DISEÑO DE UN SISTEMA DE VIDEOVIGILANCIA POR MEDIO DE REDES LAN PARA LA ALCALDÍA DEL MUNICIPIO DE COPER BOYACÁ

DEYVIN JOAN ORJUELA CASTILLO

UNIVERSIDAD COOPERATIVA DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTRÓNICA
SECCIONAL BOGOTÁ D.C.
JUNIO, 2019

DISEÑO DE UN SISTEMA DE VIDEOVIGILANCIA POR MEDIO DE REDES LAN PARA LA ALCALDÍA DEL MUNICIPIO DE COPER BOYACÁ

DEYVIN JOAN ORJUELA CASTILLO

MONOGRAFIA DE GRADO
Trabajo para optar al título de Ingeniero Electrónico

Fabian Blanco Garrido

UNIVERSIDAD COOPERATIVA DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTRÓNICA
SECCIONAL BOGOTÁ D.C.
JUNIO, 2019

TABLA DE CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

RESUMEN

En la Alcaldía municipal de Coper cuenta con más de 50 funcionarios, los cuales requieren de este sistema de videovigilancia para mejorar la calidad de vida de las personas brindando seguridad en el conjunto, ya que se puede ver lo que está pasando en tiempo real.

Se debe obtener los datos para ver cuantas cámaras pueden ser necesarias en la alcaldía, cuales pueden ser los mejores lugares al momento de hacer su instalación y el presupuesto que se requiere para llevar acabo un proyecto como este.

Al momento de su ejecución no se necesita de mucho tiempo para llevar acabo el montaje de las cámaras y estas tienen muchos años de vida útil.

INTRODUCCIÓN

La presente monografía se refiere al tema de seguridad por cámaras ya que hoy en día se presentan muchos robos ya sea en empresas o en las mismas viviendas y al utilizar estos dispositivos a través de redes LAN estamos promoviendo nuevas tecnologías que en muchos lugares es indispensable y no se es consciente de ello.

Las redes se pueden definir como un grupo de computadores asociados entre sí, que permiten al usuario compartir información, estas redes se interconectan a los dispositivos que en este caso sería cámaras y se transmite para su visualización.

La característica principal es que las redes tienen muchos tipos de aplicaciones como son tiendas virtuales, portales web, entre otros y estas se pueden usar en diferentes proyectos con el fin de mejorar la calidad de vida de las personas ya que cada día la tecnología avanza para facilitar los diferentes problemas que se presentan.

Esta monografía se hace con el interés de aprovechar las redes, ya que son muy utilizadas en el área de las telecomunicaciones y al tratarse de seguridad cada día se presentan más ataques en las diferentes empresas una buena opción son las cámaras están nos brindan seguridad sin estar pendiente de todo lo que pasa a nuestro alrededor.

Capítulo I: Esquematización del Tema

1.1 Descripción del Tema

En la Alcaldía municipal de Coper se hace necesario tener un sistema de seguridad en el cual si se presenta cualquier inconveniente se tiene la destreza de contar con cámaras que nos brinden la información de lo que está pasando sin que las personas estén presentes al momento de presentarse cualquier problema. Al contar con este diseño de la red LAN los habitantes tienen la destreza de ver en tiempo real lo que está pasando y sin errores asegurando una mejor calidad de vida y promoviendo una tecnología que se debe estar usando en este tipo zona.

1.2 Descripción del Problema

En las instalaciones de la Alcaldía aún no se han implementado un sistema de cámaras, lo que hace dejar desprotegida los objetos que se manejan y al presentarse cualquier inconveniente no se tiene un sistema fiable de seguridad que nos brinde una solución.

Muchas personas en la alcaldía pueden presentar conflictos entre ellos ya que si se presenta cualquier robo no se sabría quien fue la persona, esto generaría desconfianza y un entorno de trabajó más irritante al estar pendiente de los objetos de valor.

1.3 Justificación

El presente diseño se hace con el fin de estudiar las redes para sus diferentes aplicaciones en el área de ingeniería, en este caso un sistema de cámaras a través de la red ya que es de vital importancia para la seguridad y vigilancia del edificio. De esta manera seria más organizado el trabajo y a su vez innovando nuevas tecnologías en la alcaldía.

1.4 Objetivos

1.4.1 Objetivo General

Diseñar el sistema de videovigilancia por medio de redes LAN para la Alcaldía del municipio de Coper Boyacá.

1.4.2 Objetivos Específicos

Reunir información de los diferentes componentes de la red.

Analizar la información para su diseño.

Diseñar una red con sus diferentes componentes.

Simular y probar el funcionamiento del mismo.

CAPITULO II. Esquematización Teórica

2.1 Marco Teórico

2.1.1 Concepto de red.

Una red de comunicaciones es un conjunto de nodos que están interconectados a través de un medio de comunicación, que comparten recursos e intercambian información por medio de reglas de comunicación, conocidas como protocolos.

Una red se compone de uno o varios transmisores o receptores que intercambian mensajes e información, para eso deben de utilizar un canal de comunicación el cual puede ser un medio confinado o no confinado.

Figura 1. Redes.
Fuente: https://lapublicidad.net/y-despues-de-la-transformacion-digital/

Una red se compone de uno o varios transmisores o receptores que intercambian mensajes e información, para eso deben utilizar un canal de comunicación el cual puede ser un medio confinado o no confinado. Para efectuar una comunicación exitosa, los nodos conectados a la red, deben tener el mismo idioma o código. Los nodos en una red se basan en protocolos de comunicación comunes para que éstos puedan entenderse. Los protocolos proveen mecanismos de control y verificación de errores, así como control de flujo de la información, entre otras funciones. Los mensajes y la información están en una variedad de formatos, por ejemplo voz, datos y video. Los sistemas que forman los nodos pueden ser computadoras, enrutadores, conmutadores de paquetes, conmutadores telefónicos, puntos de acceso, multicanalizadores, teléfonos, etcétera.

Las redes de los proveedores de servicios de telecomunicaciones por ejemplo, las redes telefónicas y de telefonía celular deben incluir sistemas para operar, monitorear y administrar los recursos de la red. De esta manera, aseguran a sus usuarios servicios con un nivel de calidad que cumpla con la normatividad correspondiente.[1]

2.1.2 Tipos de redes

Al margen de que puedan hacerse por cable estructurado, o por vía inalámbrica, las redes pueden dividirse por su alcance o cobertura. Lógicamente, cuanto mayor sea el espacio que queremos abarcar, más difícil y costosa puede resultar la instalación de cables (de hecho, la instalación de algunas de estas redes serían absurdas e impensables para una gran mayoría de las empresas). En cualquier caso, son las siguientes:

1. RED DE ÁREA PERSONAL (PAN)
Hablamos de una red informática de pocos metros, algo parecido a la distancia que necesita el Bluetooth del móvil para intercambiar datos. Son las más básicas y sirven para espacios reducidos, por ejemplo si trabajas en un local de una sola planta con un par de ordenadores.

