_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE UPV INGENIEROS DE TELECOMUNICACIÓN

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

SISTEMA DE GESTIÓN INTEGRADO PARA LA VIGILANCIA DE UN ÁREA RESIDENCIAL

Alumno: José Fuster Sánchez

Tutora: Clara Pérez Fuster

Cotutor: Fulgencio Montilla Meoro

Trabajo Fin de Grado presentado en la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universitat Politècnica de València, para la obtención del Título de Graduado en Ingeniería de Tecnologías y Servicios de Telecomunicación

Curso 2016-17

Valencia, 21 de marzo de 2017

Resumen

La renovación e introducción de nuevos medios guiados e inalámbricos ha permitido la consolidación de las tecnologías móviles. Es por este motivo que la implementación de una red de elementos de vigilancia y control de accesos con su correspondiente aplicación, que permita su monitorización y manejo a través de un smartphone sea, a día de hoy, una idea prometedora.

El proyecto propuesto trata de abarcar los elementos más relevantes de un sistema de seguridad y vigilancia a gran escala, tales como los sistemas CCTV con tecnología IP, el control de acceso a áreas públicas y privadas y el manejo de la iluminación deportiva a través de un terminal móvil. La aplicación incluirá, además, un sistema de geolocalización y posicionamiento GPS de los vehículos designados al patrullaje del área residencial.

Dicho proyecto irá dirigido a los responsables encargados de la gestión y administración de un área residencial con su correspondiente club deportivo, así como a los activos humanos designados por la empresa de seguridad competente.

Resum

La renovació i introducció de nous medis guiats e inalàmbrics ha permés la consolidació de les tecnologies mòbils. Es per aquest motiu que la implementació de una xarxa d'elements de vigilància i control d'accesos amb la seua aplicació corresponent, que permeta la seua monitorització i maneig a través d'un smartphone siga, a dia d'avui, una idea prometedora.

El projecte proposat tracta d'abarcar els elements més relevants d'un sistema de seguretat i vigilancia a gran escala, com ara el sistemes CCTV amb tecnologia IP, el control d'accés a àrees públiques i privades i el maneig de la il·luminació deportiva mitjançant de una terminal mòbil. La aplicació inclourà, a mes, un sistema de localització i posicionament GPS dels vehícles designats per al patrullatge del area residencial.

Aquest projecte anirá dirigit als responsables encarregats de la gestió i l'administració d'una àrea residencial amb el seu club esportiu corresponent, aixi com als actius humans designats per la empresa de seguretat competent.

Abstract

The renewal and introduction of new wireless and guided media has allowed the consolidation of mobile technologies. It is for this reason that the implementation of a network of monitoring elements and access control with its corresponding application, which allows monitoring and management through a smartphone that is, today, a promising idea.

The proposed project is to cover the most relevant elements of a security system and surveillance on a large scale, such as CCTV systems with IP technology, access control to public and private areas and the management of the lighting sport through a mobile terminal. The application shall include, in addition, a system of geolocation and GPS positioning of vehicles patrolling the residential area.

The project will be directed to those responsible for the management and administration of a residential area with its corresponding sports club, as well as to the human assets designated by the competent security company.

Índice

1. MEMORIA DESCRIPTIVA

1.1. ANTECEDENTES

A lo largo de esta memoria se propone un proyecto de seguridad y control destinado a cubrir una serie de deficiencias y carencias dentro del ámbito de la seguridad en una de las urbanizaciones de lujo más relevantes de la provincia de valencia. Se trata pues, de una zona residencial que, a pesar de hallarse a varios kilómetros de un núcleo urbano, cuenta con todas las comodidades y todos los servicios que puede ofrecer una zona residencial de esta índole. Se pueden destacar los siguientes:

- Servicio de Club Social
- Servicio de vigilancia 24/7
- Servicio de mensajería
- Servicio de restaurante
- Servicio de jardinería
- Servicio de recogida de basura y podas

De entre todos los servicios que ofrece la urbanización a sus residentes, este proyecto se centra en las insuficiencias y debilidades del servicio de vigilancia y control de accesos de personas, tanto en el club social, como en otras zonas y sectores de la urbanización.

En lo que al servicio de vigilancia y seguridad se refiere, actualmente está compuesto por una plantilla de 9 vigilantes de seguridad, los cuales realizan turnos de 8 horas en grupos de tres. Cada uno de los guardas tiene asignada una tarea concreta, permaneciendo uno de ellos, de forma continua, en la sala de control, mientras el equipo restante se dedica a tareas de patrullaje y asistencia de incidencias. Para las tareas de patrullaje, la urbanización cuenta con dos vehículos claramente identificativos que permiten minimizar el tiempo de respuesta ante incidencias, y ayuda a establecer medidas disuasorias ante intrusiones, actos vandálicos o accesos no permitidos.

La urbanización cuenta también con una sala de control (garita de vigilancia), a través de la cual se monitorizan y se controlan los distintos sistemas con los que cuenta la zona residencial. Además, es donde se almacenan todos los protocolos de actuación ante cualquier tipo de incidencia. La sala de control se encuentra ubicada en la entrada/salida de la urbanización, junto a la sala de telecomunicaciones y a las oficinas de administración.

Figura 1. Sala de control.

Actualmente hay instaladas una serie de cámaras de video-vigilancia analógicas en algunos puntos clave de la urbanización, siendo estas visualizadas y gestionadas desde la sala de control. Otra de las infraestructuras con las que cuenta la urbanización es la sala de telecomunicaciones, que se puede apreciar en la *Figura 2*. Está dedicada al alojamiento del servidor de administración y al grabador analógico sobre el que recae a día de hoy todo el peso del sistema CCTV, así como la matriz de video que permite al guarda de seguridad de la sala de control poder visualizar varias cámaras al mismo tiempo en sus dos monitores. También se encuentra alojado en la sala de telecomunicaciones el sistema de alarmas privadas de las viviendas que cuentan con sistema anti-intrusión. Será en esta sala de telecomunicaciones donde se ubicarán todos los equipos y servidores relacionados con los sistemas que se implementarán y que se proponen en este proyecto:

- Servidor principal, que alojará el software de gestión de control de accesos y el sistema SCADA
- Video-grabador digital o NVR
- Equipos de fibra óptica
- Servidor secundario

Ubicadas junto a la sala de telecomunicaciones se encuentran las oficinas de administración de la urbanización (Figura 2). En ellas se realizan labores de gestión, administración y dirección de la zona residencial en cuestión. Entre otras, las tareas que atañen a este proyecto son funciones de altas de inscripciones de usuarios para el club social, reserva de pistas deportivas, recepción de paquetes de mensajería, etc.

Figura 2. Oficinas y sala de telecomunicaciones.

Una vez implementado el proyecto quedarán instalados los siguientes equipos:

- Equipo PC de dirección con el software de control de accesos, sistema SCADA y accesos al NVR
- Equipo PC de recepción con acceso al software de control para realizar altas o bajas de usuario, reservas, etc
- Impresoras de tarjetas MIFARE
- Validador de tarjetas

En lo que al club social se refiere, se encuentra en la parte alta de la urbanización y es de carácter privado. Cuenta con multitud de instalaciones deportivas, así como con un restaurante y salas de actividades lúdicas. Actualmente, el acceso a este club social es libre a pesar de que se considera privado. Por este motivo, es necesaria y urgente la instalación de un sistema de control de accesos de personas que registre y filtre los accesos.

El club social cuenta con tres puntos de acceso, sin incluir la entrada de suministros. Cada uno de los accesos cuenta con la cobertura de una cámara analógica fija, que permite controlar las entradas desde la sala de control. Cuando se implante el proyecto, las cámaras actuales quedarán sustituidas por otras con mayor resolución y capacidades, y se instalará un control de accesos que podrá gestionarse a través de una aplicación web y móvil.

1.2. DESCRIPCIÓN DE LA ZONA RESIDENCIAL

1.2.1 FORMA, TOPOGRAFÍA, SUPERFICIE Y LINDES

En la *figura 3* se aprecia la topografía y la forma que posee la zona residencial en la cual se desarrollará el proyecto. La superficie total aproximada ronda las 80 hectáreas y se encuentra en la falda de un monte, por lo que se encuentra ligeramente inclinada hacia el sur. La distancia que existe entre los extremos opuestos de la urbanización es de 1,07 kilómetros. El perímetro linda, prácticamente en su totalidad, con campos de cultivo y otra urbanización con la que es limítrofe en su zona sur.

Figura 3. Mapa físico.

Toda la información relacionada con superficie construida, sin construir, dedicada al club social y dedicada a zonas comunes se adjunta en la siguiente tabla:

Cuadro de superficies	Datos
Número de parcelas	240
Superficie media por parcela	1000 m^2
Superficie construida	240.000 m^2
Superficie Jardines/ Parques	200.000 m^2
Superficie Club Social	130.000 m^2
Superficie restante	230.000 m^2

Tabla 1. Datos territoriales de la urbanización.

1.2.2 USO DE LA URBANIZACIÓN Y OCUPACIÓN

La urbanización se clasifica como zona residencial de carácter privado, aplicándose un uso residencial y/o vacacional a la misma. Sin embargo cabe mencionar que el acceso a sus calles y vías es de carácter público.

1.2.3 HORARIO DE APERTURA Y CIERRE

Se han de distinguir diversas franjas horarias de atención al público ya que por un lado, el servicio de protección y vigilancia de la urbanización está operativo las 24 horas al día, siete días a la semana. En cambio, el horario de dirección y administración de la urbanización es de 08:00 am a 14:00 pm de lunes a viernes, y el horario del club social abarca desde las 08:00 am hasta la 24:00 los siete días de la semana.

1.2.4. SITUACIÓN Y EMPLAZAMIENTO DE LA INSTALACIÓN

La urbanización donde se llevará a cabo el proyecto se encuentra en la zona norte de la provincia de Valencia, próxima a las siguientes coordenadas:

Latitud	39º 38’ 1,38” Norte
Longitud	0º 20’ 14,47” Oeste

Tabla 2. Coordenadas.

El entorno físico en el que se encuentra el área residencial es generalmente montañoso y expuesto a vientos de levante y a la humedad propia de la zona, sin embargo la urbanización está perfectamente habilitada y cuenta con todas las comodidades propias de una urbanización de lujo.

La instalación abarcará prácticamente la totalidad de la zona residencial, ya que será necesario cubrir las zonas vulnerables a la intrusión, lo que implicará instalar cámaras de video-vigilancia a lo largo de todo el perímetro de la urbanización. También será necesario trabajar en el interior del club social y de la sala de control.

1.4. OBJETIVOS DEL PROYECTO

La memoria del presente documento tiene como finalidad definir y especificar las características técnicas, de gestión y económicas del proyecto de video-vigilancia y control de un área residencial de tamaño medio. Dicha memoria permitirá establecer las directrices y las bases de desarrollo y ejecución de la instalación en la urbanización pertinente, del mismo modo que estudiará los modos de minimizar las paradas y fallos técnicos de la instalación una vez implementada.

El objetivo del proyecto es proveer a la dirección de una herramienta capaz de dinamizar y minimizar el tiempo y el coste humano que requiere realizar las diversas tareas de mantenimiento, seguridad y control dentro de una urbanización residencial. Así mismo, se pretende incrementar la seguridad de los residentes introduciendo herramientas que permitan a los vigilantes obtener información e imágenes en tiempo real que les ayuden a aumentar su eficacia y a minimizar su tiempo de respuesta a la hora de atender cualquier tipo de incidencia. La introducción de la plataforma móvil facilitará el control y la comunicación con el sistema en aquellas ocasiones en las que las personas responsables de su gestión no se hallen en sus bases operativas.

Para lograr el objetivo mencionado anteriormente se implementarán los siguientes sistemas:

- Sistema de circuito cerrado de TV o CCTV
- Sistema domótico de control de accesos
- Sistema de control y gestión remota Scada
- Sistema de posicionamiento GPS a través de la app

Cada uno de los sistemas presentados en esta memoria dispondrá, en mayor o menor medida, de independencia con respecto al resto de sistemas. Sin embargo, todos ellos se complementarán para dotar a la instalación de la versatilidad y la potencia necesaria para hacer frente a los problemas típicos de una zona residencial, que a saber, pueden ser:

- Intrusiones no deseadas
- Vandalismo
- Robos y hurtos de propiedades públicas y privadas
- Sabotaje

Otro de los objetivos que se ha de alcanzar con la implementación del proyecto es el de disuadir para anticiparse a la situación de intencionalidad de personas ajenas a actuar de forma malintencionada contra personas y/o bienes materiales relacionados con la zona residencial en cuestión. Partiendo de la base de que la seguridad total no es posible, el planteamiento del proyecto será minimizar al máximo las posibilidades de verse afectado por cualquier tipo de eventualidad.

1.5. LEGISLACIÓN A APLICAR

Durante la planificación y el desarrollo del proyecte se deberán tener en cuenta las siguientes consideraciones legales:

REBT: Reglamento Electrotécnico de Baja Tensión (Decreto 814/2002, de 2 de agosto) y sus instrucciones Técnicas Complementarias, ITC. BT 01 a BT 51, adjuntadas al presente Real Decreto.

REAL DECRETO 1454/2005. 02/12/2005. Ministerio de Industria, Turismo y Comercio. Modifica determinadas disposiciones relativas al sector eléctrico. *Modifica, entre otras, el Real Decreto 1955/2000 BOE 23/12/2005.

REAL DECRETO 842/2002. 02/08/2002. Ministerios de Ciencia y Tecnología. Aprueba el Reglamento Electrotécnico para Baja Tensión. *Modificado por REAL DECRETO 560/2010. BOE 18/09/2002.

Normas autonómicas - Comunidad Valenciana

ORDEN 20/12/1991. Consellería de Industria, Comercio y Turismo. Norma Técnica para Instalaciones de Media y Baja Tensión (NT-IMBT 1400/0201/1). *Ver Res 12-5-1994 (proyectos tipo) *Modificada por: Res. 22-2-2006; Res 21-3-2007; Res. 7-4-2008. DOGV 07/04/1992 Ver texto…/Resolución 20-5-94/Resolución 22-2-06/Resolución 21-3-07/ Resolución 7-4-08. Otros documentos.

