ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA DE
TELECOMUNICACIÓN
UNIVERSIDAD POLITÉCNICA DE CARTAGENA

Trabajo Final de Grado

Sistema anti-intrusión en recinto industrial con control de accesos, de presencia y CCTV 3G.

AUTOR: Pablo Alberto Alcoba Cerón
DIRECTOR: Mª Victoria Bueno Delgado
Julio / 2014

Autor	Pablo Alberto Alcoba Cerón
E-mail del Autor	pabloalbertoalcoba@gmail.com
Directora	Mª Victoria Bueno Delgado
E-mail de la directora	mvictoria.bueno@upct.es
Título del TFG	Sistema anti-intrusión en recinto industrial con control de accesos, de presencia y CCTV 3G.
Descriptores	Energía solar, CCTV, tornos, barreras, control de accesos, UMTS 3G, IPsec, fibra óptica sensora, barreras MW.

Resumen

El propósito de este proyecto es diseñar para un recinto industrial un sistema anti-intrusión perimetral que dispone de control de accesos, de presencia y CCTV 3G. La operativa de los sistemas estará centralizada en la sala de control del departamento de Seguridad Patrimonial del complejo. Si bien el estudio y diseño del sistema de control de acceso peatonal y para vehículos, control presencial de empleados mediante lectores biométricos, CCTV en báculos alimentadas con energía solar y conectividad 3G se abordaron en un proyecto anterior, realizado por el autor, en este nuevo proyecto se incorpora el estudio y diseño del sistema de alarma de intrusión disparada por fibra óptica sensora y barerras MW para completar el sistema de seguridad de la instalación.

Titulación	Grado en Ingeniería Telemática
Intensificación	
Departamento	Tecnologías de la Información y las Comunicaciones
Fecha de Presentación	Julio 2014

Índice

Índice de figuras

Índice de tablas

Capítulo 1
Introducción

1.1 Antecedentes

Anexo a un recinto cerrado de un complejo industrial existente, se va a pasar a tener un segundo recinto industrial de nueva construcción, anexo al primero y del mismo cliente.

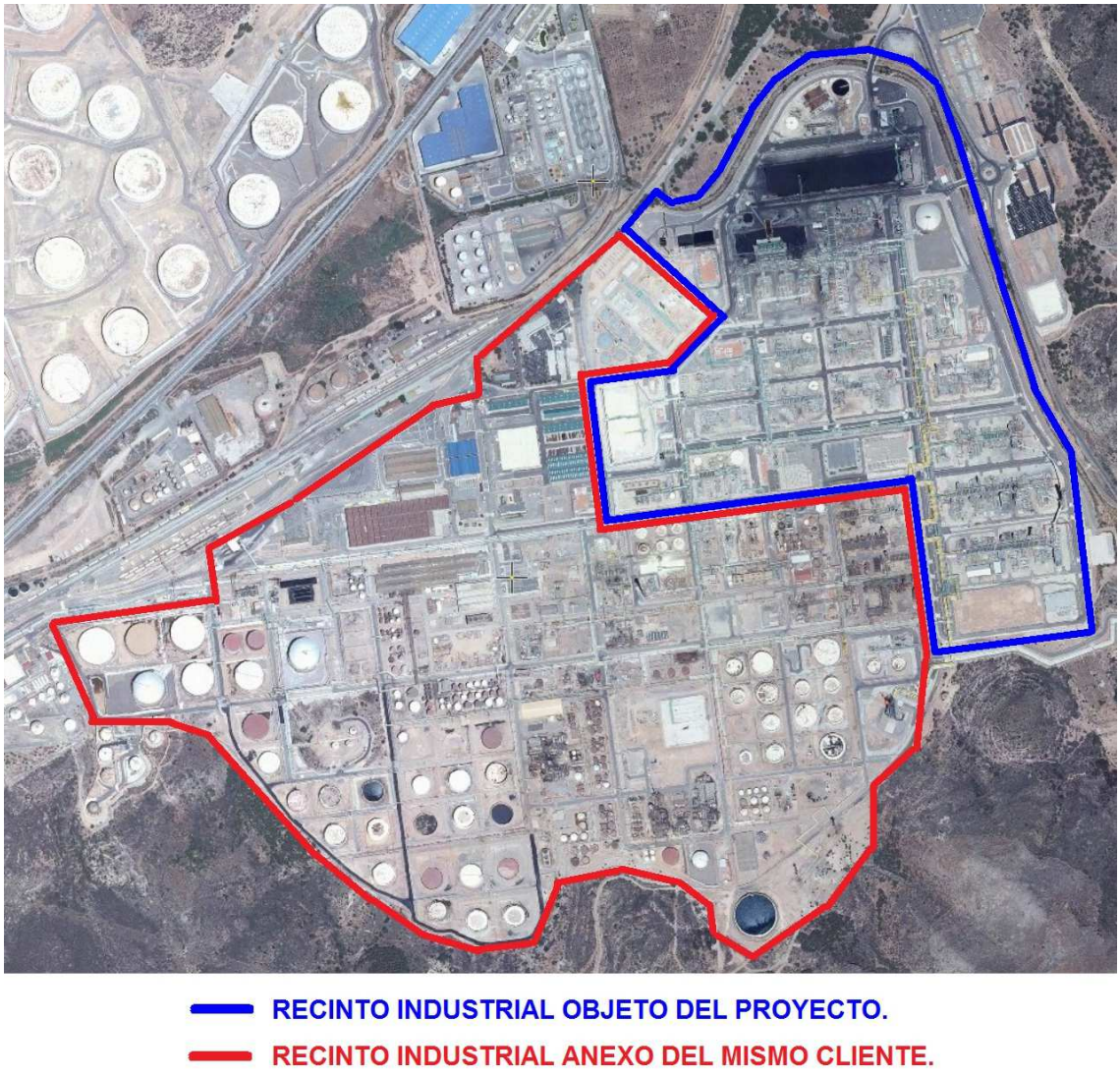


Figura 1.1 - Vista aérea de los recintos

El nuevo recinto ha de contar con una serie de servicios telemáticos con un control centralizado, los cuales se detallan a continuación.

1.2 Objetivos

En un proyecto anterior realizado por el autor se abordó la tarea de dotar al nuevo complejo industrial indicado anteriormente de servicios telemáticos requeridos para preservar la propiedad. Esos servicios abarcan, desde el control de personal por medio de lectores biométricos, hasta un sistema de CCTV basado en cámaras 3G, sin olvidar el cableado estructurado de las distintas naves que forman parte del complejo. Este trabajo consiste en una continuación del proyecto anterior, en el que se desea instalar, en el mismo complejo industrial, un nuevo servicio telemático basado en un sistema de alarma anti-intrusión. Para llevar a cabo este trabajo, primero es necesario hacer un breve repaso sobre los servicios instalados anteriormente, y hacer un estudio y diseño del nuevo servicio que se propone.

1.3 Estructura del contenido

El contenido de este Trabajo Final de Grado se estructura en los siguientes capítulos:

- El capitulo 2 se detallan los sistemas telemáticos previamente diseñados e instalados.
    - El sistema de cableado estructurado.
    - La perimetración de la planta con CCTV 3G.
    - El sistema de control de accesos, mediante barreras y tornos.
    - El sistema de control presencial. Mediante lectores biométricos.
    - La sala de pantallas y el servidor central.
- En el capítulo 3 se explica el sistema anti intrusión, su funcionamiento y elementos: Fibra óptica sensora y Barreras MW.
- Finalmente, el capítulo 4 extrae las conclusiones del trabajo realizado y líneas futuras.

Capítulo 2
Sistemas telemáticos previamente diseñados e instalados

2.1. Introducción

En un proyecto anterior, se procedió a realizar el estudio y diseño de:

- **Sistema de cableado estructurado**: para ofrecer un servicio de voz, video y datos a las instalaciones del recinto, así como la interconexión de todos los servicios telemáticos.
- **Perimetración del recinto con cámaras**: para proporcionar una vigilancia más efectiva en los perímetros de las zonas del complejo. Se utilizan torres de vigilancia, compuestos de baterías y paneles solares, cámaras de vigilancia, y un servicio de comunicación inalámbrica que permita la transmisión y recepción de vídeo y audio por 3G.
- **Sistema de control de acceso:** que restringe el acceso al complejo mediante tornos para peatones y barreras para vehículos. Un programa software adaptado autoriza el acceso a las tarjetas expedidas por el cliente que cumplen sus requisitos explícitos. Estos requisitos son por ejemplo, cursos de seguridad realizados, revisiones médicas, carnet de conducir, etc., controlando sus caducidades en tiempo real. Así mismo los vehículos con sus revisiones o ITV son controlados en el acceso.
- **Sistema de control presencial:** junto con el sistema de control de acceso se puede contabilizar las horas trabajadas por cada empleado y sus empresas, así como cualquier otra aplicación que de este sistema de control quiera hacer el cliente. Mediante este sistema se puede saber en tiempo real el listado completo de personas que están en el complejo, por lo que si hiciese falta una evacuación se podría saber si queda alguien en el recinto. Aparte del control de acceso al complejo, en las oficinas del cliente y en el de las contratas de servicios, se impone un control presencial al personal. Este control de presencia no conlleva un control de acceso. Este control presencial se llevará a cabo con unos lectores biométricos los cuales leerán las huellas dactilares. Los empleados se identificarán al entrar y salir de las oficinas en dicho lector de huellas y éste, mediante la comparación de un patrón tomado el día de la incorporación del empleado, guardará en el servidor, o en su propia memoria, registro de ello. El cliente, a través de su departamento de costes, usará estos datos para reembolsar después el coste de las horas trabajadas a las distintas empresas contratistas de mantenimiento del complejo.

