplen y superan estas especificaciones. Cabe mencionar que no necesariamente todos los componentes mencionados deben ser del mismo fabricante.

Independientemente de la marca de cámara que se elija, este debe cumplir con los requisitos técnicos mínimos y debe ser de un fabricante reconocido de cámaras IP, como lo son AXIS, Sony, BOSCH o Pelco.

Para esta aplicación, sólo para propósitos referenciales, se va a seleccionar para las cámaras fijas el modelo **221 de AXIS**. La figura 3.5 muestra físicamente la cámara.

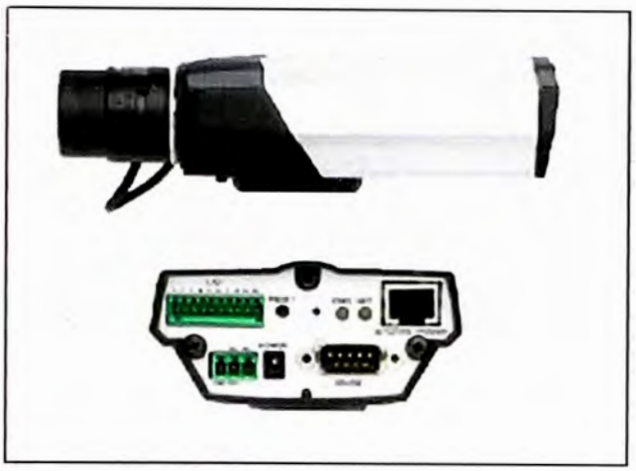


Figura 3.5 Cámara 221 de AXIS

Para proteger la cámara contra la intemperie, se debe agregar el cobertor para exteriores. Es importante mencionar que no necesariamente los cobertores deben ser del mismo fabricante de las cámaras, sino que cumplan lo especificado. Teniendo en cuenta las condiciones ambientales detalladas en el capítulo I, el cobertor debe cumplir las siguientes características técnicas mínimas:

- Material de Aluminio con protector solar
- Grado de protección IP 66
- Calefactor y Ventilador
- Accesorios de montaje en pared o poste
- Entrada 220 VAC
- Certificación de calidad de alguna entidad independiente como UL o ETL

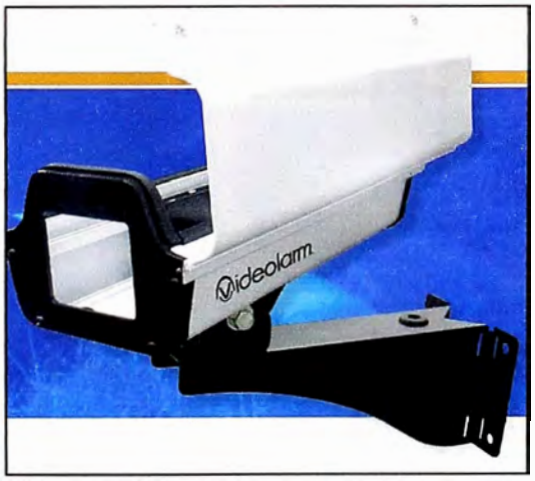


Figura 3.6 Modelo ACH13HBN

Figura 3.7 Cámara 233D

A modo de referencia, se plantea el modelo ACH13HBN del fabricante Videolarm con sus accesorios de montaje y fuente de poder como se muestra en la figura 3.6.

Para la cámara Domo PTZ se propondrá, a modo de referencia, el modelo 233D de AXIS. Esta cámara supera largamente las especificaciones técnicas mínimas, pero se debe precisar que puede utilizarse cualquier otra que satisfaga las especificaciones. La figura 3.7 muestra la cámara 233D de AXIS.

Al igual que para la cámara fija, es necesario agregar un cobertor para exteriores. Las características técnicas mínimas que debe cumplir el cobertor son:

- Material de Aluminio o policarbonato
- Cobertor presurizado
- Grado de protección IP 67
- Debe incluir: Calefactor, Ventilador y desempañador
- Accesorios de montaje en pared o poste
- Entrada 220 VAC
- Certificación de calidad de alguna entidad independiente como UL o ETL

A modo de referencia, se propone el modelo PFDW75C2N de Videolarm. Este ya incluye el soporte para montaje en pared y la fuente de poder.

Se debe incluir el adaptador de montaje en poste APM3 y el kit de recarga de nitrógeno NPK01 para la presurización del cobertor, cómo se muestra en la figura 3.8. En la tabla 3.2 se muestra la relación de equipos a modo de referencia para el proyecto.

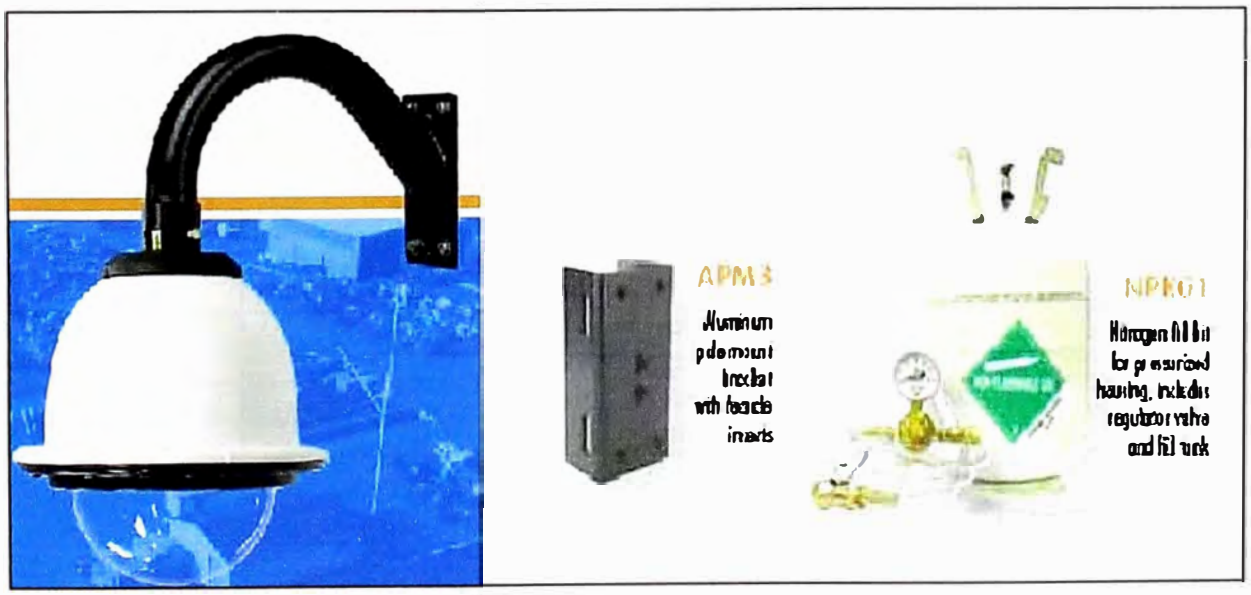


Figura 3.8 Adaptador de montaje en poste APM3 y kit de recarga de nitrógeno NPK01

Tabla 3.2 Relación de Equipos

MODELO	FABRICANTE REFERENCIAL	DESCRIPCION	CANTIDAD
CAMARAS FIJAS			
AXIS 221	AXIS	**Varifocal DC-iris lens**. 1/3" **progressive scan CCD**. Down to 0.65 lux in color. **Auto day/night mode**. Up to VGA 640x480 resolution at **45 frames per second**. **Motion JPEG and MPEG-4**. **Video Motion Detection and I/O** for alarm/event handling. **Power over Ethernet**. **RS-232/485** for data and PTZ control. Includes adjustable stand and power supply.	16
ACH13HBN	VIDEOLARM	IP Network Ready Outdoor Environmental hsg with metal wall/pole mount, w/24Vac input, 12 or 24 output for camera, thermostatically controlled heater/blower, for an IP Network camera, 40vA transformer, MCL 10.5"	16
PB24	VIDEOLARM	Rugged cast aluminum power box with 220/115Vac input converting to 24Vac and 84W output power. Pole mounting clips included.	16
CAMARAS DOMO PTZ			
AXIS 233D	AXIS	**35x** optical zoom **dome camera** with **WDR** and area zoom. **Auto day/night** mode down to **0.5 lux** in color and **0,008 in night** mode. Continuous 360º rotation and 180º tilt with **E-flip. Progressive Scan 4CIF** resolution at **30/25fps in MPEG-4 or Motion JPEG**. Two-way **audio**, **I/O** for alarm/event handling. Includes **hard and drop ceiling** mount kit, **smoked and clear** transparent covers and **power supply**.	15
PFDW75C2N	VIDEOLARM	IP Network Ready 7" Outdoor pressurized dome hsg w/ WM20G gooseneck wall mount, clear dome, w/24Vac input, heater/blower, for an IP Network PTZ camera, 120 to 24Vac, 96vA transformer	15
APM3	VIDEOLARM	Aluminum pole mount bracket with female inserts	15
NPK01	VIDEOLARM	Nitrogen fill kit for pressurized housing, includes regulator valve and fill tank	1

3.2.5 Software de Administración de Video

Una vez que son seleccionadas las fuentes de video apropiadas para el proyecto, es importante tener un programa de cómputo que permita gestionar todas las fuentes de video, así como brindar una interfaz gráfica a los operadores del sistema de video. Tal interfaz permite, no solo visualizar en tiempo real las imágenes que envían cada una de las cámaras, sino también grabar las imágenes en un arreglo de discos.

El programa también debe crear la lista de usuarios en el sistema que tiene acceso a monitorear las cámaras, así como los diferentes privilegios de usuario según la función que tenga este en el centro de control.

3.2.6 Especificaciones Técnicas Mínimas del Software de Administración de Video

Se considera la estructura Cliente Servidor, que sea de plataforma abierta, que sea escalable, así cómo su capacidad de integración con otros programas.

a. Estructura Cliente Servidor

La estructura preferida para el software de administración es la de cliente servidor, donde el servidor del sistema almacena toda la información de la configuración de las cámaras en el sistema y así mismo, guarda en una base de datos los archivos de video de cada una de las cámaras. Dependiendo de la cantidad de cámaras, puede que sea necesario tener más de un servidor en el sistema.

El software cliente se instala en cada una de las estaciones de trabajo que requieran visualizar el video en tiempo real o reproducir un video guardado. También debe ser posible acceder al sistema a través de PDAs o Palm.

b. Plataforma Abierta

Es recomendable que el software de gestión sea de plataforma abierta, es decir que independientemente de la marca de cámara que este utilizándose en la solución, el software debe poder gestionarlo. Se recomienda que sea compatible con las marcas más reconocidas del mercado como AXIS, Sony, Pelco, BOSCH, etc.

c. Escalable

El software no debe tener limitaciones en el número de cámaras, ni de servidores, ni de usuarios conectados. Debe permitir hacer actualizaciones de versiones conforme el usuario lo necesite. En conclusión, tiene que ser multisitio y multiusuario

d. Integración

El software de administración debe permitir integrarse con otras aplicaciones como analítica de video y/o análisis de transacciones, así como con sistemas de control

de acceso. El SDK / API debe estar disponible para integrar con cualquier interfaz de software.

3.2.7 Elección del Software de Administración del Video

Existen múltiples fabricantes en el mercado que satisfacen largamente las especificaciones técnicas mínimas, tales como Milestone, Genetec, Verint, Lenel, etc.

Cualquiera de los mencionados cumple y supera largamente las características mínimas expuestas. A modo de referencia, se va a proponer el software XProtect Enterprise de Milestone. La versión XProtect Enterprise soporta más de 50 fabricante de cámaras, y no tiene restricciones en cuanto al número de cámaras y servidores. Para la elección de las licencias adecuadas, solo se debe tener en cuenta la cantidad de cámaras y/o canales de video.

Si se revisa las tablas anteriores, se puede observar que en la instalación existente se tiene:

39 cámaras analógicas entre fijas y móviles

31 cámaras IP entre fijas y móviles

Para escoger el tipo y cantidad de licencias, no importa el tipo de cámara, sino solamente la cantidad de canales de video. En la Tabla 3.3 se muestran las licencias necesarias para la gestión de la totalidad de cámaras:

Tabla 3.3 Licencias Necesarias para la Gestión

MODELO	FABRICANTE	DESCRIPCION	CANTIDAD
LICENCIAS			
XPEBL	MILESTONE	XProtect Enterprise 6.5 Base License	1
YXPEBL	MILESTONE	1 year PMA for XPEBL	1
XPECL	MILESTONE	XProtect Enterprise 6.5 Camera License	70
YXPECL	MILESTONE	1 year PMA for XPECL	70

Donde el XPEBL es la base de la licencia y el XPECL es la licencia por cada cámara IP o canal del codificador de video. El YXPEBL y YXPECL son programas de mantenimiento anual, que permite obtener actualizaciones de software sin costo adicional y migrar de forma económica a una versión superior como el XProtect Corporate. Ahora que ya se cuenta con las licencias necesarias, se debe establecer el hardware necesario para instalar el software.

3.2.8 Cálculo de Ancho de Banda y Capacidad de Almacenamiento

Los parámetros para el cálculo de la capacidad de almacenamiento y ancho de banda dependen de los siguientes parámetros:

- Número de cámaras
- Formato de compresión
- Calidad de Imagen: Viene dado por la resolución y cuadros por segundo del video.
- Modo de grabación: Continua o por detección de movimiento
- Días que permanecerá el video almacenado

Para pequeños sistemas de 8 a 10 cámaras, se puede utilizar un switch de 100 Mbps sin preocuparnos por el ancho de banda. Cuando se implementan 10 o más cámaras, la carga de la red debe estimarse usando unas pocas reglas:

Una cámara que es configurada para enviar imágenes de alta resolución y 30 cuadros por segundo consume alrededor de 2 a 3 Mbps de ancho de banda disponible en la red. Cuando se tenga entre 12 o 15 cámaras, se debe considerar un switch con una interfaz Gigabit, al cual se instalará el servidor donde se ejecuta el software de administración y de grabación de video. El servidor debe tener una tarjeta de red Gigabit.