REAL DECRETO 1000/2010. 05/08/2010. Ministerio de Economía y Hacienda. REGULA EL VISADO COLEGIAL OBLIGATORIO. *Entra en vigor el día 1 de octubre de 2010. *Deroga toda norma de igual o inferior rango que se oponga a lo dispuesto en este Real Decreto. BOE 06/08/2010.

Ley 23/1992, de 30 de julio, de Seguridad Privada. (Boletín oficial del Estado núm. 186 de 4 de agosto de 1992).

Modificación de la Ley 23/1992 de julio, de Seguridad Privada.

Real Decreto 1628/2009, del Ministerio del Interior, de 30 de octubre de 2009, por el que se modifican determinados preceptos del Reglamento de Seguridad Privada, aprobado por Real Decreto 2364/1994, de 9 de diciembre, y del Reglamento de Armas, aprobado por Real Decreto 137/1993, de 29 de enero. (Boletín oficial del Estado número 263 de 31 de octubre de 2009).

Real Decreto 4/2008, del Ministerio del Interior, de 11 de enero de 2008, por el que se modifican determinados artículos del Reglamento de Seguridad Privada (Boletín oficial del Estado núm. 11 de 12 de enero de 2008)

Real Decreto-Ley 8/2007, de la Jefatura del Estado de 14 de septiembre de 2007, por el que se modifican determinados artículos de la Ley 23/1992, de 30 de julio, de Seguridad Privada (Boletín oficial del Estado núm. 225 de 19 de septiembre de 2007)

Real Decreto-Ley 2/1999, de 29 de enero, por el que se modifica la Ley 23/1992, de 30 de julio, de Seguridad Privada (Boletín oficial del Estado núm. 26 de 30 de enero de 1999)

Real Decreto 195/2010, del Ministerio del Interior, de 26 de febrero de 2010, por el que se modifica el Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada, para adaptarlo a las modificaciones introducidas en la Ley 23/1992, de 30 de julio, de Seguridad Privada, por la Ley 25/2009, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la ley sobre el libre acceso a las actividades de servicios y su ejercicio. (Boletín oficial del Estado número 60 de 10 de marzo de 2010)

Real Decreto 195/2010, de 26 de febrero, por el que se modifica el Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada, para adaptarlo a las modificaciones introducidas en la Ley 23/1992, de 30 de julio, de Seguridad Privada, por la Ley 25/2009, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la ley sobre el libre acceso a las actividades de servicios y su ejercicio.

Normas de las Políticas de Seguridad Informática

Las normas son un conjunto de lineamientos, reglas, recomendaciones y controles con el propósito de dar respaldo a las políticas de seguridad y a los objetivos desarrollados por éstas, a través de funciones, delegación de responsabilidades y otras técnicas, con un objetivo claro y acorde a las necesidades de seguridad establecidas para el entorno administrativo de la red organizacional.

Normas a aplicar: debe contener los requisitos de seguridad que se declaran de obligado cumplimiento. Podrán agruparse los requisitos por categorías, estableciendo apartados donde se agrupen los requisitos relacionados. También los enunciados pueden numerarse para poder posteriormente referenciarlos. Documentos relacionados: se indican otros documentos del marco normativo que pudieran estar relacionados con el cumplimiento de la norma.

Normas: Con el fin de proporcionar un marco de Gestión de la Seguridad de Información utilizable por cualquier tipo de organización, independientemente de su tamaño o actividad, se ha creado un conjunto de estándares bajo el nombre de ISO/IEC 27000. MARCO LEGAL Y JURÍDICO DE LA SEGURIDAD. NORMATIVAS DE SEGURIDAD. Desde la publicación del la Ley Orgánica de Protección de Datos de Carácter personal en el año 1999 hasta la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos del año 2007, hay una serie de leyes que, de una manera u otra, están relacionadas con la seguridad de la información, además de numerosas regulaciones sectoriales en diversos ámbitos: seguridad, financiero, telecomunicaciones, agrario, etc.

Ley Orgánica 15/99 de Protección de Datos de Carácter Personal

Esta ley se complementa con el reglamento estipulado en el Real Decreto RD 1720/2007.

El objetivo de esta Ley es garantizar y proteger, en lo concerniente al tratamiento de los datos personales (automatizados o no), las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor e intimidad personal y familiar.

Los derechos recogidos en la LOPD son:

- Las personas de las que se almacena datos de carácter personal, tienen una serie de derechos amparados por esta ley.
- Derecho de información: Cuando alguien proporciona sus datos debe ser informado de que van a ser almacenados.
- Derecho de acceso, cancelación, rectificación y oposición: la persona puede ver la información que se dispone de él, puede cambiar esos datos para que sean correctos y exactos, cancelar la información que se almacene de él y oponerse a que se almacene.

Normativa sobre instalaciones de cámaras de CCTV y videograbadores

En relación sobre la normativa que regula la instalación de cámaras y videograbadoras de imágenes, por motivos de seguridad, en un establecimiento público, se expone lo siguiente:

En el plano normativo que regula la seguridad privada, la Ley 23/92, de 30 de Julio, de Seguridad Privada, en su artículo 5 y el Reglamento de Seguridad Privada, aprobado por Real Decreto 2364/1994, de 9 de diciembre, en su artículo 1.

Posteriormente, la Orden Ministerial de 23 de abril de 1997, por la que se concretan determinados aspectos en materia de empresas de seguridad, contribuyó a clarificar más la cuestión, al establecer en su apartado vigésimo cuarto que *"a los efectos de la normativa reguladora de la seguridad privada, se entenderá por sistema de seguridad, el conjunto de aparatos o dispositivos electrónicos contra robo e intrusión, cuya activación sea susceptible de producir intervención policial"*.

Continua este apartado vigésimo cuarto de la citada Orden Ministerial, estableciendo que: *"su instalación deberá ser efectuada por una empresa de seguridad autorizada para dicha actividad y ajustarse a lo dispuesto en los artículos 40 (aprobación de material), 42 (certificado de instalación) y 43 (revisiones) del Reglamento de Seguridad Privada"*.

Sin embargo, es necesario tener presente la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la propia Imagen, con objeto de conocer las responsabilidades en las que se puede incurrir,

Cuando la utilización de las vídeo cámaras tenga la consideración de intromisión ilegítima en el ámbito de protección de dicha Ley.

Finalmente, sería necesario tener en cuenta lo regulado por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, para el supuesto de que las imágenes grabadas tengan la consideración de dato personal y pudieran ser incorporadas a un fichero.

Normativa UNE

UNE 50136-7:2005. EX.
Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte7: Guía de aplicación.

UNE 50136-4:2005.EX.
Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 4: Equipos anunciadores usados en centrales receptoras de alarma.

Seguridad y salud en el trabajo

REAL DECRETO 337/2010. 19/03/2010. Ministerio de Trabajo y Asuntos Sociales. Modifica:R.D.39/1997, que aprueba el Reglamento de los Servicios de Prevención; R.D. 1109/2007, que desarrolla la Ley 32/2006, reguladora de la subcontratación en el sector de la construcción y el R.D.1627/1997, seguridad y salud en obras de construc. BOE 23/03/2010.

LEY 54/2003. 12/12/2003. Jefatura del Estado. Reforma del marco normativo de la prevención de riesgos laborales. Modifica la Ley 31/1995, de Prevención de riesgos laborales. BOE 13/12/2003.

REAL DECRETO 780/1998. 30/04/1998. Ministerio de Trabajo y Asuntos Sociales. Modifica el R.D.39/97, de 17 de enero, que aprueba el Reglamento de los Servicios de Prevención de Riesgos Laborales. *Modifica los plazos para el cumplimiento del R.D. 39/97. BOE 01/05/1998.

REAL DECRETO 773/1997. 30/05/1997. Ministerio de la Presidencia. Establece las disposiciones mínimas de seguridad y salud relativas a la utilización por los trabajadores de equipos de protección individual. BOE 12/06/1997.

1.6. SISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN

1.6.1 INTRODUCCIÓN A LOS SISTEMAS DE CCTV

Es correcto afirmar que un circuito cerrado de televisión es un sistema de captación, transmisión y visualización de imágenes únicamente accesible a ciertas personas. Teniendo en cuenta la situación en la que se halla la industria de la seguridad desde hace unos años, este es un sistema imprescindible en cualquiera de los ámbitos profesionales y/o domésticos que se nos puedan presentar. Las utilidades y aplicaciones de los sistemas de CCTV contemplan un gran abanico de posibilidades, desde control del tráfico o video-vigilancia de complejos industriales hasta las captación de imágenes en remoto de una vivienda en tiempo real.

Desde el comienzo del empleo de estos sistemas, se han ido introduciendo mejoras y prestaciones que han mejorado enormemente las capacidades de los sistemas CCTV. A día de hoy, y en referencia al sistema que se estudia a lo largo de esta memoria, se emplearán sistemas IP que incorporan imágenes en alta definición e infinidad de algoritmos de tratamiento de la imagen que incrementan de manera significativa las posibilidades de estos. La topología típica que presentan los sistemas CCTV basados en tecnología Ethernet es la que se muestra a en la siguiente imagen:

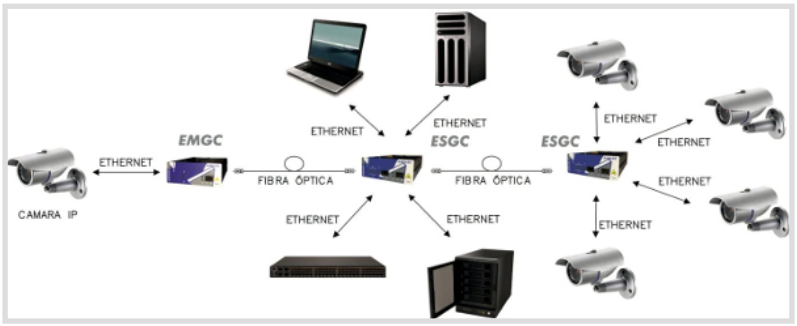

Figura 4. Topología CCTV IP.

Sistemas de CCTV sobre tecnología *Ethernet*

Para este proyecto se ha decidido implantar un sistema CCTV basado en tecnología IP por distintas razones, siendo una de las más relevantes la posibilidad de visualizar las imágenes en tiempo real desde un terminal móvil. Además, este tipo de sistemas presenta numerables ventajas frente a los sistemas analógicos:

- **Accesibilidad remota:** todos los componentes de un sistema IP se pueden gestionar y configurar de manera remota, lo que nos ofrece la característica más deseada dentro de este proyecto, que es la posibilidad de visualizar imágenes desde cualquier lugar que cuente con acceso a la red.

- **Gran calidad de imagen:** con este tipo de sistemas se logran unas calidades y resoluciones muy superiores a las de las cámaras analógicas. Esto es debido, en parte, a que la imagen se degrada en menor medida a lo largo de la línea de transmisión, y puesto que el conjunto del sistema cuenta con tecnología IP, no existen pérdidas en la calidad de imagen debido a las conversiones analógico/digital.

- **Procesamiento digital de la señal:** esta es una de las mejores cualidades de este tipo de sistemas, ya que permiten la incorporación de algoritmos y subrutinas al procesado

de las imágenes y evita la subjetividad del ojo humano a la hora de detectar una incidencia o una situación de riesgo. Del mismo modo, es posible ajustar y configurar los parámetros de entrada, tanto de las cámaras como de los grabadores, para atender a las necesidades exactas del usuario.

- **Infraestructura:** la gran ventaja que posee este sistema frente al sistema analógico es que no es necesaria la instalación de líneas de alimentación para cebar a las cámaras, ya que se alimentan a través de los cables UTP (tecnología PoE). Esto se traduce en un decremento de los costes de instalación.

- **Escalabilidad y flexibilidad:** es otra de las ventajas que presenta este sistema frente al analógico. Ante cualquier cambio significativo en la topología de la red o de la instalación, no sería necesaria una reestructuración completa del sistema, ya que podrían añadirse o modificarse componentes sin necesidad de una inversión considerable, es decir, el sistema de CCTV podría creer de forma paralela a las necesidades del usuario.

En lo que se refiere a costes no existe una gran diferencia entre los elementos con tecnología IP y los componentes analógicos, ya que durante los últimos años ha crecido de forma considerable la oferta de este tipo de sistemas reduciendo, de este modo, el coste de los mismos.

1.6.2 NECESIDADES DE LA INSTALACIÓN

Tal y como se ha explicado en el capítulo de antecedentes, la urbanización cuenta con una basta extensión de terreno y está rodeada, en parte, por campos de cultivo muy expuestos a la intrusión. Por este motivo es de vital importancia estudiar la estructura y la topografía de la urbanización con la intención de poder ofrecer una cobertura tan completa como sea posible.

Teniendo en cuenta la proximidad de cada zona de la urbanización al perímetro exterior, la composición de cada sector y la estructura que conforma cada parte de esta zona residencial, ha sido necesario acudir a distintos tipos de cámaras de seguridad para hacer frente a las necesidades tan dispersas de cada uno de los sectores.

Se han escogido pues tres tipos de cámaras distintas:

- **Cámaras IP fijas:** son dispositivos que únicamente cubren un determinado espacio. Ideales para zonas que no requieren un control exhaustivo o un gran número de cámaras.

- **Cámaras IP domo/*bullet*:** son elementos que cuentan con telemetría y pueden cubrir un amplio margen de espacio. Pueden ser manejas de forma manual por el operario, pero también pueden ser programadas para que hagan un recorrido o un barrido de la zona cada pocos segundos.

- **Cámaras térmicas:** se trata de elementos que cuentan con propiedades del ámbito militar, siendo componentes con un alto grado de especialización y capacidades. Detectan el calor que desprende cualquier cuerpo o volumen que posea una temperatura superior a la del ambiente. Son perfectas para entornos que no cuentan con iluminación.

Así pues, en esta instalación se aplicará un sistema que cuente con cámaras fijas para las zonas menos expuestas, donde se presenten cuellos de botella o calles estrechas rodeadas por viviendas. También se incluirán cámaras domo, que se instalarán en zonas más abiertas y donde sea necesario realizar barridos en bucles para cubrir toda la zona. Por último, se emplearán cámaras térmicas, que detectan la temperatura de los objetos o cuerpos que exceden la temperatura ambiente, y se ubicarán en las zonas perimetrales más expuestas de la urbanización y que linden con campos de cultivo y/o terrenos muy vulnerables ante la intrusión.

