

DISEÑO Y EJECUCIÓN DE LA INFRAESTRUCTURA CCTV Y CONTROL DE ACCESO PARA CENTRO DE ATENCIÓN AL CLIENTE SITEL

YURI VANNESA SANTAMARIA SANDOVAL

Universidad de Cundinamarca
Ingeniería electrónica
Facultad de ingeniería
Fusagasugá, Colombia,
2020

DISEÑO Y EJECUCIÓN DE LA INFRAESTRUCTURA CCTV Y CONTROL DE ACCESO PARA CENTRO DE ATENCIÓN AL CLIENTE SITEL

Trabajo de grado presentado como requisito parcial para optar por el título de ingeniero electrónico

YURI VANNESA SANTAMARIA SANDOVAL

Director:

Leonardo Rodríguez

Codirector:

Nora Katuska Smith Carreom

Línea de investigación:

Software, sistemas emergentes y nuevas tecnologías

Universidad de Cundinamarca

Ingeniería electrónica

Facultad de ingeniería

Fusagasugá, Colombia

Año

Resumen

En este documento nos centramos en el desarrollo de los sistemas de seguridad de videovigilancia y control de acceso en el proyecto Sitel piso 7, para el sistema CCTV fueron instaladas 40 cámaras IP ubicadas estratégicamente alrededor del piso buscando el mayor porcentaje de cobertura para cada una de las áreas y cuartos existentes. El sistema implementado trabaja mediante tecnología IP, lo que le permite al usuario acceder a la información recolectada en tiempo real desde cualquier servidor conectado a la red en cualquier parte del mundo. Por otra parte, fue implementado un sistema de control de acceso para el personal y visitantes del establecimiento que cuenta con seguridad en 10 de las puertas encontradas al interior del piso, el sistema cuenta con un conjunto de dispositivos de identificación de usuario, manejo de permisos y operatividad en caso de emergencia con la liberación de espacios y activación de alarmas.

Contenido

Resumen	10
1. Capítulo. Contexto	14
2. Capítulo. Actividades	15
2.2. Actividades adicionales	15
3. Capítulo. Marco de referencia.....	16
3.1. Antecedentes	16
3.1.1. Sistemas de seguridad CCTV.....	16
3.1.2. Sistemas de control de acceso	17
3.2. Fundamentos Teóricos.....	18
3.2.1. Sistemas de seguridad CCTV.....	18
3.2.2. Sistemas de control de acceso	27
4. Capítulo. Plan de trabajo	32
4.1.1. Diseño de infraestructura de red para el sistema de seguridad CCTV	32
4.1.2. Distribución de elementos de sistema de seguridad CCTV	32
4.1.3. Montaje del sistema en AutoCAD sistema de seguridad CCTV:	33
4.1.4. Diseño de infraestructura de red para el sistema de control de acceso	35
4.1.5. Distribución de elementos sistema de control de acceso	37
4.1.6. Montaje de sistema en AutoCAD sistema de control de acceso	37
4.1.7. Cálculo de longitudes de cableado CCTV y Control de acceso.....	38
4.1.8. Acompañamiento en instalación de infraestructura CCTV y Control de acceso	39
4.1.9. Acompañamiento en instalación de cableado CCTV y Control de acceso	40
4.1.10. Instalación de equipos sistema de seguridad CCTV	40
4.1.11. Configuración de dispositivos CCTV.....	41
4.1.12. Instalación de equipos para el sistema de control de acceso	43
4.1.13. Configuración de equipos sistema de control de acceso	44
5. Capítulo. Análisis de resultados	46
6. Referencias.....	47

Índice de figuras

Ilustración 1 Sistema de vigilancia IP	19
Ilustración 2 Sistema de vigilancia análogo	19
Ilustración 3. Esquema básico cámara IP.....	22
Ilustración 4. Diagrama comunicación NVR en red	26
Ilustración 5 Infraestructura de red para el sistema de seguridad CCTV.....	32
Ilustración 6 Cobertura del Sistema de seguridad CCTV	34
Ilustración 7 Configuración de ángulo y línea de vista de las cámaras para el sistema de seguridad CCTV	34
Ilustración 8 Rutas de cableado del Sistema de seguridad CCTV	35
Ilustración 9. Infraestructura de red sistema de control de acceso	36
Ilustración 10 Cobertura Sistema de control de acceso	38
Ilustración 11 Plano arquitectónico del piso	39

Índice de tablas

Tabla 1. Niveles de resolución cámaras IP	22
Tabla 2. Tipo de compresión tecnología IP	24
Tabla 3. Tecnologías ethernet.....	25
Tabla 4. Clases de potencia POE según la norma 802.3af.....	25
Tabla 5. Tipos de almacenamiento sistema de seguridad IP	26
Tabla 6. Diagrama sistema de control de acceso autónomo	27
Tabla 7. Diagrama sistema de control de acceso IP	28
Tabla 8. Frecuencias RFID y características.....	29
Tabla 9 Listado de distribución de elementos sistema de seguridad CCTV	33
Tabla 10 Dispositivos sistema de seguridad CCTV.....	33
Tabla 11 Listado de distribución de elementos sistema de control de acceso.....	37
Tabla 12 Dispositivos sistema de control de acceso	37
Tabla 13. Longitudes de cableado y tubería para los sistemas de seguridad	38
Tabla 14. Características de red.....	41
Tabla 15. Tipos de configuración IP.....	41
Tabla 16. Nombre de identificación de dispositivos de video Sitel piso7	43
Tabla 17. ID módulos control de acceso	44
Tabla 18. Credenciales de usuario Sitel piso7	45

1. Capítulo. Contexto

Los sistemas de seguridad permiten realizar un seguimiento constante de diferentes áreas o espacios de forma sincronizada mediante técnicas de monitoreo. Un ejemplo de esto son los sistemas electrónicos CCTV o de redes, que mediante el uso de técnicas de video vigilancia pueden detectar y visualizar los espacios deseados por el usuario mediante el uso de dispositivos capaces de identificar rostros, patrones de comportamiento, placas, números de identificación, entre otras características. Además, es posible la visualización y grabación en tiempo real de las imágenes, así como la exportación y reproducción de información recolectada por el sistema previamente.

Podemos sumar a este tipo de sistemas el control de acceso, que mediante la identificación de usuarios y la gestión de permisos puede hacer un seguimiento a los individuos vinculados identificando sus movimientos al interior de un establecimiento. Además, pueden asociarse a los sistemas de detección y extinción de incendios, contando con alarmas y herramientas de liberación de puertas de emergencia siendo de gran ayuda en casos de emergencia.

SITEL PISO 7 es un proyecto que abarca diferentes áreas de la ingeniería, desde las actividades civiles hasta los sistemas eléctricos y electrónicos, en este documento nos centraremos en el diseño, desarrollo e implementación de los sistemas de seguridad CCTV y control de acceso. El sistema de videovigilancia cuenta con 40 cámaras de tipo digital ubicadas de forma estratégica al interior del piso. El sistema al ser de tipo digital permite visualizar la respuesta de los dispositivos conectados a la red mediante su dirección IP, por lo cual el cliente podrá observar en tiempo real lo que esté ocurriendo en el piso.

Por otra parte, el piso cuenta con 27 puertas de las cuales 10 son controladas mediante el sistema de control de acceso ubicadas en el Lobby principal, salidas de emergencia, área de producción, cuartos técnicos UPS e IDF y cuarto de entrenamiento. Cada uno de estos espacios cuenta con dos puertas controladas de forma automática mediante electroimanes, quienes sólo responden a la señal de las tarjetas lectoras, los dispositivos breakglass o los botones de apertura, además se cuenta con una base de datos en la cual se programan los permisos para cada individuo, teniendo en cuenta su cargo y responsabilidades.

2. Capítulo. Actividades

Las actividades de tipo ingenieril que serán desarrolladas se enfocarán en los sistemas de seguridad CCTV y control de acceso para el piso siete del proyecto SITEL, en el que se incluyen infraestructura, cableado, instalación y configuración de equipos.

2.1. Actividades propuestas

- Diseño de infraestructura y red para sistema de seguridad CCTV según normativas y requerimientos de usuario.
- Diseño de infraestructura y red para sistema de control de acceso según normativas y requerimientos de usuario.
- Distribución de elementos según normativas y requerimientos de usuario.
- Cálculo de longitud de cableado para cada sistema.
- Montaje de cada sistema en AutoCAD
- Acompañamiento en instalación de infraestructura y cableado.
- Documentación de montaje e instalación de equipos.
- Acompañamiento den configuración y prueba de equipos en cada sistema.
- Entrega de planos récord.

2.2. Actividades adicionales

- Seguimiento en requerimientos de material para los sistemas de seguridad CCTV y control de acceso
- Seguimiento diario del porcentaje de avance de cada sistema
- Acompañamiento en actividad de certificación sistema de seguridad CCTV
- Acompañamiento y sustentación semanal de porcentaje de avance de los sistemas de seguridad al cliente.

3. Capítulo. Marco de referencia

3.1. Antecedentes

3.1.1. Sistemas de seguridad CCTV

Los sistemas CCTV se refieren a circuitos cerrados de televisión encargados de la transmisión de imágenes en movimiento que sólo pueden visualizarse por un grupo selecto de personas, dependiendo de su aplicación y las necesidades por las que fueron diseñados. Estos sistemas son utilizados para el monitoreo y vigilancia de diferentes espacios como edificios, aeropuertos, zonas residenciales e incluso para la identificación del estado del tráfico y el reconocimiento de vehículos, además, son una herramienta útil para la identificación facial cuando se presentan situaciones que comprometen la integridad de los individuos. [1]

Los primeros sistemas de seguridad CCTV transmitían señales a través de un monitor remoto conectado por medio de cable coaxial, eran sistemas muy rígidos y limitados. Posteriormente fueron desarrollados los secuenciadores que permitían utilizar más de una cámara para la recolección de información y con la ayuda de dispositivos multiplexores fue posible lograr generar un sistema capaz de mostrar las imágenes capturadas por cada cámara de forma simultánea. Con la implementación VHS esta información podía grabarse y reproducirse una y otra vez.

Tiempo después con la aparición de las imágenes digitalizadas estos sistemas pudieron desarrollarse aún más, siendo capaces de grabar la información recopilada de forma automática sin la necesidad de la intervención de un ser humano. Pero existía una problemática, el sistema seguía siendo analógico ya que el dispositivo DVR (grabador de video) poseía una entrada análoga por cada cámara en el sistema. [1]

Con los años se desarrolló un sistema capaz de transmitir imágenes por medio de una red TCP/IP utilizando diferentes medios de transmisión como cableado estructurado o fibra óptica, incluso la misma red wifi. El grabador de video para estos sistemas fue denominado NVR, el cual no era necesariamente parte del sistema, es decir que podía accederse a las cámaras de forma remota por medio de un servidor online mediante el cual la información requerida por el usuario era almacenada. El dispositivo NVR sólo era utilizado en caso de que fuera necesaria la visualización y grabación simultánea de la información captada por las cámaras. [1]

Con todo esto se desarrollaron las cámaras IP, las cuales poseen una memoria interna que puede guardar la información recopilada, además de alcanzar un nivel de calidad de la imagen superior en comparación con las de origen analógico. Este tipo de cámaras permiten que el sistema trabaje

más rápido, evitando sobrecargas de la red debido a la cantidad de información manejada, dando como resultado un sistema de seguridad con características más detalladas, como el cubrimiento de áreas extensas, con una capacidad de reconocimiento más sofisticada pudiendo identificar rostros, matriculas de automóviles e incluso el nombre en una tarjeta de usuario.