Es recomendable que el switch a instalarse en el centro de control y los de borde donde se conecte cada cámara, soporten VLAN y QoS.

a. Cálculo de Almacenamiento

Como fue mencionado, el tipo de compresión de video es uno de los factores que afectan los requerimientos de almacenamiento. El H.264 es de lejos, el más eficiente formato de compresión disponible a la fecha.

Debido a que el número de variables que afecta el nivel promedio de la tasa de bits, los cálculos para H.264 y MPEG-4 son muy complejos. A diferencia del M-JPEG, que cuenta con una formula muy simple debido a que M-JPEG consiste de un único archivo por cada imagen, ya que solo depende de los cuadros por segundo, resolución y nivel de compresión que se esta utilizando.

En los siguientes párrafos se presentan las fórmulas simplificadas para el cálculo del almacenamiento.

a.1 H.264 y MPEG-4

La formula de cálculo de la capacidad de disco duro es como sigue:

- Tasa de bits aproximada / 8(bits en un byte) x 3600s = KB por hora / 1000 = MB por hora
- MB por hora x horas de operación por día / 1000 = GB por día
- GB por día x días de almacenamiento = Capacidad Necesaria

Se observa que para el cálculo del almacenamiento se debe conocer la tasa de bits que envían las fuentes de video. Se puede utilizar las siguientes tablas para conocer un valor estimado de la tasa de bits en H.264 y MPEG-4 respectivamente a diferentes resoluciones y cuadros por segundo. Ver las tablas 3.4 y 3.5 para el H.264 y el MPEG-4 respectivamente.

Tabla 3.4 H.264

Camera	Resolution	Approx. bit rate (Kbit/s)	Frames per second	MB/ hour	Hours of operation	GB/day
No. 1	CIF	110	5	49.5	8	0.4
No. 2	CIF	250	15	112.5	8	0.9
No. 3	4CIF	600	15	270	12	3.2
Total for the 3 cameras and 30 days of storage = 135 GB						

Tabla 3.5 MPEG-4

Camera	Resolution	Approx. bit rate (Kbit/s)	Frames per second	MB/ hour	Hours of operation	GB/day
No. 1	CIF	170	5	76.5	8	0.6
No. 2	CIF	400	15	180	8	1.4
No. 3	4CIF	880	15	396	12	5
Total for the 3 cameras and 30 days of storage = 204 GB						

a.2 M-JPEG

La fórmula para el cálculo de la capacidad de disco duro es:

- Tamaño de Imagen x Cuadros por Segundo x 3600s = Kilobyte (KB) por hora/1000 = Megabyte (MB) por hora
- MB por hora x horas de operación por día / 1000 = Gigabyte (GB) por día
- GB por día x días de almacenamiento = Capacidad Necesaria (GB)

En la tabla 3.6 se muestra el mismo ejemplo de los casos anteriores con M-JPEG.

Tabla 3.6 M-JPEG

Camera	Resolution	Bit Rate (Kbit/s)	Frames per second	MB/ hour	Hours of operation	GB/day
No. 1	CIF	13	5	234	8	1.9
No. 2	CIF	13	15	702	8	5.6
No. 3	4CIF	40	15	2160	12	26
Total for the 3 cameras and 30 days of storage = 1002 GB						

En la pagina Web de los fabricantes de cámaras de video IP, muchas herramientas de cálculo que nos facilitan el trabajo al obtener rápidamente tanto el ancho de banda como la capacidad de almacenamiento.

Una sencilla herramienta para estos cálculos se puede obtener en el siguiente enlace de AXIS: http://www.axis.com/products/video/design_tool/calculator.htm. Según la información brindada en el capítulo I. Los parámetros de cálculo son los siguientes.

- Numero de cámaras: **70**
- Formato de compresión: **Depende del tipo de cámara seleccionado, pero debe ser H.264 ó MPEG-4**
- Calidad de Imagen: **4CIF, 18 fps**
- Modo de grabación: **Por detección de movimiento. 90% de actividad**.
- Días que permanecerá el video almacenado: **30 días**

Para hacer el ingreso de datos a la herramienta de AXIS se debe tener a la mano los modelos de los equipos propuestos en las páginas anteriores. En resumen son:

- 07 AXIS Q7406
- 16 AXIS 221
- 15 AXIS 233D

Los resultados se muestran en la figura 3. 9.

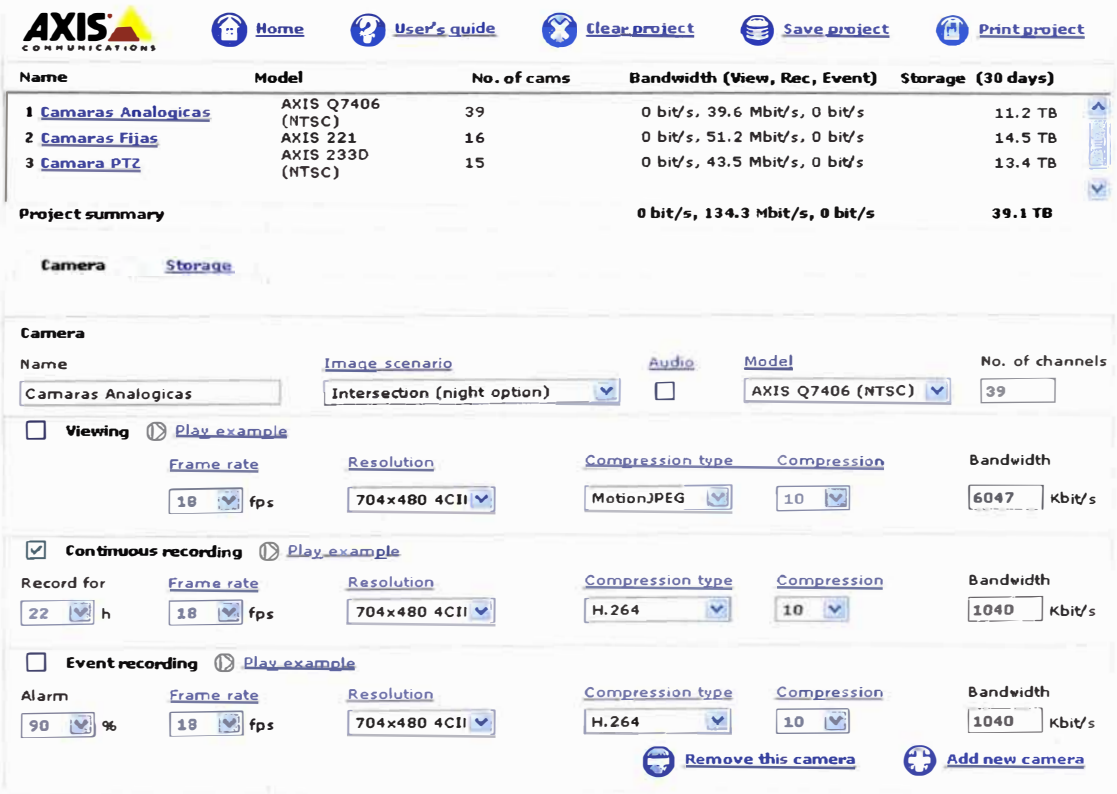


Figura 3.9 Resultados en la Herramienta de Cálculo

Nota: En el Anexo A se muestra la misma ilustración pero con mayor detalle y resolución.

Como se observa, se necesita alrededor de 39 TB de discos duros para almacenar 30 días de grabación. A una resolución de 4CIF y 18 fps.

Un dato importante a observar es el ancho de banda que consume cada cámara. De los resultados se puede observar que:

Cada canal de los codificadores AXIS Q7406 consume 1040 Kbps. Los 39 canales consumirán por tanto 39.06 Mbps

Las 16 cámaras fijas AXIS 221 consumen 51.2 Mbps, por lo que cada cámara consumiría 3.2 Mbps en promedio

Las 15 cámaras Domo AXIS 233D consumen en promedio 2.9 Mbps

Según esta información, ahora se deberá seleccionar el tipo de almacenamiento adecuado para esta gran cantidad de información. Como lineamientos generales, se deberá tener en cuenta los diferentes tipos de unidades de almacenamiento utilizados actualmente para los sistemas de video.

b. Tipos de unidades de Almacenamiento

Existen 2 tipos claramente definido, los directamente conectadas al servidor y los NAS y SAN.

b.1 Directamente Conectadas al Servidor

Dependiendo del procesador, tarjeta de red y memoria RAM, un servidor puede manejar un cierto número de cámaras, cuadros por segundo y tamaño de las imágenes. Muchas de las PCs pueden albergar entre 2 y 4 discos duros, y actualmente cada disco duro puede almacenar hasta 1000 GB.

En pequeñas o medianas instalaciones, un único servidor puede contener el software de administración de video y también el de grabación (generalmente ambos módulos vienen incluidos en las licencias). Esto, en el mundo de la informática es llamado Direct-Attached Storage

Cuando se tienen entre 12 y 15 cámaras, al menos se deberá tener dos unidades de disco para compartir la carga. Un servidor puede manejar en promedio hasta 50 cámaras, si se tienen más de esa cantidad, se deberá colocar un segundo servidor.

b.2 NAS y SAN

Cuando la cantidad de datos a almacenar y los requerimientos de administración exceden los límites de un Direct-Atached Storage, se deberá pensar en un Network –

Attached Storage (NAS) o en un Storage Área Network (SAN), lo que permite incrementar el espacio de almacenamiento, la flexibilidad y la redundancia (Ver la figura 3.10).

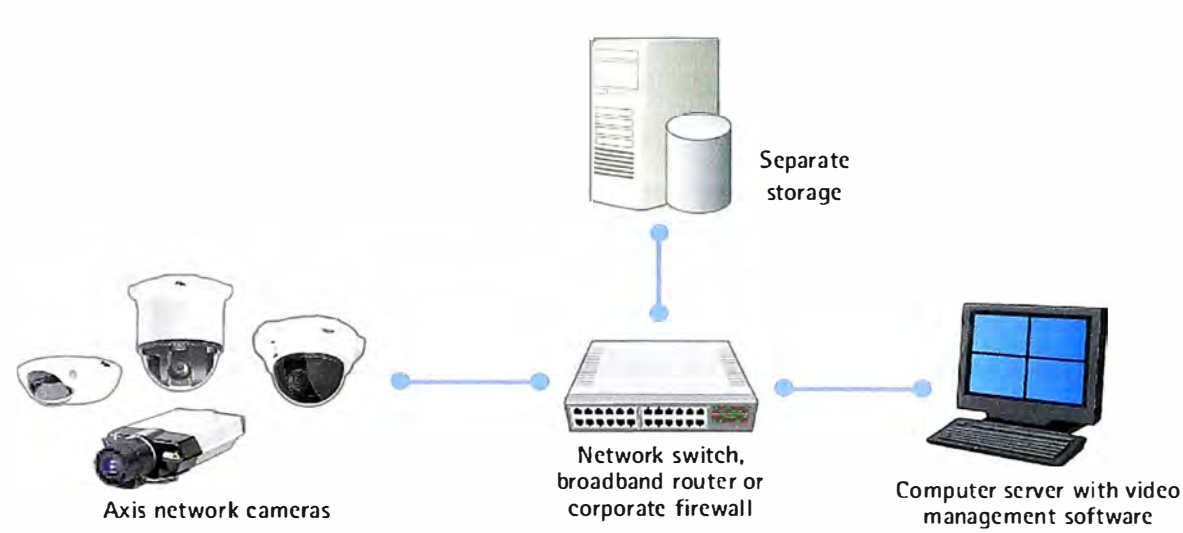


Figura 3.10 NAS

NAS provee un único dispositivo de almacenamiento, el cual es directamente conectado a la red LAN y ofrece, almacenamiento compartido a todos los clientes en la red. Un NAS es simple de instalar y administrar, brindando una solución de bajo costo. Sin embargo, provee un limitado throughput para los datos entrantes, ya que únicamente tiene un puerto de red, el cual puede convertirse en un problema en sistemas de alta performance.