- **Control de la sala de pantallas**: La sala de pantallas se diseñó como una sala localizada en el edificio de seguridad del complejo correspondiente a la empresa de vigilancia y clínica principal de servicios sanitarios. Contiene los equipos informáticos y pantallas necesarias para administrar el sistema de vigilancia 3G.
- **Servidor central:** está hospedado en el CPD (Centro de Proceso de Datos) de las oficinas del cliente. Contendrá el programa que administrará los accesos y los datos presenciales para el departamento de control de costes. En este servidor se dan las altas de los trabajadores y vehículos y será administrado por el departamento de control de accesos. Este departamento del cliente es el que gestiona todas las tarjetas de acceso: alta de las tarjetas, bajas de las tarjetas, reactivación de permisos de acceso a las tarjetas una vez se compruebe que se han cubierto las exigencias (caducadas) para el acceso, etc.

En este capítulo se hace un breve resumen de cada uno de los sistemas estudiados y diseñados previamente, para conocer los sistemas telemáticos proyectados, antes de iniciar el estudio y diseño del sistema anti-intrusión que se aborda en este trabajo.

2.2. Sistema de cableado estructurado

En las oficinas del edificio de administración (ed. Principal) se alojan operadores y administradores del departamento de control de accesos con un total de 10 empleados, y CPD (Centro de proceso de datos). Las oficinas están dotadas de la infraestructura de red correspondiente para que sus empleados puedan disfrutar de los servicios de voz (telefonía), datos (Internet), video, etc. Se ha tenido en cuenta el posible crecimiento de la red.

Para realizar el diseño del cableado estructurado se hizo uso de los planos facilitados por el cliente con la distribución de estancias y canalizaciones del edificio. La disposición de los puestos de trabajo se realizó sobre dichos planos. Así mismo se satisfizo todas las normas vigentes relativas a la instalación de este tipo de infraestructura: *TIA/EIA 568-A, TIA/EIA 568-B, TIA/EIA 568-B.1, TIA/EIA 568-B.1.1, TIA/EIA 568-B.2, TIA/EIA 568-B.2.1, TIA/EIA 568-B.3, TIA/EIA 569-A y TIA/EIA 606-A.*

La infraestructura de telecomunicaciones diseñada está formada por:

- Punto de demarcación o POP, donde se realiza la conexión de los cables externos del proveedor de servicios con los cables del cliente de la instalación. Representa el límite entre la responsabilidad del proveedor de servicios (ISP) y las oficinas. Se ha situado en una sala de comunicaciones situada en la planta baja, justo debajo de la sala principal del presente proyecto.
- Sala de Telecomunicaciones, donde se albergan todos los equipos referentes y el material referente a la infraestructura de la red de voz y

de datos. Se ha situado en la parte central de la primera planta. La razón de esta situación se debe a la forma de las oficinas, lo que hace que la situación de dicha sala evite un gasto innecesario de cable. El diseño de las salas de telecomunicaciones se especifica en la norma TIA/EIA 569-A.

- Centro de cableado, donde se alberga el cableado y se realizan las interconexiones.
- Cableado horizontal, que es la porción de cableado de telecomunicaciones que se extiende desde la sala de telecomunicaciones a las distintas zonas de las oficinas a cablear. El cableado horizontal incluye, además de los cables, las tomas y conectores, las terminaciones y las interconexiones en la sala de telecomunicaciones. Para realizar el cableado horizontal, por cada toma se tomaron 6 cables UTP categoría 6, de 100 ohmios, 24 AWG de 4 pares. Y se han seguido las condiciones establecidas en el anterior trabajo.

2.2.1. Puestos de trabajo

En los puestos de trabajo se ha distinguido lo que se llama “área de trabajo”, que es la parte del cableado que se extiende desde la toma hasta el equipo de trabajo (PC, impresora, teléfono, fax, etc.). Para cada puesto de trabajo se han distinguido 2 tomas:1 toma de voz, datos y reserva y 1 toma de datos extra (impresora en red). Por tanto, cada puesto de trabajo está formado por puntos de cuatro tomas para jacks RJ-45 hembra con codificación T-568-B.

2.2.2. Sala de telecomunicaciones

Por otro lado, en la sala de telecomunicaciones se ha tenido especial cuidado, siempre poniendo junto al Patch Panel un listado de los puntos de voz y datos para su localización y un plano de la planta con ellos indicados. La conexión de cada uno de los equipos que forman parte del puesto de trabajo con las tomas se ha realizado con cable UTP categoría 6, conectores RJ-45 macho, y la distancia entre toma y equipo no podrá sobrepasar los 3 metros.

2.2.3. Sistemas de alimentación ininterrumpida

En cuanto al Sistema de Alimentación Ininterrumpida (SAI), se ha tenido en cuenta el uso del mismo para proporcionar energía eléctrica si se sucede un apagón a todos los dispositivos. Además, los SAI mejoran la calidad de la energía eléctrica que llega a los aparatos, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar Corriente Alterna. Los SAI utilizados en la instalación son los APC modelo SMART-UPSRM3000, cuyas características principales se listaron en el anterior trabajo. El resto de los detalles técnicos, así como el manual de funcionamiento y uso, también se adjuntaron en el DVD del proyecto anterior.

2.2.4. Equipamiento

La instalación se realizó un diseño LAN (*Local Area Network*), cumpliendo los requisitos de diseño de este tipo de redes. La selección de los switch, router, firewall y transceiver obedeció a sus grandes capacidades de trabajo bajo altas cargas de transmisión y gestión datos.

2.2.4.1. Switches

El switch, dispositivo de capa de enlace (nivel 2) es el encargado de la conmutación de los datos mediante la interconexión de múltiples segmentos de una red LAN. Cada puerto del switch separa segmentos (un host por segmento), evitando colisiones y por tanto incrementando la fiabilidad de las transmisiones. Para ello trabaja con las direcciones MAC de los dispositivos Ethernet haciendo un seguimiento de estas direcciones localizando el segmento en el que están. De esta forma, los switches proporcionan a cada uno de los host el ancho de banda completo, controlando el flujo de datos a nivel 2.

Cuando se habla de switches hay que hacer referencia a VLAN (*Virtual Local Access Network*). VLAN no es más que una de las configuraciones lógicas que puede realizarse con uno o múltiples switches añadiendo escalabilidad, y seguridad a la red diseñada. En una VLAN, los equipos que forman parte de ella, en principio, solo son capaces de mantener conectividad lógica con los de su propia VLAN. Esto tiene sentido, por ejemplo, si una empresa está formada por diversos departamentos, y cada uno de esos departamentos debe tener conectividad solo con aquellos que pertenecen al departamento en cuestión. La configuración y puesta en marcha de una VLAN debe ser realizado por el administrador de la red siguiendo las necesidades de la empresa.

Hoy día también se pueden encontrar switches trabajando a nivel 2/3. Estos switches presentan ciertas ventajas ya que ofrecen: calidad de servicio, reenvío de paquetes, conmutación de paquetes de alto rendimiento, escalabilidad a una alta velocidad, baja latencia, seguridad, etc.

En esta instalación se han utilizado unos switches de 24 puertos marca DELL modelo PowerConnect 2724 cuyas principales características se detallan en el trabajo anterior. Se puede consultar el manual del dispositivo utilizado en el DVD adjunto al proyecto.

2.2.4.2. Routers

Los routers son los dispositivos encargados de enrutar la información por las interfaces indicadas para que dichos paquetes lleguen a su destino. Para el caso que nos compete, el router, además de hacer la funcionalidad antes descrita, hace de interfaz entre la red pública (Internet) y la red privada de la empresa. En esta red se ha utilizado un router marca ZYSEL modelo D1 de la serie P-660HW, proporcinado por telefónica, el proovedor de servicios de Internet (ISP) de la zona. En el DVD adjunto del trabajo anterior se encuentra el

manual del dispositivo (procedimientos de instalación, problemas comunes, ficha técnica detallada, cómo configurarlo y administrarlo), la hoja de características con las especificaciones técnicas, y la guía rápida del usuario.

2.2.4.3. Firewall

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del firewall, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al firewall a una tercera red, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior. Un firewall correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

En esta instalación se ha utilizado el firewall SONICWALL modelo 240 de la serie NSA cuyas principales características se detallan en la memoria del trabajo anterior. También se puede encontrar el manual del dispositivo en el DVD adjunto.

2.2.4.4. Transceivers

El transceiver realiza, dentro de un mismo chasis, funciones tanto de trasmisión como de recepción, utilizando componentes de circuito comunes para ambas funciones. Interconecta dos medios de transmisión incompatibles entre sí. En el caso que compete a este proyecto se han utilizado transceivers de cobre(Ethernet) a fibra óptica, marca Allied Telesis, modelo AT-MC1004**,** con un ancho de banda de 1 Gigabit/seg, cuyas características están detalladas en la memoria del trabajo anterior así como en el DVD adjunto, en el que también se especifica el procedimiento de instalación, los problemas más comunes que pueden darse, y la ficha técnica.

2.2.5. Cableado estructurado exterior

El edificio principal de dirección de ingeniería es el que contiene la sala de datos principal (MDF) y se interconecta con el resto de oficinas (IDFs) y accesos que componen el presente sistema. Siguiendo el esquema de la Figura 2.1 se puede ver que del MDF cuelgan el “Acceso 3” de la planta, el “edificio de ingeniería 1”, y la sala de pantallas que se encuentra en el edificio de la empresa de seguridad en la campa de contratistas. De este último cuelgan a su vez dos edificios de ingeniería más y el acceso 1 de la planta, del que cuelga también el “acceso 2”.

Las cámaras se conectaran al sistema a través del proveedor de servicios de internet.