Todas las cámaras que se proponen en esta memoria poseen tecnología IP, ya que, aunque requieran mayores conocimientos técnicos a la hora de instalarse que las cámaras analógicas, ofrecen una mejor calidad de imagen y requieren de menos cableado para su puesta en marcha, ya que su alimentación es través de POE. Generalmente, todas las cámaras IP vienen de fábrica con la dirección 192.168.1.1, de modo que una vez ubicadas y posicionadas las cámaras en sus respectivas zonas se deberá asignar una IP que esté libre dentro de la red informática para poder distinguirla de las demás cámaras y elementos que la conformen. Posteriormente, una vez ya se haya completado la instalación y se tenga que configurar el NVR, se asignarán cada una de las direcciones IP de cada cámara para su correcta configuración.

Debido a las distancias tan considerables que se tendrán que cubrir para llegar a la ubicación de cada cámara se ha decidido utilizar cableado de fibra óptica. Esta se utilizará para enlazar el CPD, donde se encuentra la sala de telecomunicaciones de la urbanización, con cada uno de los *switches* que recogerán el cableado UTP de cada cámara. Debido a que hay que transformar la señal eléctrica en señal óptica y viceversa será imprescindible el empleo de elementos que conviertan las señales en ambos extremos de cada trazada.

Como muy pocas cámaras en el mercado admiten entradas de conectores LC o FC será necesario enlazar las cámara IP y los *switches* mediante cableado *Ethernet/IP*. El cableado UTP que se ha decidido emplear será de categoría 6, ya que admite un ancho de banda de hasta 1 GByte/s. De esta manera nunca se llegará a cubrir la capacidad de ancho de banda total que posee el cable, y además, por medio de un *switch*, se podrían trazar las señales de varias cámaras por un mismo cable UTP en caso de ser necesario.

Teniendo presentes los puntos descritos, se ha considerado que el número total de cámaras necesarias para ofrecer una buena cobertura a la urbanización es de 21. Se instalarán 10 cámaras fijas principalmente en el interior de la zona residencial, 9 cámaras domo o *bullet* a los largo del perímetro y en aquellos cruces que puedan ocasionar conflicto y 2 cámaras térmicas en dos puntos del perímetro que ya han sido objeto de intrusiones reiteradas.

Una vez estén todas las cámaras instaladas se podrán visualizar en cualquier punto de la red informática habilitado para ello, pero principalmente se controlarán y gestionarán desde la sala de control, donde se encuentra la base operaciones de los guardas de seguridad. Mediante el tipo de grabador que se propone más adelante, y con la ayuda de la consola de control física, será posible ajustar y configurar las opciones de cada cámara, controlarla a través de la telemetría y acceder a las grabaciones que haya guardadas en el NVR. Al tratarse de un sistema IP, también será posible visualizar las cámaras a través de un dispositivo móvil.

Tal y como se ha planteado la instalación del sistema de circuito cerrado de TV queda patente a simple vista que se trata de un sistema totalmente escalable, capaz de dar soporte a cualquier cámara nueva que se instale tras este proyecto e inmune ante caídas puntuales de algún componente del sistema.

Nota: las características y la ubicación de cada cámara, así como las trazadas del cableado necesario están recogidas en los anexos del proyecto, en el apartado de planimetría.

1.6.3 DESCRIPCIÓN DE LOS COMPONENTES DE LA INSTALACIÓN

Se proyecta pues, una instalación para la gestión de señales de video a través de un circuito cerrado de TV, y las posibilidades que ofrece el mercado son muy amplias, de modo que ha sido necesario estudiar los requerimientos de la instalación para poder ofrecer al usuario la mejor solución técnica posible.

Cámaras

Entre las distintas cámaras y la imagen a presentar al operador se presenta un gran abanico de opciones que dependerán de la arquitectura de la instalación, de las zonas que necesiten cobertura y de las posibilidades de control. Los equipos que nos ofrece el mercado, generalmente, disponen de control de posición de cámara (*pan-tilt*), controles de aproximación (*zoom*), controladores de señal (*switches*), grabadores de señal, secuenciadores de imagen, etc. Todos estos procesos se pueden controlar mediante el software aplicado, e incluso se utilizarán redes de fibra óptica para la transmisión de la señal a grandes distancias sin necesidad de repetidores.

Teniendo en cuenta los criterios mencionados en apartados anteriores, para esta instalación serán necesarias un total de 21 cámaras, teniendo en cuenta la premisa de que en un futuro el número de cámaras aumentará según las necesidades del departamento de seguridad.

- Cámaras IP fijas: 10 cámaras
- Cámaras IP domo/*bullet*: 9 cámaras
- Cámaras IP térmicas: 2 cámaras

Atendiendo a las necesidades de cada zona a cubrir se instalará una cámara fija, una cámara domo que cuenta con telemetría independiente, o una cámara térmica. Todas las cámaras serán o estarán adaptadas para exteriores, ya que la instalación es meramente exterior y, por tanto, deberán poder soportar condiciones climáticas adversas, así como posibles ataques vandálicos. También se han tenido en cuenta algunos criterios adicionales a la hora de seleccionar las cámaras a instalar:

- Altura de montaje y tipo de fijación, que puede ser para pared o para báculo
- Área a cubrir
- Resolución requerida para cada zona
- Condiciones lumínicas, tanto diurnas como nocturnas
- Exposición a condiciones climáticas

El modelo de cámaras fijas seleccionado podría ser el IPC-HFW2421R-ZS-IRE6 de ‘Ajhua’ o similar. Una cámara de exterior que posee una resolución máxima de hasta 4 Megapíxel a 20IPS con WDR. Es compatible con el tipo de grabador NVR escogido para esta instalación y cuenta con modo noche que permite, mediante 4 LED’s, vislumbrar imágenes de zonas con poca visibilidad y a una distancia de 60 metros. La alimentación de la cámara se realizará vía Ethernet (PoE), pero también cuenta con un conector de 12 Vdc.

El equipo domo/*bullet* que se escogería es el SD6AL230-HNI o similar. Es una cámara de exterior que cuenta con telemetría y una resolución Megapíxel de 1080P a 25IPS con análisis de video. Del mismo modo que las cámaras fijas también es compatible con el NVR

seleccionado. Posee unas características que le otorgan un alto rendimiento en condiciones de baja iluminación, con iluminación láser de hasta 500 metros.

Grabador

Para recoger y tratar las imágenes captadas por la cámaras se instalará la unidad de procesamiento de imágenes (CPU), que estará basado en un PC con windows como sistema operativo. Las tarjetas DVR (*Digital Video Recorder*) incrementarán la capacidad del sistema, permitiendo incorporar hasta 64 cámaras IP. Además, se podrá incluir un equipo servidor donde quedarían guardados los archivos grabados por una duración de tiempo preestablecida, y que dispondría de hasta 8 salidas a monitores por medio de conexiones VGA o HDMI.

Se ha seleccionado pues un grabador NRV (*Network Video Recorder*) para almacenar las imágenes y audio captados por las cámaras. El modelo escogido es el DS-9664NI-I16 Series o similar, principalmente porque permite conectar hasta 64 cámaras IP e incorpora el formato de compresión H.264. Entre sus especificaciones podemos destacar las siguientes características:

- Conexión con hasta 64 cámaras IP
- Formatos de video H.264, H.264+, H265 y MPEG4
- Grabaciones de hasta 12 MP de resolución
- Conexiones HDMI y VGA, así como HDMI2 y VGA2
- Salida de video con resolución de hasta 4K
- 8/16 salidas PoE
- Interface de red auto-adaptivo con 10M/100M/1000M

Figura 5. NVR Hikvision.

Es necesario tener en cuenta el número de canales que vamos a utilizar en el grabador, ya que las cámaras con resolución 4CIF ocupan un canal del grabador, mientras que las que poseen una resolución MegaPixel ocupan 4 canales en el grabador. Por este motivo es importante tener claro el tipo y el número de cámaras que se va a seleccionar para poder hacer una buena elección del elemento grabador. En este caso se ha seleccionado un NVR de alta gama y con multitud de funcionalidades, de modo que no habrá que preocuparse de sustituirlo por otro con más capacidad en el futuro cuando se añadan nuevas cámaras al sistema.

Formato de compresión

Debido a las necesidades del proyecto será necesario acudir al formato de compresión más avanzado que existe a día de hoy, ya que contra más avanzado sea este mejor visualizaremos las cámaras desde la aplicación móvil que se va a desarrollar. En este caso acudimos al formato de compresión conocido como H.264 o MPEG-4. Básicamente se trata de un códec de video digital utilizado para alcanzar una alta compresión de datos. Para ello recurre

a un nuevo principio de codificación, nuevos tipos de imágenes y nuevos filtros dando como resultado unos ahorros sustanciales de *bit rate* respecto a otros estándares, aun manteniendo la calidad de imagen y la relación S/N.

Sin embargo, existen algunos inconvenientes a la hora de emplear este códec, ya que cada fabricante utiliza un lenguaje que genera incompatibilidad entre equipos de distinta procedencia. De todos modos, cabe mencionar que recientemente se ha resuelto este problema estandarizando los protocolos de comunicación cámara/grabador. Otro de los grandes problemas que puede generar el uso de esta tecnología es la necesidad de poseer de equipos que cuenten con CPU's muy potentes y capaces de llevar a cabo la descompresión de las imágenes, aunque esta desventaja queda saldada con el ahorro de infraestructura de red. Por último, es importante resaltar que se tendrán que descomprimir únicamente los *I-frane* para evitar saturar la CPU y generar cortes en la descompresión.

Teniendo en cuenta que muy probablemente se utilizarán algoritmos durante la captura de imágenes, en este proyecto se implementará uno de los más avanzados sistemas inteligentes de video: el IVS. Algunas de la características de esta esta tecnología son:

- Conteo de personas
- Conteo de objetos
- Mascara de privacidad
- Pre-grabación de movimiento
- Zoom inteligente
- Configuración inteligente de niveles de brillo y contrastes
- Video-sensor de altas prestaciones
- Detección de corte en la señal de video
- Reconocimiento y detección facial
- Seguimiento y detección de objetos
- Detección de sabotaje

Mediante el sistema inteligente de video, el usuario puede realizar búsquedas de archivo o grabaciones en función de las condiciones de grabación y/o búsqueda. Además, se le ofrece la posibilidad de reproducción remota, de la cual hablaremos más adelante. Algunas de las características de grabación de video y audio que presenta este sistema son:

- Grabación H.264 hasta 64 cámaras en tiempo real
- Soporte para pre-registro
- Búsqueda inteligente por canales, fecha, hora y eventos
- Reproducción de hasta 16 canales al mismo tiempo
- Exportación a formato AVI/BMP.
- Reproducción instantánea de archivos remotos
- Telemetría remota

La grabación del video podrá realizarse manualmente, por alarma o programada:

- ***Manualmente:*** el operador selecciona una o un conjunto de cámaras a grabar, pudiendo indicar también el fin de la grabación.

- ***Por alarma:*** Cuando una alarma es activada, ya sea por un sensor externo o por vídeo detección, el sistema graba vídeo de la cámara asociada a dichas alarmas. Tanto la resolución del vídeo grabado como su duración puede ser configurables. Cuando se

detecta una alarma puede asociarse un mapa, donde se indique la situación de la alarma, enviar una notificación a un sistema remoto cliente, enviar un mensaje de alarma por Email ó asociar un sonido a la alarma.

- ***Programada:*** Puede programarse la fecha y hora de la grabación así como su duración. También se puede configurar la resolución y el número de "frames/seg" de la grabación.

Por otro lado, la visualización de los ficheros de video y audio guardados se efectuará de forma muy sencilla, seleccionando la fecha y la hora a partir de la cuales se quiere visualizar las imágenes. Del mismo modo se podrán buscar las grabaciones por eventos, acotando mucho más la búsqueda en caso de incidencia.

Cabe mencionar también, que es posible jerarquizar a los usuarios del sistema de CCTV con diferentes niveles de privilegios o acceso mediante distintos usuarios y contraseñas, dependiendo de si se trata de "Administrador" u "Operador". De este modo se puede realizar una jerarquización del sistema, donde el encargado de la seguridad puede administrar el nivel de actuación sobre el mismo, tanto en conexión, como en ajustes o configuración.

Cableado

Para interconectar todos los elementos del sistema se deberá tener en cuenta la distancia existente entre todos ellos, ya que no se va a emplear el mismo tipo de cableado para las distancias cortas que para las distancias largas.

En las distancias cortas, para conectar y alimentar las cámaras IP se empleará cableado UTP-CAT6. Mediante este cable se transmitirá la señal de video hasta los cuadros de comunicaciones donde se instalarán los equipos de transmisión de datos por fibra óptica. De tal modo, se situarán en el interior de los cuadros los conversores electro-ópticos y los *switches* necesarios para poder transmitir todas las señales de video por una o varias fibras ópticas hasta la sala de control.

El cable de categoría 6 (ANSI/TIA/EiA-568-B.2-1) es un estándar de cables para *Gigabit Ethernet* y otros protocolos de redes. Es compatible con estándares anteriores a él y posee características y especificaciones para evitar la diafonía (*Crosstalk*) y el ruido. Es capaz de alcanzar frecuencias de hasta 250 MHz en cada par, así como una tasa de transmisión de 1 Gbps. El cable contiene 4 pares trenzados de cobre, del mismo modo que estándares anteriores, aunque en algunas ocasiones también se emplea cable 23 AWG. La longitud máxima permitida o efectiva del cable es de 96 metros de sólido horizontal cableado entre el panel de conexiones y la toma de pared, además de 10 metros de cable de conexión.

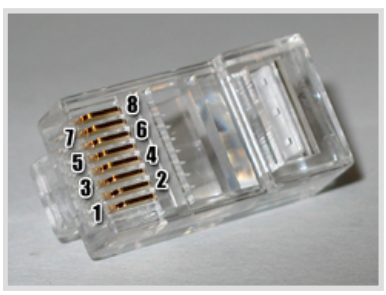

Figura 6. Conector RJ-45.

A la hora de realizar la instalación de este tipo de cable se deberán tener en cuenta algunas consideraciones de seguridad para evitar que el cable pierda sus propiedades. Entre ellas destacan la de no retorcer el cable o doblarlo demasiado fuerte, así como establecer una conexión a tierra para garantizar la seguridad y la eficacia del sistema. Las conexiones del cable se suele realizar por medio del conector RJ-45, que posee inmunidad a las interferencias por encima de tasas de transmisión de 100 Mbps.