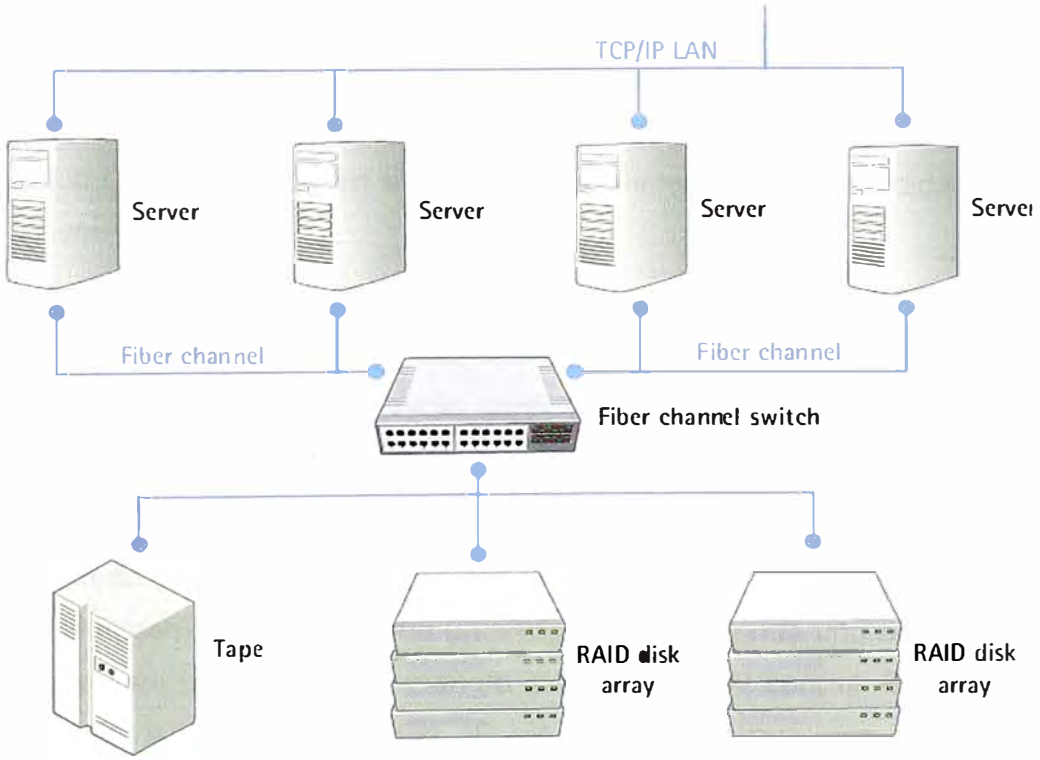


Figura 3.11 SAN

SAN provee alta velocidad y es de propósito especial para almacenamiento, típicamente conecta uno o más servidores a través de fibra óptica. Los usuarios pueden acceder a cualquiera de los dispositivos de almacenamiento en el SAN a través de los servidores, y el almacenamiento puede ser escalable a cientos de Terabytes. El almacenamiento centralizado reduce la administración y provee una alta performance, es un sistema de almacenamiento flexible para uso en ambientes multi-servidor. La figura 3.11 (página anterior) muestra una arquitectura típica de un SAN.

c. Almacenamiento Redundante

Los sistemas de almacenamiento deben ser redundantes, ya sea que se utilicen cualquiera de los métodos mencionados arriba. La redundancia permite guardar video y cualquier otra data simultáneamente en más de una sede. Esto provee un respaldo para recuperar el video si no se puede acceder a una porción del sistema de almacenamiento.

Existe un número de opciones para proveer esta capa adicional de almacenamiento en sistemas de video vigilancia IP, incluyendo arreglos de discos en RAID (Redundant Array of Independent Disks), replicación de datos, Server Clustering y múltiples receptores de video.

c.1 RAID

Es un método de arreglo estándar, independiente de la plataforma de los discos, tal como el sistema operativo ve a ellos como una sola unidad de disco. Una configuración RAID expande datos sobre múltiples discos duros con la suficiente redundancia, tal que los datos pueden ser recuperados si uno de los discos falla. Existen diferentes niveles de RAID, que van desde no redundancia hasta soluciones de redundancia total (full mirrored), en el cual no existe interrupción ni pérdida de datos si uno de los discos falla.

c.2 Replicación de Datos

Es una característica común en muchos sistemas operativos de red. Los servidores de archivos en una red están configurados para replicar sus datos a otro servidor, brindando un backup si uno de los servidores falla.

c.3 Server Clustering.

Este método consiste en tener dos servidores idénticos que trabajen con el mismo dispositivo de almacenamiento, tal como un arreglo RAID. Cuando uno de los servidores falla, el otro que está configurado de manera idéntica toma el control. Estos servidores pueden compartir la misma dirección IP, lo que hace que sea completamente transparente para los usuarios. Es también llamado servidor de “Fail-over”

c.4 Múltiples Servidores de Video.

Un método común para asegurar la recuperación de desastres y almacenamiento fuera del sitio en una red, es enviar simultáneamente el video a dos servidores ubicados en diferentes ubicaciones. Estos servidores pueden ser equipados con arreglos de disco en RAID, trabajar en clústeres o replicar sus datos entre servidores si es necesario. Esto es recomendable en aplicaciones de misión crítica como seguridad ciudadana, transporte público o plantas industriales.

d. Configuración de Sistemas

La configuración del sistema está basada en el número de cámaras, destacando cuatro casos:

- Sistemas Pequeños (1 a 30 cámaras).
- Sistemas Medianos (25 a 100 cámaras).
- Grandes Sistemas Centralizados (50 a +1000 cámaras).
- Grandes Sistemas Distribuidos (25 a +1000 cámaras).

d.1 Sistemas Pequeños (1 a 30 cámaras)

Usualmente un sistema pequeño consiste de un servidor corriendo un software de software de gestión y grabación de video, y almacenando el mismo en discos duros locales. El video es visualizado y administrado en el mismo servidor. Aunque gran parte de la visualización y administración es hecha directamente en el servidor, un cliente (local o remoto) puede conectarse para los mismos propósitos. Un ejemplo de un sistema pequeño se muestra en la figura 3.12.

Figura 3.12 Sistemas Pequeños

d.2 Sistemas Medianos (25 a 100 cámaras)

Una instalación típica de tamaño mediano tiene un servidor con una unidad de almacenamiento adicional conectada a el. La unidad de almacenamiento es usualmente configurada en un arreglo RAID para incrementar la performance y la confiabilidad. El

video es visualizado y administrado desde una estación de trabajo remota que tiene instalado un software cliente. Un ejemplo típico de un sistema mediano se muestra en la figura 3.13.

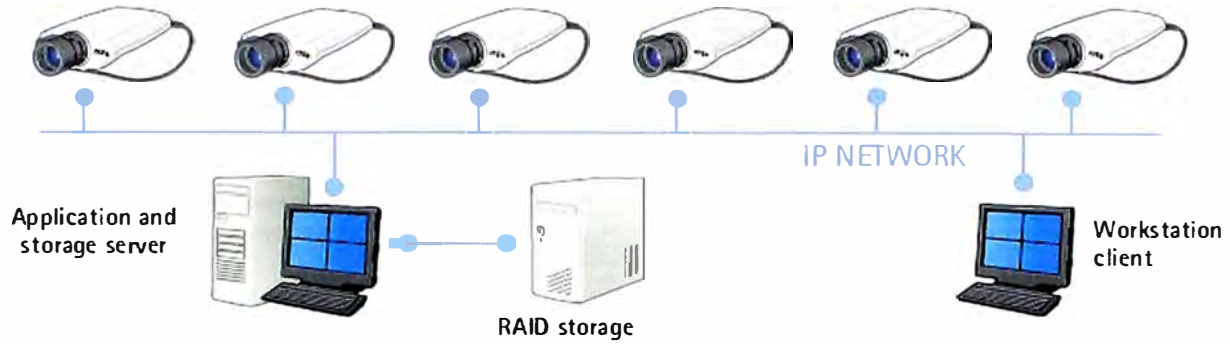


Figura 3.13 Sistemas Medianos

d.3 Grandes Sistemas Centralizados (50 a +1000 cámaras)

Una instalación grande requiere un sistema de alta performance y confiabilidad para administrar una gran cantidad de datos y ancho de banda. Este requiere de múltiples servidores con tareas dedicadas. Un servidor maestro controla el sistema y decide que tipo de video es almacenado y en cual de los servidores de almacenamiento. Como existen servidores de almacenamiento dedicados, es posible hacer balance de carga. En tal configuración también es posible extender el sistema añadiendo más servidores de almacenamiento y hacer mantenimientos sin detener el sistema entero. Un ejemplo de este sistema se muestra en la figura 3.14.

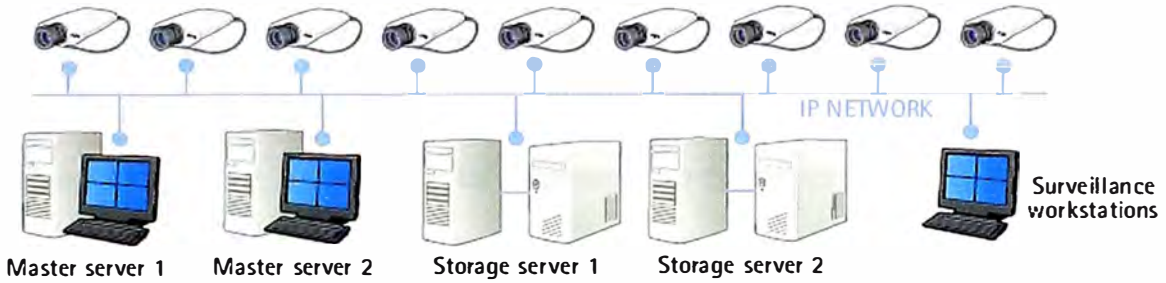


Figura 3.14 Grandes Sistemas Centralizados

d.4 Grandes Sistemas Distribuidos (25 a +1000 cámaras)

Cuando se tienen múltiples sedes que requieren video vigilancia con administración centralizada y grabación distribuida. Es decir cada sede graba y almacena de forma local video de sus cámaras. El servidor maestro, puede visualizar y administrar los servidores de almacenamiento de cada sede. Un ejemplo de este sistema se observa en la figura 3.15.

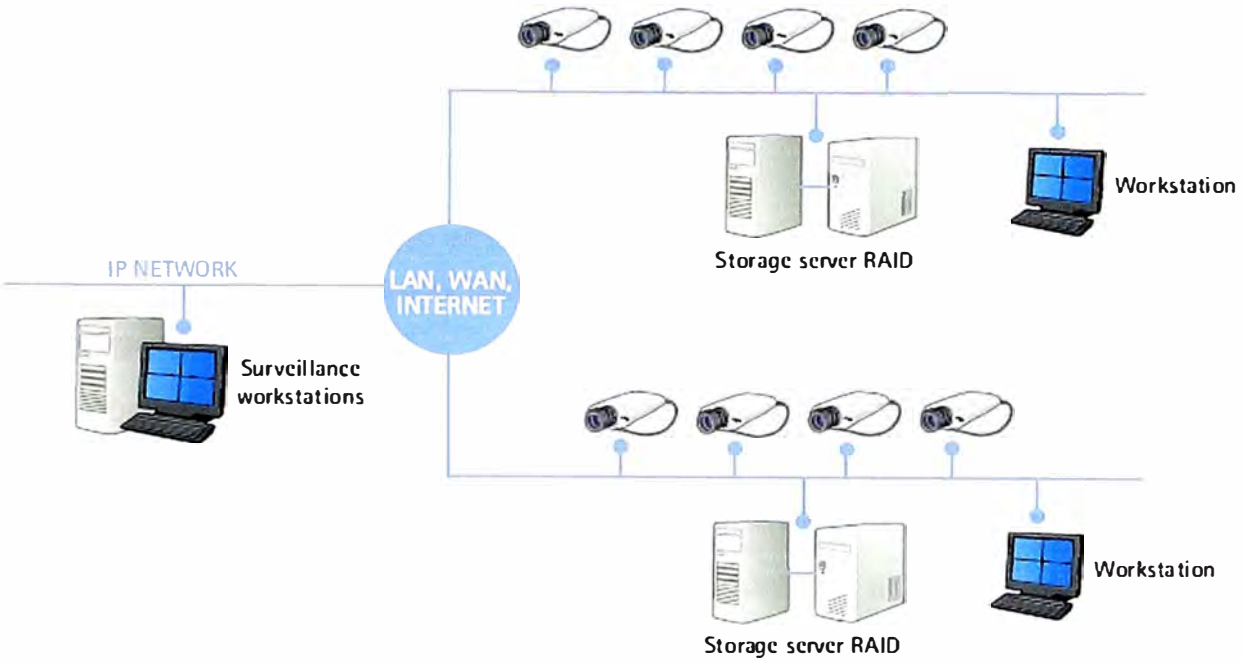


Figura 3.15 Grandes Sistemas Distribuidos

3.2.9 Selección del Hardware de Almacenamiento

Nuestro sistema consta de 70 cámaras en total, por lo que se deberá decidir que tipo de configuración se adecúa mejor a nuestro proyecto. En vista que nuestro proyecto es para una compañía minera que tiene altos estándares de seguridad, el sistema debe ser altamente confiable y tener redundancia.

La configuración que mejor se adecua es la de Grandes Sistemas Centralizados, por lo que se va a tener un servidor de administración, que puede también operar como servidor de almacenamiento y un servidor de almacenamiento adicional que haga balance de carga con el primero.

Cada Servidor tendrá conectado un arreglo de discos externos ISCSI en una configuración RAID 5. El tamaño total del arreglo de discos es de 20 TB cada uno.

Cada servidor debe tener para el sistema operativo y el software de administración – grabación, dos discos duros SAS de 146 GB en un arreglo RAID 1 (Mlrroring) y tres discos SATA en RAID 0 para la base de datos primaria.

Las características mínimas del servidor deben ser las siguientes:

- Procesador: Intel Dual Core Xeon E3060 (2,4 GHz o superior)
- Memoria RAM: 4 GB
- Interfaz de red: 2 de 1Gb
- Caché del Controlador del Arreglo de Discos: 512 MB

3.2.10 Diseño del Centro de Control

El centro de control es el elemento de todo el sistema de video vigilancia en el cual estarán centradas todas las miradas, ya que es la parte más visual del sistema y el que muestra todas las funcionalidades del mismo.

Si se ha tenido cuidado en todas las etapas del diseño, se obtendrán imágenes de muy buena calidad y el operador del sistema podrá realizar una buena labor de monitoreo e investigación posterior.

Dependiendo de la cantidad de cámaras, puede sugerirse la cantidad de operadores. Pero en estos días, para aplicaciones dentro de compañías privadas, es usual que solo haya una persona para monitorear la totalidad de las cámaras.

Esto es posible hacerlo debido a que las cámaras IP, al tener un procesador, actúan como pequeñas computadoras distribuidas y pueden generar alarmas ante un evento que este fuera de los parámetros normales cómo vandalismo, cámara desenfocada, detección de movimiento, etc., y que ayudan al operador en su labor diaria para que sea más provechosa y eficiente.