3.1.2. Sistemas de control de acceso

Los sistemas de control de acceso se encargan de restringir selectivamente el acceso a un lugar o espacio físico, a través de herramientas que permiten identificar de forma automática al usuario. Para realizar este proceso son asignados permisos y derechos de accesos al personal vinculado al sistema, la forma de identificación puede variar dependiendo del tipo de control implementado, puede realizarse a partir de un número de ID o contraseña hasta utilizando datos biométricos donde el sistema responde a las características físicas de los individuos.

Los sistemas para la prevención del control de acceso no autorizado han evolucionado notablemente en última década, desde sus inicios han dado un vuelco hasta llegar a lo que hoy día conocemos como sistemas electrónicos sofisticados, capaces de monitorear constantemente un espacio asignado e identificar si su integridad o seguridad se puede ver afectada por algún tipo de individuo [2].

En sus primeras aplicaciones el control de acceso se mostró con tarjetas de identificación en las cuales se imprimía un código de barras que era reconocido por una máquina y de este modo se hacía un monitoreo del usuario, aunque no tuvo mucho éxito ya que podían falsificarse con facilidad. Lo que dio paso a las tarjetas de banda magnética, capaces de almacenar un número de identificación dentro de una pista designada que se leía a partir de un lector magnético, quien se encargaba de determinar el número de la pista mediante un proceso de inducción electromagnética.

Todo esto llevó a la necesidad de generar un sistema más sofisticado y confiable, fue allí donde la tecnología de radiofrecuencia aparece con las tarjetas de proximidad, quienes internamente traen incorporada una antena que permite que el lector identifique la información almacenada simplemente con acercarla a unos cuantos centímetros. A raíz de esto surgió una tecnología de radio similar, menos robusta en la que las tarjetas ahora llamadas tarjetas inteligentes, cuentan con un chip en el que pueden almacenarse una variedad de datos que pueden leerse o escribirse en la tarjeta mediante el uso de lectoras o escritoras, según la necesidad del usuario. Gracias a esta tecnología cada persona es identificada en el sistema mediante un código personal e intransferible, lo que obliga al individuo a movilizarse junto con su tarjeta de acceso a las diferentes áreas de la instalación donde deba desplazarse, además mediante el software de control pueden manejarse los permisos de acceso de cada persona teniendo en cuenta su cargo y responsabilidades[2].

A los sistemas de control de acceso se suman los lectores biométricos que, mediante la identificación de características humanas únicas como huellas dactilares, iris y rostro pueden identificar a los usuarios sin necesidad de portar una credencial, los datos del usuario son almacenados en el sistema al igual que sus rasgos físicos y la identificación se hace con ayuda de dispositivos electrónicos, que mediante sensores ópticos intuitivos identifican rápidamente el sujeto, así mismo mediante el software de control se asignan los permisos y restricciones específicas para cada usuario.

Una nueva alternativa de control son las credenciales virtuales, donde las tarjetas de identificación son reemplazadas por un teléfono inteligente, cada individuo cuenta con un código de identidad unipersonal que es enviado de forma segura a través de una aplicación móvil haciendo uso de medios de comunicación integrados al teléfono como bluetooth, tecnología NFC o códigos QR. La eficiencia del sistema dependerá estrictamente de las capacidades de la unidad lectora y del tipo de teléfono inteligente que se utilice. Este tipo de alternativas permiten que los sistemas sean cada vez más flexibles, fiables y sofisticados, permitiendo asegurar la integridad de los usuarios e instalaciones[2].

3.2. Fundamentos Teóricos

3.2.1. Sistemas de seguridad CCTV

La necesidad de protección que tienen las personas y el afán por mantener bajo vigilancia sus activos físicos han llevado a las empresas, campus educativos y almacenes a sumergirse en busca de sistemas de seguridad flexibles, adaptables y eficientes, que sean capaces de brindar la protección y seguridad que están buscando. Esta demanda tecnológica ha llevado al desarrollo de sistemas de seguridad con mayor autonomía, más precisos y escalables que permiten el monitoreo de casi cualquier espacio.

En este grupo podemos encontrar los sistemas de videovigilancia CCTV o circuitos cerrados de televisión que han evolucionado en tecnología como en diseño, adaptándose según sus aplicaciones y escenarios a las necesidades del usuario, como es el caso de la tecnología de videovigilancia IP que está creciendo rápidamente y su implementación se hace cada día más fuerte[3].

a. ¿Qué es un sistema CCTV?

Un sistema CCTV se refiere a circuito cerrado de televisión encargado de la transmisión de imágenes en movimiento que sólo pueden visualizarse por un grupo selecto de personas a

diferencia de la televisión abierta o pública [1], dependiendo de su aplicación y las necesidades por las que fueron diseñados.

b. Video vigilancia IP

La vigilancia IP es un término utilizado para definir los sistemas de seguridad que brindan al usuario la capacidad de monitorear, grabar y almacenar información de audio y video mediante una red con base en un protocolo de internet. Los sistemas de vigilancia IP sencillos cuentan con una cámara de red, un conmutador de red y un servidor para la administración de la información recolectada. Muy diferente a los sistemas analógicos quienes utilizan una conexión física punto a punto desde cada dispositivo hasta el servidor. La vigilancia IP utiliza la tecnología de red IP para transportar la información hacia cualquier ubicación en la que el usuario se encuentre conectado a la red para su visualización, permitiendo un sistema de monitoreo y grabación desde cualquier lugar con posibilidad de acceso a la red [4].

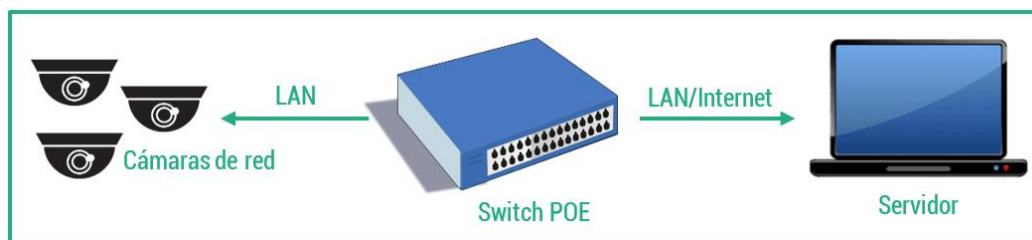


Ilustración 1 Sistema de vigilancia IP

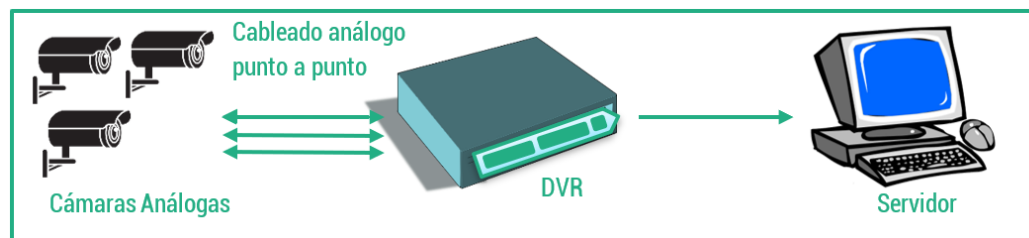


Ilustración 2 Sistema de vigilancia analógico

Los sistemas de videovigilancia analógicos son portadores de señales que viajan en un único sentido, mientras los sistemas IP pueden tanto transmitir como recibir información, el usuario puede recibir una respuesta de video de los dispositivos al igual que generar instrucciones para que el sistema ejecute una acción. Además, le es posible mantener una comunicación en paralelo y dar respuestas a diversas tareas como detección de movimientos, identificación de individuos, envío de secuencias de video, bloqueo de áreas o activación de alarmas, lo que le convierte en un sistema con gran flexibilidad y posibilidad de escalamiento [4].

c. Sistema de video vigilancia IP

Un sistema de vigilancia IP básico cuenta con un conmutador que permite la conexión y comunicación de diferentes dispositivos en el sistema, además de un cableado ethernet desde el dispositivo de video hacia el conmutador y del conmutador al servidor grabador y/o reproductor de video [4]. El equipo o cámara de video se conecta a la red y una vez configurada es posible que el usuario visualice y almacene la información recolectada con la ayuda de un navegador, ya sea en una computadora local o remota vía internet, si se requiere recolectar información simultanea de varios dispositivos puede adaptarse un equipo de grabador de video en red.

d. Beneficios de la tecnología IP

- **Acceso remoto:** Permite que se realice la visualización de la información recolectada en vivo o almacenada desde prácticamente cualquier ubicación con acceso a la red, lo que permite que los usuarios autorizados puedan ingresar desde cualquier parte del mundo. El caso contrario sucede en los sistemas analógicos que sólo puede monitorearse en un espacio específico adaptado con un codificador para lograr la visualización las secuencias de vídeo [4].
- **Imágenes de alta calidad:** En un sistema de seguridad la calidad de la captura es muy importante, ya que es gracias a esta característica que es posible visualizar con claridad un incidente en proceso, así como identificar objetos o individuos relacionados. La respuesta de la tecnología IP presenta grandes ventajas frente la analógica, debido a que | 0 en un sistema análogo la imagen pierde calidad en los procesos de conversión requeridos, así como con en la distancia del cableado, mientras que en un sistema digital la información se digitaliza una vez y la imagen permanece de esta manera sin perder calidad en el proceso [4].
- **Integración sencilla:** Los dispositivos de video con base en estándares abiertos pueden integrarse fácilmente a sistemas informáticos, sistemas de audio y seguridad, aplicaciones y softwares de manejo, así como con otros dispositivos digitales. Una cámara de red puede asociarse a un software que puede realizar una integración de video con un sistema de venta o realizar un estudio de las capturas y el sonido para identificar individuos dentro de una multitud en áreas de acceso restringido [4].
- **Escalabilidad y flexibilidad:** Un sistema de video IP se adapta a los requerimientos del usuario, brindando la posibilidad de ampliar los productos de video y realizar una

modificación en su infraestructura sin presentar cambios abruptos o costos elevados. Permite la conexión de otros productos en red desde casi cualquier lugar, permitiendo que el sistema se tan amplio o sencillo como se desee [4].

- **Gestión de eventos y video inteligente:** Las cámaras de red y codificadores de video permiten identificar la información útil recolectada por el sistema de seguridad reduciendo el impacto de búsqueda proporcionando respuestas programadas. Estos dispositivos en su infraestructura incorporan alarmas de detección de audio, alarmas de manipulación, conexiones de entrada y salida para la gestión de eventos, entre otros. Tener este tipo de dispositivos con inteligencia incorporada minimiza el uso del ancho de banda y optimizan el almacenamiento, siendo portadores sólo de datos procesables a través de la red [4].

e. Cámara de red:

Existe una amplia gama de cámaras y codificadores de video, en las que pueden encontrarse cámaras de red fijas, panorámicas, con inclinación, zoom PTZ, domos, entre otras. Cada una con características únicas que pueden adaptarse a diferentes espacios y necesidades. Estos dispositivos ofrecen características muy variadas y un número amplio de capacidades como por ejemplo: Secuencias de video mediante diferentes formatos de compresión que se encuentran optimizados para mejorar el ancho de banda y calidad de la imagen capturada; puertos de entrada y salida para la conexión de otros dispositivos de seguridad como sensores o sirenas; tecnología inteligente para la identificación de factores como el movimiento o detección de elementos específicos; gestión de sucesos y comunicación continua con aplicaciones simultaneas; tecnología POE permitiendo la alimentación del dispositivo y el intercambio de información a través de un mismo puerto [1].