Las redes PAN pueden serte útiles si vas a conectar pocos dispositivos que no estén muy lejos entre sí. La opción más habitual, sin embargo, para aumentar el radio de cobertura y para evitar la instalación de cablea estructurado, suele ser la compra de un router y la instalación de una red de área local inalámbrica.

2. RED DE ÁREA LOCAL (LAN).
file0001407535981Es la que todos conocemos y la que suele instalarse en la mayoría de las empresas, tanto si se trata de un edificio completo como de un local. Permite conectar ordenadores, impresoras, escáneres, fotocopiadoras y otros muchos periféricos entre sí para que puedas intercambiar datos y órdenes desde los diferentes nodos de la oficina.

Las redes LAN pueden abarcar desde los 200 metros hasta 1 kilómetro de cobertura.

3. RED DE ÁREA DE CAMPUS (CAN).
Vale, supongamos que tenemos varios edificios en los que queremos montar una red inalámbrica. ¿Qué pasa si el área de cobertura debe ser mayor a los 1000 metros cuadrados? Y no lo digo sólo por las universidades; las instalaciones de los parques tecnológicos, recintos feriales y naves comerciales pueden superar perfectamente esa superficie.

En tal caso, tenemos las redes CAN. Habría varias redes de área local instaladas en áreas específicas, pero a su vez todas ellas estarían interconectadas, para que se puedan intercambiar datos entre sí de manera rápida, o pueda haber conexión a Internet en todo el campus.

4. RED DE ÁREA METROPOLITANA (MAN)
Mucho más amplias que las anteriores, abarcan espacios metropolitanos mucho más grandes. Son las que suelen utilizarse cuando las administraciones públicas deciden crear zonas Wifi en grandes espacios. También es toda la infraestructura de cables de un operador

de telecomunicaciones para el despliegue de redes de fibra óptica. Una red MAN suele conectar las diversas LAN que hay en un espacio de unos 50 kilómetros.

5. RED DE ÁREA AMPLIA (WAN)
red WlanSon las que suelen desplegar las empresas proveedoras de Internet para cubrir las necesidades de conexión de redes de una zona muy amplia, como una ciudad o país.

6. RED DE ÁREA DE ALMACENAMIENTO (SAN)
Es una red propia para las empresas que trabajan con servidores y no quieren perder rendimiento en el tráfico de usuario, ya que manejan una enorme cantidad de datos. Suelen utilizarlo mucho las empresas tecnológicas. En Cisco te cuentan las ventajas de una red SAN.

7. RED DE ÁREA LOCAL VIRTUAL (VLAN)
Las redes de las que hablamos normalmente se conectan de forma física. Las redes VLAN se encadenan de forma lógica (mediante protocolos, puertos, etc.), reduciendo el tráfico de red y mejorando la seguridad. Si una empresa tiene varios departamentos y quieres que funcionen con una red separada, la red VLAN. [2]

2.1.3 Simulador de Redes – Cisco Packet Tracer

Es una herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA, pero bien puede ser usada por cualquier persona que quiera conocer referente al funcionamiento de las redes de datos, lógica del funcionamiento de las redes y pues, comercial a parte, conocer los equipos y configuraciones de los equipos CISCO, el cual es una empresa global principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones líder a nivel mundial.

Esta herramienta (PT) les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Se enfoca en apoyar mejor los protocolos de redes que se enseñan en el currículum de CCNA, el cuál es un certificación muy aceptado a nivel Internacional sobre las redes de datos. [3]

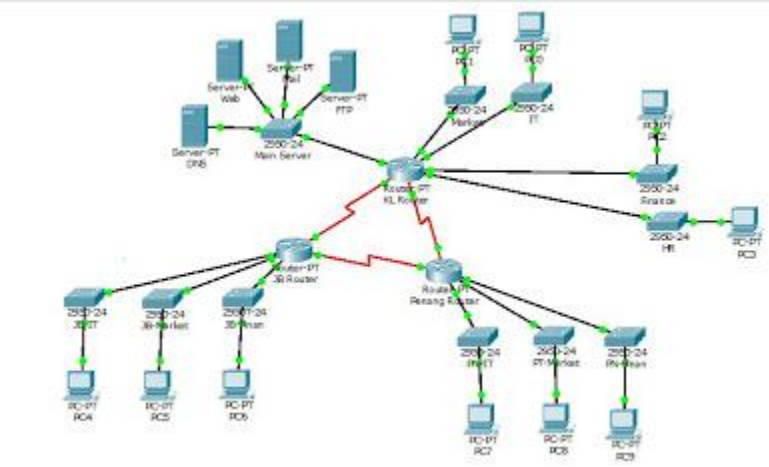


Figura 2. Cisco Packet Tracer
Fuente: http://redes-de-compu.blogspot.com

2.1.4 Componentes de una red

Una red de computadoras está conectada tanto por hardware como por software. El hardware incluye tanto las tarjetas de interfaz de red como los cables que las unen, y el software incluye los controladores (programas que se utilizan para gestionar los dispositivos y el sistema operativo de red que gestiona la red. A continuación se listan los componentes:

Figura 3. Componentes de una red.
Fuente: http://redes-de-compu.blogspot.com

Servidor: este ejecuta el sistema operativo de red y ofrece los servicios de red a las estaciones de trabajo.

Estaciones de Trabajo: Cuando una computadora se conecta a una red, la primera se convierte en un nodo de la última y se puede tratar como una estación de trabajo o cliente. Las estaciones de trabajos pueden ser computadoras personales con el DOS, Macintosh, Unix, OS/2 o estaciones de trabajos sin discos.

Tarjetas o Placas de Interfaz de Red: Toda computadora que se conecta a una red necesita de una tarjeta de interfaz de red que soporte un esquema de red específico, como Ethernet, ArcNet o Token Ring. El cable de red se conectara a la parte trasera de la tarjeta.

Sistema de Cableado: El sistema de la red está constituido por el cable utilizado para conectar entre si el servidor y las estaciones de trabajo.