Los valores que se deben cumplir para trabajar en redes de 250 MHz son los que se muestran en la siguiente tabla:

Frecuencia (MHz)	PS Atenuación (dB)	Pr-pr NEXT (dB)	PS NEXT (dB)	Pr-pr ELFEXT (dB)	PS ELFEXT (dB)	Pérdida de retorno (dB)	Retraso de fase (ns)	Retraso torre (ns)
250	36,0	33,1	30,2	17,2	14,2	8,0	548,2	50,0

Tabla 3. Especificaciones del estándar.

La estructura del cable, así como sus dos modelos para crimparlo se muestran en la siguiente tabla:

Patilla	T568A Par	T568B Par	Cable	T568A Color	T568B Color
1	3	2	tip	blanco/linea verde	blanco/linea naranja
2	3	2	ring	verde	naranja
3	2	3	tip	blanco/linea naranja	blanco/linea verde
4	1	1	ring	azul	azul
5	1	1	tip	blanco/linea azul	blanco/linea azul
6	2	3	ring	naranja	verde
7	4	4	tip	blanco/linea marrón	blanco/linea marrón
8	4	4	ring	marrón	marrón

Tabla 4. Composición del cable.

El medio de transmisión para las distancias largas que se ha escogido para esta instalación es la fibra óptica. Esta se utilizará para enlazar el CPD, donde se encuentra la sala de telecomunicaciones de la urbanización, con cada uno de los *switches* que recogerán el cableado UTP de cada cámara.

La utilización de la fibra óptica es cada vez más habitual, no solo en la industria, que era el ámbito más común en el que se usaba, sino también en aplicaciones o sistemas de seguridad, telecontrol, detección de intrusiones y en todas aquellas instalaciones que requieren el envío y

recepción de datos a grandes distancias y de forma segura. Dentro del campo o ámbito que nos atañe, emplear fibra óptica presenta las siguientes ventajas:

- **Mayor distancia efectiva:** dependiendo del tipo de fibra que se utilice, se pueden alcanzar distancias realmente grandes sin necesidad de repetidores ópticos. Con fibra óptica multimodo se pueden alcanzar distancias de hasta 10 km, mientras que si empleamos fibras monomodo esa distancia se incrementa considerablemente.
- **Mayor seguridad en las transmisiones:** este es un punto muy importante, ya que la fibra óptica no induce ningún tipo de señal y es inmune a las interferencias y radiaciones externas. Además, cualquier defecto o rotura en el cable es fácilmente localizable.
- **Mayor calidad de la imagen:** la calidad de las imágenes captadas por las cámaras y transmitidas al grabador por la fibra óptica no sufren ningún tipo de deterioro, por lo que la calidad de las imágenes se mantienen durante toda la transmisión.
- **Duración del cableado:** el cable de fibra óptica no contiene materiales degradables u oxidables que puedan mermar sus características, de modo que su vida útil es considerablemente mayor que la del cable coaxial.

A pesar de las ventajas descritas anteriormente, también existen inconvenientes a la hora de elegir la fibra óptica como medio de transmisión. En primer lugar el coste de instalación es mayor debido a los equipos que se necesitan para su funcionamiento, como los convertidores electro-ópticos (*trans-receiver*). En segundo lugar, hay tener en cuenta la falta de formación especializada de los técnicos instaladores, ya que este tipo de redes requieren de unos conocimientos y aptitudes muy específicas para su implementación.

El cable de fibra óptica está formado por el núcleo y su recubrimiento, que dota a la fibra de resistencia y flexibilidad. El índice de refracción es distinto entre el núcleo y el recubrimiento para poder propagar las ondas luminosas desde el emisor hasta el receptor óptico. También se encuentra en el interior del cable de fibra óptica el *buffer*, que protege a la/s fibras de la humedad y de las roturas. Por último, la aramida proporciona a la fibra resistencia a la tracción. En la *Figura 7* se puede apreciar con detalle la composición de la fibra óptica:

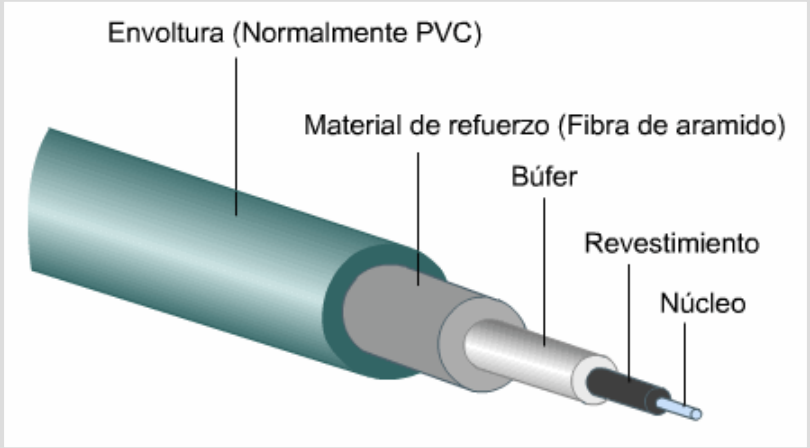

Figura 7. Composición de la fibra óptica.

Aunque la fibra multimodo es capaz de abarcar distancias de hasta 10 Km, se ha escogido una fibra monomodo cuya longitud de onda es de 1310 nm, por lo que la distancia a cubrir no será un problema en este proyecto.

La fibra óptica a instalar será del tipo monomodo para exterior, de 32 fibras en función de los requerimientos de la zona, con una longitud de onda de 1310 nm. Debido a las altas tasas de transmisión (STM-256) y a los sistemas de multiplexado por división de longitud de onda densa (DWDM) se exige la implementación de una nueva generación de fibra óptica monomodo que supera las tradicionales fibras en términos de:

- Mayor tasa de transmisión (compensación de la dispersión cromática)
- Mayor ganancia tras la regeneración (menor dispersión cromática)
- Sistemas actualizables en función de la tasa de transmisión

Para esta instalación se proyectará una trazada de fibra óptica capaz de llegar a todas las cámaras y elementos del proyecto sin necesidad de emplear excesivo cableado de UTP. En los planos que se adjuntan (Ver Anexo II, planos 2 y 4) se puede apreciar el recorrido que seguirá el cable de fibra óptica a través de la zona residencial, llegando prácticamente a todas y cada una de las cámaras que se instalarán. Aunque no se vayan a emplear las 32 fibras de las que dispone el cableado propuesto, es interesante que queden fibras libres que puedan ser utilizadas en ampliaciones futuras, ya que una de las ventajas de este tipo de sistemas o instalaciones es que puedan ser totalmente escalables.

Convertidores Electro-Ópticos

Para realizar la conversión y el envío de la señal óptica en eléctrica y vice-versa se emplearán convertidores electro-ópticos, instalándose en cada uno de los extremos de los enlaces. Evidentemente se ubicarán los equipos Tx en el extremo de las cámaras o switches y los equipos Rx en el CPD o sala de control. Debido a que se cuenta con la función de telemetría para algunas de las cámaras será necesario optar por equipos mixtos de video y señal de control mediante ‘interfaces’ (RS-232 ó RS-422). En este caso no será necesario ocupar dos fibras para video y para telemetría, ya que en la mayoría de las situaciones es posible transmitir ambas señales por la misma fibra.

Figura 8. Convertidor electro-óptico.

Consola de programación y gestión

Aunque el software que incluye el NVR ya cuenta con una consola virtual desde la que gestionar y controlar cada de las cámaras, es conveniente incluir en el sistema una consola física, de manera que facilite, no solo la operatividad de los sistemas de movimiento manual de las cámaras domo con telemetría, sino también la gestión del sistema matricial de conmutación de video.

Aunque el mercado ofrece un amplia oferta de estos dispositivos, se ha optado por el modelo CSM-900J del fabricante OMIKRON. Se ha escogido este modelo por la sencillez de uso a la hora de emplear el zoom de la óptica o el movimiento de las cámaras, que se realizar través de un *joystick*.

Figura 9. Consola de programación CSM-900J.

La consola tiene un diseño compacto y presenta una pantalla gráfica retro iluminada de cristal líquido, dónde se presentan de forma dinámica las funciones de las siete teclas asociadas, permitiendo la utilización de las mismas de una forma intuitiva partiendo de la información presentada en la pantalla de inicio o principal.

Mediante la consola de control y programación CSM-900J, es posible realizar entre otras, las siguientes funciones:

- Programación del tipo de entrada de cámara
- Seleccionar manualmente una cámara
- Seleccionar de forma correlativa todas las cámaras
- Elegir el monitor para la selección de las cámaras
- Programación de 30 secuencias
- Programación de 128 presentaciones fijas
- Selección y activación de dos secuencias programadas
- Programación independiente para cada entrada de alarma
- Acceder al menú principal de programación
- Visionar el sinóptico de las cámaras en servicio
- Anular y restaurar la hora, fecha y textos en todos los monitores
- Control de telemetría por línea bifilar de cámaras tipo domo
- Programación de horarios para activación de secuencias y alarmas
- Ajuste de las diferencias de fase en cámaras con control de fase

1.7. SISTEMA DE CONTROL DE ACCESOS

1.7.1 INTRODUCCIÓN A LOS SISTEMAS DE CONTROL DE ACCESOS

Dada la importancia que tiene en una instalación de este tipo, es indispensable y prioritario realizar una dotación tecnológica y humana perfectamente estructura e integrada, y para ello es necesario implementar un sistema de control de accesos.

La función básica de un sistema de control de accesos es la de gestionar de manera racional y controlada la entrada y salida de personas y vehículos, así como la de evitar intrusiones no deseadas y monitorizar el movimiento puntual de mercancías dentro de la instalación. Todo esto diferenciando zonas y tipos de accesos, clasificados en tres grupos:

- Personas
- Vehículos
- Mercancías y paquetería

En el siguiente gráfico se presenta la arquitectura tipo de un sistema de control de accesos integral, sin embargo, este proyecto no contempla el control de acceso a mercancías ni a vehículos:

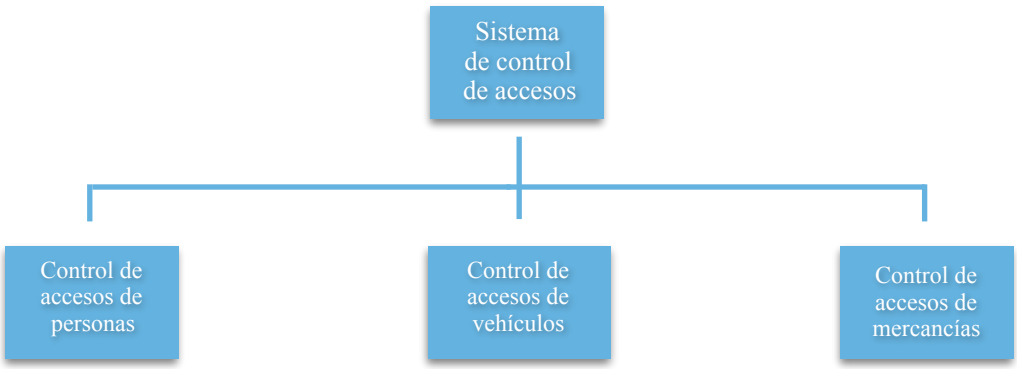

Gráfico 1. Arquitectura control de accesos.

La gestión de un sistema de control de accesos ha de realizarse siempre combinando medios humanos y medios técnicos. Dentro de los medios humanos se incluyen los operadores y administradores del sistema, el director de seguridad y demás responsables que tendrán un adecuado plan de formación continuado, lo que permitirá que actúen diligentemente ante cualquier situación imprevisible. Dentro de los medios técnicos se abarca todo el equipamiento electrónico y electromecánico que permitirá realizar un meticuloso control de las entradas y las salidas.

Con una buena implementación del control de accesos, el sistema será capaz de monitorizar toda la estructura operativa de forma que se obtenga información detallada de:

- **Entradas/salidas:** control detallado de entradas y salidas, con la posibilidad de indexarlo con el departamento de R.R.H.H para la gestión de nóminas.
- **Control de aforos:** limita y controla el número de persona que puede acceder a un sector, zona, o recinto.
- **Control de rondas:** garantiza la eficacia del personal de vigilancia sobre las distintas zonas de la urbanización y ante cualquier eventualidad.

1.7.2 CONTROL DE ACCESOS DE PERSONAS

El control de accesos peatonal debe proporcionar al usuario una serie de funciones operativas que le permitan obtener información para:

- Impedir la entrada a personas no autorizadas a zonas restringidas
- Identificar a personas que accedan o pretendan acceder a cada una de las zonas a proteger
- Controlar aforos y permanencia en zonas controladas
- Interaccionar con otros sistemas
- Secuenciar la habilitación y/o autorización de los accesos.

Para este proyecto se plantea un control de accesos que cubra cada una de las tres entradas de usuarios del club social, así como las puertas de acceso a la sala de control y a la sala de telecomunicaciones. Se instalará pues, una serie de lectores de proximidad para tarjetas MIFARE en todos los accesos que se desea controlar. De esta manera será posible monitorizar y gestionar los accesos que se realizan en distintas áreas de la urbanización con la intención de proteger y dar soporte a las estructuras que pueden verse más comprometidas ante una intrusión y/o acceso no deseado. Algunas de las características del sistema son las siguientes:

- Las tarjetas que se emplearán para el control de acceso al club social son con aro de proximidad Mifare® de 13,56 MHz, con memoria de lectura/escritura de 8K e interface Banda Magnética Hi-Co.
- El método de acceso será programable en función del calendario definido para cada lector.
- El sistema se podrá configurar de tal modo que solo el administrador tenga acceso a él.
- El número de edificios que dispondrán de control de accesos peatonal son 2, el club social (que cuenta con tres puertas de acceso) y la sala de control de comunicaciones.
- El número de clientes con acceso simultáneo al servidor para la gestión de la aplicación será de mínimo 16.