Las tecnologías digitales actuales permiten desarrollar dispositivos IP con niveles de resolución más altos a escala de megapíxeles, por lo cual se han ido generando nuevos estándares de resolución y es posible ofrecer al usuario un equipo con características mejoradas, flexible y capaz de trabajar en escenarios bajo condiciones variables o desfavorables del ambiente.

Formato de resolución	N° Megapíxeles	Píxeles
SXGA	1.3 megapíxeles	1280x1240
SXGA – (EXGA)	1.4 megapíxeles	1400x1050
UXGA	1.9 megapíxeles	1600x1200
WUXGA	2.3 megapíxeles	1920x1200
QXGA	3.1 megapíxeles	2048x1536
WQXGA	4.1 megapíxeles	2560x1600
QSXGA	5.2 megapíxeles	2560x2048

Tabla 1. Niveles de resolución cámaras IP

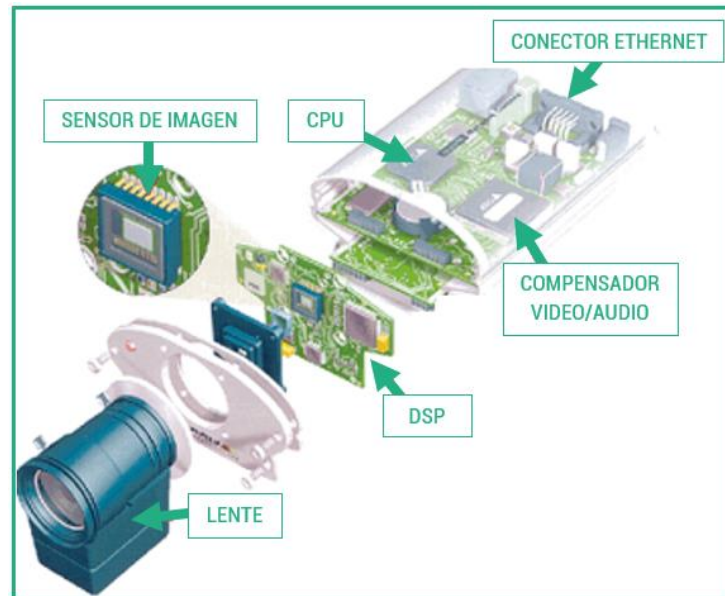


Ilustración 3. Esquema básico cámara IP

- ❖ **Lente:** se encarga de determinar la escena que se visualiza en el servidor mediante la distancia o longitud focal (distancia que existe entre el sensor de la imagen y el centro de la lente.), así como de controlar la cantidad de luz que recibirá el sensor. Existen tres tipos de lentes clasificados en: lentes fijas, lentes vari focales y lentes zoom motorizadas. En el caso de las lentes fijas es necesario realizar un cálculo preciso que nos permita trabajar en el área seleccionada, mientras que las lentes de tipo vari focal ofrecen al usuario la capacidad de modificar la longitud focal y acoplarla a las diferentes escenas con que cuenta el sistema de seguridad CCTV, permitiendo mayor flexibilidad en comparación con el anterior [1].

Otra variable importante que se debe tener en cuenta es la corrección IR, luz que no es perceptible por el ojo humano pero que afecta el porcentaje de exactitud de la imagen, por lo que este tipo de elementos traen incorporado un filtro que se encarga de eliminar o minimizar los impactos de esta luz en el sensor. Por último, encontramos las lentes zoom motorizadas quienes brindan al usuario la posibilidad de ajustar el valor de distancia focal realizando zoom de forma remota a través del servidor principal de la red CCTV, pudiendo capturar detalles de forma inmediata obteniendo respuesta en tiempo real de lo que se desea capturar, además de contar con un iris encargado de controlar la magnitud de la luz que recibirá la cara de cada uno de los sensores en el dispositivo [1].

- ❖ **Sensor de imagen:** Para el desarrollo de estos dispositivos existen dos tipos de tecnologías denominadas CCD (Charge Coupled Device) o CMOS (Complementary Metal Oxide Semiconductor) quienes trabajan mediante un mismo principio, ordenados en forma de matrices en la que se acumula la carga eléctrica dando como resultado los pixeles de la imagen. La magnitud de esta variable dependerá estrictamente de la cantidad de luz recibida por el sensor, el valor de la carga es directamente proporcional a la magnitud de luz incidente, en el caso de los dispositivos CMOS se cuenta con un amplificador interno en cada célula mientras que en el caso contrario este elemento debe ser externo y tiene una relación común con todas las células [1].

- ❖ **Procesador:** La imagen es enviada al procesador una vez el sensor la digitaliza, terminado el procesamiento es enviada al ciclo de compresión, mediante el procesamiento de la imagen es posible mejorar la calidad de la captura aplicando diferentes técnicas que permiten ajustar parámetros para obtener una respuesta del sistema más acertada. Entre las técnicas utilizadas podemos encontrar: ajuste del control de tiempo de exposición, ajuste de iris y ganancia, magnitud de luz y rango dinámico, procesamiento del color, minimización o eliminación de ruido mediante filtros, manejo del color y algoritmos mosaicos [1].

- ❖ **CPU:** Es el encargado del control y administración de todas las funciones y características de la cámara, además se encarga de gestionar cada proceso realizado por el dispositivo internamente, intercambio de información, compresión, envío de respuesta al sistema, gestión de avisos o alarmas, entre otros.

- ❖ **Compresión:** La cantidad de información recolectada mediante una captura es muy robusta por lo que una transmisión de imagen o video sin comprimir resulta un problema importante, tal cantidad de información no podría trabajarse a través de una red ya que haría que esta se saturara, por lo que se han desarrollado diferentes algoritmos de procesamiento de señales que permiten trabajar solo con la información relevante, dejando de lado información no útil o nula. Entre los métodos de compresión mayormente utilizados para la tecnología de cámaras IP podemos encontrar: MJPEG, MPEG-4 y H.264 [1].

Método	Definición
MJPEG	Estándar en el que cada fotograma se comprime en forma de imagen JPEG

MJPEG-4	Reúne 27 protocolos y estándares que permiten la codificación y la transmisión de imagen y video en un ancho de banda de 1,5 Mbit/s, es también aplicado para el manejo de dispositivos móviles y TVs
H.264	Este estándar ofrece mayor resolución en comparación con los métodos MJPEG o MPEG-4, trabaja a la misma velocidad y ancho de banda.

Tabla 2. Tipo de compresión tecnología IP

- ❖ **Tarjeta ethernet:** Es el dispositivo encargado de brindar la conexión de red para la transmisión de las capturas mediante la misma.

f. Transmisión:

Los dispositivos del sistema de videovigilancia deben estar conectados a una red que puede ser de tipo LAN o WAN, mediante la cual se realiza la comunicación y el intercambio de recursos. La información es enviada a través de tramos para lo que se utilizan diferentes tipos de tecnología, la más común es la conocida como Ethernet. La transmisión se puede realizar mediante un cableado UTP par trenzado o a través de fibra óptica, en el primer caso la longitud máxima debe ser de 100m, por otra parte, la magnitud de la fibra es mayor, pudiendo encontrarse entre los 10km y 100km, dependiendo de su tipo.

Las redes ethernet se componen de un grupo variado de dispositivos en los que podemos encontrar: tarjetas de red, switches, cableado, repetidores, nodos de red y bridges. Además, existen dos tipos de nodos de red, DTE encargados de dar ruta a la información y DCE, que hace referencia a los equipos intermediarios que enrutan la información para reenviarla hacia diferentes destinos a través de la red. (memoria.pdf)

Tipos de ethernet	Ancho de banda	Tipo de cableado	Duplex	Distancia máxima
10Base-5	10mbps	Coaxial thicknet	Half	500m
10Base-2	10mbps	Coaxial thinnet	Half	185m
10Base-T	10mbps	UTP Cat3/Cat5	Half	100m
100Base-T	100mbps	UTP Cat5	Half	100m
100Base-TX	200mbps	UTP Cat5	Full	100m
100Base-FX	100Mbps	Fibra multimodo	Half	400m
100Base-FX	200mbps	Fibra multimodo	Full	2km
1000Base-T	1Gbps	UTP Cat 5e	Full	100m

1000Base-TX	1Gbps	UTP Cat 6	Full	100m
1000Base-SX	1Gbps	Fibra multimodo	Full	550m
1000Base-LX	1Gbps	Fibra monomodo	Full	5km
10GBase-CX4	1Gbps	Twianxial	Full	15m
10GBase-T	1Gbps	UTP Cat6/Cat7	Full	100m
10GBase-LX4	1Gbps	Fibra multimodo	Full	300m
10GBase-CX4	1Gbps	Fibra monomodo	Full	10km

Tabla 3. Tecnologías ethernet

g. Alimentación:

En el caso de las cámaras IP la alimentación se realiza mediante tecnología POE, la cual permite alimentar los dispositivos a través del cableado de datos, evitando la implementación de un cableado exclusivo para la energización de los equipos. Lo que conlleva a una reducción de costes, un manejo más sencillo en la instalación y mantenimiento de equipos, permitiendo tener un sistema menos robusto. La normativa que rige esta tecnología es la IEEE 802.3af [1].

Clase	Uso	Potencia del PD (W)	Corriente de clasificación (mA)
0	Por defecto	0.44 a 12.95	>5.0
1	Opcional	0.44 a 3.84	10.5
2	Opcional	3.84 a 6.49	18.5
3	Opcional	6.49 a 12.95	28
4	Reservado	12.95 a 25.5	40

Tabla 4. Clases de potencia POE según la norma 802.3af

h. Grabación

Los dispositivos de almacenamiento son importantes en un sistema de videovigilancia IP, ya que es a través de ellos que se realiza el manejo de la información recolectada, dado la posibilidad al usuario de grabar, monitorear y administrar de datos recopilados por el equipo.

Almacenamiento en la cámara IP	Almacenamiento en servidor PC	Almacenamiento en dispositivo NVR
Se utiliza la memoria interna del equipo que puede ser SD o USB, permitiendo sólo horas de grabación. Se utiliza para transmisiones de video en una ventana de tiempo específica.	Mediante un software de control se almacena la información en la memoria interna del equipo, quien determina la cantidad de datos que pueden ser almacenados. Generalmente es utilizado en sistemas de seguridad sencillos para el	Un dispositivo NVR ofrece un soporte de grabación amplio, puede conectarse a un servidor mediante el que puede visualizarse la respuesta en tiempo real de cada cámara, realizar movimiento, acercamiento, zoom y demás acciones que permita el dispositivo de

	monitoreo de áreas pequeñas.	video. El equipo se conecta a la red y puede intercambiar información con otros equipos. Es implementado en lugares donde se maneja una cantidad importante de datos.
--	------------------------------	---

Tabla 5. Tipos de almacenamiento sistema de seguridad IP

- ❖ **Grabador NVR:** Es un dispositivo utilizado para la grabación y reconocimiento de la información proporcionada por un sistema de seguridad CCTV IP, el cual permite al usuario el acceso y almacenamiento de la información de video en red, así como su visualización, reproducción y búsqueda [5].