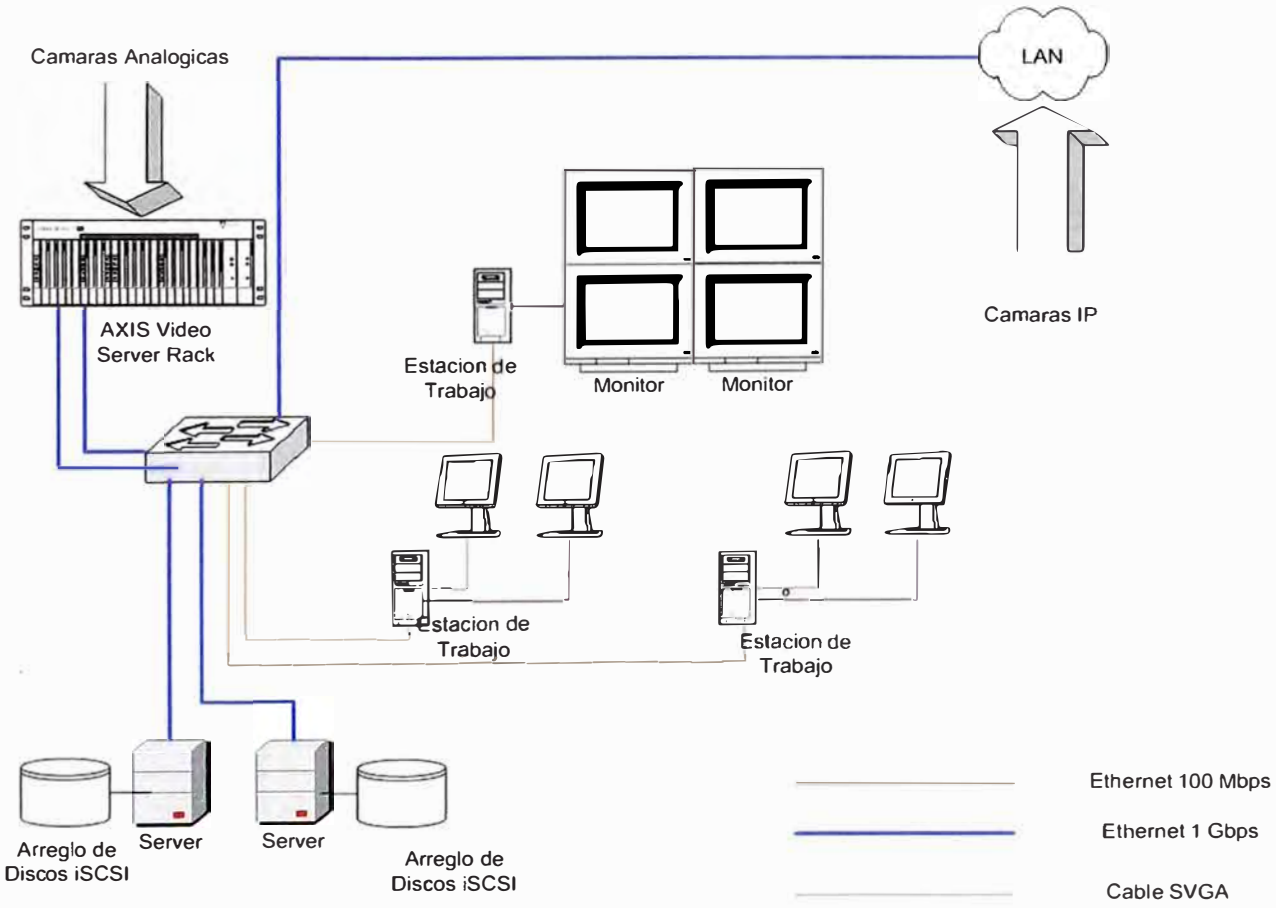


Figura 3.16 Diagrama Esquemático de la Solución de Video Vigilancia

Para nuestro ejemplo, se va a diseñar el centro de control para dos operadores. Cada operador cuenta con una estación de trabajo donde se encuentra instalado el software cliente para monitoreo.

Cada estación de trabajo tiene una tarjeta de video con dos salidas de monitor, lo que permite instalar dos monitores de 19" en cada estación de trabajo. La configuración es tal que los dos monitores estén en el mismo escritorio del operador.

Para el control de las cámaras móviles, es necesario que cada operador cuente con teclado tipo joystick para mover las cámaras. Esta puede hacerse con el mouse de la estación de trabajo, pero el teclado tiene mayores funcionalidades y es más práctico.

Para que puedan colocar en primer plano alguna de las cámaras, se instalarán en la pared frontal del centro de control, 4 monitores LCD de 40". Estos monitores irían conectadas a una estación de trabajo que tiene instalada una tarjeta de video de 256 MB con 4 salidas de video. El modelo de la tarjeta recomendado por Milestone es el VDA 464. El gráfico 3.16 (página anterior) muestra el diseño del centro de control, así como el diagrama esquemático de la solución de video vigilancia.

3.3 Diseño del Sistema de Control de Acceso

Para restringir el ingreso de las personas no autorizadas a las áreas de administración de la compañía, se requiere instalar sistemas de control de acceso en las puertas de ingreso al edificio de administración.

El edificio cuenta con 4 pisos y dentro de el se encuentra el centro de datos de la compañía. Al ingreso del centro de datos se deberá instalar un sistema de control de accesos.

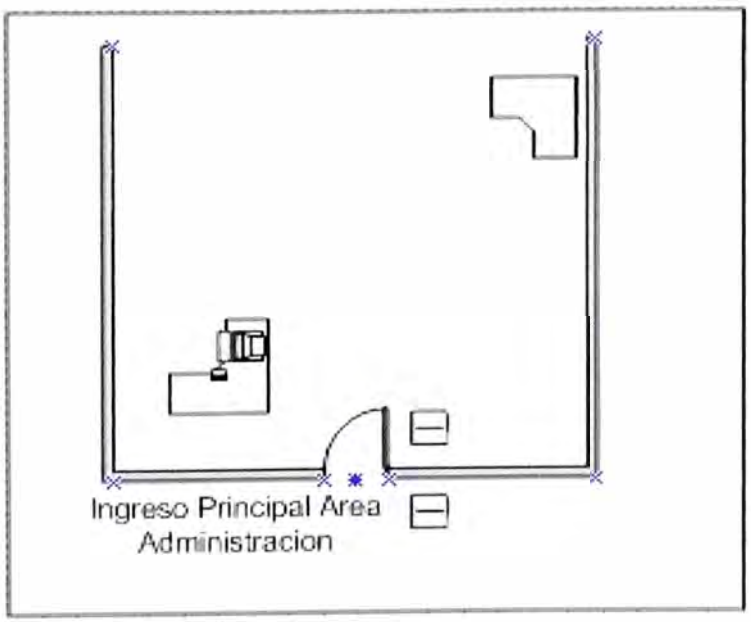


Figura 3.17 Disposición del Sistema

Para ingresar a cada piso, cada empleado debe presentar su tarjeta a un lector y dependiendo del nivel de autorización que tenga este ultimo, se le permitirá o restringirá el ingreso. En la figura 3.17 (página anterior) se muestra el diagrama con la disposición física del sistema por cada piso.

Para el ingreso del personal de campo a la zona de operaciones, cada trabajador debe cruzar un molinete de cuerpo completo. En esta zona existen tres molinetes de cuerpo entero para recibir alrededor de 400 operarios cada día, tal como se muestra en la figura 3.18.

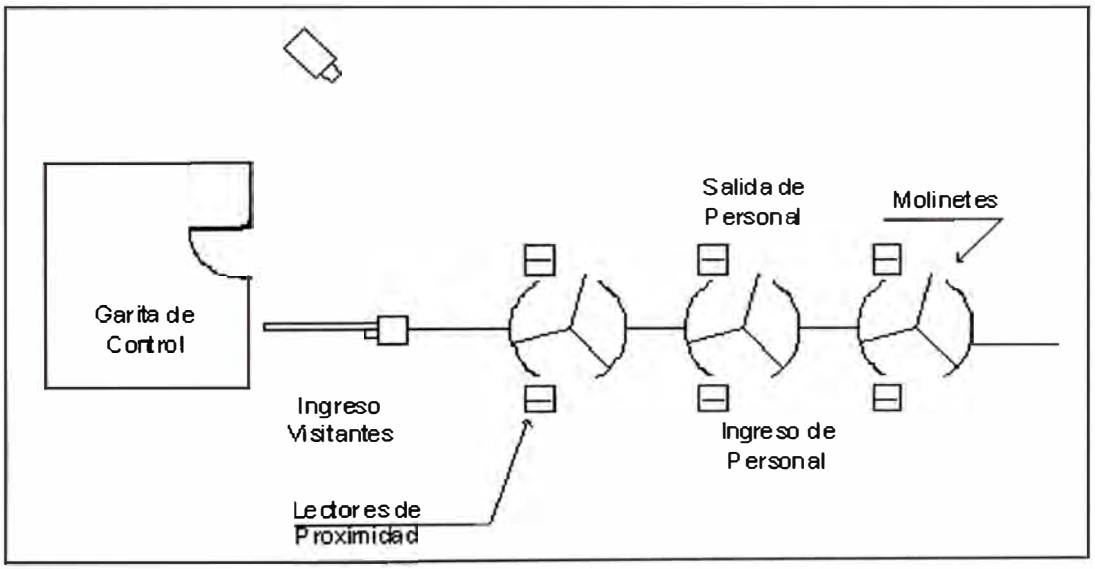


Figura 3.18 Disposición de la Zona de Ingreso peatonal

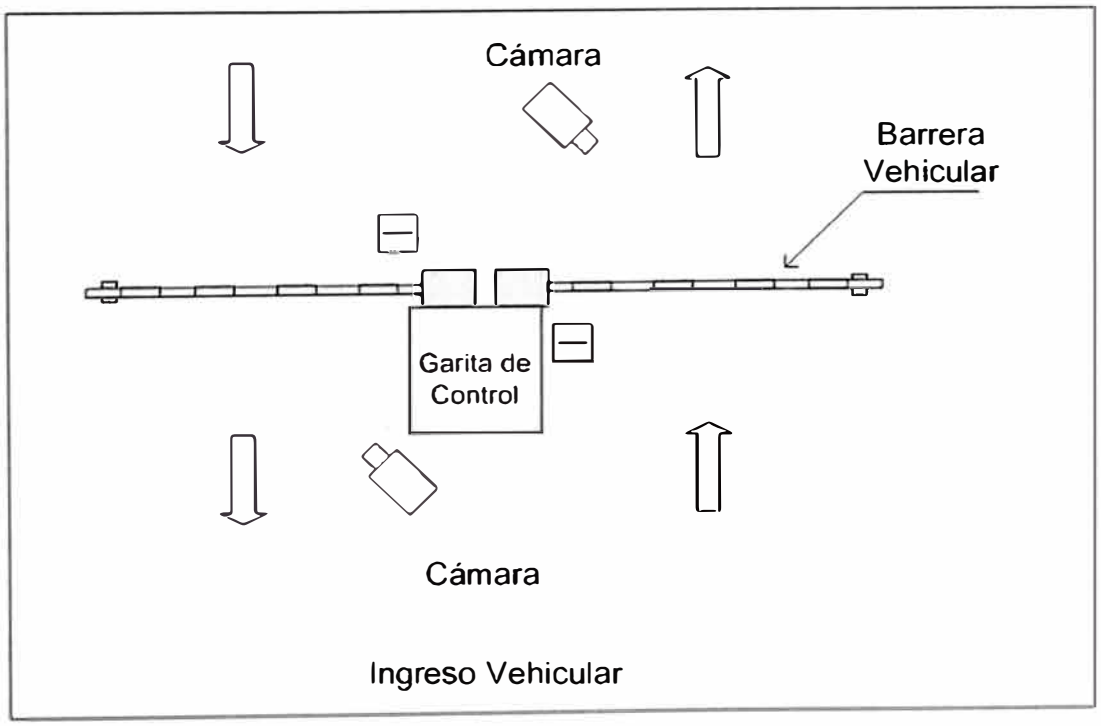


Figura 3.19 Disposición de la Zona de Ingreso vehicular

Algunos de los empleados de la compañía minera, tienen asignados vehículos para movilizarse dentro de la zona de producción, pero deben pasar por unas tranqueras vehiculares antes de ingresar a la zona de producción. En la figura 3.19 (página anterior) se muestra el diagrama con la disposición física del sistema de control de acceso vehicular

El principio de funcionamiento es el siguiente: Cuando un vehículo se dispone a ingresar a la zona de producción, el conductor deberá presentar su tarjeta de control hacia el lector quien recibe la información de la tarjeta, la decodifica y envía al controlador del sistema.

El controlador revisa en su registro si el conductor y vehículo tienen la autorización de ingresar a esta zona. Si la autenticación es correcta, el controlador enviara una señal eléctrica que activará el motor de la tranquera vehicular. Este procedimiento es realizado tanto para ingresar o salir de esta zona.

Para el caso del ingreso de los operarios, cada trabajador cuenta una tarjeta de control de acceso. La tarjeta contiene los datos del trabajador y es un elemento de identificación intransferible. Cada que vez que un operario desea ingresar a esta zona, debe presentar la tarjeta al lector instalado a lado del molinete de cuerpo entero. El lector recibe y decodifica los datos de la tarjeta y se la envía al controlador. El controlador comprueba si el usuario tiene o no los suficientes permisos para ingresar a esta zona. Si el usuario es válido, el controlador envía un pulso eléctrico para liberar el la cerradura del molinete.