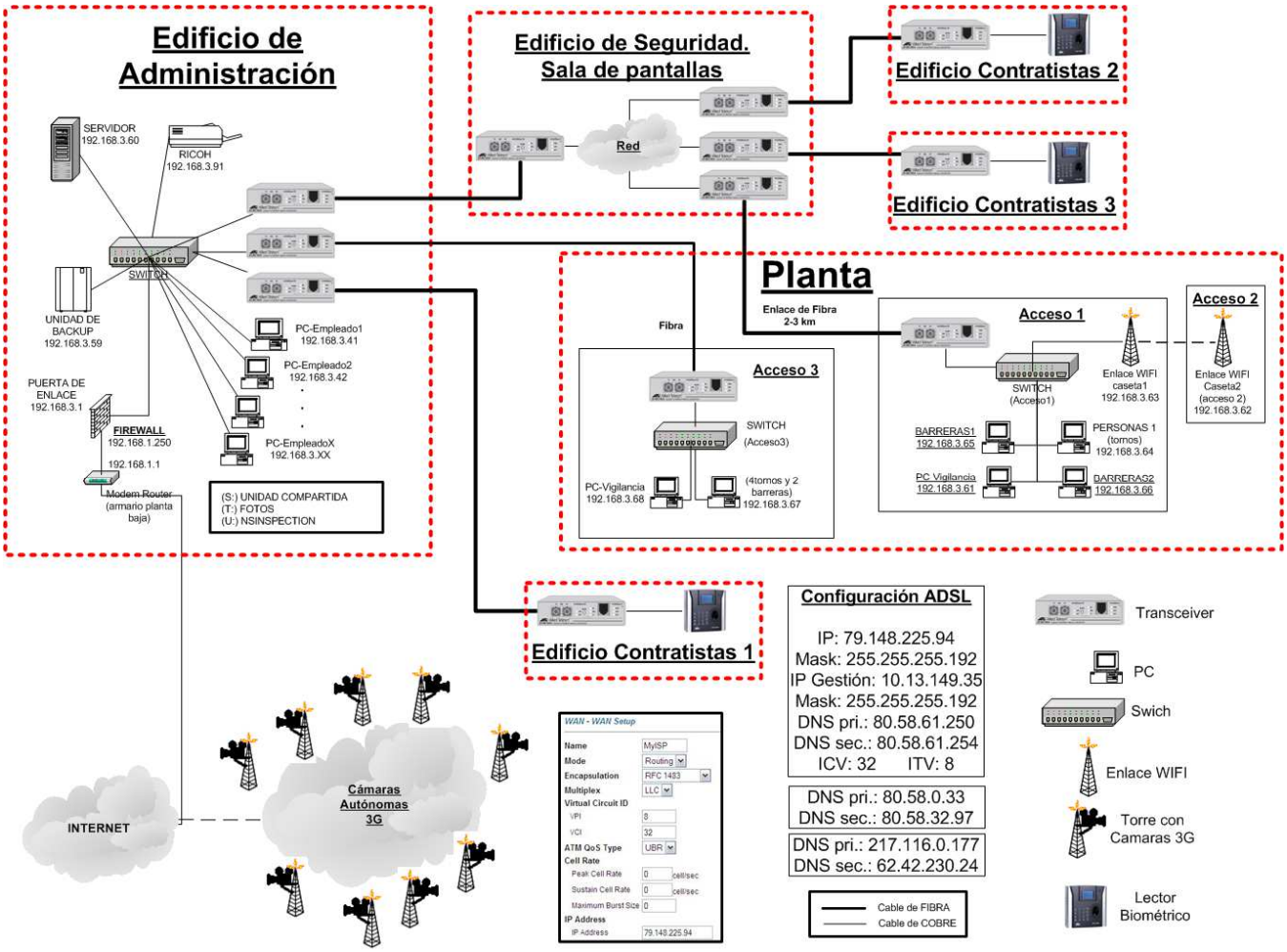


Figura 2.1 –Sistema de cableado estructurado exterior: Esquema general

Al switch principal del MDF se conectan tres transceivers de los indicados en el apartado anterior. Estos se interconectan en cada una de las ramas del sistema. Mediante una obra civil se hace llegar los cables de fibra óptica a los siguientes IDFs.

Rama 1

El edificio seguridad tiene una sala pantallas que contiene un Rack de comunicaciones donde llegará el cable del MDF. Del switch principal de la sala de pantallas cuelgan a su vez otras 3 ramas, también con fibra y los transceivers.

Rama 1.1 y 1.2

A cada uno de los dos edificios de las contratistas de mantenimiento llega un cable de fibra óptica desde el edificio de seguridad. Estos cables llegan a los MDF de estas instalaciones donde mediante el uso de un transceiver y el sistema de cableado estructurado se hará llegar la red del presente sistema hasta los lectores biométricos. Los planos de estas infraestructuras no están a disposición del presente proyecto por encontrarse administrado por otra empresa.

Rama 1.3

En el acceso principal (acceso 1) de planta hay un edificio de vigilancia que contiene un armario de comunicaciones. A dicho armario llega un cable de fibra óptica desde el edificio de vigilancia. Mediante un transceiver y un switch se interconectan las barreras y tornos al sistema. Las Interface del punto 2.4.2 se conectan por Ethernet al switch. También se pone un enlace wifi para intercomunicarlo con el acceso de vehículos pesados, acceso 2. En dicho acceso 2 se conecta el interface que controla la barrera al enlace wifi para interconectarlo al presente sistema.

Rama 2

En el acceso 3 de planta hay una caseta de vigilancia que contiene un armario de comunicaciones. A dicho armario llega otro cable de fibra desde el MDF. Me mediante un transceiver y un switch se interconectan las barreras y tornos al sistema. Las Interface se conectan por Ethernet al switch.

Rama 3

A otro edificio de contratistas llega un cable de fibra óptica desde el MDF. Este cable llega al MDF de estas instalaciones donde mediante el uso de un transceiver y el sistema de cableado estructurado se hace llegar la red del presente sistema hasta el lector biométrico.

2.3. Perimetración de zonas: cámaras torre 3G

Para tener un control perimetral con cámaras de las zonas de la factoría se instalaron unas torres de vigilancias autónomas con conectividad 3G.

A continuación se detalla lo necesario para llevar a cabo la instalación, desde el estudio de cobertura 3G hasta los elementos que conforman las torres. Se explicitará las localizaciones de las cámaras, aunque dado el carácter autónomo de dichas torres, según las necesidades cambiantes de producción y de los trabajos posteriores de la planta, las cámaras se podrán reubicar.

Nota.- La obra civil necesaria no viene especificada en este documento.

2.3.1. Estudio de cobertura

Fue necesario un estudio de cobertura para determinar la cantidad, la ubicación y la configuración óptima de puntos de acceso para proporcionar la cobertura de radiofrecuencia en las zonas necesarias de sus instalaciones. Es un procedimiento imprescindible a la hora de ajustar el diseño y la planificación de una red de radiocomunicaciones.

El proveedor de servicios de Internet, Vodafone, a través de una subcontrata local, realizó cálculos de cobertura y de propagación radioeléctrica. La capacidad de obtener predicciones radioeléctricas precisas y detalladas supone una información fundamental en la gestión del espectro, planificación, diseño y optimización de redes y de servicios inalámbricos. Para la realización de los análisis y simulaciones radioeléctricas el ISP se apoya en datos cartográficos específicos de alta y media resolución para el ámbito de las radiocomunicaciones.

Tras el estudio por parte de técnicos del ISP de la situación de sus repetidores, de los mapas cartográficos y de la situación en estos mapas de las zonas que se quiso cubrir con estas cámaras a través de su servicio de Internet de cobertura 3G, éstos decidieron los lugares donde hacer las mediciones. Con un teléfono especial con el que se podía ver en tiempo real la cantidad de señal del repetidor en decibelios se pudo comprobar que en las zonas donde a priori debía haber menos señal (el peor de los casos posibles), había la suficiente como para que ésta empresa pudiese facilitar el servicio. En caso de que no hubiese suficiente cobertura ésta se hubiese podido suplir con un repetidor móvil, que, si el ISP lo hubiese visto necesario, podría sustituirse, más adelante, por un repetidor fijo estándar.

2.3.2. Localización de las torres

Una vez realizado el estudio de cobertura, se situaron las torres. Los planos en detalle de las zonas cubiertas y las localizaciones se encuentran en el DVD adjunto al proyecto anterior.

En la tabla que se adjunta a continuación vienen especificadas las coordenadas donde fueron ubicadas, siendo estas del sistema de referencia particular del complejo. Partiendo de un punto cero todos los puntos se localizan por coordenadas X, Y y Z. La coordenada Z, relativa a la cota (altura) se obvia ya que la torre se instala sobre lo que haya en dicha localización X Y.

Zona	Cámara nº	Ref. Planta X	Ref. Planta Y
Zona de planta	1	**1.167,663**	**386,225**
	2	**1.303,148**	**485,746**
	3	**1.243,157**	**776,010**
	4	**1.203,120**	**969,515**
	5	**1.128,240**	**1.311,490**
	6	**875,337**	**1.326,594**
	7	**768,245**	**114,912**
	8	**646,783**	**909,210**
	9	**703,685**	**906,720**
Zona de dirección	1	**504,121**	**961,383**
	2	**506,914**	**1.025,121**
	3	**591,857**	**1.121,975**
Campa de Contratistas de mantenimiento	1	**1.241,241**	**1.299,046**
	2	**1.270,992**	**1.236,807**
	3	**1.196,505**	**1.226,190**
	4	**1.270,792**	**1.171,024**
	5	**1.313,044**	**920,260**
	6	**1.223,254**	**1.175,702**
	7	**1.246,073**	**1.037,282**

Tabla 2.1 - Coordenadas de las cámaras de seguridad

2.3.3. Torre Completa

Toda la parte de comunicaciones, así como la integración de ésta con la/las cámara/s están embebidas en una caja estanca de índice de protección IP65, preparada para recibir alimentación de baterías que se recargarán con energía solar.

2.3.3.1. Soportería

La soportería necesaria está compuesta por un mástil de 4 metros de altura, con unas dimensiones de 70x70mm y un grosor de 6mm. En su base va fijada una plataforma de 400x400mm con un grosor de 10mm la cual va perforada en 4 puntos para su anclaje con pernos a Dados de hormigón. Toda esta estructura es galvanizada.