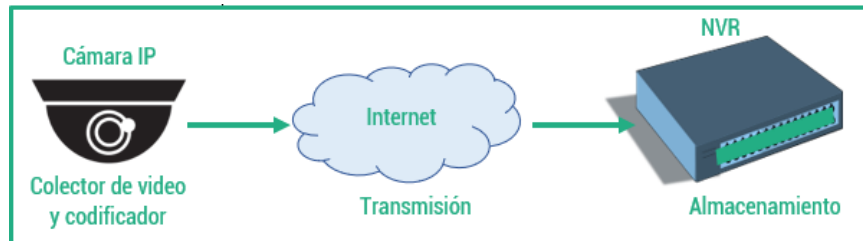


Ilustración 4. Diagrama comunicación NVR en red

Características:

- Manejo de Domos PTZ.
- Canales de Video: 4/8/12/20/40 ch.
- Entradas 1/2LAN.
- Grabación: MJPEG / MPEG4 / H.264.
- Backup: Via USB (2/4), eSata.
- Conexión: TCP/IP.
- Discos Duros: Hasta 2/6HDD de 3TBc/u.
- Alimentación: 220V.
- Incluye: Software de monitoreo remoto de hasta 120ch.

3.2.2. Sistemas de control de acceso

a. Control de acceso autónomo

Un sistema de seguridad de este tipo se encarga de controlar un punto único de acceso, es un sistema pequeño que funciona a partir de un dispositivo lector conectado a una base de datos en la que se establecen las credenciales para el usuario, de este modo se otorga o deniega el permiso de ingreso. Este tipo de sistemas no ofrecen una trazabilidad o interconexión con otros sistemas afines, por lo que sus aplicaciones son muy reducidas, generalmente aplicados a espacios que requieren un nivel de seguridad bajo o medio [6].

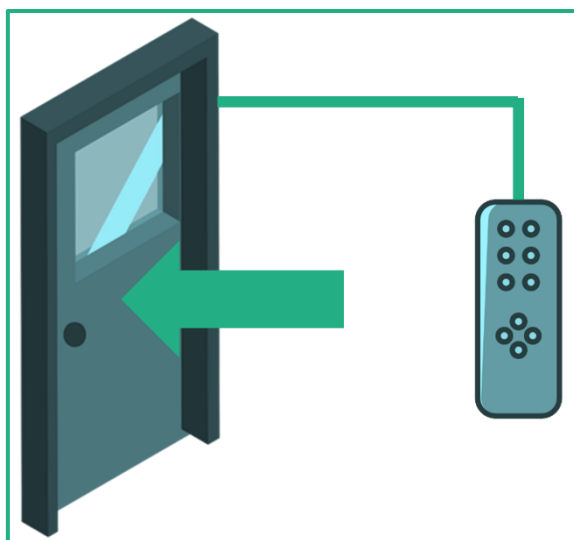


Tabla 6. Diagrama sistema de control de acceso autónomo

b. Control de acceso en red

Los sistemas de seguridad en red se componen de un conjunto de lectoras conectadas mediante una red LAN o WAN, además de un servidor que hace de dispositivo de control central y sirve para monitorear en tiempo real la actividad del sistema, pudiendo almacenar datos como fecha de ingreso, hora de entrada y salida de cada área de supervisión. Este tipo de sistemas permiten asignar o cancelar permisos de forma inmediata según sea requerido por el usuario, en caso de que un individuo pierda su credencial esta puede desactivarse de forma remota con facilidad. Son escalables y pueden asociarse a otros tipos de sistemas de seguridad como detección temprana, detección de incendios, sistemas de videovigilancia, entre otros. Son utilizados generalmente en establecimientos con un flujo constante de personas, en el que cada una cuenta con permisos específicos e intransferibles [6].

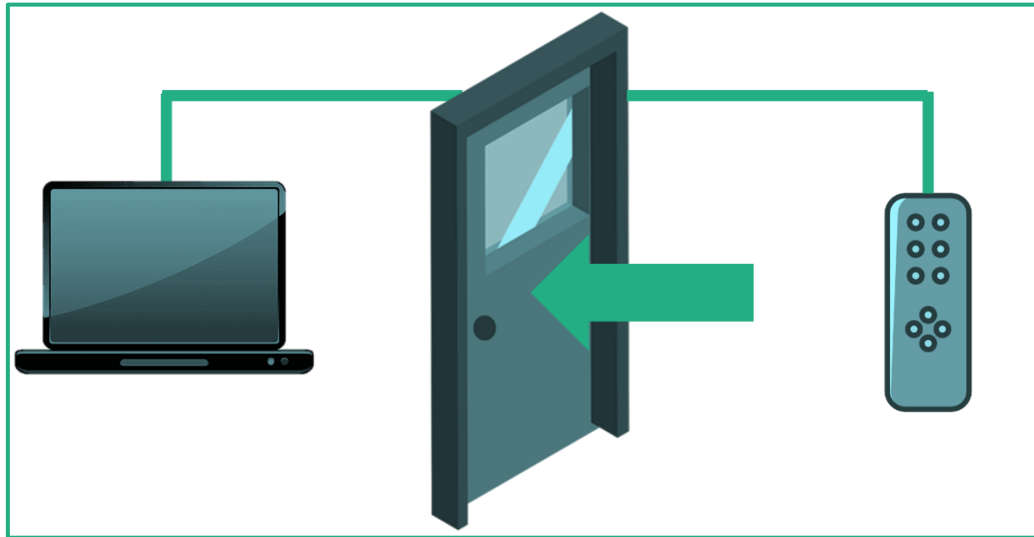


Tabla 7. Diagrama sistema de control de acceso IP

c. Tecnología RFID

Este tipo de tecnología permite trabajar con diferentes rangos de radiofrecuencia con el fin de monitorear o recibir información mediante un transmisor y un receptor sin la necesidad de existir un contacto directo, estos sistemas cuentan con dos partes fundamentales denominadas etiqueta y lectora. Las etiquetas son dispositivos pequeños que pueden instalarse o adherirse a un elemento en concreto según las necesidades del usuario, internamente contienen una antena que les permite recibir y enviar información conforme sea requerido. Existen dos tipos de etiquetas, pasivas y activas, en el caso de las primeras no se requiere una fuente de alimentación interna, mientras en las etiquetas de tipo activo si es requerida. Una de las principales características de los sistemas RFID es que no requieren que exista una línea de vista limpia entre el emisor y el receptor. Estos sistemas son utilizados para realizar seguimiento, estudio de localización, control de acceso, identificación de personal y trazabilidad para el control de inventarios [7].

Frecuencia	LF 120-134 KHz	HF 13.56 MHz	UHF 850 – 960 MHz
Distancia de lectura	05 - 1m	< 1m	>3m
Costo	Alto	Medio	Bajo
Resistencia al agua	Si	Si	No

Tipo de antena	Bobina inductiva	Bobina inductiva	Dipolo "plancha metálica"
Anticolisión	Pobre	Buena	Muy buena
Aplicaciones	Control de acceso. Identificación industrial, llaves de acceso a vehículos, auto guiado de vehículos	Farmacia, librerías, control de acceso, fidelización, pagos, pasaporte.	Trazabilidad de paquetes, trazabilidad de producto, automatización industrial, control de acceso de vehículos

Tabla 8. Frecuencias RFID y características

d. Partes de un sistema de control de acceso

- ❖ **Módulos:** Existe una gran variedad dependiendo de las necesidades del usuario, entre los que destacan podemos encontrar los módulos de control de acceso Honeywell diseñados para instalaciones de alta densidad, quienes admiten hasta 16 lectores por gabinete y 32 lectoras por controlador inteligente, junto con una capacidad cercana a las 100.000 tarjetas de usuario, permitiendo que el sistema en el que se implementa sea menos robusto, permitiendo disminuir la longitud del área de instalación y una relación costo/puerta favorable para el cliente [8].
- ❖ **Lectora de proximidad:** Este dispositivo se encarga de permitir la comunicación en un sistema de comunicación RFID, envía señales de radiofrecuencia con el objetivo de detectar las etiquetas presentes en una ventana de longitud determinada, permitiendo reconocer múltiples etiquetas en lapsus cortos de tiempo. La distancia máxima que puede existir entre un dispositivo lector y una tarjeta depende estrictamente de la frecuencia de comunicación y la potencia empleada por el lector. Toda la transmisión de datos por radiofrecuencia entre la tarjeta y la lectora es encriptada utilizando algoritmos de seguridad, además para la comunicación con las tarjetas es implementada una llave de autenticación de 64-bit para reducir los riesgos de filtración o copia no autorizada de la información almacenada [7].
- ❖ **Tarjetas, tag o etiquetas:** Es el dispositivo que se encarga del almacenamiento de la información en un sistema de radiofrecuencia, generalmente compuesto de un microchip y un medio acoplador, el primero se activa de forma inmediata cuando reconoce una señal enviada por una lectora dentro de un rango específico. Existen diferentes tipos de etiquetas cuyas características varían dependiendo de su aplicación.

- 1) **Pasiva:** reciben las señales enviadas por los lectores induciendo una corriente mínima que activa el circuito interno y permite enviar una respuesta rápida a la lectora. Está compuesta por un microchip y una antena, es un dispositivo muy pequeño que puede implementarse en forma de adhesivo y su alcance va desde los 10cm hasta unos pocos metros de distancia.
 - 2) **Activa:** Este tipo de etiquetas internamente cuentan con una fuente de alimentación encargada de la activación del microchip y la antena transmisora, logrando una comunicación con la lectora tras el envío de una señal hacia el dispositivo. Gracias a esta característica son tarjetas más fiables a comparación con las etiquetas pasivas, ya que al tener la capacidad de comunicarse de forma independiente se reduce el porcentaje de generación de errores, les es posible trabajar en ambientes complicados y su rango de comunicación va hasta los cientos de metros.
 - 3) **Semi-pasiva:** Estos dispositivos cuentan con una fuente de energía interna encargada de la alimentación solamente del microchip, por otra parte, la antena transmisora utiliza la energía generada por la lectora para enviar las señales requeridas por el usuario. El contar con una fuente interna le permite alcanzar un rango de cobertura mayor en comparación con un dispositivo pasivo, además de tener una respuesta en tiempo más rápida [7].
- ❖ **Software:** El software de manejo RFID es denominado Middleware, es el encargado de recibir la información recolectada por la lectora, es quien recopila la información, filtra los datos recibidos para descartar aquellos que no pertenecen al sistema, genera alertas de movimiento, seguimiento de tarjetas y almacenamiento de historial de usuarios [7].
 - ❖ **Breakglass:** es un dispositivo utilizado para la liberación de una puerta controlada mediante un sistema de seguridad en casos de emergencia, la acción se ejecuta por el breakglass una vez se realiza presión en el vidrio central, liberando la puerta tras un movimiento seguro ya que esta área es protegida por una capa plástica [9].
 - ❖ **Electroimán:** Este elemento funciona mediante el campo magnético generado por un imán, el cual se activa al momento de recibir la magnitud de una corriente eléctrica, sin esta inducción no es posible su funcionamiento por lo que es utilizado para el bloqueo de áreas, ideales cuando se cuenta con un flujo de alto tráfico. Puede implementarse en puertas vidrio, madera y metal, además es posible realizar el monitoreo del dispositivo mediante un control remoto o una aplicación móvil, son escalables ya que pueden interconectarse con otros dispositivos de seguridad como alarmas o mecanismos de emergencia [9].