Recursos y Periféricos Compartidos: Entre los recursos compartidos se incluyen los dispositivos de almacenamiento ligados al servidor, las unidades de discos ópticos, las impresoras, los trazadores y el resto de equipos que puedan ser utilizados por cualquiera en la red. [4]

2.1.5 Seguridad de la red

Figura 4. Seguridad en la red.
Fuente: https://www.networkworld.es/seguridad/que-es-la-seguridad-de-la-red

La seguridad de la red es la práctica de prevenir y proteger contra la intrusión no autorizada en redes corporativas. Como filosofía, complementa la seguridad del punto final, que se centra en dispositivos individuales; la seguridad de la red se centra en cómo interactúan esos dispositivos y en el tejido conectivo entre ellos.

El venerable SANS Institute lleva la definición de seguridad de red un poco más lejos: la seguridad de la red es el proceso de tomar medidas físicas y preventivas para proteger la red subyacente de uso indebido, mal uso, mal funcionamiento, modificación, destrucción o divulgación incorrecta. funciones críticas dentro de un entorno seguro.

Pero el impulso general es el mismo: la seguridad de la red se implementa mediante las tareas y herramientas que utiliza para evitar que personas no autorizadas entren en sus redes. En esencia, su computadora no puede ser pirateada si los hackers no pueden acceder a ella a través de la red.

Conceptos básicos de seguridad de red
Las definiciones son buenas como declaraciones de intenciones de alto nivel. ¿Cómo planeas implementar esa visión? Stephen Northcutt escribió una introducción a los conceptos básicos de la seguridad de la red durante más de una década atrás CSOonline, nosostros nos fijamos en tres fases de la seguridad de la red que deberían ser el marco de referencia base para su estrategia.

Protección: debe configurar sus redes y redes lo más correctamente posible

Detección: debe ser capaz de identificar cuándo ha cambiado la configuración o si algún tráfico de red indica un problema
Reacción: después de identificar los problemas rápidamente, responderlos y regresar a un estado seguro.
Esto, en resumen, es una estrategia de defensa en profundidad. Si hay un tema común entre los expertos en seguridad, es cualquier herramienta defensiva individual puede ser derrotada por un adversario determinado. Su red no es una línea o un punto: es un territorio, e incluso si ha organizado su defensa correctamente.

Métodos de seguridad de red
Para implementar este tipo de defensa en profundidad, hay una variedad de técnicas especializadas y tipos de seguridad de red.

Control de acceso: debe poder bloquear a usuarios y dispositivos no autorizados de su red. Los usuarios que tienen acceso autorizado a Internet solo han sido autorizados para utilizar el sitio web.
Antimalware: virus, gusanos y troyanos por definición de una red, y puede permanecer inactivo en las máquinas infectadas durante días o semanas. Su esfuerzo de seguridad debe hacerse para prevenir infecciones y también para el malware raíz que se dirige a su red.
Seguridad de la aplicación: su red suele acceder a las aplicaciones no seguras. Debe usar hardware, software y procesos de seguridad para bloquear esas aplicaciones.
Análisis de comportamiento: debe saber cómo es el comportamiento normal de la red para poder detectar anomalías o infracciones a medida que ocurren.
Prevención de pérdida de datos: los seres humanos son inevitablemente el enlace de seguridad más débil. Debe implementar tecnologías y procesos para garantizar que los empleados no envíen deliberadamente o inadvertidamente datos confidenciales fuera de la red.
Seguridad del correo electrónico: el phishing es una de las formas más comunes de obtener acceso a una red. Las herramientas de seguridad de correo electrónico pueden bloquear tanto los mensajes entrantes como los salientes con datos confidenciales.
Firewalls: quizás el abuelo del mundo de la seguridad de la red, siguen las reglas de su red o de Internet, estableciendo una barrera entre su zona de confianza y el salvaje oeste. No excluyen la necesidad de una estrategia de defensa en profundidad, pero siguen siendo imprescindibles.
Detección y prevención de intrusos: estos sistemas escanean el tráfico de red para identificar y bloquear ataques.

Movíl y seguridad inalámbrica: los dispositivos inálambricos tienen todos los posibles fallos de seguridad de cualquier otro dispositivo conectado en red. Se puede conectar a casi cualquier red inalámbrica en cualquier lugar, lo que requiere la seguridad extra.

Segmentación de red: la segmentación definida por software en diferentes clasificaciones y facilita la aplicación de políticas de seguridad.

Información de seguridad y gestión de eventos (SIEM): estos productos pretenden reunir información de una variedad de herramientas de red para proporcionar los datos que necesita para identificar y responder a las amenazas.

VPN: Una herramienta (típicamente basado en IPsec o SSL) que autentica la comunicación entre un dispositivo y una red segura, creando un "túnel" seguro y encriptado a través de la Internet abierta.

Seguridad web: debe poder controlar el uso del personal interno para bloquear amenazas basadas en la web del uso de navegadores como vector para infectar su red.

Seguridad de la red y la nube

Cada vez más empresas están desconectadas. cargando algunas de sus necesidades de cómputo a proveedores de servicios en la nube, creando infraestructuras híbridas donde su propia red interna tiene que interoperar de forma fluida y segura con servidores alojados por terceros. A veces esta infraestructura en sí misma es una red autónoma, que puede ser física (varios servidores en la nube trabajando juntos) o virtual (varias instancias de VM ejecutándose juntas y "interconectando" entre sí en un solo servidor físico).

Para manejar los aspectos de seguridad , muchos proveedores de servicios en la nube establecen políticas centralizadas de control de seguridad en su propia plataforma. Sin embargo, el truco aquí es que esos sistemas de seguridad no siempre coincidirán con sus políticas y procedimientos para sus redes internas, y esta falta de coincidencia puede aumentar la carga de trabajo para los profesionales de seguridad de redes. Hay una variedad de herramientas y técnicas disponibles que pueden ayudar a aliviar parte de esta preocupación, pero la verdad es que esta área todavía está en flujo y la conveniencia de la nube puede significar problemas de seguridad para la red.