Lectores y unidades de control

- Los lectores escogidos para este proyecto cuentan con tarjeta lectora compatible con las tarjetas mencionadas anteriormente. Son lectores sin display ni teclado, con relé y LED tricolor, *buzzer* y entradas digitales. Además están diseñados para instalaciones en exterior, de tal modo que presentan estanqueidad ante todo tipo de condiciones climáticas.
- El protocolo de comunicación con los lectores es el RS-485.
- Todos los lectores podrán ser gestionados desde el software de control.
- El servidor CPU tendrá comunicación con los lectores para gestionar su funcionamiento. Podrá almacenar hasta un mínimo de 30.000 tarjetas, 255 calendarios de acceso, 255 horarios de acceso y 25.000 marcajes o eventos de seguridad.
- La unidad de control activará la apertura de las puertas de acceso mediante cerraduras eléctricas y controlará el estado de la puerta, generando un aviso hacia el software de control en caso de que la puerta esté abierta. El tiempo que permanecerá la puerta abierta tras realizar la maniobra se configurará desde el programa de control, así como las alarmas, los avisos y los protocolos a seguir tras cualquier tipo de evento.
- Las cerraduras eléctricas cuentan con estándares de seguridad, de tal forma que ante un accidente o fallo del sistema quedarán abiertas para la evacuación de las personas.

Software de control

El software de control será el encargado de gestionar y dar servicio a todos los terminales de acceso. Permitirá crear altas a nuevo usuarios del club social y controlar los accesos a aquellas zonas o edificios donde se implante el sistema. A través de él se configurarán los eventos de los lectores, las puertas y las unidades de control y se gestionarán las alertas ante cualquier tipo de eventualidad (Ver Anexo II, plano 6).

El software de control se ubicará en el servidor principal, y habrá un segundo servidor que dará servicio a todos los terminales de acceso. El servidor principal también contendrá la base de datos de los usuarios del control de accesos, de tal forma que cada vez que se realice un alta, una baja o modificación de algún usuario, la base de datos del servidor del control de accesos quedará actualizada en tiempo real.

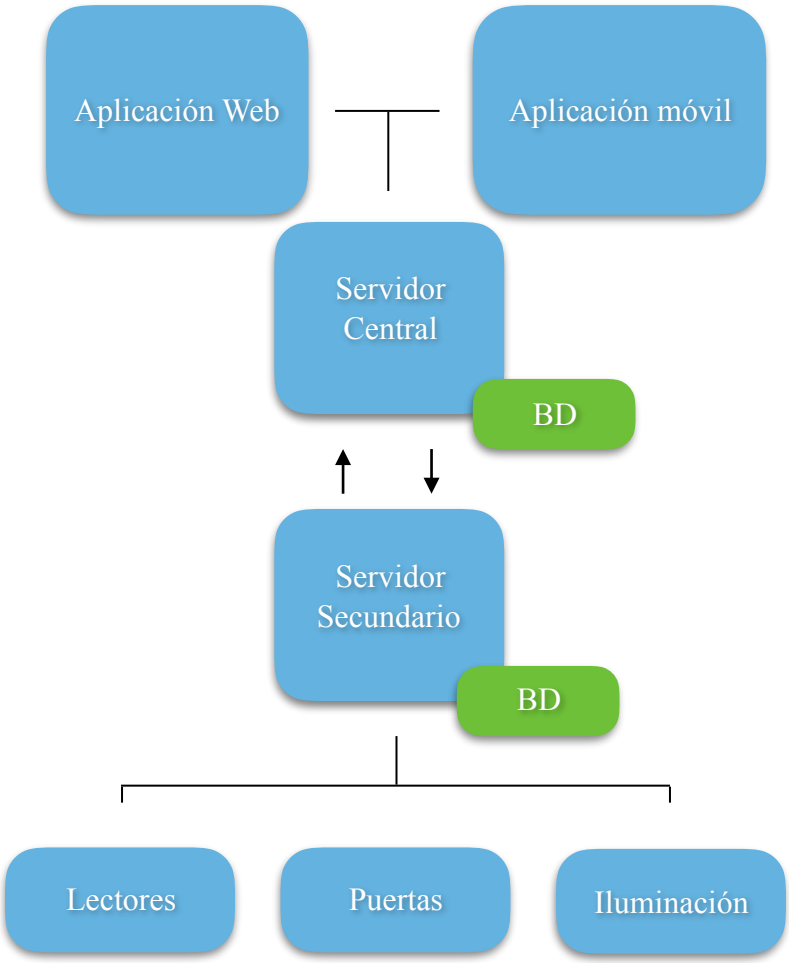

Gráfico 2. Topología sistema de control de accesos.

Las características o funcionalidades que incorpora el software de control son las siguientes:

- Todos los eventos que se produzcan quedarán registrados en el servidor central y podrán ser visualizados desde la sala de control, sin embargo las maniobras eléctricas que accionan las puertas también podrán ejecutarse desde cualquier terminal móvil que tenga instalada la aplicación gracias al sistema SCADA.

- Todas las unidades de control de accesos serán informadas a través del protocolo de comunicación RS-485.

- Mediante un PC Cliente se podrán configurar los permisos y/o maniobras de accesos a terminales o puertas. Además, al igual que desde la sala de control, se podrán gestionar los lectores y las tarjetas de usuario a través de la aplicación web, así como las fichas de los usuarios del club social.

- La aplicación de control de accesos tendrá dos *interfaces*, una móvil y otra web. Tanto la aplicación web como la aplicación móvil permitirán aperturas, bloqueos, estados abiertos, etc. Sin embargo, los usuarios solo podrán ser gestionados desde la aplicación web.

El software de gestión contempla tres perfiles de acceso al sistema:

- **Administrador:** posee acceso ilimitado a todas las funcionalidades del sistema. Solo el administrador puede dar de alta a nuevos usuarios del sistema y tener acceso a la información recogida en las bases de datos.

- **Usuario de seguridad:** posee acceso a todos los lectores de la zona residencial, así como a las maniobras de las puertas y barreras. En la aplicación móvil también tendrá acceso a la localización GPS de los vehículos de patrullaje.

- **Usuario de centro de control:** tiene acceso a todos los lectores del área designada y a ciertas funcionalidades preestablecidas desde cualquier puesto PC cliente.

1.7.3 DESCRIPCIÓN DE LOS COMPONENTES DE LA INSTALACIÓN

Servidor de gestión

Puesto que el sistema de control de accesos a implantar requiere de unos recursos considerables y posee unas altas prestaciones, se debe dotar al sistema con un servidor gestor común que sea capaz de interaccionar con otras aplicaciones informáticas, además de gestionar y protocolizar las comunicaciones con los buses de los lectores.

La opción elegida para la gestión del software de control de accesos es un servidor FUJITSU, que cuenta con un alto nivel de computación y de fiabilidad. Concretamente, el modelo seleccionado es el “FUJITSU PRIMERGY RX300 S7” o similar.

Se trata pues, de un servidor para *rack* de 2U que ha sido optimizado para los propósitos de la virtualización. Proporciona un alto y escalable rendimiento I/O, amplias opciones de memoria, soporte para los principales productos de hipervisor y el máximo rendimiento con una tecnología de Intel®, se podría decir, actual. Contiene una 7xPCIe Gen2 para evitar cuellos de botella en la entrada y salida de datos, que combinado con Intel® Xeon® serie 5600 ofrecen un rendimiento superior de CPU.

Cuenta con un elemento de seguridad llamado “*Cool-Safe*”, un diseño optimizado de enfriamiento del sistema que le otorga al equipo una alta eficiencia a la hora de hacer frente a los retos de las tecnologías de la información. De tal modo, este potente servidor también es utilizado para llevar a cabo procesos críticos de negocio o aplicaciones de servicio pesado, tales como bases de datos.

Figura 10. Servidor Fujitsu Primergy Rx300 S7.

Durante la implementación del proyecto de optará por instalar dos unidades del servidor en espejo y con redundancia absoluta, debido a la importancia y relevancia del sistema que controla. Al emplear dos servidores en paralelo, es muy sencillo reemplazar cualquiera de los componentes de hardware de manera rápida sin que el sistema sufra caídas o retrasos.

Ambos servidores, tanto el principal como el servidor réplica, se instalarán en el armario *rack* de la sala de comunicaciones y control (CPD) de la urbanización.

Impresora de acreditaciones

Con el fin de lograr la autonomía e independencia de la instalación de proveedores de servicios externos, se propone la adquisición e instalación de una impresora de tarjetas que realice de manera autónoma sus propias acreditaciones, de manera automática y sin tiempos de espera.

Dicha impresora se ubicará en las oficinas, cercanas al CPD, donde se imprimirán y se darán de alta las tarjetas o acreditaciones para cada uno de los usuarios. La impresora propuesta es la FARGO HDP5000 o similar.

Figura 11. Impresora de tarjetas Fargo HDP5000.

La impresora de tarjetas plásticas de alta definición HDP5000 destaca por su capacidad de actualización en el terreno y por su diseño modular, lo que la convierte en un dispositivo muy versátil y adaptativo. Está diseñada para la impresión autónoma o para aplicaciones que conecten más de una impresora.

La impresora HDP5000 incluye un puerto *Ethernet* y un servidor de impresión que ofrecen la conectividad para operaciones en red. Además, está dotada con tecnología de alta

definición de impresión (HDP), que permite imprimir, codificar y laminar tarjetas con las siguientes tecnologías:

- *Smart Cards* de contacto
- *Contactless*
- *WIEGAND*
- Proximidad
- Memoria óptica

Al contrario que otras impresoras de sublimación tradicionales, en esta impresora el cabezal no entra en contacto directo con la tarjeta, sino que la imagen se imprime en un *film* transparente que luego se adherirá a la tarjeta. En caso de querer otorgar más protección a las acreditaciones, esta impresora puede incluir un módulo de laminación a través de holograma, cuya laminación se lleva a cabo en ambas caras del plástico. Las características principales del dispositivo son las siguientes:

- El método de impresión es el "HDP Dye" con transferencia térmica de resina.
- La resolución alcanza los 300 d.p.i (11,8 dots/mm).
- La velocidad de impresión es de 38 seg/tarjeta a una cara.
- Las tarjetas aceptadas por la impresora son las CR-80.
- La tolva de entrada admite hasta 100 tarjetas, mientras que la tolva de salida admite hasta 200.
- A día de hoy, los *drivers* que nos ofrece Fargo abarcan los sistemas operativos más relevantes, incluido el "Windows Server 2016".

Tarjetas con tecnología MIFARE

MIFARE es una tecnología de tarjetas inteligentes sin contacto (TISC), siendo las más comunes en instalaciones de todo el mundo, con aproximadamente 250 millones de tarjetas y 1,5 millones de módulos lectores instalados.

Las tarjetas MIFARE son tarjetas plásticas que incorporan una tecnología de comunicación de radiofrecuencia. Del mismo modo que las tarjetas con chip de contacto, las tarjetas MIFARE incorporan un chip electrónico. La diferencia entre estas tarjetas y las tarjetas de chip radica en que el chip no se encuentra en la superficie, sino que se halla hundido dentro del corazón PVC de la tarjeta. Además del chip, la tarjeta incorpora una antena que le permite comunicar con el receptor radiofrecuencia. En la siguiente imagen (Figura 12) se puede apreciar con detalle la composición de las tarjetas MIFARE:

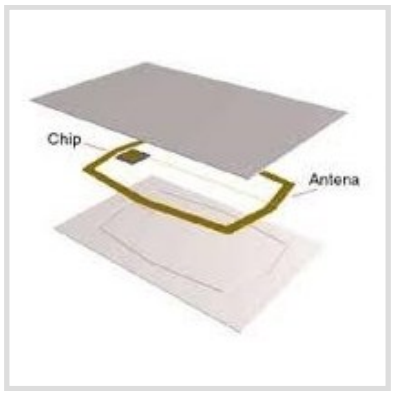

Figura 12. Elementos de las tarjetas MIFARE

La distancia típica de lectura ronda los 10 cm, aunque la distancia máxima de lectura varía en función de la potencia del módulo lector. En el caso de la frecuencia empleada por ellas, trabajan en la frecuencia de 13,46 MHz.

Una de las ventajas que presenta la tecnología MIFARE es que no necesita ningún contacto físico para leer o codificar una tarjeta, sino que basta con acercarla al lector o codificador para transferir datos. Otra ventaja de este sistema es que las tarjetas y los lectores que lo emplean no necesitan de ningún mantenimiento, ya que no existe desgaste de los equipos y dispositivos que conforman la instalación.

Si analizamos el chip MIFARE podemos destacar una serie de características que destacan sobre las demás:

- Transfiere datos sin contacto a una frecuencia de 13,46 MHz
- Velocidad de transferencia de lectura y escritura: 106 Kbit/seg
- Tiempo de transacción: <100 ms
- Distancia de lectura/escritura: 100 mm
- Capacidad de memoria total: 1024 bytes x 8 bits EEPROM
- Memoria disponible: 752 bytes
- Distribución de la memoria: 16 sectores con 4 bloques, siendo cada bloque de 16 bytes
- Sistema anti-colisión
- Vida estimada del chip: 100.000 ciclos de escritura con 10 años de retención de datos

Puertas de control de accesos

Debido a la naturaleza de la urbanización y a las peticiones de acceso que van a recibir, tanto el club social como la propia urbanización, se requiere la instalación e implantación de un sistema mecánico de control de acceso que impida la entrada a aquellas personas ajenas al sistema.

Actualmente, la urbanización ya cuenta con una serie de accesos utilizados por los usuarios que permiten acceder a distintas áreas en función de los privilegios de los que disponen. De tal modo, se llevará a cabo una serie de actuaciones sobre estos accesos para automatizarlos e integrar en ellos el sistema de control de accesos.

Se afrontan dos casos a la hora de plantear esta parte del proyecto. Por un lado, los accesos al club social constan de tres puertas metálicas correderas situadas en distintos puntos del perímetro del club, mientras que la sala de control y la de telecomunicaciones cuentan con una puerta de seguridad cada una.

De tal modo se instalarán y se integrarán, sobre estos elementos ya situados, una serie de componentes electro-mecánicos o actuadores que transformen la señal recibida desde el servidor en un movimiento mecánico. Existen multitud de actuadores en función de las necesidades que se deban cubrir.