2.3.3.2. Baterías de alimentación

Se utilizaron tres “versiones” de alimentación dado que el montante económico de ésta partida es bastante relevante dentro del proyecto original. Las tres opciones se detallan a continuación.

Alimentación 12 v

Se diseña en primer término éste sistema de alimentación donde el voltaje de la batería es de 12 v, dado que sería el necesario en la mayoría de los casos y a su vez sería el más económico de todos. Dicho sistema, está compuesto por un lado por un armario que alberga la batería comentada, un regulador y un inversor/convertidor, dado que se necesita alimentar la electrónica a dos voltajes, por un lado a 12v (router) y por otro a 24v (cámaras). El sistema se ha diseñado para una autonomía de 36 horas (dado que las opciones de 12 y 24 horas no hacían variar la partida económica). Ésta opción sería la más óptima para la incorporación al sistema de 2 cámaras fijas (no permitiendo incluir ninguna cámara más).

Alimentación 24 v

De idénticas características al expuesto en el punto anterior pero donde el voltaje que aporta la batería es de 24v. Se ha optó por ésta opción en algunos puntos donde había previsión de poner cámara adicional (de las dos para las que se ha diseñado), al permitir redimensionamiento.

Alimentación 24 v (domo)

De idénticas características al expuesto en el punto anterior, pero dimensionado para poder dar servicio a la cámara domo. Los requisitos de alimentación necesarios para poder mover el motor y la lente de la cámara domo, unidos al sistema de comunicaciones, hacen necesario utilizar 3 paneles solares (de iguales dimensiones que los indicados anteriormente).

2.3.3.3. Paneles Solares

Como característica particular del sistema de CCTV se le dotó de alimentación autónoma, basándose en paneles solares. Fueron necesarios dos paneles, cuyas dimensiones son de 1060x1210 mm (cada uno) y ubicados sobre una estructura de cuadradillo de 40x40mm y 3mm de grosor con una pletina de anclaje en cada una de las patas de 20x20 mm y 5 de grosor. Se instaló paneles **PW1650** del fabricante **PhotoWatt.** Para más información, ir a la documentación adjunta del proyecto anterior..

2.3.3.4. Comunicaciones

Independientemente del tipo de cámaras a utilizar (fijas, domo,…) el equipamiento de comunicaciones fue el mismo para todas. Se utilizó para ello un router GPRS/3G/HSDPA del fabricante REVISIO**.** De este elemento cabe destacar que está dotado de dos bocas Ethernet RJ45 10/100, dos slots PCMCIA, puerto serie para control de señales, puerto de consola y puerto usb. A nivel de router tiene como características: IP routing, incluyendo NAT/PAT (Network Address Translation / Port Address Translation), IP Aliasing, IP accounting, Firewall, Bridging y enrutamiento dinámico mediante RIP, Servidor

DHCP, Servidor Telnet, IPSec y PPTP (permitiendo la creación de VPNs), PPP con gestión de históricos de conexión, sniffer de red y balanceo de carga entre varios equipos de comunicaciones para aumentar el ancho de banda total.

Las tarjetas PCMCIA que ha de ir insertada en el router para su comunicación no se incluyó en el alcance del proyecto pues era provista por la compañía de telecomunicaciones seleccionada por el cliente.

En el DVD del proyecto anterior se adjunta un manual sobre su instalación, donde se indican las opciones de comunicación y seguridad, y su configuración.

IPSEC

IPsec (Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo IP autenticando y/o cifrando cada paquete IP en un flujo de datos. También incluye protocolos para el establecimiento de claves de cifrado.

IPsec actúa en la capa de red, la capa 3 del modelo OSI, haciendo que sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4 y superiores, incluyendo TCP y UDP. Una gran ventaja de IPsec sobre otros métodos que operan en capas superiores es que no hay que hacer ningún cambio en las aplicaciones para que se pueda utilizar**.**

Dependiendo del nivel sobre el que se actúe, podemos establecer dos modos básicos de operación de **IPsec**: **modo transporte** y **modo túnel**.

Modo túnel

Todo el paquete IP es cifrado y/o autenticado. Se encapsula en un nuevo paquete IP y se envía. El **modo túnel** se utiliza para comunicaciones red a red, por ejemplo para conectar un ordenador de manera segura y transparente al usuario a una intranet.

Modo transporte

En modo transporte, (el que fue el que se eligió**)**, sólo los datos del paquete IP son cifrados y/o se autentican. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP.

IMPORTANTE: si se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que eso invalidaría el hash. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera, por ejemplo traduciendo los números de puerto TCP y UDP. Una forma de encapsular mensajes IPsec para atravesar NAT ha sido definido por RFCs que describen el mecanismo de NAT transversal.

Protocolos

IPsec consta de dos protocolos que han sido desarrollados para proporcionar seguridad a nivel de paquete, tanto para IPv4 como para IPv6:

- **Authentication Header (AH)** proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados.
- **Encapsulating Security Payload (ESP)**, **el que se elige en este proyecto**, proporciona confidencialidad y la opción de autenticación y protección de integridad.

Encapsulating Security Payload (ESP)

El protocolo ESP proporciona autenticidad de origen, integridad y protección de confidencialidad de un paquete. ESP también soporta configuraciones de sólo cifrado y sólo autenticación, pero utilizar cifrado sin autenticación está altamente desaconsejado porque es inseguro. Al contrario que con AH, la cabecera del paquete IP no está protegida por ESP (aunque en ESP en modo túnel, la protección es proporcionada a todo el paquete IP interno, incluyendo la cabecera interna; la cabecera externa permanece sin proteger). ESP opera directamente sobre IP, utilizando el protocolo IP número 50.

2.3.3.5. Cámaras

En cuanto a las cámaras IP, se instalaron tres tipos, dos para las cámaras fijas y una para las cámaras domo.

Cámaras Fijas

Para las cámaras fijas:

- Cámara de una única lente de “día”, seleccionada en caso de zonas que cuentan con iluminación (natural o artificial) 24h.
- Cámara de iguales características a la anterior pero con doble lente, donde con una se hace la visión en buenas condiciones de luz y con la otra en condiciones de baja luminosidad.

Se podría haber optado por una cámara de una única lente de “día” incorporando focos infrarrojos, pero había un serio problema con la alimentación dado el consumo.

En cualquier caso, para éstas cámaras se destacan como características fundamentales: estanqueidad IP65, soporte de VoIP (Voice over IP), cumplen el estándar PoE (Power over Ethernet), detección de movimiento, configuración horaria de la actividad de la detección, etc.

Las cámaras elegidas fueron las **DualNight M12D** del fabricante **MOBOTIX.**

Respecto al metraje de las lentes, dada toda la gama disponible se optó por la más conveniente en función de distancias (se estiman inicialmente unos 50 metros de visión por cámara).

Se adjunta la documentación referente a las cámaras en el DVD del proyecto anterior. En ella se podrán ver manuales de instalación, funcionamiento, gestión, etc.

Cámaras Domo

La tercera opción en cuanto a cámara IP, fue la correspondiente a la cámara DOMO, es decir, aquella que va a ofrecer al operador la posibilidad de interactuar con la cámara con un grado de giro de 360º en el eje horizontal y 180º en el vertical, así como un zoom óptico de 23 aumentos. Ésta cámara al igual que las anteriores, posee un grado de estanqueidad IP65. Las cámaras domo instaladas fueron **CAM-6600 Series** del fabricante **ACTI,** cuyas principales características se detallan en el proyecto anterior. En el DVD del proyecto anterior también se adjuntan los manuales con documentación respecto a la instalación, configuración, mantenimiento, etc.

2.4. Sistema de control de acceso: barreras y tornos

En las entradas a la zona de planta, los tornos y barreras permiten el control de acceso a la misma. La localización de estos dispositivos se encuentra en el apartado de sistema de cableado estructurado, y también en la documentación del DVD del proyecto anterior.

Todo el personal que entre al recinto lo hace mediante el uso de una tarjeta (personal e intransferible). Estas tarjetas identifican al personal en el servidor de control de accesos, donde están reflejados todos los permisos.

Las barreras y tornos funcionan por igual y de la siguiente manera: cada torno o barrera tiene una placa CPU que controla los mecanismos físicos de los mismos. Estas placas CPU se conectan a unos interface que a su vez se conectan a la red de datos TCP/IP del presente sistema.

2.4.1. Placas CPU

La placa CPU se encuentra físicamente dentro de los tornos y las barreras y se considera como zona de acceso para mantenimiento el cual solo deberá realizarse por personal cualificado, así como en caso de fallo o avería. Se adjunta en el DVD del proyecto anterior el manual de instalación, y mantenimiento

2.4.2. Interfaces

Al igual que las placas CPU las interfaces se considerarán también como zona de acceso solo para personal cualificado. Estas interface se encuentran en cajas para electrónica en las garitas de los vigilantes anexa a los accesos de tornos y barreras.

Las interface son las encargadas de realizar la gestión del bus de comunicaciones y permitir la comunicación entre el sistema informático y los tornos y barreras.

Una interfaz permite entre otras funcionalidades guardar en memoria los ticajes de salida y entrada en caso de pérdida de comunicación con el servidor, para volcarlos posteriormente en este cuando se restablezca la conectividad. Otra función que realiza este dispositivo es el sistema AntiPassBack, que consiste en impedir que un usuario pueda entrar 2 veces seguidas sin haber salido entremedias, o viceversa, evitando la picaresca.

2.5. Sistema de control presencial: lectores de huellas

Los lectores biométricos realizan un control presencial del personal ubicado en las oficinas de las contratas de mantenimiento y en el edificio de administración. Al ser control presencial no limita ni controla el acceso a dichas zonas. El personal dado de alta en el sistema se identificará en ellos mediante la huella dactilar, al entrar y salir de las oficinas, descanso de comer, los festivos, etc., pudiendo así justificar su presencia en su lugar de trabajo

2.5.1. Lector KZSoftware FPW-4000

Estos terminales, con conexión Ethernet, se conectan directamente a la red de datos. Se utilizará el cableado de datos de los edificios para conectarlos. A través de esta red los terminales registrarán en el servidor los accesos y salidas en tiempo real. Esto conlleva muchas útiles funcionalidades, a la vez que sirve al cliente para controlar las horas declaradas por estos empleados.