Software de seguridad de red

Para cubrir todo esas bases, necesitará una variedad de herramientas de software y hardware en su kit de herramientas. Lo mejor son un elemento en su estrategia híbrida de defensa en profundidad. Algunas de estas herramientas son productos corporativos de grandes proveedores, mientras que otras vienen en la forma de utilidades gratuitas y de código abierto. Las categorías principales incluyen: analizadores de paquetes, que ofrecen una visión profunda del tráfico de datos, exploradores de vulnerabilidades como el software de detección y prevención de instrusos. En un entorno donde necesita obtener muchas herramientas para trabajar Juntos, es posible que también desee implementar el software SIEM, que mencionamos anteriormente. Los productos SIEM evolucionaron a partir del software de registro y analizan los datos de red recopilados por varias herramientas diferentes para detectar comportamientos sospechosos en su red. [5]

2.1.6 Cables de par trenzado

Los cables de pares trenzados consisten en dos alambres de cobre, aislados con un grosor de 1 mm aproximado. Los alambres se trenzan con el propósito de reducir la interferencia eléctrica de pares similares cercanos. Los pares trenzados se agrupan bajo una cubierta común de PVC (Policloruro de Vinilo) en cables multipares de pares trenzados (de 2, 4, 8, y hasta 300 pares). Actualmente se han convertido en un estándar en las redes LAN. A pesar que las propiedades de transmisión de cables de par trenzado son inferiores y en especial la sensibilidad ante perturbaciones extremas a las del cable coaxial, su gran adopción se debe al costo, su

flexibilidad y facilidad de instalación, así como las mejoras tecnológicas constantes introducidas en enlaces de mayor velocidad, longitud, etc.

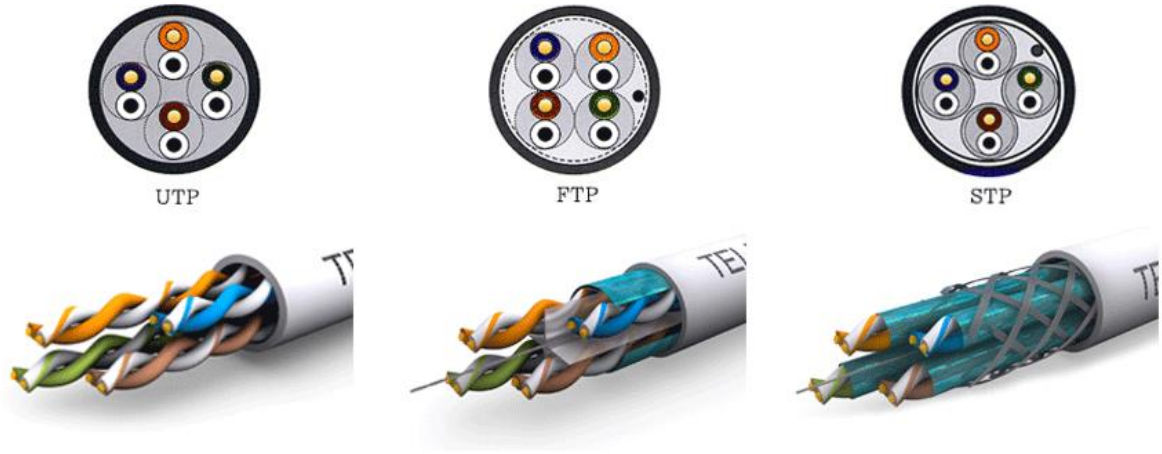


Figura 5. Tipos de Cable de par Trenzado.
Fuente: https://www.telecocable.com/blog/diferencias-entre-cable-utp-stp-y-ftp/1374

Los tipos de cables de par trenzado más usados en las redes LAN son:

Cable UTP (Unshielded Twisted Pair – Par trenzado no apantallado)
Es el cable de pares trenzados más utilizado, no posee ningún tipo de protección adicional a la recubierta de PVC y tiene una impedancia de 100 Ohm. El conector más utilizado en este tipo de cable es el RJ45, parecido al utilizado en teléfonos RJ11 (pero un poco más grande), aunque también puede usarse otros (RJ11, DB25,DB11, entre otros), dependiendo del adaptador de red.
Es sin duda el que hasta ahora ha sido mejor aceptado, por su costo accesibilidad y fácil instalación. Sin embargo, a altas velocidades puede resultar vulnerable a las interferencias electromagnéticas del medio ambiente.

Cable STP (Shielded Twisted Pair- Par trenzado apantallado)
En este caso, cada par va recubierto por una malla conductora que actúa de apantalla frente a interferencias y ruido eléctrico. Su impedancia es de 150 Ohm.
El nivel de protección del STP ante perturbaciones externas es mayor al ofrecido por UTP. Sin embargo, es más costoso y requiere más instalación. La pantalla del STP para que sea más eficaz requiere una configuración de interconexión con tierra (dotada de continuidad hasta el terminal), con el STP se suele utilizar conectores RJ49.
Es utilizado generalmente en las instalaciones de procesos de datos por su capacidad y sus buenas características contra las radiaciones electromagnéticas, pero el inconveniente es que es un cable robusto, caro y difícil de instalar.

Cable FTP (Foiled Twisted Pair- Par trenzado con pantalla global)
En este tipo de cable como en el UTP, sus pares no están apantallados, pero sí dispone de una apantalla global para mejorar su nivel de protección ante interferencias externas. Su impedancia típica es de 120 Ohm y sus propiedades de transmisión son más parecidas a las del UTP. Además puede utilizar los mismos conectores RJ45.

Tiene un precio intermedio entre el UTP y STP.
El EIA/TIA define el estándar EIA/TIA 568 para la instalación de redes locales (LAN). El cable trenzado más utilizado es el UTP sin apantallar. Existen dos clases de configuraciones para los pines de los conectores del cable trenzado denominadas T568A y T568B. [6]

2.1.7 Conector RJ45

El conector RJ45 (Registered Jack) es el principal conector usado en la conexión de tarjetas de red Ethernet. Este conector se emplea con cables de par trenzado, por lo que el mismo conector se puede emplear para tipos de comunicación diferente, dependiendo del orden de conexión de los pares trenzados.

Figura 6. Conector RJ45
Fuente: https://tuelectronica.es/conector-rj45/

El conector RJ45 es un conector estándar de red, que permite la interconexión de dispositivos de red entre sí mediante un cable UTP de 4 pares (8 cables). Existen dos formas de unir estos conectores a los cables:

De forma manual mediante el crimpado con una tenaza.
Mediante un proceso industrial de vacío que fija los contactos y el conector al cable.
Normalmente este conector se fabrica en plástico, y sus conexiones metálicas. Se usa plástico trasparente para los conectores que se unen a los cables de forma manual, de esta forma, se puede visualizar si los pares trenzados se conectan correctamente.