Los visitantes, deberán ingresar por una zona diferente ya que ellos no cuentan con tarjetas de identificación, y deben completar una serie de registros antes de ingresar a la planta. Existe una cámara de video vigilando la zona para verificar visualmente que se cumpla el procedimiento de ingreso a la planta.

3.3.1 Criterios de Selección para los Controladores de Acceso

Se asume que existe un puerto de red disponible en cada una de las garitas de vigilancia. El diseño de la infraestructura de red no es parte del alcance de este informe.

El controlador de acceso es el componente principal del sistema. Es el que toma las decisiones de permitir o no, el ingreso de una persona o vehículo a la zona restringida y lleva un registro de cada una de las transacciones en el sistema. Al controlador se conectan físicamente cada uno de los componentes mostrados en las figuras 3.18 y 3.19.

Es importante que el controlador tenga una interfaz Ethernet ya que el medio de comunicación debe ser IP. Cada controlador debe ser modular y tener escalabilidad

ilimitada, es decir, que pueda ir creciendo según las necesidades del usuario. Debe soportar desde una aplicación básica de 2 lectoras hasta cientos de ellas.

Respecto al software de gestión del sistema de control de acceso, debe permitir integración con sistema de video IP a través de software y debe ser de arquitectura abierta. El controlador debe tener un certificado de calidad de un laboratorio independiente como UL, ETL, CE, etc.

Existen varios fabricantes de control de acceso en la industria de seguridad que han adaptado sus productos para operar en entornos de red IP y que permiten la integración con diferentes soluciones de video a través de software.

Para este caso particular, uno de los criterios de selección válidos es hacer referencia a la lista de fabricantes compatibles con la solución de administración de video escogida. El producto a modo de referencia seleccionado para la administración de video fue Milestone. Al revisar con qué fabricantes de control de acceso es compatible se obtendrá una lista de entre 5 y 6 distintos fabricantes, de los cuales se puede mencionar a S2 Security Corporation, Paxton Access, Solus Access Control Systems, Keeneo.

Para la selección final del producto a utilizar se realiza una evaluación técnico-económica considerando factores tales como la presencia y soporte local, el idioma del soporte, características técnicas y los precios del producto. Muchas veces es más importante la presencia y soporte local que se pueda obtener del fabricante a través de un distribuidor o representante.

De los fabricantes mencionados, S2 Security tiene origen americano y cuenta con un equipo de soporte técnico para Latinoamérica en español. Así mismo, cuenta con un distribuidor mayorista para la comercialización del producto, a diferencia de los demás que son fabricantes europeos con poca o nula presencia en Latinoamérica. Si se escogiera otro fabricante de software de video, se tendría que haber aplicado un análisis similar.

S2 Security Coporation, cuenta con diferentes productos de control de acceso, el principal llamado Netbox supera largamente las especificaciones descritas en los párrafos anteriores. Antes de seleccionar los productos adecuados para cada ubicación, se explica a continuación, de manera breve, la arquitectura de funcionamiento.

Un sistema de control de acceso tradicional tiene dos componentes básicos: Controladores y Software. Cada Controlador se conecta directamente a la red y puede soportar desde 2 a más lectores. El software es la interfaz para que el usuario pueda configurar todos los parámetros en el controlador, tales como crear usuarios, permisos de

cada usuario, horarios y cronogramas, etc. Se tiene una base de datos que permite almacenar todos los eventos que ocurren en el sistema. Todas las decisiones las toma el controlador, y es este último el que envía los registros de cada decisión tomada hacia la base de datos. El software puede ser instalado en una PC o servidor, o puede venir incorporado en algún hardware especial como parte del controlador.

Cada aplicación requiere de un S2 Network Controller, quien tiene incorporado el software de gestión. Solo se necesita uno en toda la red (ver figura 3.20).

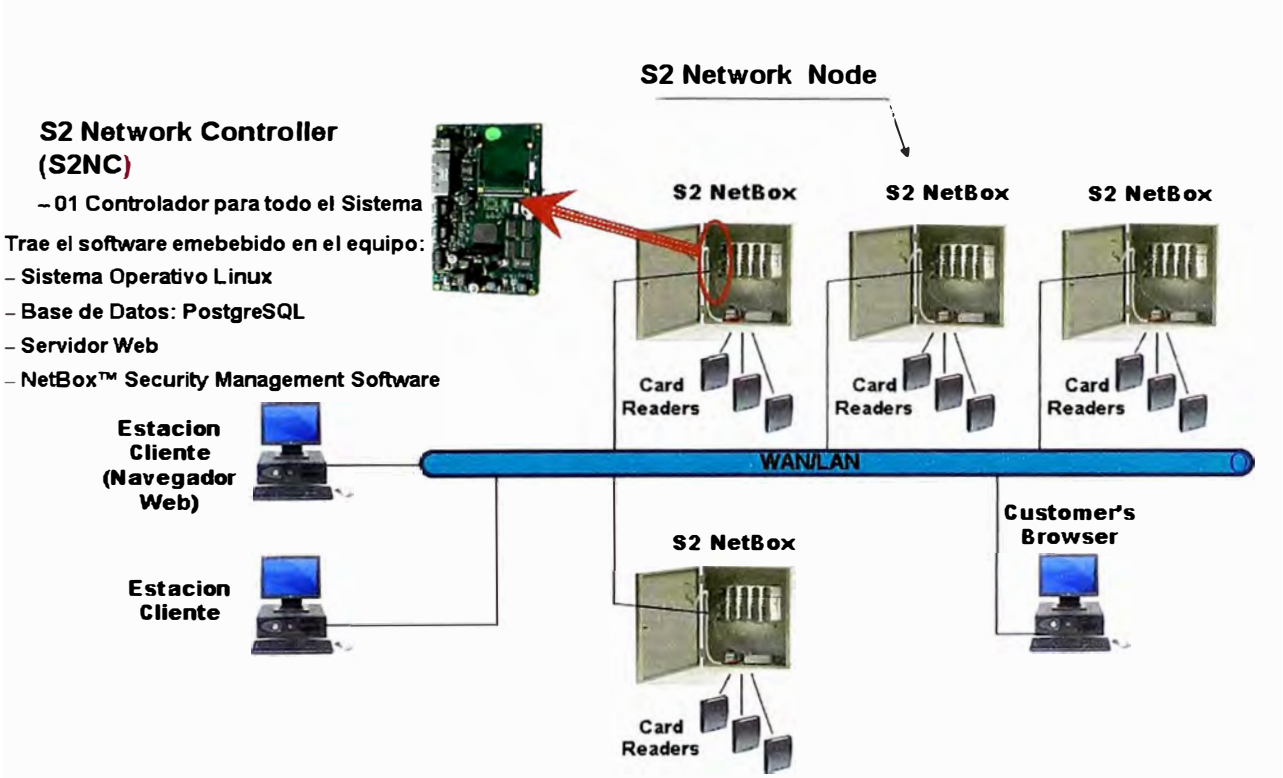


Figura 3.20 Arquitectura del S2 Security.

Si la compañía tuviera varias ubicaciones, se deberá colocar un S2 Network Node. Cada Network Node viene en un gabinete metálico que poses 8 ranuras de expansión. Para comprender la arquitectura es necesario ver el interior de un gabinete (figura 3.21 en página siguiente).

Nota: En el Anexo B se muestra la misma ilustración pero con mayor detalle y resolución.

En el primer gabinete está instalado el S2 Network Controller en la primera ranura. Es necesario solo uno por compañía o red. En la misma ranura, se instala el S2 Network Node para controlar los demás módulos de expansión que se instalan en las ranuras 1 al 7 del gabinete. En el segundo gabinete la primera ranura sólo tiene instalada el S2 Nework Node, debido a que ya se tiene el S2 Network Controller en el primer gabinete.

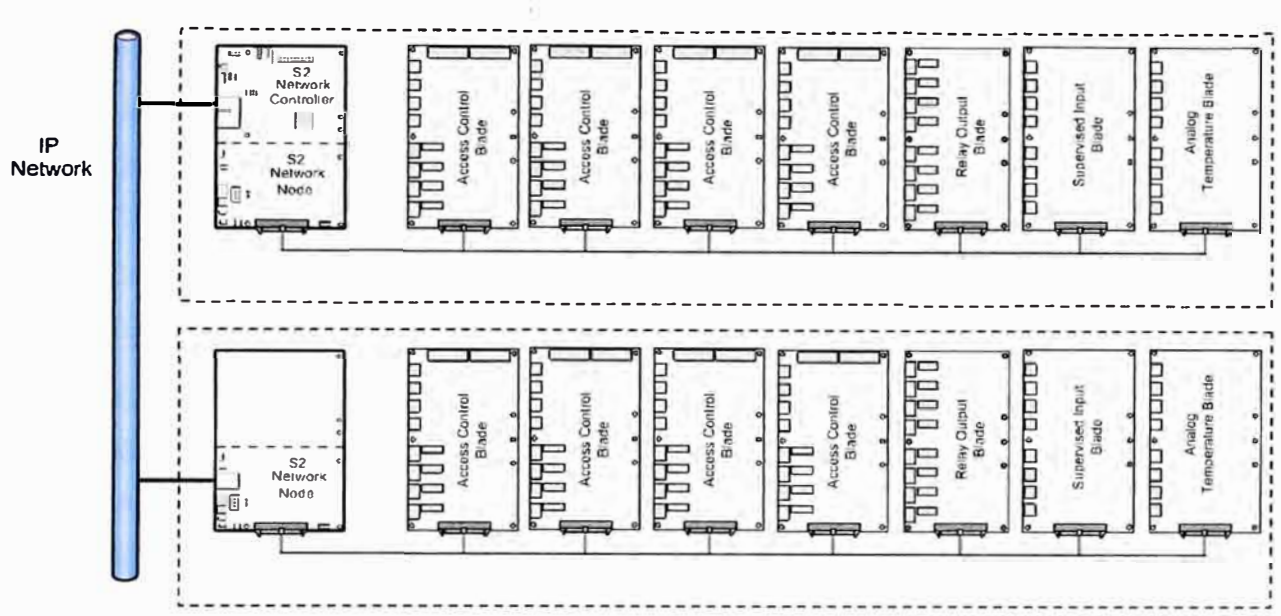


Figura 3.21 Diagrama de Gabinete del S2 Network Node

En las demás ranuras pueden instalarse alguno de los siguientes módulos de expansión:

- Módulo de Lectores: 2 Lectores, 4 entradas y 4 salidas.
- Módulo de Entradas: 8 entradas de contacto seco
- Módulo de Salidas: 8 salidas de colector abierto
- Módulo de Entrada de Sensores de Temperatura: 8 entradas

La figura 3.22 muestra los elementos típicos de una puerta con control de acceso y es de suma ayuda para una mejor comprensión de cual de estos módulos deben ser agregados al gabinete.

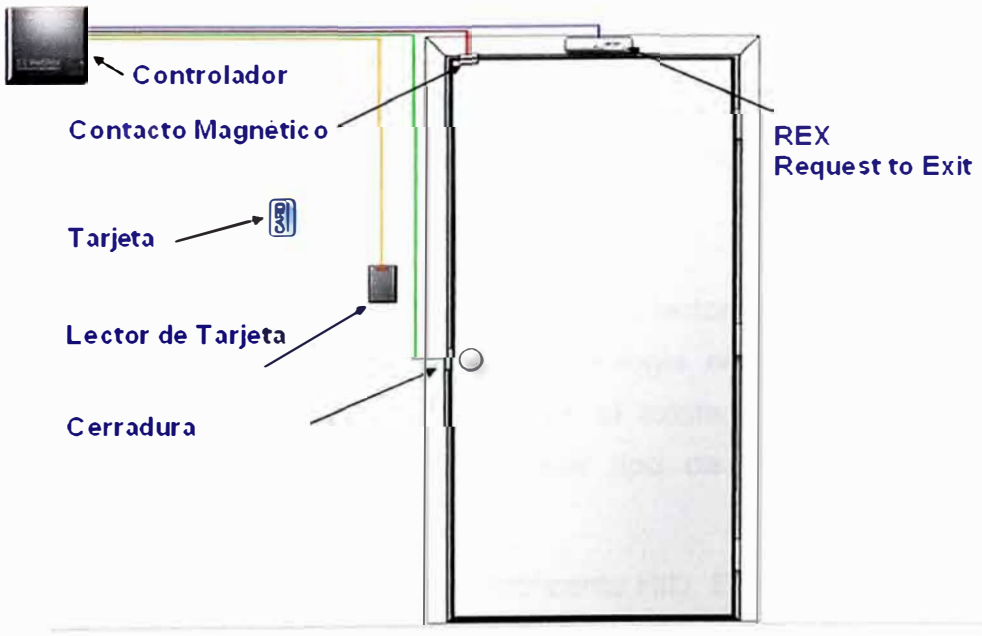


Figura 3.22 Elementos Típicos de una Puerta con Control de Acceso.

Cada puerta con control de acceso generalmente lleva:

- 01 Lector de tarjeta para ingreso
- 01 Lector de tarjeta para salida
- 01 Contacto magnético para supervisión del estado de la puerta (abierta o cerrada)
- 01 Cerradura eléctrica o electromagnética
- 01 Dispositivo de solicitud de salida REX (Request to Exit)

Cada uno de estos elementos va conectado a alguno de los módulos de expansión que se mencionaron anteriormente.

A continuación se detallan los elementos necesarios en cada área de la compañía: Las áreas son:

- Edificio Administrativo.
- Zona de ingreso Peatonal a la Planta de Producción.
- Zona de ingreso Vehicular a la Planta de Producción.

a. Edificio Administrativo

Aquí se involucra la selección de los controladores, de los lectores y de los accesorios

a.1 Selección de los Controladores

El Edificio administrativo cuenta con 5 puertas (una puerta por cada piso y una puerta en el centro de datos). Cada puerta requiere de un lector para el ingreso y otro para la salida. De ello se concluye que es necesario 10 lectores de control de acceso.