Se adjunta en el DVD del proyecto anterior el manual de este modelo donde se detalla el procedimiento de instalación de los dispositivos, así como cómo administrarlos, solución los problemas más comunes, etc…

2.5.2. Situación de los lectores

Dada la versatilidad que ofrece el sistema de cableado estructurado de los edificios, la localización de los lectores dentro de los mismos se puede cambiar sin problema.

2.6. Sala de pantallas y servidor central

La sala de control de acceso y monitores se encuentra en el edificio de seguridad, donde trabaja la empresa de vigilancia.

Dicha sala contiene los elementos necesarios para poder hacer sus tareas de vigilancia y control de manera telemática. Se puede hacer entre otras cosas:

- Visualizar las imágenes proporcionadas por las cámaras.
- Visualizar las grabaciones de las cámaras.
- Comprobar el censo del personal en planta en tiempo real (control de accesos).
- Comprobar el censo del personal de contratas (control presencial, lector de huellas).

- Consultar el estado de los permisos de acceso de personal en caso de problemas de estos al intentar acceder.
- Proporcionar información al personal de vigilancia repartido por todas las zonas (sistema de radio fuera del alcance del presente documento).
- Esta sala quedará disponible para otras necesidades futuras de centralización operativa de dicha empresa en su tarea de vigilancia.

Esta sala de monitores, es un IDF directo del MDF. Al armario de comunicaciones llega un par de fibras del MDF (más los pares de backup) y salen otros pares para conectar a los siguientes IDFs.

2.6.1. Monitores: Dell UltraSharp 307WFP-HC 30”

El número de cámaras simultáneas que se quieran visualizar y el modo de visualización dentro de los monitores es seleccionable. Como hay modos de visualización en los que se pueden visualizar hasta 4x4 cámaras, la resolución nativa de los monitores debía ser la mayor posible, para que a cada cámara le corresponda una porción de imagen lo más nítida posible.

Los monitores elegidos para este proyecto fueron los **UltraSharp 307WFP-HC** de la marca **DELL** de tamaño 30 pulgadas. Tienen una resolución original de 2.560x1.600 pixels, por lo que en el peor de los casos, en el que el modo de visualización sea 4x4 cámaras, estas se mostrarán en una resolución de 640x400 cada una.

2.6.2. Rack de comunicaciones

Un rack es un bastidor destinado a alojar el equipamiento electrónico, informático y de comunicaciones. Sus medidas están normalizadas para que sea compatible con equipamiento de cualquier fabricante. Los racks son un armazón metálico con un ancho normalizado de 19 pulgadas, mientras que el alto y el fondo son variables para adaptarse a las distintas necesidades. El armazón cuenta con guías horizontales donde puede apoyarse el equipamiento, así como puntos de anclaje para los tornillos que fijan dicho equipamiento al armazón.

El Rack elegido fue de la gama **LOGIC** del fabricante **RETEX.** Toda la gama se adjunta en el DVD del proyecto anterior. Así mismo se incluyeron manuales de instalación y mantenimiento.

2.6.3. Videograbador: SCATI LABS – VisionSurfer

VisionSurfer Serie M de **Scati Labs** es un vídeo grabador digital con conectividad IP de hasta 32 cámaras IP (según modelo). El almacenamiento se realiza en un sistema rack que ofrece un total de **800/960 (PAL/NTSC)** imágenes por segundo para los 32 canales de vídeo. Herramientas de software como SurferWatcher permiten acceder y gestionar el equipo de forma remota y segura por personal autorizado. Se incluye un Servicio Web para el acceso mediante navegador.

2.6.4. Software: SCATI LABS – VisionSurfer

El software de visualización mural **SurferWall** de **Scati Labs, S.A.** está formado por hasta 4 monitores TFT en los que es posible configurar de forma totalmente flexible qué se desea visualizar y con qué formato. Se puede organizar el puesto de control de acuerdo a las necesidades y preferencias de seguridad. Permite definir el formato de pantalla que se aplica a cada uno de los monitores y qué ventanas van a actuar como monitores de alarma. En cada una de las ventanas definidas se asigna la cámara deseada, una preposición o una secuencia de cámaras para la monitorización en tiempo real. Para facilitar estas tareas se utilizan los escenarios de visualización, un conjunto de configuraciones que se aplican en bloque.

Capítulo 3
Sistema Anti-Intrusión

3.1 Introducción

El sistema de Intrusión actuará sobre el vallado perimetral de la planta. Este sistema se encargará de comunicar al centro de seguridad las alarmas por posibles intentos de acceso no permitido que se estén produciendo en el recinto.

El conjunto del sistema estará compuesto por 2 sistemas de tecnología diferente, además del CCTV, lo que dotará de una seguridad redundante frente a sistemas de una sola tecnología. Estos sistemas serán:

- Sistema de detección en vallado perimetral mediante fibra óptica sensora.
- Sistema de detección perimetral mediante barreras de microondas.

Ambos sistemas generan señales actuando sobre contactos cuando detectan un evento como alarma. Como a continuación se describirá, estos sistemas quedarán centralizados en el correspondiente rack de intrusión.

Para centralizar el sistema e integrarlo en la plataforma de seguridad WinPack, se instalará una central de alarmas Honeywell Galaxy G3. En esta central se cablearán los contactos generados por las diferentes zonas de cada uno de los 2 sistemas de detección perimetral.

Esta central dispondrá de conexión ETH, por lo que se conexionarán a la red LAN de seguridad. De esta manera podrá integrarse en la plataforma central de seguridad, permitiendo la visualización, control y monitorización de las zonas y las alarmas generadas por estos sistemas.

3.2 Fibra óptica sensora

El sistema de fibra óptica sensora requerirá de los siguientes materiales:

- Fibra óptica monomodo no sensora
- Fibra óptica monomodo sensora
- Cajas de empalme/terminación
- Electrónica de control

La electrónica de control se instalará en el correspondiente rack de la sala de control. Los equipos se integrarán en un subchasis de formato 19”, que alojará la correspondiente fuente de alimentación, y las tarjetas de detección por zonas. Para ello se instalará en el subchasis una tarjeta de control de 4 zonas y una tarjeta de control de 1 zona. Cada una de las zonas requiere para su funcionamiento de 2 fibras ópticas, una de ida o transmisión, y otra de vuelta o recepción, que se instalan en forma de bucle cerrado.

Desde este chasis que albergará la electrónica necesaria y mediante los correspondientes paneles de parcheo, se tenderá fibra óptica NO SENSORA hasta alcanzar la zona perimetral. Esta fibra óptica será una mera transmisora de la información, y su fin no será el de detección.

Debido a que en la parte de la electrónica de red requerimos de 2 fibras ópticas para cada zona(una de tx y otra de rx), se tenderá una manguera de fibra no sensora de 4 fibras ópticas por cada una de las zonas, de manera que podamos disponer de fibras ópticas de reserva.

Una vez en el perímetro, se instalarán en el vallado cajas de empalme/terminación. En estas cajas se realizará la transición de fibra óptica sensora a fibra óptica no sensora. Se ubicará una caja en el inicio y en el final de cada una de las zonas de detección.