- ❖ **Contacto magnético:** es el dispositivo que se encarga de permitir o interrumpir el paso de la corriente eléctrica en el circuito de control del sistema de seguridad, interactuando junto con el electroimán para la liberación y apertura de la puerta una vez es identificado y aprobado el usuario [8].

4. Capítulo. Plan de trabajo

4.1. Desarrollo de actividades

4.1.1. Diseño de infraestructura de red para el sistema de seguridad CCTV

Para el proyecto SITEL piso 7 se realizó el diseño de un sistema de seguridad CCTV de tipo digital, con una capacidad de cubrimiento de 40 cámaras, la topología de red diseñada para este proyecto puede observarse en la Ilustración 5. El sistema será completamente digital, por lo que cada dispositivo conectado a la red contará con una dirección IP propia que permitirá observar la respuesta del sistema desde cualquier punto siempre y cuando este se encuentre conectado a la red.

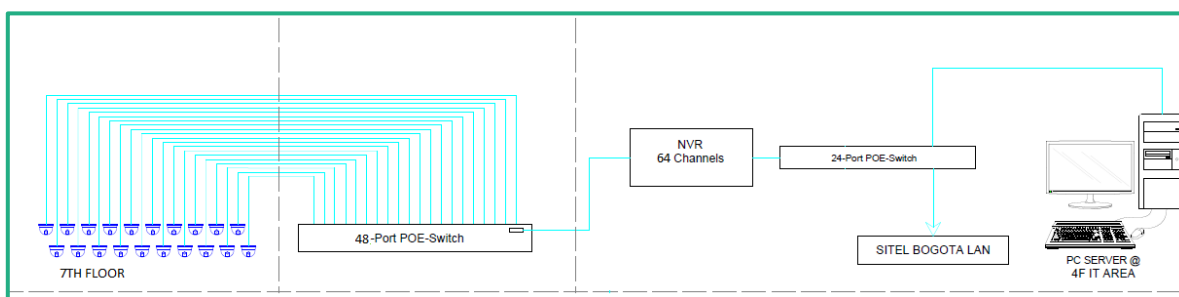


Ilustración 5 Infraestructura de red para el sistema de seguridad CCTV

Las cámaras serán conectadas a un Switch POE de 40 canales, este tipo de dispositivos permiten que la alimentación eléctrica sea suministrada a través del mismo cable de conexión de red, es decir que se utiliza un mismo canal para la alimentación y la transmisión de datos, lo que nos permite tener un sistema menos robusto.

El Switch se conectará a una NVR POE con capacidad de 64 canales, este equipo será el encargado de grabar y administrar la información proporcionada por cada una de las cámaras que compondrá el sistema. Este dispositivo estará conectado a un Switch POE de 24 canales con conexión a la red LAN del establecimiento y al servidor principal que se encuentra ubicado en el piso número 4 del edificio.

4.1.2. Distribución de elementos del sistema de seguridad CCTV

Este sistema contará con 40 cámaras IP que serán ubicadas de forma estratégica al interior del piso con el fin de obtener la mayor cobertura posible, luego de realizar un análisis del espacio en

compañía del ingeniero a cargo mediante una serie de visitas, se determinó que las cámaras serán distribuidas de la siguiente manera:

Área	N° de cámaras
Área recreacional	1
Cuarto técnico IDF	1
Cuarto técnico UPS	1
Cuarto de aprendizaje	1
Cuarto de entrenamiento	2
Cafetería	3
Lobby	1
Pasillo principal Lockers	7
Pasillo cafetería	2
Área de producción	20
Ascensor	1
Total	40

Tabla 9 Listado de distribución de elementos sistema de seguridad CCTV

a) Equipos sistema de seguridad CCTV:

Teniendo en cuenta los requerimientos del cliente y los análisis realizados junto con el ingeniero a cargo de los diferentes proveedores y equipos disponibles en el mercado, se determinó que se implementarán los siguientes dispositivos:

Dispositivo	Referencia	Fabricante
Cámara IP domo	DS-2CD2183G0-I(S) 8 MP	IKVISION
NVR	DS-9600NI-I16	IKVISION
Sistema de video central	HikCentral-VSS-Base/HW/300Ch	IKVISION
Servidor	POWEREDGE R240	DELL EMC
Disco duro	Enterprise capacity 3.5 HDD	SEAGATE

Tabla 10 Dispositivos sistema de seguridad CCTV

4.1.3. Montaje del sistema en AutoCAD sistema de seguridad CCTV:

En el software de diseño AutoCAD fue realizado el montaje de las rutas y la ubicación de los dispositivos, la ilustración 3 nos muestra la distribución de cámaras en cada una de las áreas y cuartos que serán implementados, además, nos permite visualizar la cobertura que tendrá cada dispositivo. Durante el proceso de diseño fueron realizadas varias pruebas de rendimiento del sistema mediante la identificación de la cobertura, Basados en la configuración del ángulo de cada una de las cámaras fue posible identificar el punto de vista óptimo para el dispositivo. Esto permitió mejorar la simulación para tener como resultado un sistema eficaz, con una capacidad de rendimiento alta capaz de cumplir con los requerimientos solicitados por el cliente. El posicionamiento y configuración angular pueden observarse en la ilustración número 6.

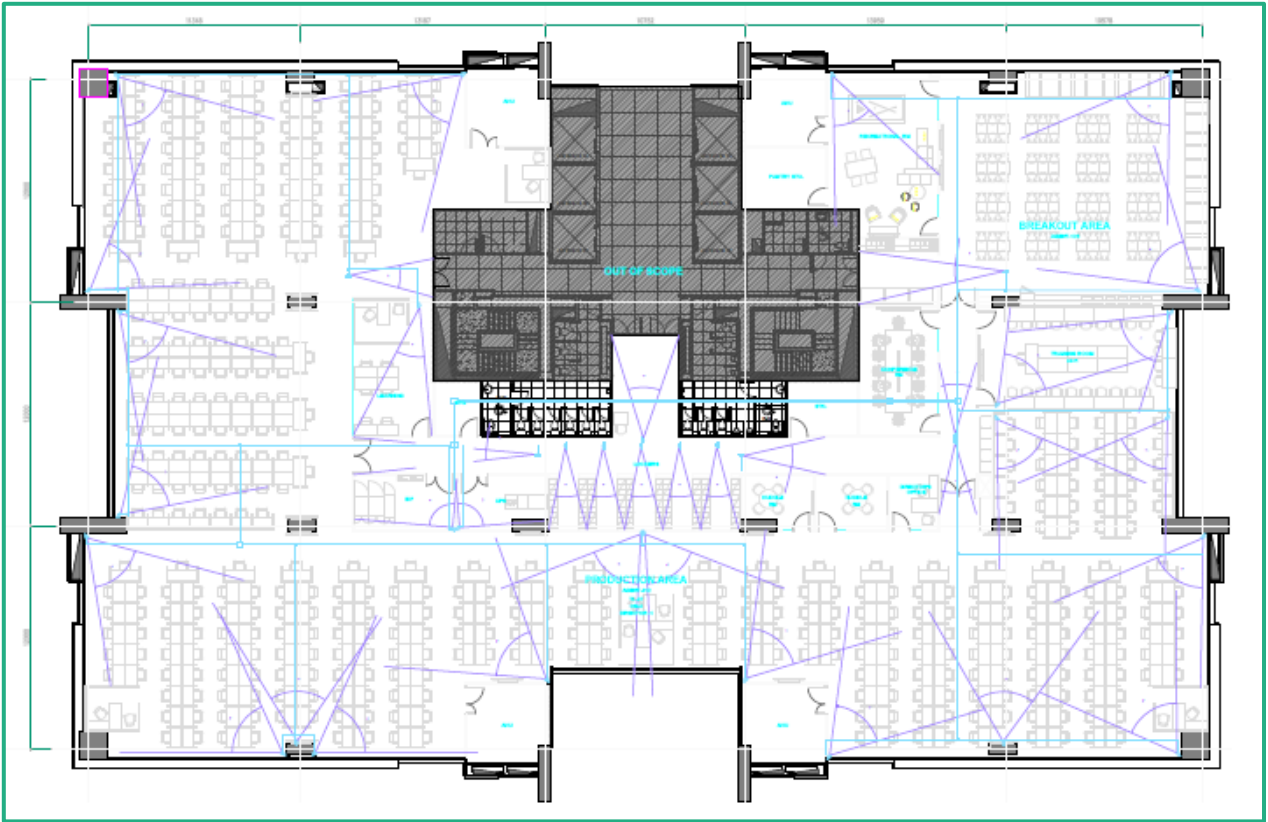


Ilustración 6 Cobertura del Sistema de seguridad CCTV

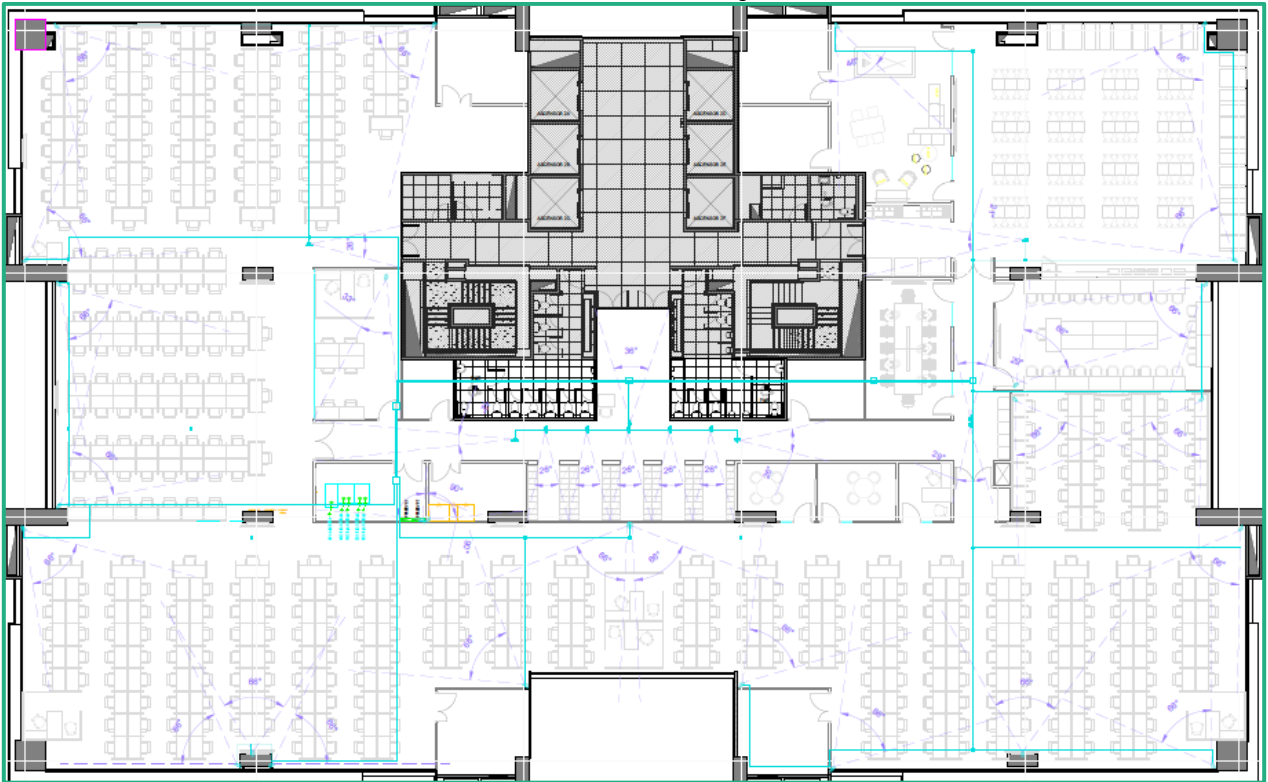


Ilustración 7 Configuración de ángulo y línea de vista de las cámaras para el sistema de seguridad CCTV

En la ilustración número 8 se pueden observar las rutas que se implementaran para el sistema, serán la base para la instalación de la tubería por parte del personal técnico y el proceso de cableado, se contará con cajas de paso para protección del cableado, la hechura de empalmes y derivaciones necesarias, estas serán ubicadas en techos y muros según corresponda.