Algunos conectores tienen un recubrimiento metálico utilizado como pantalla electromagnética para evitar interferencias. Estos conectores se utilizan para cables UTP con malla o recubrimiento electromagnético. De esta forma, cuando el conector es crimpado en el cable UTP, el apantallamiento del cable se extiende también hasta el conector. [7]

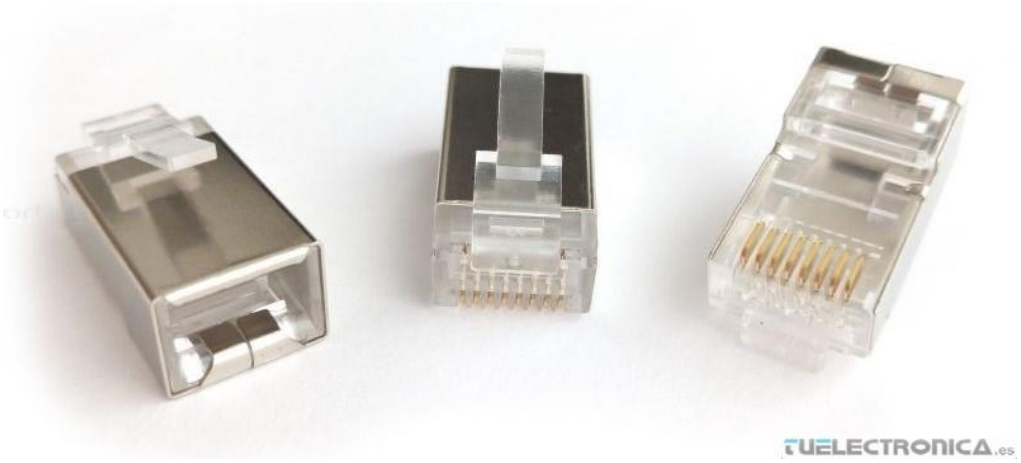


Figura 7. Conector RJ45 apantallado.
Fuente: https://tuelectronica.es/conector-rj45/

2.1.8 Router

Básicamente el router es un dispositivo dedicado a la tarea de administrar el tráfico de información que circula por una red de computadoras. Existen dispositivos específicamente diseñados para la función de router, sin embargo, una computadora común puede ser transformada en un router, tan sólo con un poco de trabajo, conocimiento y paciencia.

En la actualidad, un router puede ser usado para compartir internet, a través de cable, ADSL o WiFi con otras computadoras, proveer protección de firewall, controlar la calidad del servicio y otras varias tareas, principalmente en el ámbito de la seguridad.

Un router Wireless o WiFi nos provee acceso a la red local y a internet de forma inalámbrica a cualquier dispositivo, ya sea notebook, tablet, impresoras, discos de almacenamiento o smartphones que esté dentro del alcance de la señal.

Un router WiFi para el hogar o para pequeñas empresas, generalmente viene equipado de fábrica con 4 puertos para red local por cable (LAN) y un puerto Ethernet para conectar el modem de internet (puerto WLAN). Así, de forma simple, internet se puede compartir con cualquier dispositivo WiFi que se encuentre al alcance de la señal y que esté configurado para eso.

Figura 8. Router.
Fuente: https://tecnologia-informatica.com/que-es-router-wifi-comprar-ampliar-alcance/

Es posible dar permisos a través de la dirección física de la red, del Medía Access Control Address (MAC Address), configurar los puertos de acceso a VNC, Spotify y software de descarga. Asimismo, si un padre cree que sus hijos no deben navegar por internet a la madrugada, el router posee controles para impedir la navegación en determinadas horas. El control de internet y de la red está a disposición del administrador del router. Y todo es realizado a través de una interfaz web, en el propio dispositivo. [8]

2.1.9 DVR (Digital Video Recorder)

Hoy en día es muy común escuchar la palabra DVR (Digital Video Recorder) o en castellano, grabador de video digital.
Los Dvrs utilizados con cámaras de seguridad y vigilancia cumplen varias funciones.
Son los encargados de digitalizar y grabar las imágenes y audios que nos llegan desde las cámaras de seguridad.

Figura 9. Grabador de video digital.
Fuente: http://www.seguridadsos.com.ar/dvr/

Estos Dvrs, además de la grabación, nos permiten mediante un soft provisto por el fabricante, ver en una pantalla nuestras cámaras de seguridad, elegir que o cuales cámaras ver a la vez, agrandar o achicar los tamaños de las imágenes, mover las cámaras, programar horarios de grabación, programar grabación por detección de movimiento, setear la calidad de las imágenes y muchas funciones mas que dependerán de las características particulares de cada equipo.
La gran mayoría de estos dispositivos de grabación y control, cuentan además con la posibilidad de acceso remoto, es decir, que voy a poder por ejemplo ver las cámaras de seguridad desde una computadora conectada a mi red, desde una computadora en otro lugar físico a través de Internet o desde mi teléfono celular.

Algunos Dvrs cuentan con un estándar de comunicación de bus en serie llamado RS485 o EIA-485, este sistema es utilizado para mover cámaras de seguridad motorizadas (PTZ) , Pan (Paneo o giro hacia la derecha o izquierda), Tilt (Inclinación hacia arriba o hacia abajo) Zoom (Acercamiento). [9]

2.1.10 Cámaras de Seguridad

Las cámaras de videovigilancia son las encargadas de captar todo lo que ocurra en su casa o negocio, por lo que son un elemento vital en cualquier instalación. Las cámaras analógicas ofrecen una buena calidad de imagen a un precio insuperable, por lo que siguen siendo una opción excelente para pequeños negocios y viviendas. Disponemos de un amplio catálogo de cámaras de videovigilancia para que utilice la que realmente se adapta a sus necesidades. [10]

Figura 10. Cámara de Vigilancia.
Fuente: https://www.ipcenter.es/sam-2983n.html

2.2 Marco Jurídico

2.2.1 Organismos

Estos son algunos de los organismos que rigen las normas que supervisan el desarrollo de procesos y sistemas tecnológicos y de comunicaciones y garantizan los estándares de calidad.

- TIA: Telecommunications Industry Association.
- ANSI: American National Standards Institute.
- EIA: Electronic Industries Alliance.
- ISO: International Standards Organization.
- IEEE: Instituto de Ingenieros Eléctricos y de Electrónica.