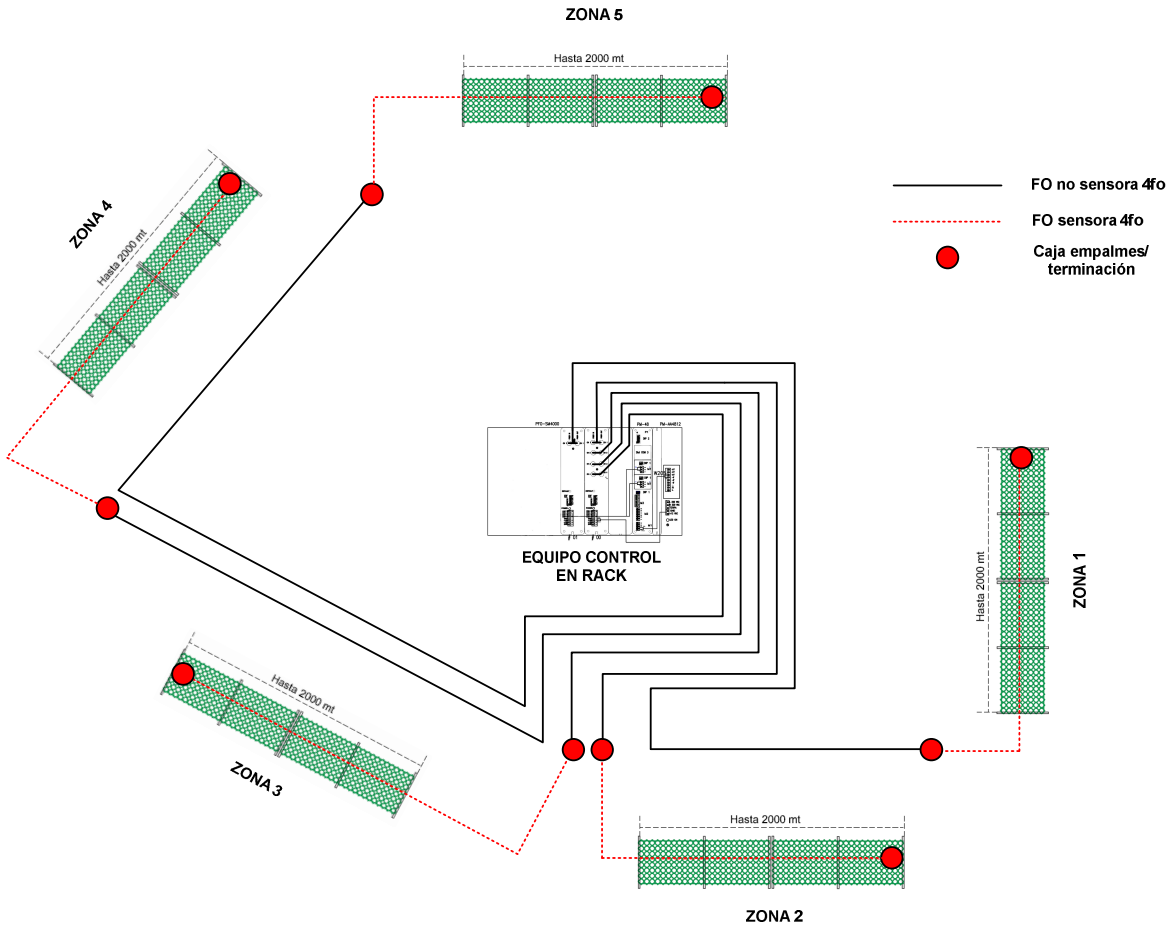


Figura 3.1 – Esquema de instalación del recinto

A lo largo de cada una de las zonas del vallado, se tenderá fibra óptica SENSORA de 4 fibras ópticas. Se instalará una única línea de fibra en el vallado por zona, ya que se considera que no es necesario ampliar con más líneas puesto que el perímetro dispone de otras medidas de seguridad como barreras MW y CCTV. La fibra sensora iniciará su recorrido en una caja de empalme/terminación, y lo finalizará en la

correspondiente caja de final de zona. La fibra óptica se anclará al vallado con los medios apropiados en función del tipo de valla y recorrido, pero principalmente se anclará mediante bridas o alambre metálico. Los accesos del cableado al vallado, se realizarán por el interior de tubo metálico instalado para este fin.

3.3 Sistemas de barreras MW

El sistema de detección de intrusión mediante barreras de microondas requerirá de los siguientes elementos:

- Conjunto emisor/receptor barrera MW
- Postes para instalación de barreras
- Armario de equipamiento conteniendo:
    1. Trafos de alimentación de emisores/receptores barreras
    2. Convertidores de contactos a fibra óptica
    3. Cajas de segregación y conexionado de fibra óptica
- Fibra óptica de transmisión de datos desde elementos de campo a sistema de control
- Cableado eléctrico para alimentación de los armarios que alojan los trafos
- Convertidores de fibra óptica a contactos
- Chasis para convertidores en rack

Cada una de las barreras está compuesta por un transmisor, que únicamente requiere de alimentación eléctrica, y de un receptor, que se configura para trabajar y enlazarse únicamente con el transmisor correspondiente. Este receptor, es quien genera las correspondientes alarmas por detección o por intento de sabotaje, trasmitiéndolas al sistema de control. El receptor requiere por tanto además de alimentación eléctrica, de un sistema que permita la transmisión de los correspondientes contactos cuando se genere alguna alarma.

Las barreras se irán enlazando una con otra, solapándose entre si la distancia suficiente para que no quede ningún espacio del vallado sin cobertura. En los puntos donde se realiza el cambio de una barrera a otra, se instalará un equipo transmisor de una barrera y el equipo receptor de la otra barrera.

Los equipos se instalarán sobre postes metálicos de entre 1 y 1,5 metros de altura, de manera que garanticen la cobertura total del vallado, tanto en altura, como en longitud, instalando equipos de rango de alcance adecuado. Se instalarán sobre estos postes armarios o cajas de intemperie que alojarán los trafos de alimentación eléctrica, y en el caso de los equipos receptores, alojarán los conversores de contactos a fibra óptica, para su transmisión al sistema de control y supervisión. En los puntos donde se enlaza una barrera con otra, se unificará todo el equipamiento en un único armario. Estos armarios dispondrán de tamper de alarma antisabotaje para detectar su apertura.

Las alarmas generadas por los equipos receptores de las barreras, serán convertidas a fibra óptica monomodo de 4 f.o. mediante conversores adecuados. Esta información será transmitida hasta el centro de control mediante una fibra óptica monomodo tendida para este fin.

Se tenderá una manguera de f.o. monomodo de 4 f.o. desde el rack de centralización hasta cada uno de los conversores de contactos a fibra distribuidos en

campo, uno por barrera. En los mismos armarios que alojan estos conversores, se instalarán cajas de conexiones de fibra, que nos permitirán realizar las conexiones correspondientes, estableciendo la comunicación entre los equipos de campo y el sistema central.

Una vez la fibra acceda al rack, se conexionará mediante los paneles de parcheo de fibra a los equipos de recepción, que se instalarán en un subchasis de 19" con fuente de alimentación incluida en el rack, sobre el que se instalarán las tarjetas con convertirán de fibra óptica a contactos secos de nuevo. Estos contactos, serán cableados hasta la central de alarmas de intrusión Honeywell Galaxy correspondiente.

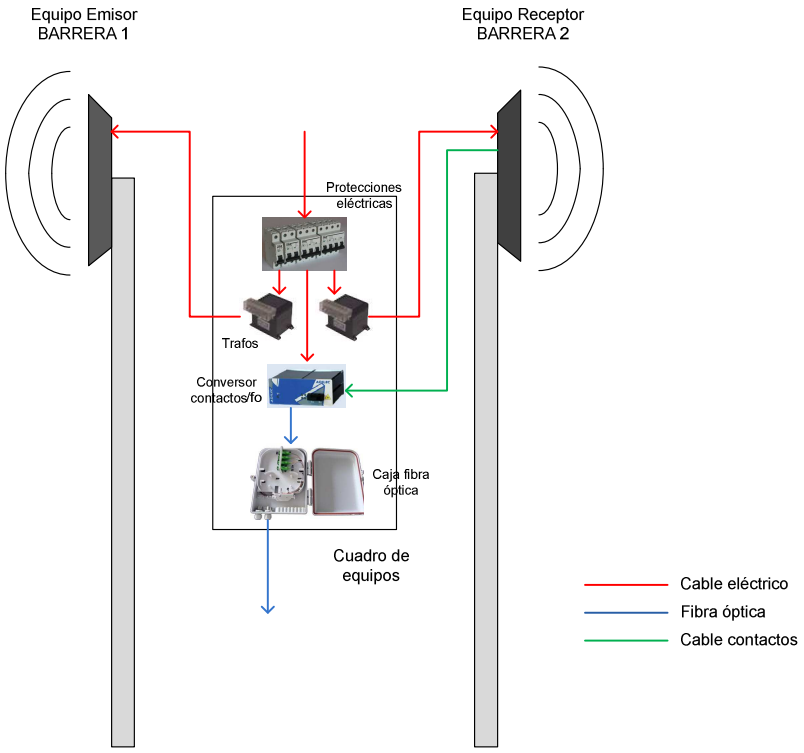


Figura 3.2 – Esquema de instalación de básica de barrera MW

3.4 Funcionalidades

Mediante la fibra óptica y los correspondientes conversores de medio, se podrá transmitir a la central de intrusión la alerta por un evento de detección, avería en alguno de los equipos o intento de sabotaje. Las alarmas generadas se gestionarán por una central de intrusión grado 3 Honeywell Galaxy de hasta 96 entradas. Se instalará la central en el edificio de seguridad y vigilancia, junto al rack de intrusión. Esta central recogerá las alarmas generadas en recinto.

Esta central se instalará con la tarjeta de red ETH, de modo que pueda ser conectadas a la red LAN. Una vez realizado esto, la central de intrusión se integrará en la plataforma de gestión WinPack, donde el conjunto se configurará de manera que reflejen en el software cada una de las diferentes alarmas que detectan los sistemas, provocando si es necesario una respuesta automática en el sistema CCTV mediante presets predefinidos.

En esta central podrán implementarse además de las alarmas generadas por los sistemas de protección perimetral, otras alarmas que se consideren de importancia, como por ejemplo las protecciones tamper de los armarios de equipamiento de campo de CCTV.