En el centro de datos se instalará el gabinete que contiene el S2 Network Controller, el S2 Network Node y 5 módulos de expansión de lectores. Cada módulo soporta 2 lectores, 4 entradas y 4 salidas. Los componentes que serán instalados en el centro de datos que realiza el control de todo el edificio son mostrados en la tabla 3.4.

a.2 Selección de Lectores

Una de las tecnologías más utilizadas para los lectores y tarjetas de control de acceso son de proximidad. Con este tipo de tecnología no es necesario que exista contacto físico entre la tarjeta y el lector, como si existe con tecnología de banda magnética y/o código de barras. Además, este tipo de tecnología es vulnerable comparado con la de proximidad.

A modo de referencia se propone al fabricante HID. El modelo sugerido para las puertas interiores del edificio es el iClass R10. En la figura 3.24 se muestra el lector iClass R10. Los equipos descritos en la tabla 3.4 se muestran en la figura 3.23.

Tabla 3.4 Componentes Seleccionados

Modelo	Fabricante	Descripción	Cantidad
S2-NC-M200	**S2**	**Model 200** Includes S2 NetBox™ system license for up to 32 readers up to 24 nodes (32 nodes in version 3.1 or later) and 10 concurrent system users. Unlimited live view IP cameras. Must be purchased with either a NC-CNTL-x or an NN-ExR-xx .1 year software upgrade and support warranty & 2 year hardware warranty included.	1
S2-NN-E10R-RM	**S2**	**S2 Network Node with 10 readers, 20 inputs, 20 outputs capability** S2 Network Node Base Blade in S2NetBox Lightweight Rack Mount Enclosure with Status LED and 12VDC power supply, plus five 2 reader Access Control Blades	1

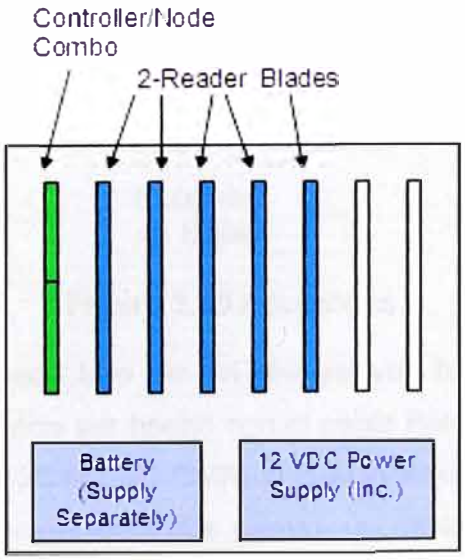


Figura 3.23 Distribución Física de Equipos Seleccionados

Figura 3.24 Lector iClass R10

Es necesario recalcar que puede escogerse cualquier lector siempre y cuando soporte el protocolo Wiegand, que es universal para comunicar los lectores con el controlador.

a.3 Selección de Accesorios

Los accesorios son.

- Contacto Magnético.
- Pulsador de Salida.
- Cerradura Eléctrica.

En la figura 3.25 se muestran los accesorios mencionados.

Figura 3.25 Accesorios

El cableado desde cada uno de los dispositivos hacia el controlador no debe exceder los 150 metros, y puede ser hecho con el cable Belden B558AFS "Banana Peel" no jacket – 18-4C+22-4P+22-2C+22-4C CMR, el cual incluye ya cuatro pares de 18 AWG para los lectores (cada lector necesita dos pares), un cable de 22 de dos conductores para el contacto magnético, un cable de cuatro conductores de 18 AWG, para alimentar la cerradura (quedarían dos libres) y un cable de cuatro conductores de 22AWG para el pulsador de salida (ver figura 3.26).

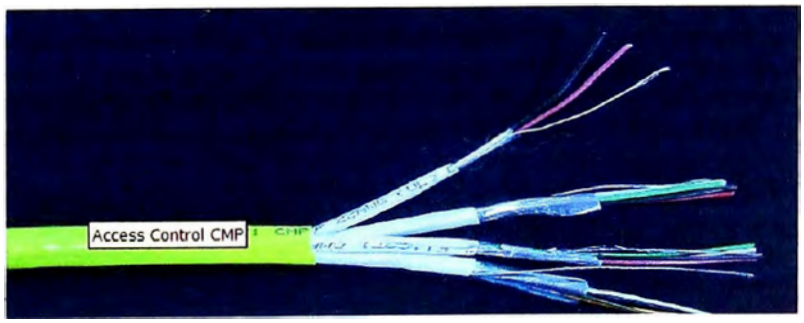


Figura 3.26 Cable Compuesto

b. Zona de ingreso Peatonal a la Planta de Producción

Aquí se contempla también la selección de los controladores, de los lectores y accesorios.

b.1 Selección de los Controladores

En la zona de ingreso peatonal se tienen tres molinetes de cuerpo entero con lectores de entrada y salida. Lo que da un total de seis lectores. En este caso, el molinete se comporta como una puerta y ya viene con diferentes accesorios para la supervisión de giro (horario y antihorario) y una traba mecánica. El controlador debe ir instalado en la garita de vigilancia, conectarse a un puerto de red disponible y a una toma eléctrica. Ver tabla 3.5. Los equipos listados en la tabla 3.5 serian como se muestra en la figura 3.27.

Tabla 3.5 Equipos de S2 Security para la Zona de Ingreso Peatonal

		S2 Network Node with 6 readers, 12 inputs, 12 outputs capability	
S2-NN-E6R-WM	**S2**	S2 Network Node Base Blade in S2NetBox Lightweight Aluminum Enclosure with key lock, Status LED, tamper switch, 12VDC power supply and battery backup capable, plus three 2 reader Access Control Blades	1

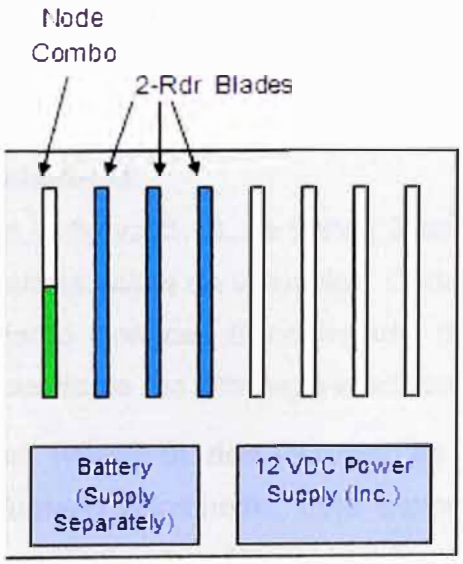


Figura 3.27 Distribución Física de Equipos Seleccionados

b.2 Selección de Lectores y Accesorios

La consideración para la selección del lector es que este debe estar preparado para funcionar en exteriores.

Es suficiente con el modelo R10 de HID que se planteó para el edificio de administración.

Los molinetes de cuerpo entero, deben tener un motor bidireccional, es decir que puedan ser utilizados para entrar y salir.

El grado de protección debe ser como mínimo IP 54 (Protegido contra polvo y rocío directo en todas las direcciones). La entrada de voltaje 220 VAC y en caso de falla debe liberarse de manera automática para permitir el libre tránsito en situaciones de emergencia. Debe tener además, entradas de contacto seco para liberar el molinete a través del controlador. En la figura 3.28 se muestra un molinete de cuerpo entero.

Figura 3.28 Molinete de Cuerpo Entero

c. Zona de ingreso Vehicular a la Planta de Producción

De igual forma a las otras áreas, se analiza la selección de los controladores, los lectores y accesorios.

c.1 Selección de Controladores

Como se muestra en la figura 3.19, se tienen 2 barreras vehiculares, la primera para ingreso y la segunda para la salida de vehículos. Cada barrera vehicular cuenta con un lector de proximidad de largo alcance. El controlador debe ser instalado en la garita de control, donde existe un puerto de red y energía eléctrica.

En vista que solo se necesitan dos lectores, se seleccionará el equipo más pequeño de S2 Security llamado Micronode. Este soporta solo dos lectores, cuatro entradas y cuatro salidas de contacto seco. Ver tabla 3.6

Tabla 3.6 Características de Equipo Seleccionado

S2-NDMN	**S2**	S2 NetDoor MicroNode, 2 readers, 4 inputs, 4 outputs (two outputs switchable to power locks, one temp input port, locking enclosure with network status light	1

Físicamente el NetDoor Micronode, al contener sólo una tarjeta para dos lectores, viene en un gabinete más pequeño que permite reducir costos considerablemente. Ver figura 3.29.

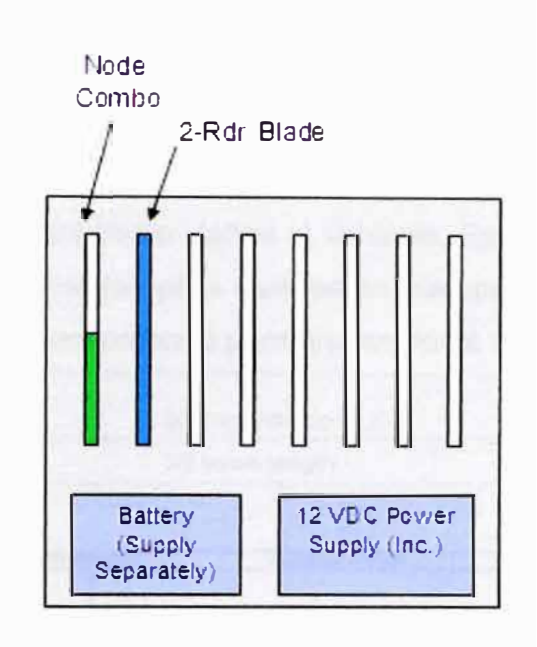


Figura 3.29 Distribución Física de, NEtDoor Micronode

c.2 Selección de Lectores y Accesorios

El lector sugerido para instalarse en un pedestal para el control de acceso vehicular debe ser de largo alcance (alrededor de 2 a 3 metros). El modelo sugerido es el iClass R90 de HID. Ver figura 3.30.

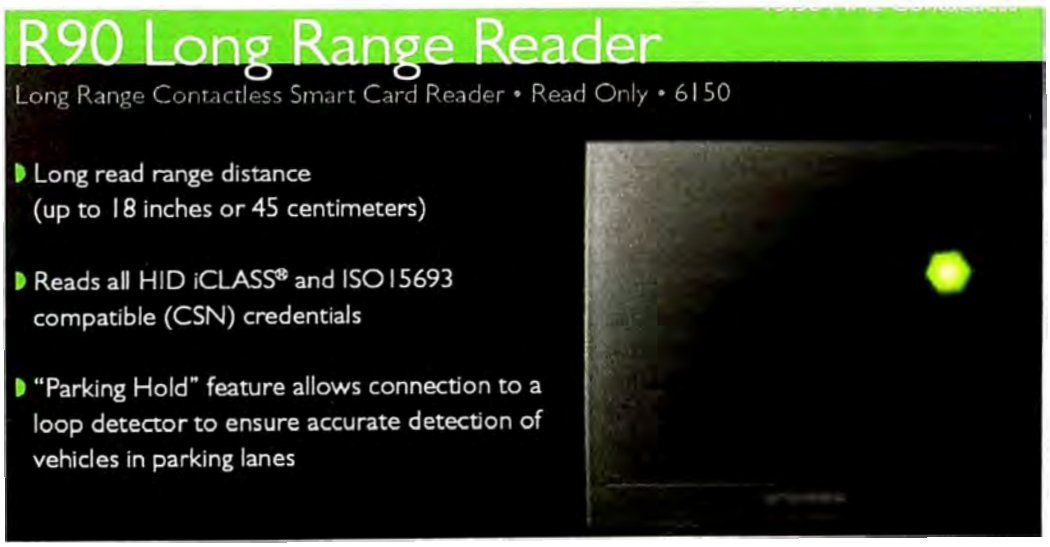


Figura 3.30 iClass R90 de HID

Para el caso de la tranquera vehicular, se deben tener algunas consideraciones sobre el terreno donde se instalará la barrera vehicular, ya que se debe preparar una loza de concreto para soportar el pedestal, tal como se muestra en la figura 3.31.

Cuando un conductor presenta su tarjeta al lector, éste envía la información al controlador quien valida si éste puede o no ingresar. Si está autorizado, envía un pulso al motor para que levante la barrera y el vehículo pueda cruzar. Para que la barrera regrese a su posición original, el auto debe haber cruzado totalmente el campo de acción de un sensor de presión instalado bajo la superficie.

Si el auto se detiene al medio de la barrera, el sensor le indica al motor que aún no debe bajar la barrera para evitar daños al vehiculo. Estos estados son comunicados permanentemente al controlador para que estén siempre sincronizados. Así mismo, existe un par de cámaras monitoreando permanentemente esta zona.