2.2.2 Protección de datos personales en sistemas de video vigilancia.

Esta guía está dirigida (i) a las personas, compañías u organizaciones que utilizan SV recolectando datos personales, ya sea en calidad de Responsables5 o Encargados6 del Tratamiento de datos personales, por medio de cámaras, videocámaras, análogas o digitales, cámaras IP o mini-cámaras, circuitos cerrados de televisión (CCTV) y, en general, cualquier medio por el cual se realice el Tratamiento7 de imágenes de Titulares de datos personales, en especial con nes de vigilancia, para orientarlos en el cumplimiento de sus deberes en materia de protección de datos personales, y (ii) a los Titulares de la información, para que tengan conocimiento de cómo ejercer sus derechos frente a los primeros, garantizando así el respeto por sus derechos fundamentales a la intimidad, al buen nombre y a la protección de datos personales, consagrados en el artículo 15 de la Constitución Política a partir del cual se desarrolla el derecho de habeas data en Colombia. Las grabaciones que se realicen (i) dentro del ámbito exclusivamente personal o doméstico, (ii) con nes periodísticos, o (iii) que tengan como nalidad la seguridad nacional del Estado, no están cobijadas por lo señalado en esta guía.
Recuperado de:
http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Guia_Vigilancia_sept16_2016.pdf

CAPITULO III. Esquematización Ingenieril

3.1 Análisis del Proyecto:

3.1.1 Situación actual

En la Alcaldía municipal de Coper no cuenta con un sistema de cámaras que brinden seguridad a las personas dejando desprotegidos los objetos de valor que se encentran en las oficinas, tienen una conexión a internet donde están van distribuidas a las oficinas por medio del router, ya sea en el primer y segundo piso. Esta red se puede usar para el proyecto sin generar costos mayores aprovechando los recursos que tenemos a nuestra disposición.

3.2 Estructura Temática

3.2.1 Metodología.

La metodología de este proyecto se llevará a cabo mediante una serie de etapas que se irá desarrollando en cisco.

Las cuales son:

- Planteamiento.
- Diseño y organización.
- Implementación.
- Operación.

3.3 **Análisis y definiciones de Requerimientos**

3.3.1 Estudio.

La Alcaldía cuenta con la red instalada para sus equipos en cada oficina, se tendría la primera instalación en el frente que es el lugar donde comúnmente entra y sale gente todos los días, luego se tendría el primer piso donde hay varias oficinas con implementos importantes, después se tendría el segundo piso donde está ubicada la oficina del Señor Alcalde y otros funcionarios públicos y por último se tiene el patio donde es el lugar más expuesto y menos seguro.

3.3.2 Materiales

- 4 camaras.
- 1 Dvr para cámaras
- Cable UTP cat 6 para exteriores
- Conector Rj45
- 1 Router wifi
- 1 computador.

3.4 Diseño del Proyecto

3.4.1 Identificación de las Necesidades de los Clientes

Se hizo una visita a la Alcaldía para dar a conocer la importancia de este proyecto dando a conocer lo que implica su desarrollo. En el cual se requiere implementar unas 4 cámaras para las zonas principales y tener en cuenta un sistema Dvr para estas 4, si se requiere para un futuro colocar más cámaras por motivos de seguridad colocar un sistema Dvr que cumpla con el número que se va requerir para no tener más gastos.

También se provee que desde cualquier smartfone se pueda ver que es lo que está pasando sin ir al sitio donde se hizo la instalación, facilitando el manejo de este tipo de tecnología.

3.4.2 Fase de Diseño Lógico.

Se utilizará una red privada para el reconocimiento de cada cámara con un direccionamiento DHCP que permita obtener su IP automáticamente con la máscara de red por defecto “255.255.255.0”.

Datos:
Dirección de red -> 192.168.1.0
Primer host utilizable -> 192.168.1.1
Ultimo Host utilizable -> 192.168.1.254
Broadcats->192.168.1.254
Mascara de red-> 255.255.255.0

Se instala al pc una versión de Windows compatible con los componentes ya sea Windows XP, 7, 8, 8.1 o 10. En este pc se guardará toda la información que se vaya registrando por tanto también se debe tener en cuenta las especificaciones que se necesitan dependiendo los requisitos que pidan las cámaras.

3.4.3 Fase de Diseño Físico.

Primero se sitúa dónde quiere que vayan las cámaras para su instalación ya sea en la pared, el techo o ya sea en los postes, se hacen los canales por donde se cableara la red, se sitúa en un cuarto el PC donde no estará alejado del sol y la humedad.

Los equipos y materiales son:

Nombre	Cantidad	Valor
Camara HAC-HBDW1100RN-VF-S3	1	$102.500
Computador Lenovo Tiny M73	1	$ 660.000
Cable de red UTP cate 6	1 mt	$1.600
Dvr 4 canales	1	$150.000
Licencia Windows 10 Home	1	$550.000
Cable Utp Cat. 6 Para Exterior Miokee, Carrete.	305 mt	$169.900
Rack Gabinete 5ru Pared Ideal Para Dvr Switch Router	1	$130.000
Conector De Red Rj45 Bolsa 10	1	$300
Rack: Gabinete De Pared 5ru X 51	1	$159.000
Monitor Dell 18.5 E1916hv	1	$377.703
Total		$2’301.003

Tabla1: Materiales a utilizar.

3.4.4 Simulación

Teniendo en cuenta los requerimientos, se procedió con su respectiva simulación en el cual se ha usado Cisco Packet Tracer que es uno de los mejores programas al tratarse de montajes en la red.

Se configuraron dos VLAN, una para las cámaras del primer piso y el patio, y otra para las cámaras del segundo piso y el frente.

Se configuraron los router y se realizó pruebas.

Se montaron las cámaras donde se conectaron a través del puerto Ethernet al Router donde hubo conectividad entre los dispositivos dando así buen funcionamiento de la red.

BIBLIOGRAFÍA

Diseño de un sistema de video vigilancia por medio de enlaces microondas para la empresa disam sucursal santa marta.

Recuperado de:
http://repository.ucc.edu.co/bitstream/ucc/6175/1/2018_diseño_sistema_vigilancia.pdf

Lo que usted necesita saber sobre routers y swiches Cisco.

Recuperado de:
https://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectadosanonimos/routing/pdfs/brochure_redes.pdf.

Protección de datos personales en sistemas de videovigilancia.