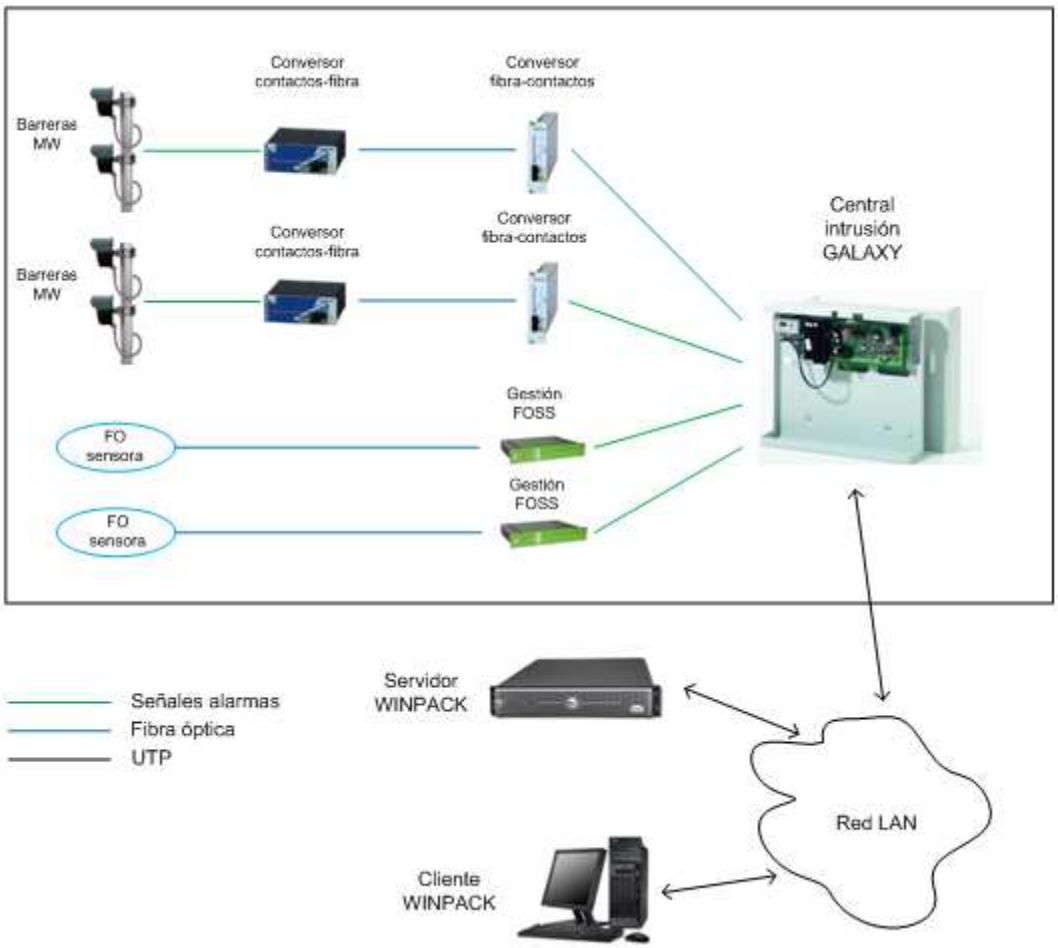


Figura 3.3 – Esquema general de conexionado del sistema anti-intrusión

3.5 Listado de material a instalar

DESCRIPCION ELEMENTO	UNIDADES	MODELO	FABRICANTE
Barreras MW 125 mts alcance	7	SI-125H	SICURALIA
Barreras MW 200 mts alcance	1	SI-300H	SICURALIA
Conversor TX contactos-fibra SM	8	NTO812M16	ADILEC
Conversor RX fibra-contactos	8	NRO812M11	ADILEC
Chasis 19” conversores	1	PAWAL	ADILEC
Procesador 1 zona fibra óptica sensora	1	PFO-SM10	GPS-SNAKE
Procesador 4 zonas fibra óptica sensora	1	PFO-SM40	GPS-SNAKE
Chasis 19” módulos SNAKE	1	PM-AR	GPS-SNAKE
Caja de empalmes/terminación fibra sensora	10	PSKA-JB	GPS-SNAKE
Central alarma hasta 96 zonas con tarjeta ETH y baterías	1	GALAXY C-096-D-E1	Honeywell
Módulo expansor 8E/4S	3	GXY-RIO	Honeywell
Teclado central intrusión	1	GXY-MK7	Honeywell

Tabla 3.1 – Listado de materiales para Sistema Anti-Intrusión

Capitulo 4
Conclusiones y líneas futuras

En este Trabajo Final de Grado se ha completado un sistema de seguridad de administración centralizada (previamente diseñado e instalado) con un sistema anti-intrusión, por lo que finalmente se han cubierto las siguientes necesidades:

Nuevo sistema

- Un sistema de alarma anti intrusión que valida todos los datos obtenidos en los otros sistemas, asegurándonos que solo el personal registrado en los accesos son los que realmente están en planta. Si se produce un acceso o intento de este en el perímetro una alarma advertirá de ello y se visualizará el lugar. Este sistema se ha integrado en los existentes.

Sistemas existentes (previamente diseñados e instalados)

- Control de acceso a la planta mediante el uso tornos, barreras y tarjetas, que identificarán a los trabajadores en una base de datos. El cliente, mediante la gestión de esta base de datos, autoriza o no el acceso a aplicando criterios como, por ejemplo, caducidad de cursos de seguridad, de carnets de conducir, revisión médica anual, etc.

- Control presencial del personal de las contratas en sus puestos de trabajo mediante el uso de lectores biométricos de huellas dactilares. El cliente proporciona a su departamento de costes un justificante de la presencia de dichas personas a fin de autorizar el pago por las horas trabajadas.

- Vigilancia activa del perímetro con una red cámaras de video. Estas cámaras están instaladas en torres autónomas pues se alimentan de energía solar y tienen una conectividad inalámbrica 3G. Una sala de pantallas centraliza el visionado y grabación de las imágenes para optimizar la gestión de estas.

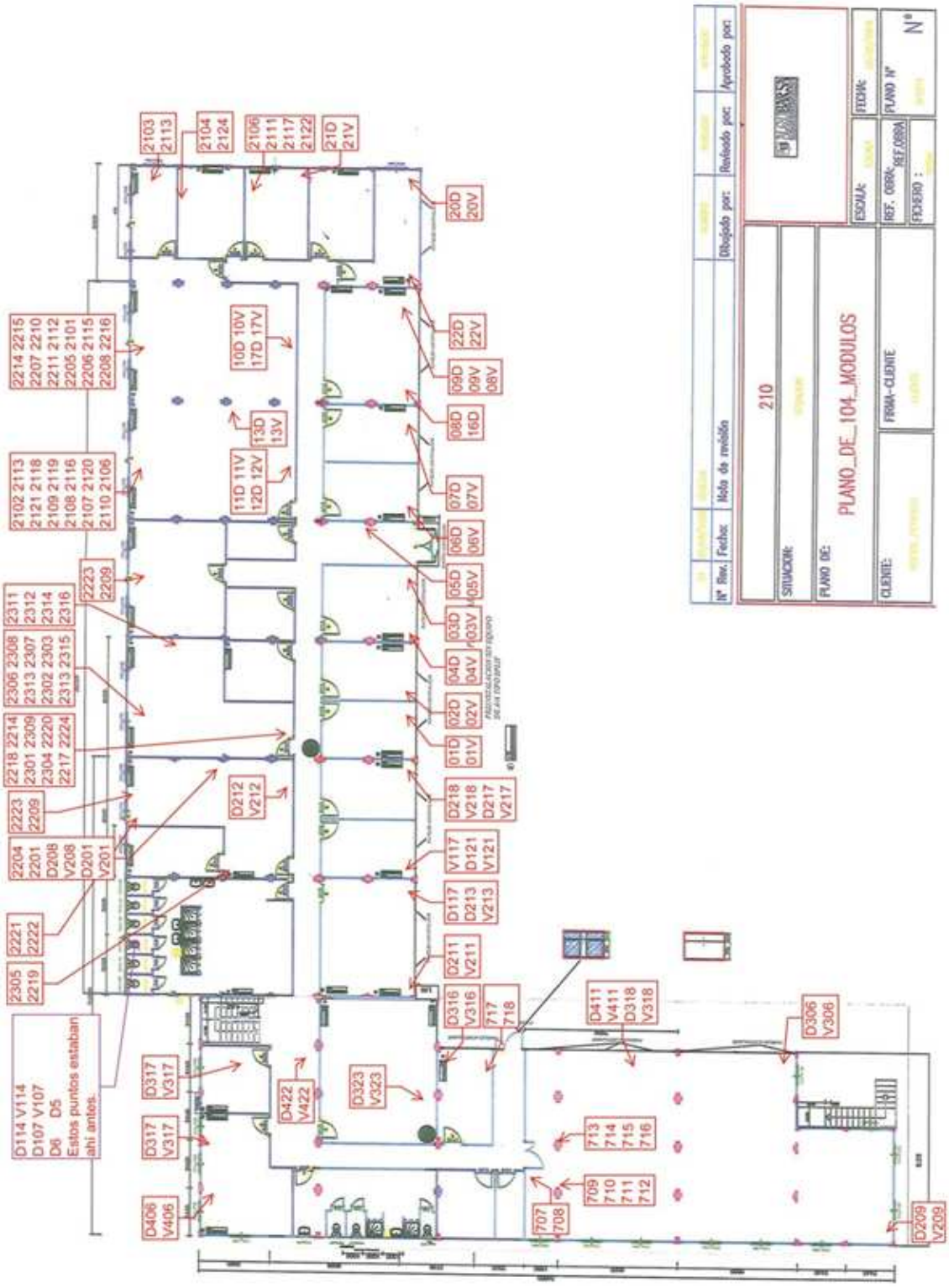
- Red cableada de las oficinas del edificio del cliente. El estudio, planificación y diseño de este tipo de redes se puede encontrar hoy día en cualquier local comercial de nueva construcción que quiere dotar a su empresa de las nuevas tecnologías para trabajar, así como en cualquier otra oficina que decide renovar sus instalaciones.

La gran escalabilidad y adaptabilidad del proyecto anterior ha permitido la integración del nuevo sistema: el sistema anti-intrusión. Esta versatilidad que caracteriza todo el sistema final permite la agregación de nuevos sistemas y servicios, así como adaptar los existentes.