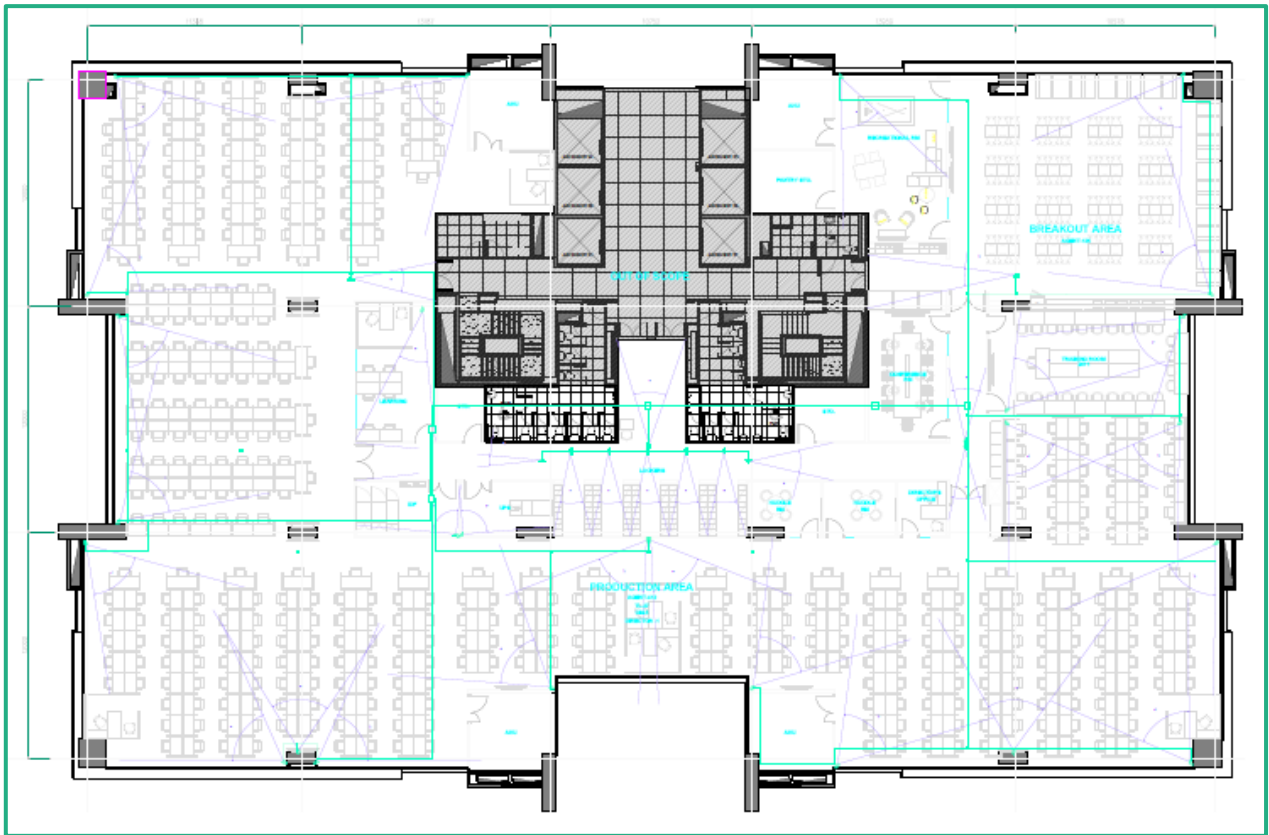


Ilustración 8 Rutas de cableado del Sistema de seguridad CCTV

4.1.4. Diseño de infraestructura de red para el sistema de control de acceso

El sistema de control de acceso que se implementará permitirá realizar el control de cada persona que ingresa al piso desde el momento en que esta abandona el ascensor, Permitiendo el ingreso sólo a personal autorizado. Se instalarán dispositivos de control en la entrada principal al lobby y en los diferentes cuartos al interior del piso siendo los de mayor importancia los cuartos técnicos UPS e IDF. A demás, el piso contará con dos salidas de emergencia en el costado derecho e izquierdo que serán controladas mediante este sistema. La topología que se implementará puede observarse en la ilustración 9.

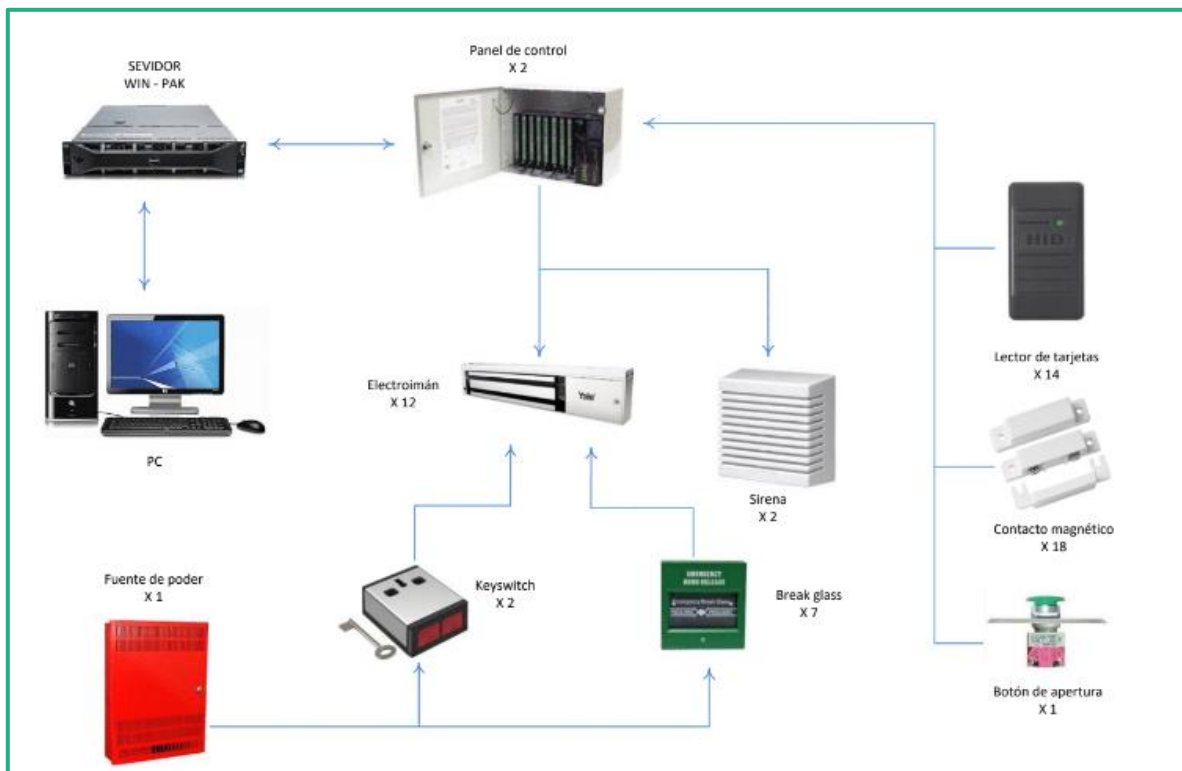


Ilustración 9. Infraestructura de red sistema de control de acceso

Este sistema parte del servidor Win-Pak quien es conectado al panel de control en el que deben conectarse los siguientes dispositivos: electroimanés, breakglasses, botones de emergencia, lectoras, contactos magnéticos, botones de apertura y sirenas. Para este sistema se utiliza una fuente de 12V a 24A para la alimentación de los electroimanés. Los contactos magnéticos son la base del funcionamiento del sistema de intrusión, mediante ellos es posible identificar el estado de las puertas, en caso de que la puerta este abierta se enviará un pulso que activará la sirena, además, permite identificar mediante el panel de control la cantidad de veces que es accionada la puerta.

Los electroimanés se encargan de abrir o cerrar la puerta según sea necesario, se activan a partir de las tarjetas lectoras, los dispositivos breakglass o los botones de apertura. Estos dos últimos dispositivos se encuentran conectados a los electroimanés y si en caso de emergencia son activados, el circuito se abrirá permitiendo al usuario desactivar el sistema de seguridad y salir de forma inmediata.

4.1.5. Distribución de elementos sistema de control de acceso

De las 27 puertas que serán instaladas en el piso 10 de estas serán controladas por este sistema, descartando el uso de control de acceso para entradas de áreas comunes como: baños, cafetería, cuarto de conferencias y oficinas pequeñas. A demás de bodegas y cuartos de almacenamiento que serán controlados por cerradura normal, a diferencia de los cuartos de aire acondicionado que contarán con un sistema de cerradura más complejo. Los espacios en los cuales se instalará el sistema son:

Área	N° de entradas o salidas
Entrada a lobby principal	2
Salidas de emergencia	2
Entradas a área de producción	2
Cuartos técnicos UPS e IDF	2
Cuarto de entrenamiento	2
Total	10

Tabla 11 Listado de distribución de elementos sistema de control de acceso

i. Equipos sistema de control de acceso:

Teniendo en cuenta los requerimientos del cliente y los análisis realizados junto con el ingeniero a cargo de los diferentes proveedores y equipos disponibles en el mercado, se determinó que se implementarán los siguientes dispositivos:

Dispositivo	Referencia	Fabricante
Módulo	PRO3200	Honeywell
Lectora de proximidad	iCLASS® R10	HID
Break glass	DS-K7PEB	IKVISION
Contacto magnético	B-7939WG	Honeywell
Electroimán	350 lb - 600 lb - 1200 lb	YALE
Botones Hold-Up	S-077Q y SS-078Q	ENFORCER
Botón de salida	SD-7201GCPE1Q	ENFORCER
Sirena	SDR15W	DSC

Tabla 12 Dispositivos sistema de control de acceso

4.1.6. Montaje de sistema en AutoCAD sistema de control de acceso

El diseño en AutoCAD desarrollado para el sistema de control de acceso nos muestra los puntos específicos y cuartos en que será implementado, se observan los botones de emergencia, apertura y lectoras. Este fue realizado en compañía del ingeniero residente y configurado para las entradas y salidas especificadas por el cliente. Este sistema no cuenta con un plano de rutas para

instalación de tubería ya que para el proceso de cableado será utilizada la misma que se implementará para el sistema de seguridad CCTV.