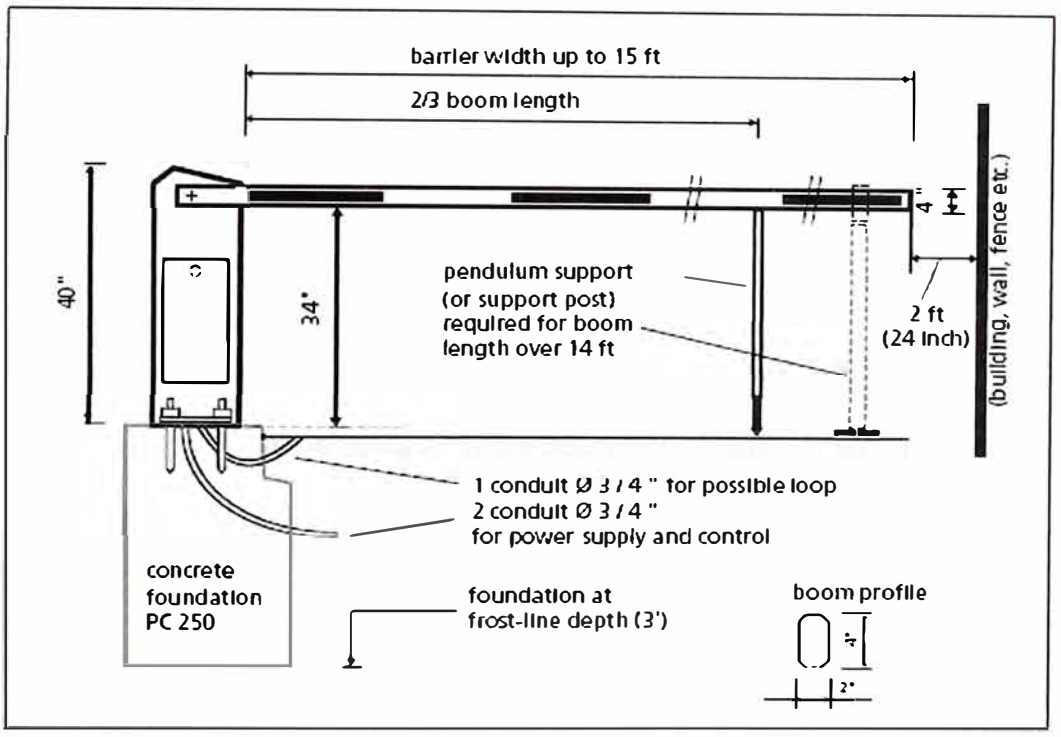


Figura 3.31 Consideraciones sobre el terreno para la barrera vehicular

Al momento de seleccionar la barrera apropiada, se deben tener en cuenta las dimensiones geométricas de los carriles de ingreso, el grado de protección para exteriores y la velocidad de giro del motor, así como su potencia. Como referencia, se puede utilizar el modelo MBE 50 de Magnetic Autocontrol.

3.4 Integración de los Sistemas

Hasta este punto se tienen listos los diseños del sistema de video vigilancia IP y el sistema de control de accesos. Ambos operarían sin mayor problema pero de manera independiente. Lo que resta es la integración de ambas aplicaciones. Esto se logra mediante la activación de licencias de integración entre el software de video y el software de control de acceso.

La integración permite asociar una imagen de una cámara de video que está monitoreando una puerta de ingreso a los registros de entrada y salida. Por ejemplo, a puerta del datacenter se encuentra con un sistema de control de accesos y tiene además una cámara analógica en su interior.

Si una persona presenta su tarjeta al lector y éste ingresa al datacenter, (previamente se ha marcado el datacenter como una zona critica y de alta seguridad) automáticamente se le muestra al operador en la consola del sistema de control de acceso, el video al momento que la persona ingresa, y se almacena esta información visual junto con el nombre de la persona que ingreso para posteriores auditorias. Este es solo un ejemplo de la utilidad de este tipo de funcionalidad.

Obviamente, solo es necesario integrar aquellas cámaras de video que guardan una relación con las puertas que están monitoreadas. Como para el proyecto solo se tienen 3 cámaras asociadas al control de acceso, la relación de licencias es la que se muestra en la tabla 3.7.

Tabla 3.7 Relación de Licencias de Software

Video Integration Software License for S2 NetBox / Milestone Integration , when Milestone XProtect Enterprise is purchased outside of S2			
S2-NVR-SMS	**S2**	Video Management System Integration Option, Milestone Systems XProtect Enterprise integration license up to 4 cameras	1
S2-NVR-CAM	**S2**	Video Management System Integration Option integration license fee per camera beyond the initial 4 camera integration licenses included with Option license	3

En el siguiente capítulo se expone el análisis de costos de la solución.

CAPÍTULO IV
ANÁLISIS DE COSTOS DE LA SOLUCIÓN

4.1 Propuesta Económica

La propuesta económica es presentada en las siguientes tablas de equipos y de costos de mano de obra y gastos generales, tanto para los subsistemas de vigilancia cómo para el de control de acceso.

- Tabla 4.1 Presupuesto Codificadores de Video
- Tabla 4.2 Presupuesto Cámaras Fijas
- Tabla 4.3 Presupuesto Cámaras Domo PTZ.
- Tabla 4.4 Presupuesto Licencias de Software
- Tabla 4.2 Presupuesto de Servidores de Almacenamiento y Estaciones de Trabajo
- Tabla 4.7 Presupuesto de Sistema de Control de Acceso para Ingreso Peatonal
- Tabla 4.6 Presupuesto de Sistema de Control de Acceso para Edificio Administrativo
- Tabla 4.8 Presupuesto de Sistema de Control de Acceso para Ingreso Vehicular
- Tabla 4.9 Presupuesto de Integración y Costo Total
- Tabla 4.10 Costos de Mano de Obra y Gastos Generales.

Tabla 4.1 Presupuesto Codificadores de Video

MODELO	FABRICANTE	CODIFICADORES DE VIDEO	CANTIDAD	PRECIO UNITARIO (USD$)	TOTAL (USD $)
AXIS Q7406	AXIS	**6 channel video encoder blade. Multiple, individually configurable H.264 and Motion JPEG streams; max. D1 resolution at 30/25 fps per channel**. Video motion detection. Active tampering alarm. **COMPATIBLE WITH AXIS Q7900 RACK AND AXIS 291 1U VIDEO SERVER RACK**	7	2,167.72	15,174.05
AXIS Q7900 Rack	AXIS	**4U 19" rack with 14 slots for Axis video encoder blades.** Supports up to 84 analog channels. Multiple video streams per channel through **four Gigabit Ethernet ports. Two redundant power supply** units. Each slot offers six RS-485 connectors for PTZ control and 12 I/O ports for connections to external devices. **Compatible with all current Axis video encoder blades**	1	5,783.79	5,783.79

Tabla 4.2 Presupuesto Cámaras Fijas

MODELO	FABRICANTE	CÁMARA FIJAS	CANTIDAD	PRECIO UNITARIO (USD $)	TOTAL (USD $)
AXIS 221	AXIS	**Varifocal DC-iris lens**. 1/3" **progressive scan CCD**. Down to 0.65 lux in color. **Auto day/night mode**. Up to VGA 640x480 resolution at **45 frames per second**. **Motion JPEG and MPEG-4**. **Video Motion Detection and I/O** for alarm/event handling. **Power over Ethernet**. **RS-232/485** for data and PTZ control. Includes adjustable stand and power supply.	16	1,444.50	23,112.00
ACH13HBN	VIDEOLARM	IP Network Ready Outdoor Environmental hsg with metal wall/pole mount, w/24Vac input, 12 or 24 output for camera, thermostatically controlled heater/blower, for an IP Network camera, 40vA transformer, MCL 10.5"	16	449.11	7,185.74
PB24	VIDEOLARM	Rugged cast aluminum power box with 220/115Vac input converting to 24Vac and 84W output power. Pole mounting clips included.	16	176.40	2,822.47

Tabla 4.3 Presupuesto Cámaras Domo PTZ

MODELO	FABRICANTE	CAMARAS DOMO PTZ	CANTIDAD	PRECIO UNITARIO (USD $)	TOTAL (USD $)
AXIS 233D	AXIS	**35x** optical zoom **dome camera** with **WDR** and area zoom. **Auto day/night** mode down to **0.5 lux** in color and **0,008 in night** mode. Continuous 360º rotation and 180º tilt with **E-flip. Progressive Scan 4CIF** resolution at **30/25fps in MPEG-4 or Motion JPEG**. Two-way **audio**, **I/O** for alarm/event handling. Includes **hard and drop ceiling** mount kit, **smoked and clear** transparent covers and **power supply**.	15	3,614.15	54,212.22
PFDW75C2N	VIDEOLARM	IP Network Ready 7" Outdoor pressurized dome hsg w/ WM20G gooseneck wall mount, clear dome, w/24Vac input, heater/blower, for an IP Network PTZ camera, 120 to 24Vac, 96vA transformer	15	994.37	14,915.54
APM3	VIDEOLARM	Aluminum pole mount bracket with female inserts	15	35.48	532.17
NPK01	VIDEOLARM	Nitrogen fill kit for pressurized housing, includes regulator valve and fill tank	1	589.33	589.33

Tabla 4.4 Presupuesto Licencias de Software

MODELO	FABRICANTE	LICENCIAS	CANTIDAD	PRECIO UNITARIO (USD $)	TOTAL (USD $)
XPEBL	MILESTONE	XProtect Enterprise 6.5 Base License	1	2.00	2.00
YXPEBL	MILESTONE	1 year PMA for XPEBL	1	360.00	360.00
XPECL	MILESTONE	XProtect Enterprise 6.5 Camera License	70	196.01	13,720.35
YXPECL	MILESTONE	1 year PMA for XPECL	70	49.00	3,430.00

Tabla 4.5 Presupuesto de Servidores de Almacenamiento y Estaciones de Trabajo

MODELO	FABRICANTE	SERVIDORES DE ALMACENAMIENTO Y ESTACIONES DE TRABAJO	CANTIDAD	PRECIO UNITARIO (USD $)	TOTAL (USD $)
MHW-SM4M1-US	BOSCH	Server Sml, 1x72GB HDD (BVMS/VIDOS/NVR)	2	11,200.00	22,400.00
DSA-S5B50-12AT	BOSCH	Arreglo Discos SV500 Unidad Basica 12x1000GB	4	17,320.00	69,280.00
	IBM	Work Station for Video Monitoring	3	3,100.00	9,300.00
	Viewsonic	Monitor 19" VGA	4	500.00	2,000.00
	Sony	Monitor 40" Bravia	4	3,500.00	14,000.00

Tabla 4.6 Presupuesto de Sistema de Control de Acceso para Edificio Administrativo

MODELO	FABRICANTE	EDIFICIO ADMINISTRATIVO	CANTIDAD	PRECIO UNITARIO (USD $)	TOTAL (USD $)
S2-NC-M200	**S2**	**Model 200.** Includes S2 NetBox™ system license for up to 32 readers up to 24 nodes (32 nodes in version 3.1 or later) and 10 concurrent system users. Unlimited live view IP cameras. Must be purchased with either a NC-CNTL-x or an NN-ExR-xx .1 year software upgrade and support warranty & 2 year hardware warranty included.	1	3,071.25	3,071.25
S2-NN-E10R-RM	**S2**	**S2 Network Node with 10 readers, 20 inputs, 20 outputs capability.** S2 Network Node Base Blade in S2NetBox Lightweight Rack Mount Enclosure with Status LED and 12VDC power supply, plus five 2 reader Access Control Blades	1	4,457.25	4,457.25
R10	**HID**	i Class Card Reader	10	100.00	1,000.00
sm-200	**SECOLARM**	Door Contact	5	3.00	15.00
	SECOLARM	Door Lock	5	80.00	400.00
	SECOLARM	Push to Exit	5	50.00	250.00

Tabla 4.7 Presupuesto de Sistema de Control de Acceso para Ingreso Peatonal

MODELO	FABRICANTE	INGRESO VEHICULAR	CANTIDAD	PRECIO UNITARIO (USD $)	TOTAL (USD $)
S2-NDMN	**S2**	S2 NetDoor MicroNode, 2 readers, 4 inputs, 4 outputs (two outputs switchable to power locks, one temp input port, locking enclosure with network status light	1	1,094.63	1,094.63
R-90	**HID**	iCLASS R90 Long Range Contactless Smart Card Reader, Wiegand output.	2	635.00	1,270.00
MBE 50*-C100	**MAGNETIC AUTOCONTROL**	Vehicular Barrier Gate	2	3,100.00	6,200.00

Tabla 4.8 Presupuesto de Sistema de Control de Acceso para Ingreso Vehicular

MODELO	FABRICANTE	INGRESO PEATONAL	CANTIDAD	PRECIO UNITARIO (USD $)	TOTAL (USD $)
S2-NN-E6R-WM	**S2**	**S2 Network Node with 6 readers, 12 inputs, 12 outputs capability.** S2 Network Node Base Blade in S2NetBox Lightweight Aluminum Enclosure with key lock, Status LED, tamper switch, 12VDC power supply and battery backup capable, plus three 2 reader Access Control Blades	1	3,025.58	3,025.58
R10	**HID**	i Class Card Reader	6	100.00	600.00
MPT 33C-C350G	**MAGNETIC AUTOCONTROL**	**Full Height Turnstile. Solenoide Locking System. 220 VAC**	3	5,100.00	15,300.00

Tabla 4.9 Presupuesto de Integración y Costo Total de Equipos

MODELO	FABRICANTE	INTEGRACIÓN	CANTIDAD	PRECIO UNITARIO (USD $)	TOTAL (USD $)
S2-NVR-SMS	S2	Video Management System Integration Option, Milestone Systems XProtect Enterprise integration license up to 4 cameras	1	393.75	393.75
S2-NVR-CAM	S2	Video Management System Integration Option integration license fee per camera beyond the initial 4 camera integration licenses included with Option license	3	118.13	118.13
		TOTAL EQUIPOS USD($)			**296,015.2**

Tabla 4.10 Costos de Mano de Obra y Gastos Generales.

		INGENIERIA Y PUESTA EN MARCHA	CANTIDAD	PRECIO UNITARIO (USD $)	TOTAL (USD $)
ENGINEERING		Engineering, Design and Supervising	1	14,800.76	14,800.76
INSTALLATION		Installation, setup and materials for all entirely system	1	103,605.33	103,605.33
		TOTAL INGENIERIA Y PUESTA EN MARCHA USD($)			**118,406.10**

COSTO TOTAL APROXIMADO DEL PROYECTO: USD ($) 414,421.34

4.2 Cronograma de Implementación

El cronograma del proyecto es mostrado en la tabla 4.11.