Recuperado de:
http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Guia_Vigilancia_sept16_2016.pdf

D'Amato, J.,P., Dominguez, L., Perez, A., & Rubiales, A. (2016). Plataforma abierta de gestión de cámaras IP y aplicaciones móviles para la seguridad civil ciudadana/Open platform managing IP cameras and mobile applications for civil security. Revista Ibérica De Sistemas e Tecnologias De Informação, (20), 48-61. doi:http://bbibliograficas.ucc.edu.co:2076/10.17013/risti.20.48-61

INFOGRAFIA

[1]. http://www.eveliux.com/mx/curso/concepto-de-una-red-tipos-de-redes.html 27/05/2019

[2]. http://www.gadae.com/blog/tipos-de-redes-informaticas-segun-su-alcance/ 27/05/2019

[3]. http://redes-de-compu.blogspot.com 27/05/2019

[4]. http://redes-de-compu.blogspot.com 27/05/2019

[5]. https://www.networkworld.es/seguridad/que-es-la-seguridad-de-la-red 27/05/2019

[6]. https://www.telecocable.com/blog/diferencias-entre-cable-utp-stp-y-ftp/1374 17/05/2019

[7]. https://tuelectronica.es/conector-rj45/ 17/05/2019

[8]. https://tecnologia-informatica.com/que-es-router-wifi-comprar-ampliar-alcance/ 17/05/2019

[9]. http://www.seguridadsos.com.ar/dvr/ 17/05/2019

[10]. http://www.videovigilancia.com/camaras.htm 17/05/2019

CONCLUSIONES

Al ir desarrollando está monografía se aprende sobre los sistemas de redes y la gran importancia que se tiene en el día a día.

Dependiendo del uso que se le puede dar a las redes puede ser una gran ventaja para la seguridad en dónde se esté manejando.

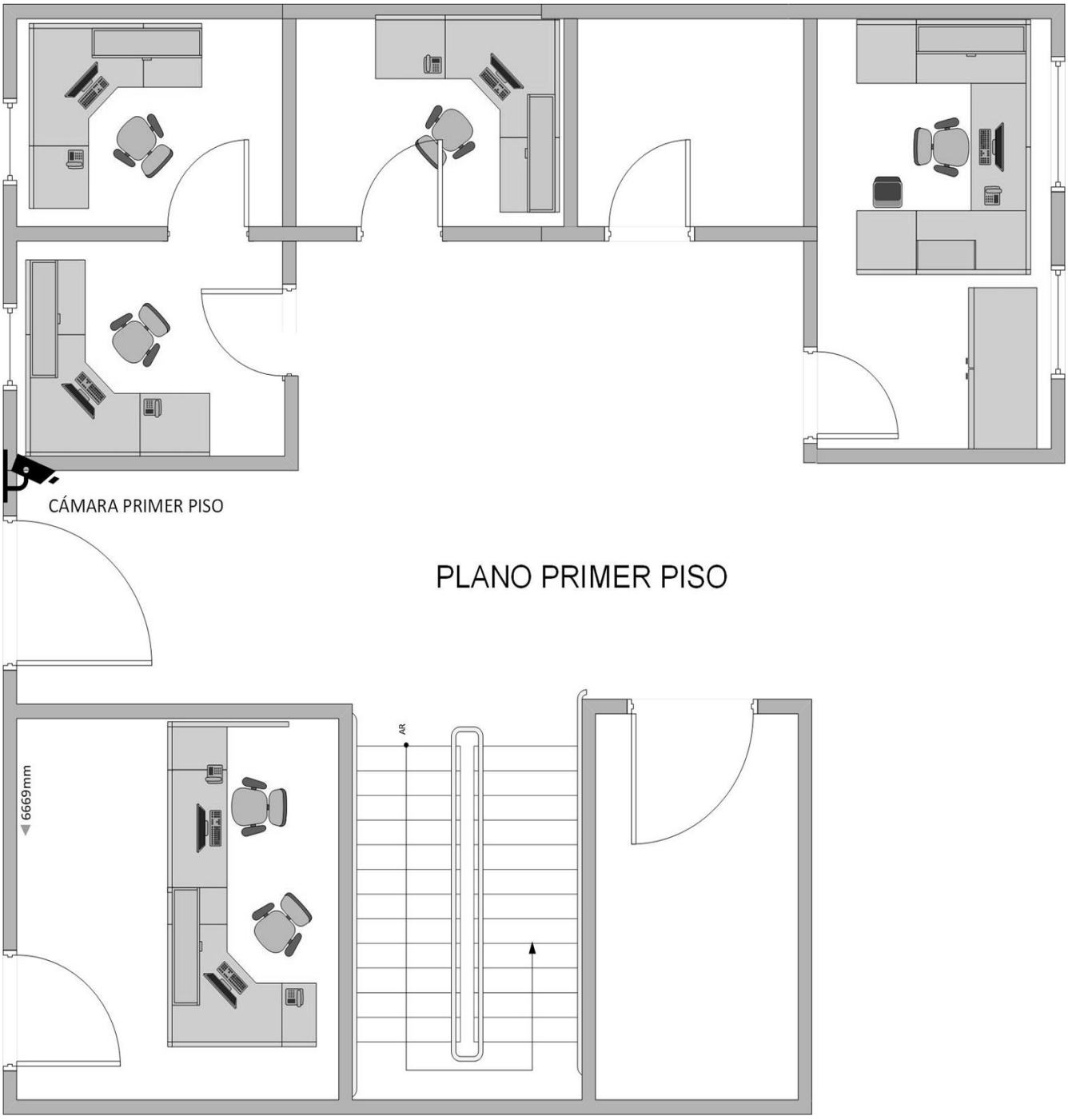
Se busco la información de diferentes fuentes y consultando con las directivas para el reconocimiento de los datos de las instalaciones.

Su diseño se hizo cumpliendo con los requerimientos de las instalaciones.