Lector de proximidad MIFARE

Como se ha mencionado anteriormente, la tecnología a implantar en este proyecto en lo que a control de accesos se refiere es la RIFD con tecnología pasiva MIFARE. Por este motivo, los dispositivos lectores, además de poder soportar esta tecnología, han de contar con una serie de características que les proporcionen fiabilidad, robustez y unas cualidades estéticas que estén

acorde al entorno en el que se instalarán, ya que son elementos que se ubicarán en zonas de gran visibilidad.

El modelo que se ha escogido para los lectores de tarjetas, perteneciente al fabricante alemán “FEIG ELECTRONIC”, es el MIFARE CPR02-10B o similar. Dicho modelo cuenta con el protocolo de comunicación RS-485, además de un relé interno que permite la maniobra de apertura de puertas sin necesidad de elementos externos, ya que todos los sistemas se encuentran integrados en el propio lector.

Figura 13. Lector de tarjetas MIFARE CPR02-10B

El dispositivo lector también está dotado de un diodo led ubicado en la parte frontal, además de un *buzzer* o vibrador acústico en su interior. Sin embargo, la característica más importante es que el software de gestión y control de accesos permite la integración de este modelo de lector que, junto a una correcta programación, ofrecerá un servicio continuado y eficiente.

La instalación de estos elementos se llevará a cabo en distintos puntos de la urbanización. Por una parte, se instalarán dos lectores en cada uno de los puntos de acceso al club social, uno para la entrada y otro para la salida de usuarios. Por otro, se deberán instalar dos lectores en las puertas que dan acceso a la sala de control y a la sala de telecomunicaciones o CPD. En el anexo que se adjunta al proyecto se podrá ver, sobre la planimetría, la ubicación de cada uno de estos elementos (Ver Anexo II).

Convertidor de protocolos RS485/RS232

Para hacer posible la comunicación entre el software de control, instalado en el servidor, y los lectores es necesario incluir en la instalación un convertidor de protocolos RS-485/RS.232. Este elemento cuenta con una importante relevancia, ya que traducirá los valores modificados en la base de datos en impulsos e instrucciones eléctricas. Se trata de un convertidor con grandes prestaciones para acoplamiento e integración en una red industrial, permitiendo aumentar el número de máquinas a comunicar y alargar las líneas de comunicación con la unidad central. El modelo seleccionado para cubrir las necesidades de la instalación es el CRS-485 del fabricante “AFEISA” o similar.

Nota: añadiendo un filtro de altas frecuencias y un mayor aislamiento se asegura la comunicación incluso en las peores condiciones de trabajo.

Figura 14. Convertidor de protocolos CRS-485.

Lector de activación y validación

Las tarjetas RFID que se emplearán en el sistema de control de accesos incorporan un código numérico único e irrepetible programado en una de sus máscaras de encriptación. Este código será con el que trabajará el software de control y la base de datos.

De tal manera es necesario asignar cada código a cada una de las tarjetas que se den de alta en el sistema. Para realizar esta tarea se empleará un lector de validación que permita a los administradores dar de alta y proveer de las llaves electrónicas a los usuarios del sistema.

Para este caso, y siguiendo la línea de los lectores MIFARE anteriormente descritos, se procederá a la instalación de un lector validador "FEIG ELECTRONIC", modelo CPR40-30U o similar.

Figura 15. Lector de validación CPR40-30U.

Pulsadores de salida

En las áreas donde no sea necesario el control de salida mediante la tarjeta de usuario podría instalarse una serie de pulsadores de apertura mediante contactos normalmente abiertos (NA). De igual modo que sucede con los lectores de tarjetas seleccionados, los pulsadores se integrarán completamente con los entornos de aquellos accesos donde se instale.

Figura 16. Pulsador de salida.

Cerraduras magnéticas

Las puertas de la sala de control y de la sala de telecomunicaciones controladas mediante lector de tarjetas estarán dotadas de cerraduras magnéticas de seguridad completamente integradas en su estructura mecánica. De este modo se deja a un lado la arcaica llave de apertura y cierre tradicional y se integra en el sistema la tarjeta MIFARE. Esto permitirá monitorizar y registrar la actividad de entradas y salidas que se lleva a cabo en la instalación.

Las cerraduras electromagnéticas cuentan con dos principales piezas, por un lado el electroimán, y por el otro lado una lámina metálica llamada pieza móvil o pieza polar. El electroimán se coloca en el marco de la puerta, y trabaja como imán en la medida que circule corriente por su bobina y cierra la puerta; al dejar de recibir corriente eléctrica permite la apertura de la puerta.

Todas estas cerraduras electromagnéticas son de tipo *Fail Safe*, lo que significa que se mantienen cerradas solo mientras exista corriente eléctrica a diferencia de los otros tipos de cerraduras eléctricas que funcionan del modo *Fail Secure*, las cuales funcionan de modo contrario cuando no hay electricidad se mantienen cerradas.

Figuras 17 y 18. Cerradura magnética de seguridad.

1.8. SISTEMA SCADA

1.8.1 INTRODUCCIÓN A LOS SISTEMAS SCADA

La integración de todos los dispositivos eléctricos o electrónicos que conforman una instalación, y la posibilidad de poder gestionarlos a través de un único software instalado en cualquier terminal es lo que se denomina sistema SCADA (*Supervisory Control And Data Adquisition*).

Este sistema permite tener un control rápido y una visión general de la instalación, reduciendo tiempo de mantenimiento y optimizando rendimiento y costes. Permite también realizar consultas remotas sobre el estado de los dispositivos desde cualquier punto con acceso a internet.

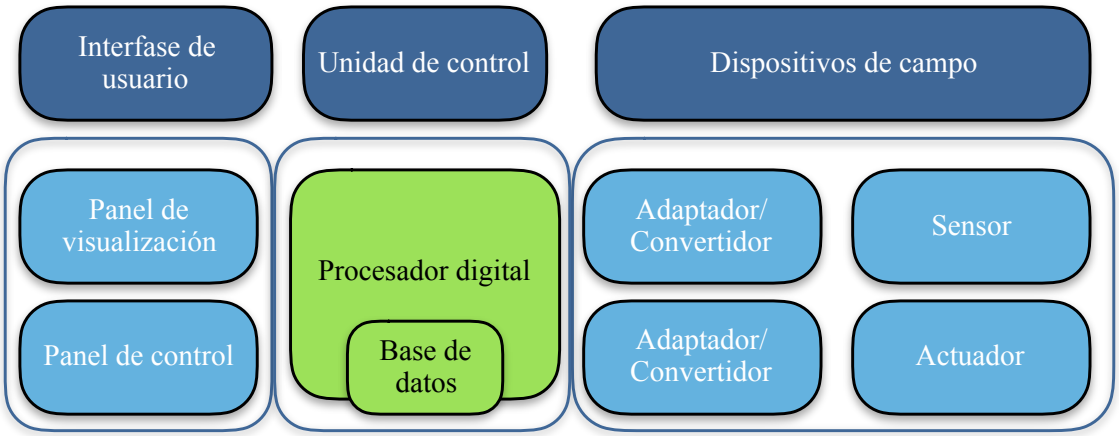

Gráfico 3. Proceso de funcionamiento del sistema SCADA.

Un sistema SCADA hace referencia a un sistema de adquisición de datos y control supervisor. En al diagrama anterior se observan las partes que componen un sistema SCADA. El proceso de control es aquel proceso que se desea supervisar y en consecuencia, es el origen de los datos que se requiere colectar y distribuir.

Para la adquisición de datos, se precisa la utilización de dispositivos e instrumentos de medición dotados de alguna interfaz de comunicación que permita su interconexión y posterior enlace con el sistema central de control, y es aquí donde entran los conversores de protocolos.

El sistema supervisor SCADA es la combinación de software y hardware que permite la colección y visualización de los datos proporcionados por los instrumentos. Dependiendo del sistema, también puede permitir la interacción con el proceso y modificar el estado del elemento que se está supervisando. Para todo esto existen los clientes, que son conjuntos de aplicaciones que hacen uso de los datos obtenidos.

1.8.2 SISTEMA SCADA EN LA URBANIZACIÓN

Para mejorar el funcionamiento de supervisión del sistema de seguridad en la urbanización, se llevará a cabo la instalación de un sistema SCADA que permitirá la supervisión de todos los elementos de una manera gráfica y funcional a través de un software de control.

Además, se podrá integrar el sistema SCADA con dispositivos de confort de la zona residencial, tales como el sistema de alumbrado deportivo de todo el recinto del club social, permitiendo conocer el estado de cada luminaria y poder interactuar encendiendo y apagando cualquier punto de luz rápidamente desde cualquier ordenador habilitado para tal efecto.

Se realizará también la integración total entre todos los sistemas, ya sean de seguridad o no, pertenecientes a nuestro proyecto o instalados por empresas externas, que permitirá un control automatizado y sistemático de todos ellos. Por esto, se puede decir que el sistema SCADA es uno de los principales elementos del presente documento, y que en cierto modo da sentido al título del proyecto, SISTEMA DE GESTIÓN INTEGRADO.

Como se ha comentado anteriormente, se interactuará con el sistema de alumbrado de la urbanización. De esta forma se puede controlar el estado de las luminarias de dos formas, manual o automática. Se podrá, a través del software SCADA cliente, apagar y encender de forma manual cualquier punto de luz de las instalaciones deportivas del club social que haya sido precisado para supervisión SCADA.

Características del sistema SCADA

- Capacidad de expansión
- Control remoto
- Capacidad de leer y escribir en múltiples fuentes de datos
- Funciona en entornos “Clientes-Servidor”, gestionando bases de datos SQL

Funciones principales del sistema SCADA en la instalación

- Facilitar la supervisión centralizada
- Controlar simultáneamente los distintos elementos de la instalación
- Registrar información del sistema en tiempo real
- Monitorización desde cualquier terminal habilitado

1.8.3 MÓDULO DE SOFTWARE DE GESTIÓN

El software de gestión es una aplicación Cliente/Servidor capaz de supervisar una red industrial de dispositivos y controlarlos desde distintos equipos de la misma red informática mediante pantalla de uso rápido e intuitivo. Este software está compuesto por dos paquetes distintos, el paquete servidor y el paquete cliente.

Paquete Servidor

Es la aplicación principal, encargada de gestionar uno o varios dispositivos. Para ello atiende todas las peticiones de supervisión o control que le lleguen desde los clientes de toda la red. Cabe mencionar que pueden existir diversos SERVER en una misma instalación, encargándose cada uno de supervisar sus dispositivos asociados.

Este módulo del software central se instalará en el mismo servidor propuesto para la gestión de control de accesos en el capítulo anterior, insertado en el *rack* de la sala de telecomunicaciones. Tanto el software de gestión de control de accesos como el software de gestión de SCADA están optimizados para que no requieran un elevado consumo de recursos del servidor, por lo que no habrá ningún problema a la hora de alojarlos en la misma máquina.

Paquete Cliente

Para poder visualizar o supervisar las distintas señales del sistema utilizamos el paquete cliente. Desde esta aplicación no sólo controlamos las señales sino que también podemos configurar una agenda de trabajo para realizar ciertas operaciones según un horario establecido. También incorpora un sistema de comprobación el cual avisará al usuario de las posibles alarmas y averías generadas en el sistema.

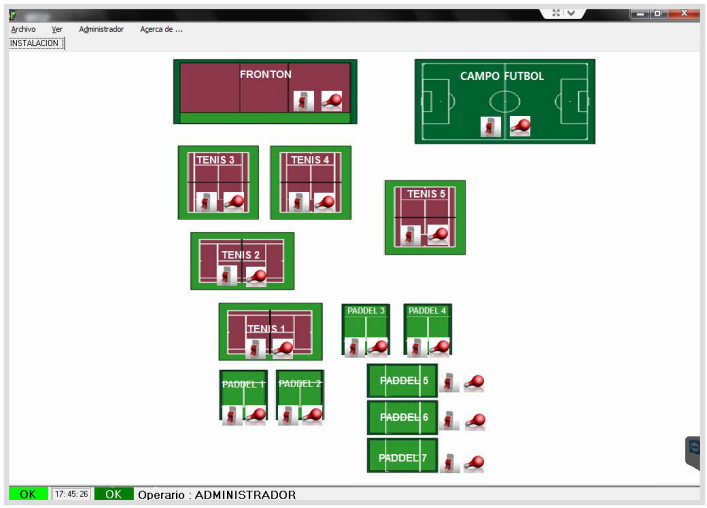

Figura 19. Interfaz cliente, pistas deportivas.

Este módulo de software cliente no tiene límite de conexiones con el servidor central, por lo que puede estar instalado en tantos equipos informáticos como se crea conveniente. Tres paquetes cliente completos se han instalado en tres equipos de la urbanización. El ordenador personal del director(administrador) en su despacho, el ordenador personal del administrador del club social en su despacho del edificio de deportes, y un ordenador ubicado en la garita exterior de vigilancia de uso exclusivo para el control SCADA. Desde cualquiera de los tres equipos se accede al sistema supervisor completo, visualizando en tiempo real el estado de las puertas, alumbrado de todo el recinto del club social, y pudiendo interactuar con los elementos que lo permitan.

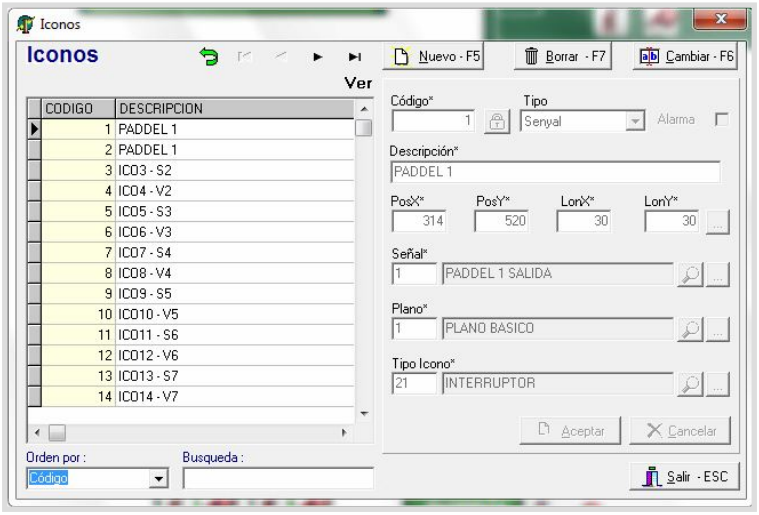

Figura 20. Paquete cliente.