Tabla 4.11 Cronograma del Proyecto

ACTIVIDADES	TIEMPO EN MESES				
	1	2	3	4	5
Diseño e Ingeniería del Sistema					
Adquisición de Equipos					
Instalación					
Pruebas					
Capacitación					
Cierre de Proyecto y documentación					

CONCLUSIONES Y RECOMENDACIONES

1. Los sistemas de seguridad basados en IP son de arquitectura abierta. Lo que significa que se puede combinar diferentes fabricantes en una misma solución. El único requerimiento es que los elementos a conectarse cuenten con protocolos de red estándares
2. Al utilizar equipos basados en IP, se puede compartir la infraestructura de redes de las compañías para transmitir la información de video y/o control de accesos. Como se ha visto en el informe, se ha considerado que toda la infraestructura de red es existente o a implementar por otros.
3. Las marcas mencionadas en el informe son solo referenciales. Solo se deben tomar en cuenta los requerimientos técnicos mínimos planteados en este informe.
4. Respecto a los sistemas de control de acceso, se debe hacer un análisis detallado de cómo es la operación y el día a día de las personas que van a utilizar el sistema, ya que la idea es que estos sistemas convivan de forma amigable con los usuarios y eviten malestares dentro del personal.
5. Siempre deben tenerse en consideración las recomendaciones de defensa civil respecto a las vías de escape y evacuación.
6. La tecnología es un complemento que ayuda a los encargados de seguridad a ser más eficientes a la hora de hacer su trabajo. Se debe siempre tener un procedimiento ante casos de emergencia. La tecnología nos ayudara a anticiparnos en la detección de ese evento y con ello mitigar o disminuir las pérdidas que esta pueda ocasionarnos.
7. Los sistemas de video vigilancia IP ya dejaron de ser de uso exclusivo del área de seguridad. Es cada vez más utilizado por diferentes áreas de las compañías del sector minero, principalmente de Operaciones Mina, Telecomunicaciones y TI.
8. La supervisión remota de los procesos reduce costos de mano de obra de forma significativa.
9. Se debe ver el costo beneficio de esta solución. Una compañía minera pierde varios cientos de miles de dólares cuando paraliza sus operaciones debido a un accidente, errores en el proceso de producción o simplemente por toma de las

instalaciones por las comunidades aledañas a la minera. Es por ello que el presupuesto obtenido es razonable dentro de los planes de ampliación de una minera. Y usualmente es el 5% del valor total del proyecto.

10. De todos modos, siempre existe la posibilidad de implementar el proyecto en etapas según las prioridades del área usuaria.

ANEXO A
RESULTADOS EN LA HERRAMIENTA DE CÁLCULO AXIS

Home | User's guide | Clear project | Save project | Print project

	Name	Model	No. of cams	Bandwidth (View, Rec, Event)	Storage (30 days)
1	Camaras Analogicas	AXIS Q7406 (NTSC)	39	0 bit/s, 39.6 Mbit/s, 0 bit/s	11.2 TB
2	Camaras Fijas	AXIS 221	16	0 bit/s, 51.2 Mbit/s, 0 bit/s	14.5 TB
3	Camara PTZ	AXIS 233D (NTSC)	15	0 bit/s, 43.5 Mbit/s, 0 bit/s	13.4 TB
Project summary				**0 bit/s, 134.3 Mbit/s, 0 bit/s**	**39.1 TB**

Camera Storage

Camera

Name	Image scenario	Audio	Model	No. of channels
Camaras Analogicas	Intersection (night option)	☐	AXIS Q7406 (NTSC)	39

☐ **Viewing** Play example

Frame rate	Resolution	Compression type	Compression	Bandwidth
18 fps	704x480 4CII	MotionJPEG	10	6047 Kbit/s

☑ **Continuous recording** Play example

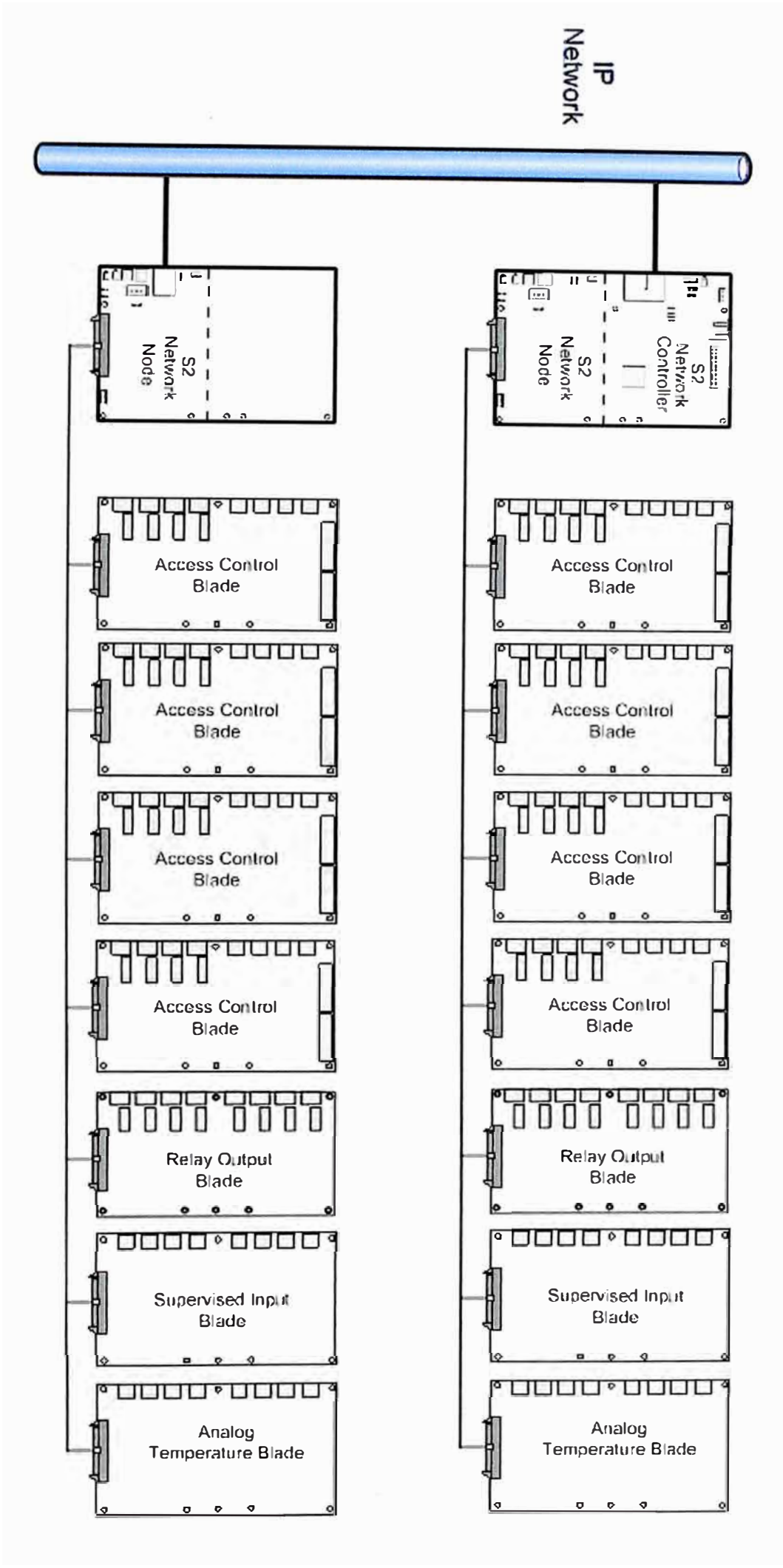
Record for	Frame rate	Resolution	Compression type	Compression	Bandwidth
22 h	18 fps	704x480 4CII	H.264	10	1040 Kbit/s

☐ **Event recording** Play example

Alarm	Frame rate	Resolution	Compression type	Compression	Bandwidth
90 %	18 fps	704x480 4CII	H.264	10	1040 Kbit/s

Remove this camera | Add new camera

ANEXO B
DIAGRAMA DEL GABINETE DEL S2 NETWORK NODE


IP Network
S2 Network Node
S2 Network Controller
Access Control Blade
Access Control Blade
Access Control Blade
Access Control Blade
Access Control Blade
Relay Output Blade
Supervised Input Blade
Analog Temperature Blade
S2 Network Node
Access Control Blade
Access Control Blade
Access Control Blade
Access Control Blade
Access Control Blade
Relay Output Blade
Supervised Input Blade
Analog Temperature Blade

ANEXO C
GLOSARIO DE TÉRMINOS

- AXIS.- Fabricante de cámaras IP.
- AWG.- Unidad de medida de calibre de cables.
- BOSCH.- Fabricante de productos de seguridad electrónica.
- CCD.- Sensor de Imagen de las cámaras de video profesionales (Charged Coupled Device).
- CCTV.- Circuito Cerrado de Televisión.
- CE.- Conformidad Europea.
- CMOS.- Sensor de Imagen de las cámaras de video domésticas (Complementary Metal Oxide Semiconductor)
- DVR.- Grabador Digital de Video (Digital Video Recorder)
- DHCP.- Protocolo de Configuración Dinámica de Estaciones IP (Dynamic Host Configuration Protocol)
- Domo PTZ.- Cámara en forma de burbuja con movimiento horizontal, vertical y zoom.
- ESPRIT.- Modelo de cámara móvil marca Pelco.
- ETL.- Certificación de calidad para diversos productos en USA y Canadá
- Frames per Second (fps).- Cuadros por segundo que forman una secuencia de video.
- Filtro IR.- Filtro infrarrojo, dispositivo utilizado al interior de las cámaras Día/Noche que se retira mecánicamente en escenas de poca luz.
- FTP.- Protocolo de Transferencia de Archivos (File Tranfer Protocol)
- H.264.- Formato de compresión de video predictivo basado en MPEG-4 part 10. Es un nuevo estándar en compresión para video vigilancia que reduce hasta un 80 % del ancho de banda respecto del M-JPEG.
- HID.- Fabricante de credenciales y lectores de control de acceso
- HTTP.- Protocolo de Transferencia de Hipertexto (Hypertext Transfer Protocol)
- HTTPS.- Protocolo Seguro de Transferencia de Hipertexto (Hypertext Transfer Protocol Secure)
- iClass.- Tecnología de HID para su nueva familia de tarjetas y lectores de control de acceso.
- IGMP.- Protocolo de Gestion de Grupo de Internet (Internet Group Management Protocol)
- MAGNETIC AUTOCONTROL.- Fabricante de barreras de control vehicular y peatonal.
- MBE50.- Modelo de barrera vehicular del fabricante Magnetic Autocontrol.
- Megapixel.- Alta resolución de cámaras digitales en órdenes de millones de pixeles.
- MILESTONE.- Fabricante de software de gestión de video

- M-JPEG.- Formato de compresión de video poco eficiente (Motion-JPEG)
- MPEG-4.- Motion Picture Expert Group. Formato de compresión de video predictivo; es un estándar en lo referente a compresión de video en sistemas de video vigilancia que reduce hasta un 50% el ancho de banda respecto del M-JPEG.
- NAS.- Network Attache Storage, Equipo de grabación en red para video vigilancia.
- NETBOX.- Producto de control de acceso de S2 Security
- NTSC, National Television System Committee. Estándar de televisión analógico en USA, y varios países de Latinoamérica incluyendo Perú.
- Pelco P o D.- Protocolos de comunicación serial propietario de Pelco para controlar cámaras móviles.
- PTZ.- Pant, Tilt, Zoom. Término utilizado para cámaras móviles con acercamiento de lente.
- REX.- Request to Exit. Dispositivo de solicitud de salida en puertas con control de acceso.
- SAN.- Storage Area Network. Sistema de almacenamiento flexible para entornos multiservidor.
- SDK.- Software Development Kit. Kit de desarrollo de software de una aplicación para integrar aplicaciones de terceros.
- SNMP.- Protocolo Simple de Gestion de Red (Simple Network Management Protocol)
- SONY.- Fabricante de cámaras IP y otros aparatos electrónicos
- Stream.- Trafico de video generado por una cámara o codificador IP
- TB.- Terabyte
- TCP/IP.- Protocolo de comunicación estándar para redes
- TVL.- Television Lines. Medida de resolución de video analógico,
- UDP.- Protocolo Datagrama de Usuario. User Datagram Protocol
- UL.- Underwriter Laboratories. Laboratorio independiente que certifica la calidad de los productos.
- VCR.- Grabador de Video en Cinta (Video Cassete Recorder)
- Wiegand.- Protocolo de comunicación entre el lector y controlador de control de acceso

BIBLIOGRAFÍA

1. IP Surveillance Design Guide. AXIS Communications 2008
2. Technical Guide to Network Video. AXIS Communications 2009
3. Guía de Video Vigilancia IP. ANIXTER INC
4. Sales, Configuration & Applications Training for ANIXTER CALA. May 2008. S2 Security Corporation.
5. IP Video Surveillance in Hasrh Enviroments- Milestone White Paper. Authors: Eric Fullerton and Kyle Johanson,
6. Closed Circuit Television.
   Author:Joe Cieszynski. IEng MIEE (elec) Cert. Ed. CGI
   Second Edition 2004
7. AXIS Communications: http://www.axis.com
8. Milestone Systems : http://www.milestonesys.com
9. HID Training Web : iCLASS Technology Basics : http://hidtraining.com
10. Videolarm: http://www.videolarm.com
11. S2 Security Corporation: http://www.s2sys.com
12. Secolarm – ENFORCER: http://www.seco-larm.com
13. Magnetic Autocontrol: http://www.ac-magnetic.com
14. Pelco: http://www.pelco.com