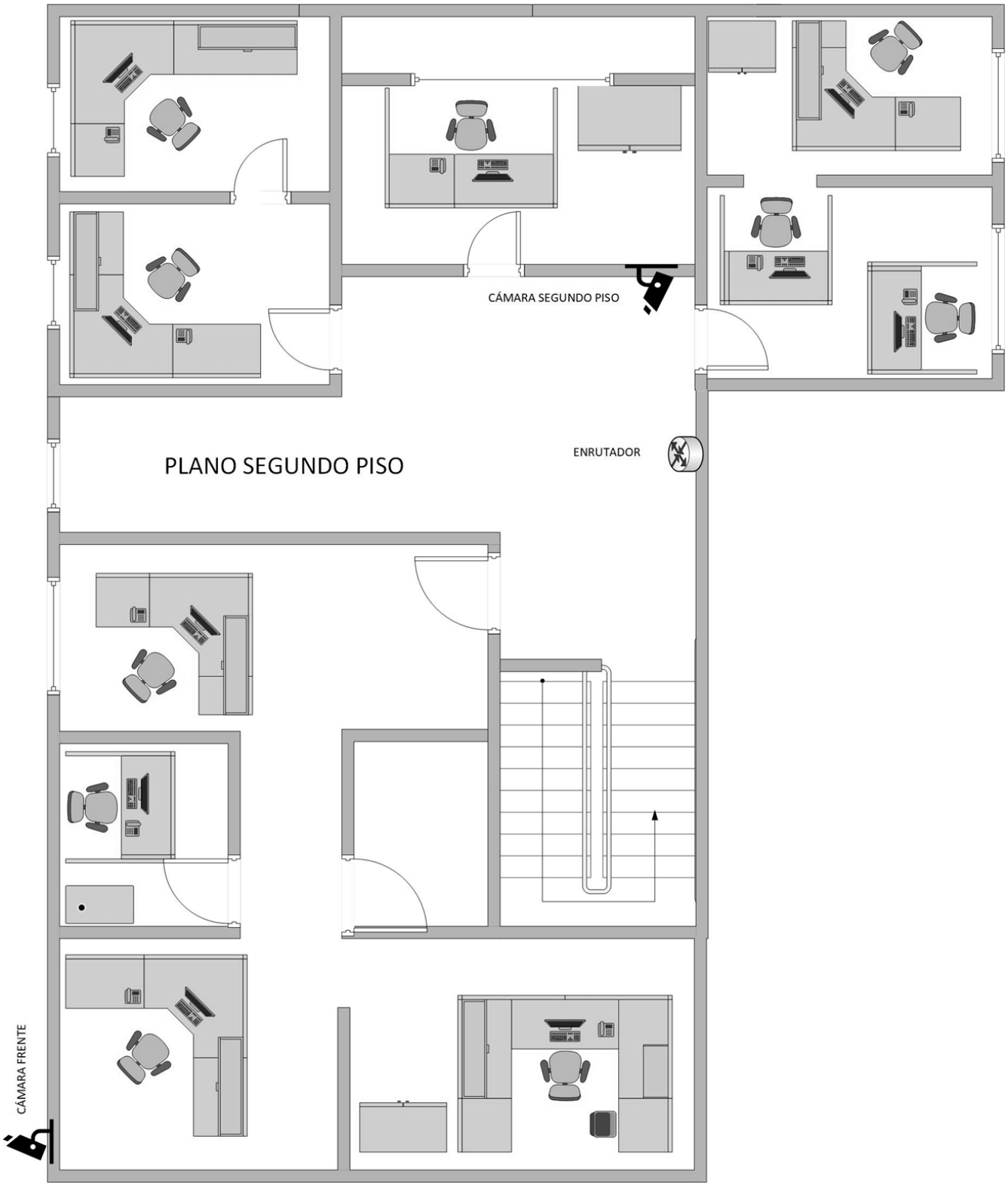
Este tipo de proyecto pueden ser usados tanto en colegios, universidades o hasta en las mismas viviendas ya que su implementación es la misma.

ANEXOS

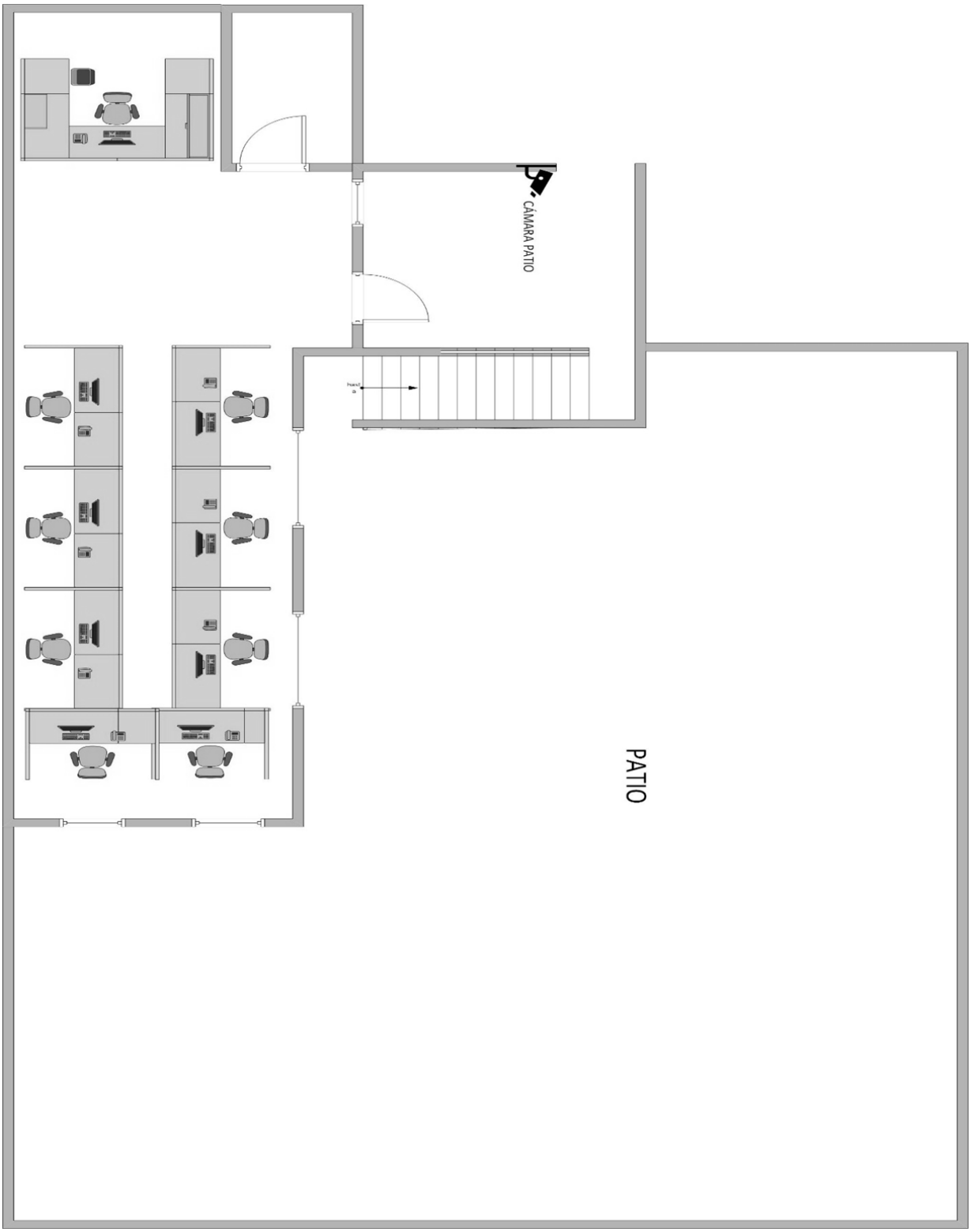
Anexo A. Plano Físico del primer piso.



Anexo B. Plano Físico del segundo piso.



Anexo C. Plano Físico del Patio.



Anexo D. Plano de Red Propuesto.