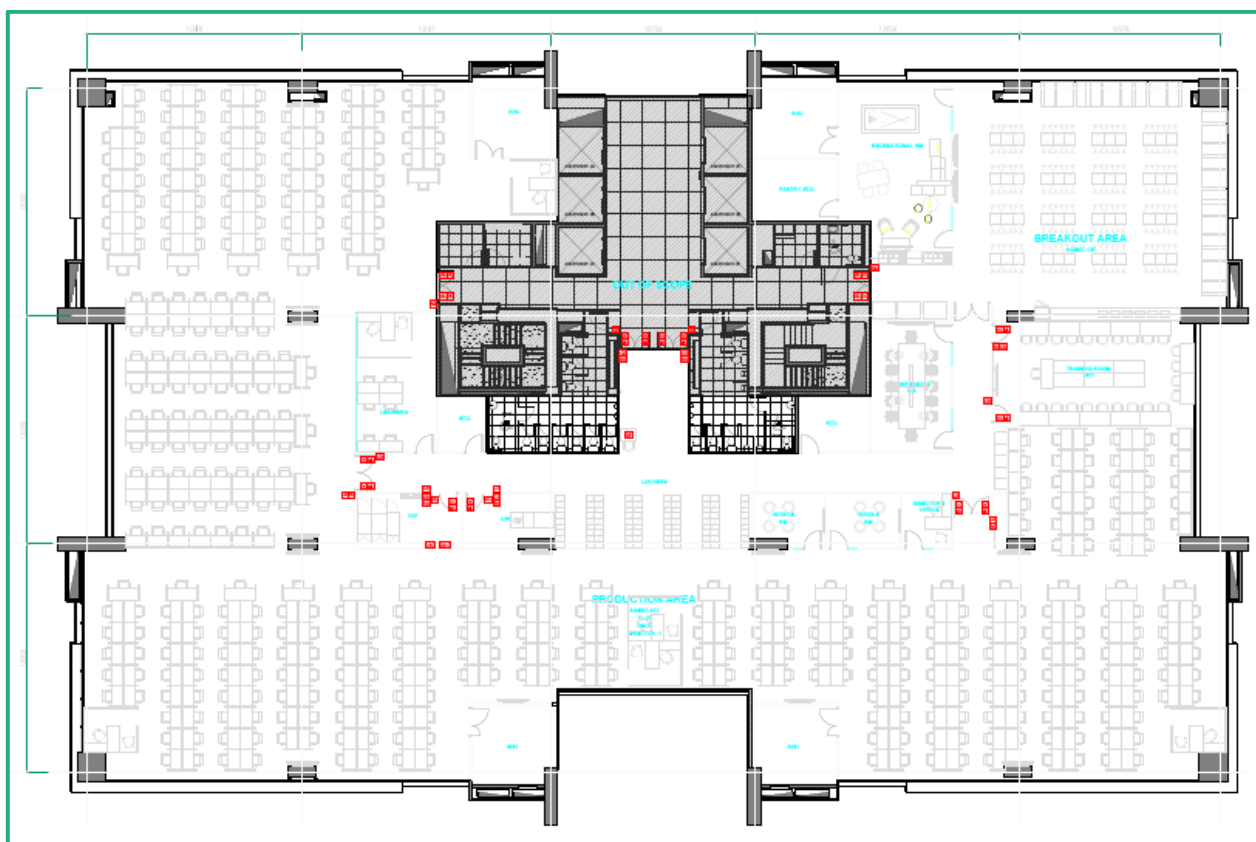


Ilustración 10 Cobertura Sistema de control de acceso

4.1.7. Cálculo de longitudes de cableado CCTV y Control de acceso

Para realizar el cálculo de longitudes se hace uso del software AutoCAD, utilizando la herramienta de medición puede calcularse la cantidad de tubería que será instalada, esto es posible debido a que el plano se encuentra acotado con las longitudes reales del piso. Para establecer la cantidad de cableado que será necesario hacer un cálculo de porcentajes teniendo en cuenta la tubería a instalar, la longitud del cable será 10% mayor a este valor.

Elemento	Longitud (m)	Longitud de cableado (m)
Dimensión del piso	133x37	-
Tubería CCTV	391	430
Tubería control de acceso	279	307

Tabla 13. Longitudes de cableado y tubería para los sistemas de seguridad

4.1.8. Acompañamiento en instalación de infraestructura CCTV y Control de acceso

Para iniciar el proceso de instalación de tubería es necesario que se hayan realizado en el piso los diferentes procesos de área civil, inicialmente se hace una actividad denominada cobertura de concreto, que se refiere a una base de concreto que debe aplicarse a lo largo del piso para realizar un engruese de la superficie. Este proceso es seguido del cimbrado y marcación para la construcción de la primera cara de los muros y divisiones, una vez se hayan hecho las marcas se hace el levantamiento de muros en drywall o superboard según corresponda.

Finalizadas estas actividades se da entrada a la instalación de tubería de los diferentes sistemas, en este caso los sistemas de seguridad CCTV y control de acceso. En la ilustración 11 puede observarse el diseño del piso y la ubicación de los muros y divisiones que se encuentran en proceso de instalación, la parte sombreada corresponde a la infraestructura existente en el edificio.

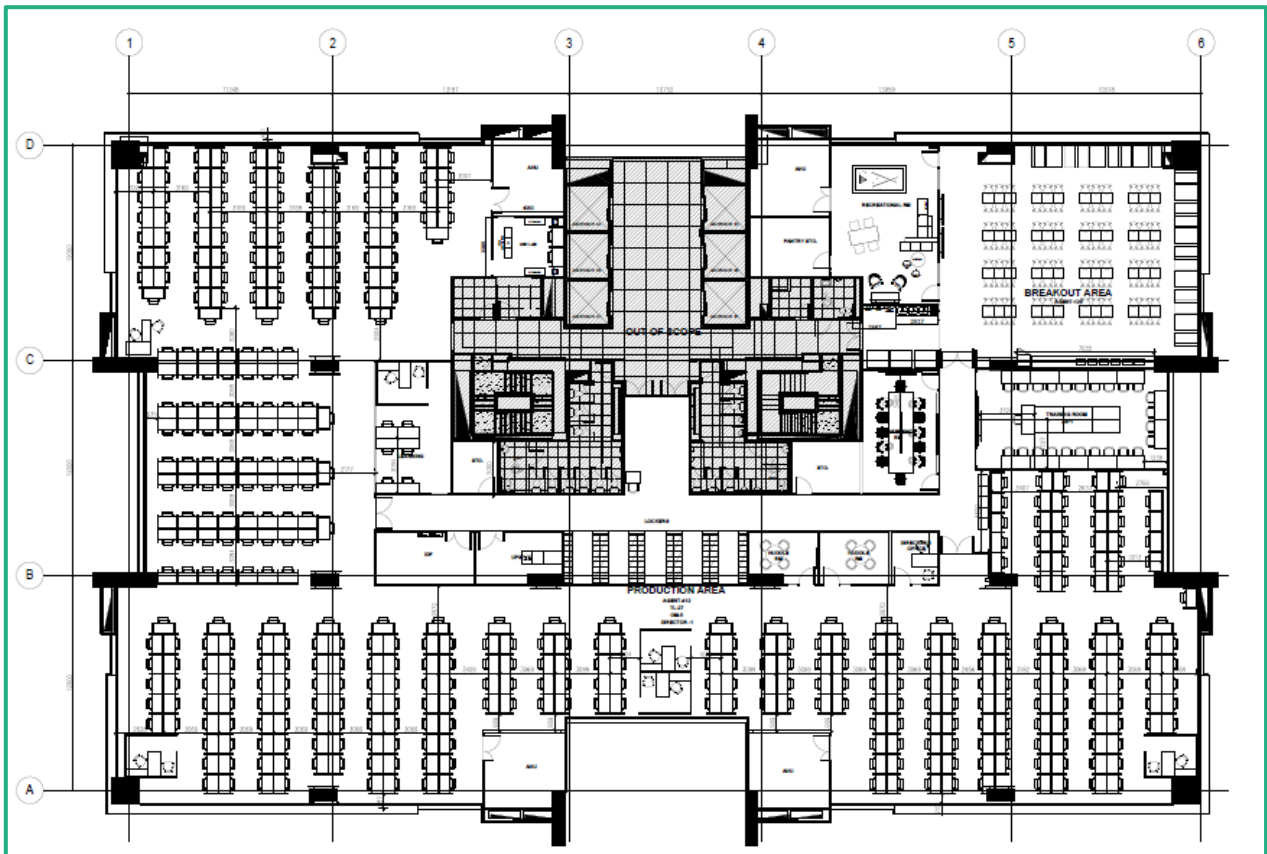


Ilustración 11 Plano arquitectónico del piso

El proceso de instalación de tubería se inició una vez obra civil dio por sentadas las actividades que nos precedían, para realizar la instalación de tubería en muros fueron necesarias las actividades de apertura de regatas para adecuación de la tubería. Para los sistemas de seguridad

CCTV y control de acceso se realizaron regatas en los muros existentes de los costados norte y sur de la recepción.

El personal técnico inició el proceso de tendido de tubería en techo en las diferentes áreas que componen el piso y ayudados de obra civil se realizaron las perforaciones en muro para el paso de tubería. Este proceso exige que sean realizadas como mínimo dos visitas diarias a la obra para revisar el avance de la instalación de cada sistema.

4.1.9. Acompañamiento en instalación de cableado CCTV y Control de acceso

Una vez se dio por terminado el proceso de instalación de tubería, el área civil inició con el remate de muros y regatas, proceso acompañado de la instalación de la segunda cara de drywall. En paralelo se dio inicio al proceso de montaje del cableado para los sistemas de seguridad CCTV y control de acceso. El cableado fue tendido en su totalidad para la fecha planteada por el cliente, no fue necesario realizar cambios de infraestructura o movimientos adicionales.

La instalación se realizó partiendo del área de producción en la que se encuentra la mayor cantidad de puntos, seguida del pasillo principal y cuartos técnicos, finalizando en el área noroccidental del piso en el que se encuentran los cuartos de cafetería, área recreacional y bodega. El cableado llega al cuarto técnico IDF en el que se ubica el rack de seguridad donde deberá organizarse y peinarse para la instalación de los equipos. En las áreas en que se ubicarán las cámaras el cableado se deja en punta al interior de una caja 10x10 doble fondo para la posterior instalación de los equipos, además se cuenta con cajas cuadradas 2400 de paso que pueden ser intervenidas en caso de fallos en el sistema de seguridad CCTV o de control de acceso.

4.1.10. Instalación de equipos sistema de seguridad CCTV

Para iniciar con el proceso de instalación de equipos es necesario el montaje del rack de seguridad, este fue ensamblado en el cuarto técnico IDF junto a los gabinetes del sistema de datos. Para la alimentación de este dispositivo es necesaria una toma L5 30P (Toma de seguridad 110V/30A), este tipo de alimentación es requerido debido a que todos los equipos activos del dispositivo son alimentados mediante una PDU (Unidad de distribución de energía), quien cuenta con un supresor de picos de tensión y ayuda a proteger los equipos al interior del gabinete.

Adicionalmente debe hacerse la puesta a tierra del equipo, proceso realizado mediante un cable número 6 que llega al barraje a tierra o TGB del rack y es conectado a la puesta a tierra de la acometida principal del piso. Además, se cuenta con un equipo UPS en caso de una caída de tensión o problemáticas en la línea de energía.

Una vez instalado el rack de seguridad se inició el proceso de instalación de los dispositivos de video en este caso cámaras de red de domo fijo IR de 8 MP marca IKVISION.