1.8.4 HARDWARE DEL SISTEMA SCADA

Para el correcto funcionamiento del sistema SCADA es necesario el empleo de equipos electrónicos de alto nivel y estándares industriales capaces de adquirir los datos necesarios de los sistemas que se deben supervisar. Además es preciso analizarlos, procesarlos y transmitirlos a los dispositivos que los requieran para, de ese modo, actuar de la manera que corresponda según la programación del software y el hardware de SCADA.

Autómata programable (PLC de control)

Para esta compleja tarea se ha optado por la instalación de un Autómata Programable, también llamado PLC (*Program Logic Controller*), con una serie de accesorios y dispositivos que en conjunto lograrán cumplir rápida y eficazmente el propósito de su instalación.

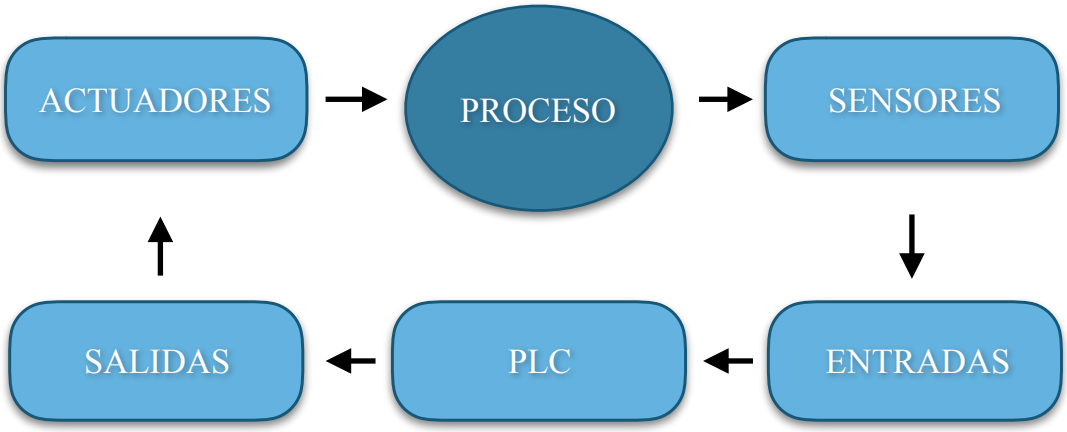

Figura 21. Proceso de automatización.

Existe una gran competencia en el mercado de la automatización industrial, con un gran abanico de marcas y modelos. Para el sistema SCADA de la urbanización, finalmente se ha optado por la instalación de equipos OMRON, por la calidad y fiabilidad de sus contrastados productos y a un coste realmente competitivo en comparación con modelos similares de la competencia. El modelo elegido es el PLC modular OMRON CJ2M CPU32 o similar, el cual nos ofrece un rendimiento excepcional y una rápida respuesta I/O. Además es fácilmente ampliable y configurable gracias al elevado número de módulos de expansión compatibles con esta serie (casi 100), lo que garantiza que se puedan controlar prácticamente todos los procesos que se requieran.

Figura 22. PLC OMRON CJ2M CPU32.

El CJ2M es una versión mejorada de modelos anteriores. Además del mayor rendimiento del procesamiento de la CPU, OMRON también ha añadido en esta versión nuevas unidades I/O de alta velocidad, como unidades de entrada analógica con un tiempo de conversión de 20 μs, mientras que las nuevas instrucciones del PLC proporcionan acceso inmediato a rápidos datos de I/O. El resultado es una mayor fiabilidad en tiempo real.

La serie de CPU de alto rendimiento utilizada ofrece escalabilidad y flexibilidad para cualquier proyecto de automatización. Las nuevas unidades CPU CJ2 ofrecen mayor capacidad, puertos USB y *Ethernet* integrados y son totalmente compatibles con la amplia gama de unidades de I/O anteriores CJ1.

Otras características son las mejoras en las estructuras y matrices, programación basada en etiquetas *(tags)* y mayor capacidad de memoria, que garantizan un desarrollo rápido y con menos costes para el usuario. El nuevo CJ2M presenta módulos de comunicación *plug-in* y más memoria de bloque de función. Las características principales del PLC CJ2M son:

- Es accesible mediante el puerto USB estándar
- Posee puerto *Ethernet* estándar con función *Data Link Ethernet/IP*
- Tiene un amplio rango de capacidades de programa, de 5 a 60 Ksteps
- Practicidad de instrucciones de posicionamiento
- Trabaja con una ejecución eficiente de los bloques de función

Fuente de alimentación del PLC

Los sistemas CJ pueden funcionar con fuentes de alimentación de 24 Vcc o conectados a una red eléctrica de 100 a 240 Vca. Para sistemas pequeños con I/O digitales principalmente, se puede utilizar una fuente de alimentación de pequeña capacidad y económica. Para sistemas con muchas I/O analógicas y unidades de control/comunicaciones, puede ser necesario utilizar una fuente de alimentación de mayor potencia.

En el presente proyecto no se propone el control de un gran número de señales en lo que al sistema SCADA se refiere, sin embargo, todas las señales que se van a manejar son de carácter analógico. Por este motivo se ha decidido utilizar una fuente de alimentación OMRON modelo CJ1W-PA205C.

Figura 23. Fuente de alimentación CJ1W-PA205C.

El rango de entrada de esta fuente es de 85 a 267 Vca y tiene un consumo máximo de 100 VA. Con ella se obtiene una potencia máxima de salida de 25W, más que suficiente para alimentar todo el sistema. Este modelo además incorpora un *Display* de estado de mantenimiento para facilitar el reconocimiento de posibles averías. El montaje del componente se realizará sobre el bastidor del autómata, junto al módulo de CPU. En caso de que fuese necesario ampliar el sistema, se podrían conectar hasta 3 expansiones al bastidor de CPU, lo que proporcionaría una capacidad total de 40 unidades de I/O. La longitud total de los cables de expansión de un sistema puede ser de hasta 12 metros.

Unidades de entrada

Las unidades de entrada digitales actúan de interfaz del PLC para lograr un control de secuencia rápido y fiable. Estos dispositivos de alta velocidad permiten la adquisición de los datos proporcionados por los sistemas bajo supervisión, para después procesarlos en la CPU.

Existe un extenso catálogo de estas unidades, analógicos y digitales, desde 8 entradas hasta 64, y con diferentes tipos de conexión, para satisfacer todas las necesidades. Para nuestro sistema se han seleccionado dos módulos CJ1W-ID232 en el bastidor a continuación del CJ2M. De estos, sólo va a utilizarse uno de ellos, porque su misión es la de recoger datos de los sistemas cercanos a su ubicación, en el edificio de Servicios, ya que se van a utilizar expansores repartidos por toda la Fundación para el resto de zonas como se detallará más adelante. El otro módulo se instala y configura para realizar cómodamente posibles ampliaciones del sistema sin modificar el montaje en el bastidor.

Figura 24. Módulo CJ1W-ID232.

Los ID232 son módulos de entrada digitales de 32 puntos que nos permiten recibir señales de estado desde dispositivos externos. El voltaje de entrada de las señales es de 24V con una corriente máxima de 4.1 mA. La conexión de las unidades de E/S de 32 y 64 puntos de alta densidad, como es este caso, se realiza con conectores de cable plano de 40 pines.

Unidades de salida

Para la interacción del sistema SCADA con los procesos supervisados es preciso, además de conocer el estado en el que se encuentran, poder interactuar y ser capaces de modificarlo.

Para ello son necesarias las unidades de salida, que convierten las señales digitales del software SCADA y los resultados de las instrucciones de salida del PLC en señales físicas de tipo contacto ON / OFF para intervenir en el estado de los dispositivos que lo precisen. Existen tres tipos diferentes de unidades de salida respecto al sistema utilizado. Pueden ser con salida de relé, con salida de triac o con salida a transistor.

Para el sistema SCADA de la urbanización se instalarán dos unidades CJ1W-OD211. Estas unidades serán con salida a transistor, de 12 a 24Vdc y 0.5 A como máximo. Disponen de 16 puntos más común cada una de ellas. La conexión del cableado de las salidas se realiza mediante bornes de conexión con tornillo.

Figura 25. Módulo CJ1W-OD211.

La ubicación de los dos módulos OD211 se encontrará en el bastidor del autómata programable, a continuación de las unidades de entrada.

Unidades de expansión de entrada

Estos dispositivos son los encargados de recoger los datos de estado de los procesos que supervisa el sistema SCADA en las instalaciones de la zona residencial. Son unidades de entrada de señales que se comunican con el PLC a través del “BUS DEVICENET" por lo que no es preciso que su ubicación sea cercana al PLC, ganando flexibilidad en la instalación. Así facilitamos la instalación y abaratamos los costes no teniendo que conectar todos los procesos al PLC, creando sub zonas de control y evitando de esta forma muchos metros de cableado.

Las unidades instaladas son las DRT2-ID16-1. Estos son terminales de 16 puntos de entrada con transistor. La alimentación de estos equipos es de 24 Vdc, y la conexión de las señales de entrada se realiza a través de bornes con tornillo sobre transistor PNP.

Figura 26. Módulo DRT2-ID16-1.

Unidades de expansión de salida

Estos módulos son similares a los anteriores en cuanto a conexión a través de DEVICENET con el PLC se refiere. La diferencia es que estos dispositivos nos permiten actuar sobre los procesos supervisados para modificar su estado a través de la señal de las instrucciones de salida del PLC.

El modelo de unidad instalado es el DRT2-ROS16. Cada uno de estos dispositivos nos ofrece 16 salidas de relé, con conexión sobre bornes con tornillo. Tanto la alimentación del equipo como la de los relés que contiene, viene suministrada por el propio BUS de comunicaciones.

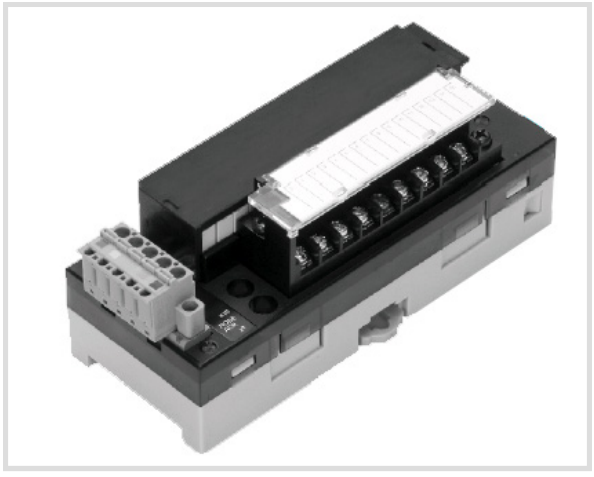

Figura 27. Módulo DRT2-ROS16.

Relés de potencia miniaturizados

Para la supervisión del sistema de alumbrado de la urbanización es precisa la utilización de relés de potencia en conjunto con los módulos de entrada ID232 y DRT2- ID16-1 descritos anteriormente. La empresa encargada de la instalación eléctrica deberá añadir unos teleruptores de control en sus cuadros eléctricos, en aquellos circuitos de alumbrado que se añadirán al

sistema SCADA. Estos teleruptores son válidos tanto para el proceso de lectura de estado como para la actuación sobre el encendido / apagado del circuito. La actuación sobre el teleruptor se realiza a través de un pulso, mediante un contacto seco libre de tensión. Cuando el teleruptor reciba un pulso cambiará el estado del circuito eléctrico al que está conectado.

Para la lectura del estado del circuito, se nos proporciona una señal de 220V en caso de que el alumbrado esté encendido. Por esto, es necesaria la instalación de relés de 220V que nos "conviertan" esa señal de 220V en una señal de 24Vdc necesaria para las entradas de nuestros módulos de entrada.

Los relés instalados son los OMRON MY2IN de 220V. Estos relés disponen de un LED indicador de estado y un pulsador de prueba para testeo del sistema.

Figura 28. Relé OMRON MY2IN.

1.9. APLICACIÓN MÓVIL

Hasta ahora se han estado comentando y analizando cada uno de los sistemas que conforman este proyecto. Dichos sistemas, aunque cuentan con una versatilidad, potencia y capacidades muy superiores a las de sus predecesores, son sistemas que necesitan avanzar y progresar hasta las nuevas tecnologías con el propósito de incrementar sus puntos fuertes y minimizar sus debilidades. El mundo de los sistemas de seguridad está en continúo cambio y crecimiento, y actualmente las posibilidades que ofrece la portabilidad de las aplicaciones móviles proporciona a los sistemas de seguridad y domótica un dinamismo y alcances sin precedentes.

Es por esta razón que en el presente documento se incluye una parte de aplicación móvil. Anexando las plataformas móviles a este proyecto es posible implementar un sistema capaz de ser gestionado desde cualquier teléfono con acceso a internet.

La aplicación que se propone será, en principio, una aplicación genérica que servirá no solo para la instalación que nos ocupa, sino para futuras posibles instalaciones que puedan surgir más adelante. De esta manera será posible dar servicio a una cartera mayor de clientes con la misma base de proyecto, realizando simplemente, una serie de cambios sencillos en el diseño, apariencia y conectividad de la aplicación. La aplicación en cuestión posee como nombre "*Domotic Wytems*" y permitirá a sus usuarios controlar y gestionar los sistemas que se han planteado en este proyecto.

Figura 29. Icono de la aplicación.

Las funciones con las que contará la aplicación son las siguientes:

- Apagado y encendido de la luminaria deportiva
- Monitorización y registro de la iluminación del club social
- Visionado del sistema CCTV a través del teléfono
- Apertura y cierre de los accesos del sistema de control de accesos
- Seguimiento GPS de los vehículos patrulla

Siendo que la app estará totalmente integrada en todos y cada uno de los sistemas de seguridad deberá contar con una serie de características que la doten de la suficiente capacidad para hacer frente a toda la carga de trabajo que tendrá. Sus características principales son:

- Escalabilidad
- Bloques modulares para mayor fiabilidad
- Interfaz de usuario sencilla e intuitiva
- Diseño personalizado
- Distinción y jerarquía de usuarios
- Consumo reducido de recursos
- Consumo reducido de datos móviles

1.9.1 PERFILES DE ACCESO A LA APP

No todos los usuarios que utilicen la aplicación necesitarán acceder a todas las funciones de esta, o simplemente la dirección de la urbanización denegará el acceso total a todos los usuarios. Por este motivo se han definido tres tipos de perfiles para acceder a la app, y en función de los privilegios de que disponga cada usuario podrá entrar en unas partes u otras de la herramienta.