ANEXOS

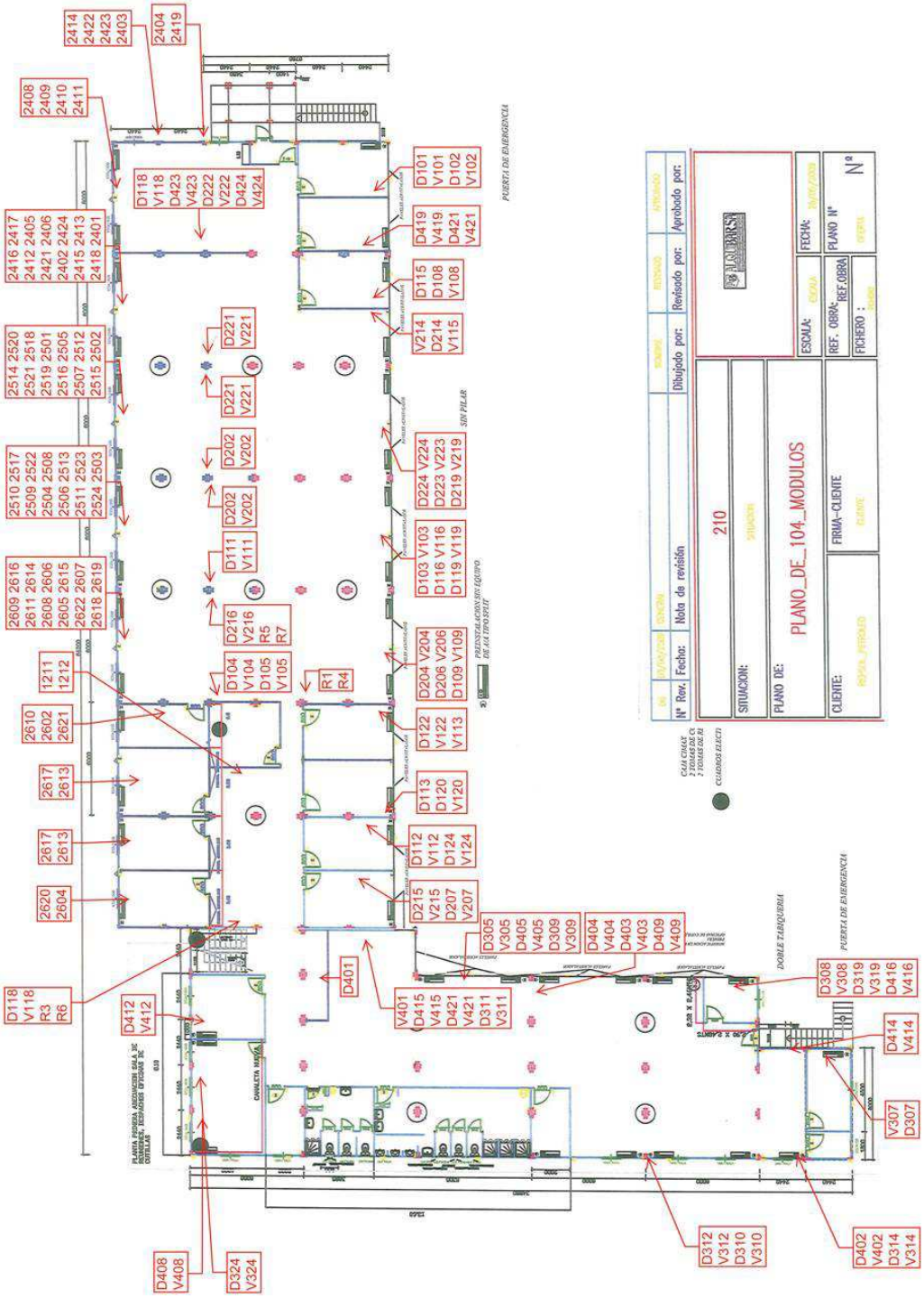
Anexo I

Correspondecias “Patch Panel”- Oficina *Planta baja*



Correspondecias “Patch Panel” Oficina

Planta primera



Anexo II

TIA-568B

La TIA/EIA-568-B son tres estándares que tratan el cableado comercial para productos y servicios de telecomunicaciones. Los tres estándares oficiales son:

ANSI/TIA/EIA-568-B.1-2001,

ANSI/TIA/EIA-568-B.2-2001

ANSI/TIA/EIA-568-B.3-2001.

Se publicaron en 2001 sustituyendo al conjunto TIA/EIA-568-A, quedando estos obsoletos.

La característica más conocida del TIA/EIA-568-B.1-2001 es la asignación de pares/pines en los cables de 8 hilos y 100 ohmios (Cable de par trenzado). Esta asignación se conoce como T568A y T568B, y a menudo es nombrada (erróneamente) como TIA/EIA-568A y TIA/EIA-568B.

TIA/EIA-568-B define estándares que permiten el diseño e implementación de sistemas de cableado estructurado para y entre edificios. Estos estándares definen los tipos de cables, distancias, conectores, arquitecturas, terminaciones de cables y características de rendimiento, requisitos de instalación de cable y métodos de pruebas de los cables instalados. El estándar principal, el TIA/EIA-568-B.1, define los requisitos generales, mientras que TIA/EIA-568-B.2 se centra en componentes de sistemas de cable de pares balanceados y el -568-B.3 aborda componentes de sistemas de cable de fibra óptica.

La intención de estos estándares es proporcionar una serie de prácticas recomendadas para el diseño e instalación de sistemas de cableado que soporten una amplia variedad de los servicios existentes, y la posibilidad de soportar servicios futuros que sean diseñados considerando los estándares de cableado. El estándar pretende cubrir un rango de vida de más de diez años para los sistemas de cableado comercial. Este objetivo ha tenido éxito en su mayor parte, como se evidencia con la definición de cables de categoría 5 en 1991, un estándar de cable que satisface la mayoría de requerimientos para 1000BASE-T, emitido en 1999.

Todos estos documentos acompañan a estándares relacionados que definen caminos y espacios comerciales (569-A), cableado residencial (570-A), estándares de administración (606), tomas de tierra (607) y cableado exterior (758). También se puede decir que este intento de definir estándares permitió determinar, además del diseño e implementación en sistema de cableado estructurado, qué cables de par trenzados utilizar para estructurar conexiones locales.

Anexo III

Barreras de microondas para protección exterior

Sicuralia

Barreras de microondas para protección exterior

Nivel III

SI-300H, SI-200H, SI-125H, SI-085H, SI-055H

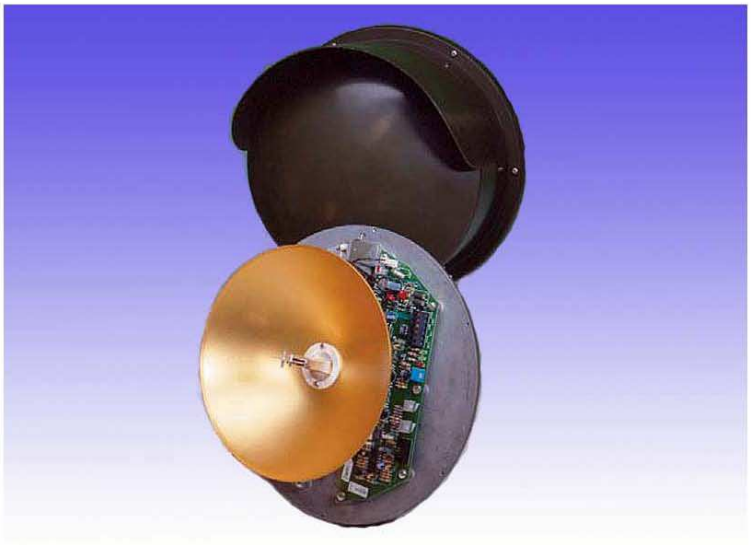
La serie de barreras de microondas SI-xxxH con sus 204m de alcance representa un descubrimiento en la protección perimetral al aire libre. Su circuito innovador y la posibilidad de ajustar sus patrones de radiación "in-situ", hace que la misma puede usarse prácticamente bajo cualquier condición medioambiental.

Es posible usar más de una barrera en la misma área, gracias a los cuatro canales de frecuencia FM disponibles y fácilmente programables en la instalación. Para proyectos de gran tamaño se pueden usar tantas barreras de microondas como sea necesario, siguiendo simplemente las instrucciones específicas del manual.

La electrónica de control y la antena, están sólidamente fijadas a una base de aluminio fundido y protegidas por una carcasa de plástico ABS resistente a UV, sellada y con visera color verde/ camuflaje.

Tiene capacidad para alojar una batería de 12Vcc/2.1Ah que le asegura una autonomía de funcionamiento en caso de pérdida de alimentación de hasta 36 horas a la vez que actúa como un filtro contra las perturbaciones eléctricas.

La barrera viene completa, lista para instalar en postes con un diámetro de 70 a 110mm. Las abrazaderas de fijación vienen incluidas.



- **Barrera de microondas biestática**
- **Insensible a vibraciones, viento, niebla, lluvia, nieve, polvo y temperaturas extremas**
- **Bajo consumo de corriente (80mA por barrera)**
- **4 canales de frecuencia FM ajustables en campo**
- **Frecuencia de funcionamiento en banda X**
- **Procesado de señal en anillo cerrado (PLL) con amplio rango dinámico**
- **Capacidad de sincronización de multiples barreras**
- **Capacidad de modificación del patrón de detección para una detección mejorada**
- **Mas de 36 horas de autonomía de funcionamiento con batería de "back-up" interna de 12V 2.1Ah**
- **Clasificación de nivel de seguridad IMQ III**

REFERENCIAS

Referencias

Transceiver Allied Telesis - AT-MC1004:

http://www.alliedtelesis.com/products/detail.aspx?pid=7&lid=2

http://www.alliedtelesis.com/media/datasheets/mc1004_ds.pdf

http://www.alliedtelesis.com/media/datasheets/guides/mc1004-5_ig_b.pdf

Switch DELL PowerConnect 2724:

http://www.dell.com/us/en/gen/networking/pwcnt_2724/pd.aspx?refid=pwcnt_2724&s=gen

http://www.dell.com/downloads/global/services/sd/sddsp0010.pdf

http://docs.us.dell.com/support/edocs/network/PC27xx/sp/UG/PDF/UG_SPd.zip

ZKSoftware - FPW-4000

http://www.zksoftware.es/products.php?id=22

http://www.tvcenlinea.com/promociones/news/20070922/manual.pdf

DellTM UltraSharpTM 3007WFP-HC 30”

http://accessories.euro.dell.com/sna/productdetail.aspx?c=es&l=es&cs=esdhs1&sku=142657

RETEX – Gama de racks LOGIC

http://www.retex.es/paginas/home_es.html

ACTi CAM-6600 Series

http://www.acti.com/product/detail/IP_Speed_Dome/CAM-6600_Series

MOBOTIX - Cam DualNight M12

http://www.mobotix.com/esl_ES/region/index/esl_ES/?URL=Productos/C%c3%a1maras/DualNight-M12

SCATI LABS - SurferWall

http://www.scati.com/product/product.php?id_category=2&id_product=24

SCATI LABS - VisionSurfer

http://www.scati.com/product/index.php?id_category=13