4.1.11. Configuración de dispositivos CCTV

Para realizar la configuración del sistema de seguridad CCTV se hace necesario que el cliente Sitel entregue la VLAN con que se trabajará, una vez se tiene esta información se selecciona un rango de IP para trabajar dependiendo la cantidad de cámaras a configurar, en este caso 40 dispositivos. Por motivos de seguridad y cláusulas del uso de la información no puede compartirse la dirección utilizada en el proyecto SITEL piso7, por lo que utilizaremos un ejemplo para dar una pauta de la actividad de configuración realizada.

Ítem	Dirección IP
VLAN (Ejemplo)	10.29.205.1
Mascara de red	254 /255.255.255.0
Rango de IP para cobertura de 40 Cámaras	10.29.205.50 a 10.29.205.90

Tabla 14. Características de red

Una vez seleccionado el rango de IPs se realiza la configuración cámara por cámara con una dirección estática, esto por exigencia del cliente para reforzar la seguridad en el sistema, puesto que la asignación de IPs dinámicas reduce esta posibilidad. Los dispositivos son conectados a un Switch tipo POE que se encarga de su alimentación y administración para realizar la comunicación entre las cámaras y la NVR. Esta asignación de IP para los dispositivos de video puede realizarse a través de dos medios:

Medio	Configuración
Switch administrable	Se realiza la conexión con el servidor (PC) y se hace la configuración mediante comandos de asignación de IP
Inyector	Mediante el inyector se ingresa a la dirección IP del dispositivo asignada de fábrica, que en cuanto a los dispositivos Ikvision es 192.168.0.68, se configura el rango de IPs a trabajar en el servidor y se realiza la asignación mediante el browser

Tabla 15. Tipos de configuración IP

Finalmente se realiza la comunicación física entre el Switch y la NVR mediante el puerto LAN 1 del dispositivo, además se realiza la conexión por Patch core del puerto LAN 2 de la NVR a un Switch local que se comunica con el servidor principal del edificio. El software para la configuración de NVR Ikvision se denomina IVMS2400, una vez instalado el software se debe establecer un nombre

de usuario y contraseña que puede ser de tipo código o patrón digital como en los dispositivos móviles. Al ingresar el dispositivo por default reconoce todas cámaras que se encuentran configuradas y conectadas al Switch, allí se realiza el nombramiento de cada uno de los dispositivos según el requerimiento del usuario, a continuación, se observa el listado de cámaras y su respectivo nombre de identificación.

Dispositivo	Nombre
Cámara 1	Recreational_Room1
Cámara 2	IDF_Room1
Cámara 3	UPS_Room1
Cámara 4	Learning_Room1
Cámara 5	Training_Room1
Cámara 6	Training_Room2
Cámara 7	Cafeteria_1
Cámara 8	Cafeteria_2
Cámara 9	Cafeteria_3
Cámara 10	Reception_Room1
Cámara 11	Locker_1
Cámara 12	Locker_2
Cámara 13	Locker_3
Cámara 14	Locker_4
Cámara 15	Locker_5
Cámara 16	Locker_6
Cámara 17	Locker_7
Cámara 18	Cafeteria_H1
Cámara 19	Cafeteria_H2
Cámara 20	Production_A1
Cámara 21	Production_A2
Cámara 22	Production_A3
Cámara 23	Production_A4
Cámara 24	Production_A5
Cámara 25	Production_A6
Cámara 26	Production_A7
Cámara 27	Production_A8
Cámara 28	Production_A9
Cámara 29	Production_A10
Cámara 30	Production_A11
Cámara 31	Production_A12
Cámara 32	Production_A13
Cámara 33	Production_A14
Cámara 34	Production_A15
Cámara 35	Production_A16

Cámara 36	Production_A17
Cámara 37	Production_A18
Cámara 38	Production_A19
Cámara 39	Production_A20
Cámara 40	Elevator_A1

Tabla 16. Nombre de identificación de dispositivos de video Sitel piso7

Una vez reconocidas y configuradas las cámaras en el software se ajustan los cuadros de visualización, en los que el usuario podrá percibir toda la información recolectada por la cámara, el software además permite manejar y variar las magnitudes de luz, brillo, nitidez, entre otras variables, que mejoran la calidad de la imagen capturada. Es posible configurar la cámara para funcionar de forma constante o sólo cuando se percibe movimiento gracias al sensor intrínseco en el dispositivo, en Sitel piso7 se seleccionó una grabación de tipo constante, además, de realizar una configuración en los dispositivos de luz nocturna para obtener una mejor respuesta del sistema en caso de variaciones abruptas de la iluminación. Una vez configurados los parámetros requeridos para cada dispositivo de forma Manual debe configurarse la distancia focal, que será quien determinará la línea de visión y área de cobertura fija de los dispositivos.

4.1.12. Instalación de equipos para el sistema de control de acceso

Para la instalación de los equipos de control de acceso se instaló en el rack de seguridad la controladora, dispositivo encargado del manejo y configuración de cada uno de los elementos que componen el sistema. A esta controladora es conectado de forma física mediante un cableado de tipo UTP un módulo por cada puerta que deberá ser controlada, a cada uno de los módulos deben conectarse los dispositivos que componen capa puerta los que corresponden a: magnético, lectora de entrada, lectora de salida, electroimán y contacto magnético sencillo. La conexión entre el módulo y los dispositivos se hace de forma independiente, instalando una línea de cableado para cada uno de los elementos.

Debido al consumo energético de los electroimanes que es de aproximadamente 300mA fue necesario instalar una fuente de alimentación externa para compensar la carencia energética exigida por el sistema, la fuente instalada fue de 12V a 10A.

Para la instalación del key switch fue instalado un interruptor en el área del lobby para permitir el ingreso al personal a través de la puerta principal, este interruptor se encarga de abrir el circuito del electroimán evitando el paso de la corriente eléctrica generando la des-energización del dispositivo permitiendo la apertura de la puerta. Por último, se realizó la instalación del dispositivo break glass el cual es conectado directamente al electroimán para en caso de emergencia liberar de forma inmediata la puerta una vez el usuario presiona el botón.

4.1.13. Configuración de equipos sistema de control de acceso

Para realizar la configuración de los equipos del sistema es necesario contar con el software Winpack programado mediante el servidor y la controladora, inicialmente se reconocen los módulos correspondientes a cada una de las puertas que serán manejadas en el piso, a continuación, se hace un listado de los nombres de identificación de cada módulo instalado.

Ítem	ID Módulo
1	Reception_D1
2	Reception_D2
3	Emergency_Out1
4	Emergency_Out2
5	WE_A1
6	WE_A2
7	UPS_1
8	IDF_1
9	Trainig_D1
10	Training_D2

Tabla 17. ID módulos control de acceso

Una vez identificados los módulos se realiza la configuración de las lectoras, en donde se define si estas serán de entrada o salida, además también es posible configurar el tiempo de encendido de la alarma generada por el electroimán en caso de que una puerta permanezca abierta durante un lapsus de tiempo constante. Una vez configurados estos parámetros se da paso a la configuración de los permisos de acceso para los usuarios. El software permite realizar la discriminación de áreas dependiendo del cargo del personal y de su actividad en el piso, cada tarjeta de acceso es configurada mediante su código serial que es único e intransferible. En la tabla número () podemos observar los permisos manejados en el piso por requerimiento y exigencia del cliente.

ítem	Credencial	Permisos de ingreso
1	Administrativos	Áreas comunes Cafetería Cuarto de reuniones Área de producción
2	Servicios generales	Áreas comunes Cafetería Bodega de mantenimiento
3	Maestra	Todas las áreas

4	Entrenadores	Áreas comunes Cuartos de entrenamiento Cafetería Área de producción
5	IT	Cuarto técnico UPS Cuarto técnico IDF Bodega de almacenamiento técnico
6	Guardas	Áreas comunes Cafetería
7	Visitante	Áreas comunes

Tabla 18. Credenciales de usuario Sitel piso 7

5. Capítulo. Análisis de resultados

Las cuarenta cámaras que conformarían el circuito CCTV para el monitoreo del piso 7 fueron instaladas con éxito, la configuración realizada se hizo en compañía del ingeniero residente junto con el personal de seguridad a cargo del edificio debido a las políticas de manejo de la información y políticas de privacidad internas. De igual manera fueron instaladas con éxito las 10 puertas para el sistema de control de acceso junto con los equipos de acción para emergencia, alarmas y botones para liberación de puertas, además de un sistema de alarma de seguridad para el control del tiempo de apertura de las puertas. La configuración del sistema de igual manera se realizó en compañía del Landlord y el director de seguridad, se establecieron las credenciales y permisos especiales para cada usuario teniendo en cuenta su cargo y responsabilidades.

Los sistemas de seguridad tanto CCTV como de control de acceso ofrecen una gran ventaja al cliente ya que le permite monitorear las actividades desarrolladas durante cualquier momento del personal activo en sitio, así como de las personas que ingresan a realizar actividades específicas ya sea de visita o mantenimiento. El manejo de credenciales para el control de acceso le permite identificar los movimientos de cada una de las personas en piso, horarios de movilidad, ingreso, salida o tiempos de permanencia. Esto enlazado con el sistema de videovigilancia le brinda la satisfacción de poder estar en constante relación con las actividades desarrolladas gracias al monitoreo remoto que ofrece la tecnología IP.

Los sistemas de seguridad de este tipo son fácilmente escalables, ya que pueden adaptarse a diferentes ambientes, en el caso del monitoreo de edificios y zonas cerradas, pueden interconectarse con sistemas de alarma mediante la detección de intrusos e incluso con los sistemas de detección o extinción de incendios, permitiendo no sólo monitorear el usuario sino estar un paso adelante en el cuidado de su seguridad y bienestar.

Para el desarrollo de un sistema de seguridad CCTV o control de acceso se debe tener en cuenta que el diseño parte de los requerimientos del cliente y los manejos de marca que se desean, una vez son establecidos estos parámetros se selecciona la topología y tecnología con que se trabajara, ya que la configuración de los dispositivos depende en gran medida de su fabricante. En el caso de los sistemas cerrados de televisión se aconseja el uso de la tecnología IP ya que proporciona un sistema menos robusto y escalable, además de permitir al usuario la posibilidad de monitorear sus espacios siempre y cuando se encuentre conectado a la red WIFI desde cualquier parte del mundo.

6. Referencias

- [1] S. M. Martí, «Diseño de un sistema de televigilancia sobre IP para el edificio CRAI de la Escuela Politécnica Superior de Gandía,» Universidad Politecnica de Valencia, p. 53, 2013.
- [2] A. Clutton, «The evolution of access control systems,» PSI, p. 2, 2018.
- [3] D. L. J. I. Surveillance, IP Surveillance 101.
- [4] A. Communucations, «IP-Surveillance design guide,» Communucations, AXIS, nº 32.
- [5] IKVISION, «Programa de certificación CCTV,» IKVISION, nº 357, 2016.
- [6] F. C. Patiño, «Diseño y evaluación de la eficacia de un sistema de control de acceso mediante RFID para implementación en entradas a la institución, al servicio de urgencias y cirugía de la IPS Universitaria,» Colombia, Antioquia, 2019.
- [7] A. L. David Montoya, «DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO,» 2016.
- [8] HONEYWELL, «HONEY WEEL PRO3200 MODULE».
- [9] ISOPTIC, «SISTEMA DE CONTROL DE ACCESO SITEL 165 PISO 7 (BOGOTA),» Colombia, Bogotá DC, 2020.