Se definen pues, tres perfiles de acceso que quedarán establecidos en el código fuente de la aplicación:

- **Administrador:** la persona que acceda a la aplicación como administrador tendrá la posibilidad de controlar todas y cada una de las funciones de la herramienta. Sin embargo, puede haber conflicto a la hora de intentar acceder al visionado de las cámaras, ya que para ello será necesario contar con otro usuario y contraseña a parte de las iniciales.

- **Conserje:** el usuario que solo posea los privilegios de este perfil de acceso únicamente podrá acceder a las funciones de la luminaria deportiva del club social, ya que este perfil se ha creado pensando en las funciones que lleva a cabo el conserje del club social.

- **Vigilante de seguridad:** el perfil de acceso a la aplicación de vigilante de seguridad contará con casi todas las funciones excepto aquellas que se encargan de controlar la iluminación del club. De tal modo, las personas encargadas del patrullaje y la seguridad de la urbanización podrán acceder al control de accesos, visionado de las cámaras y localización GPS de los vehículos patrulla.

Una vez el usuario abre la aplicación en su terminal aparece una pantalla que le pide que introduzca un usuario y una contraseña para, de ese modo, direccionarle a las funciones a las que puede acceder. La pantalla es la siguiente:

Figura 30. Pantalla de "log-in"

1.9.2 ESTRUCTURA DE LA APLICACIÓN

En lo que respecta a la estructura que presenta la aplicación, se ha intentado que fuese una herramienta dinámica y fácil de utilizar , de tal modo que su manejo ocupase el menor tiempo posible a los usuarios y no requiriese de ellos una concentración elevada. Tanto es así, que la app incorpora numerosos elementos visuales que facilitan la lectura de sus elementos y evita la cabida a confusiones y errores a la hora de usarla. Además, una de las premisas que se han tenido en cuenta la hora de se desarrollo fue que se pudiese activar cualquier elemento del sistema con tan solo tres *clicks*. Cierto es que hay funciones de la aplicación que requieren de mayor atención y dedicación, pero esto es debido a la complejidad que presentan. Algunas de estas funciones son el visionado de las cámaras y el seguimiento vía GPS.

Gráfico 4. Estructura de la aplicación.

En la imagen anterior se puede apreciar la estructura básica de la herramienta, sin embargo existen multitud de pantallas, cada una de las cuales pertenece a una modalidad deportiva o a una zona específica de la urbanización. Además, en la imagen mencionada no se contempla el perfil de usuario de administrador, ya que, tal y como se ha comentado

anteriormente es capaz de acceder a todas las funciones de la aplicación. En la imagen anterior (*Gráfico 4)*, simplemente se contempla el perfil de conserje en la parte izquierda y el perfil de vigilante en la parte derecha.

Por otro lado, es necesario tener en cuenta que cada modalidad deportiva contará con un número de pistas distinto a las demás, y en consecuencia hay pantallas que difieren de otras levemente. Esto es algo que podría cambiarse o modificarse rápidamente en caso de querer integrar la aplicación en una instalación diferente.

1.9.3 FUNCIONAMIENTO DE LA APLICACIÓN

Para que la aplicación funcione correctamente es necesario que los terminales cuenten con acceso a internet, bien sea a través de la red *wi-fi* (en caso de haberla en la urbanización) o bien a través de una tarjeta telefónica 3G o 4G. Esto es debido a que la aplicación está continuamente accediendo a la red para subir o descargar datos de ella, y más concretamente de las bases de datos alojadas en los servidores descritos en capítulos anteriores.

Ya se ha comentado que cualquier cambio en el sistema SCADA pasa a través de su software, y este está enlazado a la base de datos del servidor del sistema. Básicamente, el método de funcionamiento de la aplicación trata de acceder a esa base de datos para cambiar determinados valores de cada tabla y así hacer creer al sistema que la orden llega del software de SCADA. De tal modo se podría afirmar que la aplicación es un contenedor de listas y botones que, básicamente, cambian bits en las bases de datos.

La aplicación desarrollada para este proyecto se ha implementado en el entorno de desarrollo conocido como “Android Studio”, aunque también podrían haberse utilizado otros IDE tales como “Eclipse”, “Netbeans” o “Aide".

Los lenguajes de programación necesarios para desarrollar una aplicación de estas características son cuatro:

- Java/JavaScript
- Xml
- PHP
- SQL

El lenguaje Xml ha sido necesario para programar la interfaz del usuario dentro de la aplicación, y junto con el lenguaje Java conforman la manera de funcionar y la función de cada elemento de la app. Por otro lado, se han empleado códigos PHP escritos en el IDE llamado “Netbeans”, que actúan como puentes entre la base de datos y la aplicación. Es en estos códigos

PHP donde se insertan las consultas SQL que se han de hacer a la base de datos para consultar, modificar o borrar valores dentro de las tablas.

Como ya se ha dicho, la aplicación móvil realiza consultas continuas a la base de datos o al servidor, y la base de datos responde a la consulta con los datos solicitados de una manera similar a esta:

[{"titulo":"prueba","descripcion":"prueba1","imagen":"10646759_10203037896250548_1855274062202393600_n.jpg"}]

Figura 31. Consulta a la base de datos.

Para que la aplicación o el desarrollador pueda comprender esta respuesta y se puedan manejar los datos devueltos se ha de traducir mediante un paquete denominado JSON, de modo que se han de emplear una serie de métodos que realicen las siguientes funciones:

1. **Autenticación:** mediante este método se realiza la consulta de autenticación del usuario cuando intenta acceder a la aplicación. La manera en la que se procede comienza enviando un método "GET" a la base de datos junto al usuario y contraseña introducidos por el usuario desde la app. Una vez esta petición llega a la base de datos, esta contesta con un cero si ese usuario y/o contraseña no está registrada, o con un uno si los datos coinciden con los de las tablas. Cuando el programa java recibe el resultado de la consulta, el método que se emplea para dar paso o no al usuario es el siguiente:

```
public int obtDatosJSON(String response) {
    int res = 0;
    try {
        JSONArray json = new JSONArray ( response );
        if (json.length () > 0) {
            res = 1;
        }
    } catch (Exception e) {}
    return res;
}
```

Figura 32. Método "objDatosJSON".

2. **Conexión y petición de lectura:** esta función será muy utilizada en esta aplicación, ya que a través de ella se podrá consultar el estado de cualquiera de las pistas deportivas o de las puertas y pórticos del control de accesos. El método de funcionamiento es muy similar al explicado anteriormente, ya que tras crear la conexión con las base de datos, enviamos una consulta almacenada en los ficheros .PHP que devuelve la información demandada. Una vez recibida esta información es tratada por medio del JSON y gestionada dentro de la aplicación con el lenguaje Java.

3. **Conexión y petición de escritura:** se empleará esta función siempre que sea necesario cambiar el valor de alguna de las tablas para cambiar el estado de cualquier componente conectado al sistema SCADA. Al contrario que la petición de lectura, esta función hace uso del método "POST" para insertar o modificar el valor de alguna tabla.

La imagen que se muestra a continuación intenta explicar de manera muy ilustrativa el proceso de obtención de datos de una base de datos desde un terminal Android o IOS. Se puede apreciar que la mayor parte del trabajo recae sobre el servidor que aloja la base de datos, ya que el terminal simplemente gestiona los datos que le llegan de las consultas SQL. El paquete JSON

es el encargado de hacer legibles los datos que llegan del servidor, ya que como se puede apreciar en la imagen adjuntada anteriormente, llega una cadena de caracteres que le sería muy difícil digerir a un desarrollador.

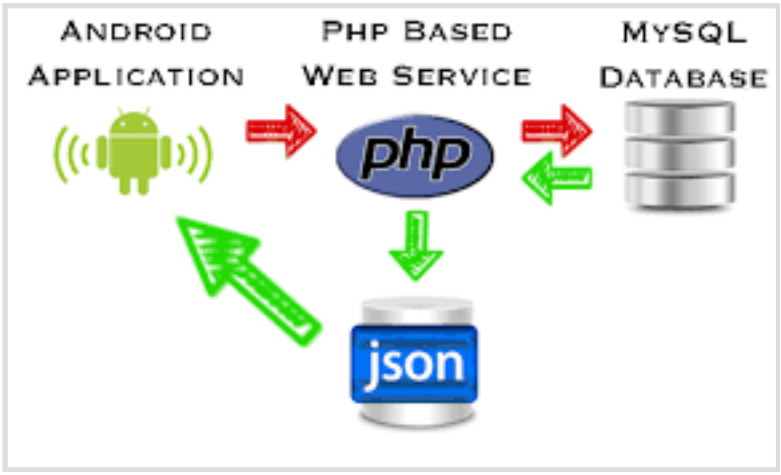

Figura 33. Proceso de obtención de datos.

La última parte de la aplicación es la geolocalización de los vehículos patrulla. La aplicación está programada para enviar los datos de su ubicación a todos los terminales que tengan instalada la aplicación, de modo que aquel usuario que tenga acceso a la localización GPS podrá ver la ubicación de cada dispositivo móvil conectado a las funciones de vigilante de seguridad. El tiempo que transcurre entre dos envíos de ubicación es de 30 segundos, pudiendo desconectar la localización GPS desde los ajustes de la aplicación.

1.9.4 PLATAFORMAS MÓVILES E IMPLANTACIÓN

Como bien es sabido, existen diversas plataformas móviles en las que se puede desarrollar una aplicación, sin embargo las más importantes son Android e IOS. La razón por la cual son las más relevantes es el número de usuarios con los que cuenta cada plataforma. En el caso de Android, que posee la mayor carga de clientes del mercado, cuenta con el 90% de los usuarios de “smartphones”, mientras que IOS, Blackberry y Windows poseen el 10% de la cuota de mercado.

A día de hoy, multitud de desarrolladores optan por implementar sus aplicaciones únicamente en las plataformas de Android e IOS, ya que sería contraproducente desarrollar aplicaciones que solo utilizarían un puñado de usuarios. En el caso de este proyecto solo se contempla la posibilidad de implementar la aplicación para las dos plataformas mayoritarias, siendo Android la que se ha utilizado de ejemplo para esta memoria.

A la hora de implantar la aplicación en el sistema, y debido a que se trata de una herramienta puramente administrativa, se podrían contemplar dos opciones según las

necesidades del cliente. Por un lado, cabe la posibilidad de cargar o subir los APK (paquetes generados que contienen el programa) a las tiendas de Android e IOS, "Play Store" y "App Store" respectivamente, de tal manera que cualquiera pudiera acceder a ellas y descargarlas. O bien instalar los APK en aquellos terminales designados por la urbanización para un uso meramente profesional y destinados a la gestión y administración de la zona residencial.

En el caso de esta instalación, será preferible no publicar las aplicaciones en las tiendas, ya que de hacerlo habría que pagar las cuotas que establecen Google y Apple para poseer una cuenta de desarrollador y además la instalación no requiere de un gran número de terminales móviles.

1.9.5 POSIBLES AMPLIACIONES

Como se ha mencionado con anterioridad, se ha diseñado la app de modo que en cualquier momento sea posible realizar ampliaciones sin necesidad de dejar al cliente sin servicio y sin que influya el nuevo código en el programa antiguo. En esta memoria se proponen un serie de ampliaciones que podrían llevarse a cabo en un futuro, no solo para mejorar las prestaciones o las deficiencias de la aplicación, sino para incrementar el alcance de esta:

- **Añadir nuevos perfiles de usuarios:** la filosofía de la aplicación podría llevarse a un nuevo nivel incluyendo nuevos perfiles de usuarios en la app. De este modo cualquier persona relacionada con la urbanización, ya sean administradores o residentes, podrían llevar a cabo tareas a través de sus teléfonos móviles. Entre estas tareas se podrían destacar el pago de la cuota del club social, incluir un boletín de noticias o un tablón de anuncios, agregar un buzón de sugerencias, añadir un botón del pánico en caso de intrusión una vivienda, etc.

- **Reserva de instalaciones deportivas y de restaurante:** el hecho de poder realizar una reserva, bien sea del restaurante o de alguna pista deportiva, añadiría un gran valor y una gran capacidad a la herramienta.

1.10. SISTEMAS AUXILIARES

1.10.1 SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA

Dadas los condicionantes de emplazamiento de la urbanización, por su lejanía a núcleos urbanos, y siendo una zona que históricamente viene padeciendo una cadencia de fluctuaciones y armónicos en la red eléctrica de suministro por parte de la empresa suministradora de energía, y conociendo las fatales consecuencias que este tipo de fluctuaciones provoca sobre los equipos electrónicos, se ha planteado la instalación de un sistema de alimentación ininterrumpida (S.A.I.).

Se ha confiado en una empresa especializada en equipos de protección de alimentación, como es EMERSON-LIEBERT. Su catálogo comprende un elevado número de posibilidades dependiendo de las necesidades. Para la instalación y la protección de todos los equipos de red, equipos de seguridad y control, se ha instalado el SAI GXT3 10KVA versión T230.

Figura 34. SAI GXT3 10KVA.

Este SAI online de doble conversión real incluye *bypass* de mantenimiento integrado además de ampliación opcional del tiempo de autonomía. Está disponible en versión sin transformador y con transformador integrado. La versión elegida es la sin transformador, la versión T230, que puede funcionar en configuración 1/1 o 3/1, lo que la hace muy flexible.

El SAI será de formato tipo torre, y con él se conseguirá un doble objetivo, proteger todos los equipos eléctricos y electrónicos a los cuales proporciona alimentación contra sobre tensiones y picos no deseados. Además, en caso de fallo de suministro eléctrico, garantizará el correcto funcionamiento de todos los sistemas durante un elevado margen de tiempo para continuar con la protección y seguridad de la zona residencial.

Se encontrará situado en la sala de telecomunicaciones, ubicado junto a la sala de control. Este equipo proporcionará alimentación limpia y protegida a los dos *racks* ubicados en la misma sala. También alimentará el cuadro donde se ubicará el sistema de supervisión SCADA, el autómata programable y sus módulos de expansión.

2. ÍNDICE DE FIGURAS, TABLAS Y GRÁFICOS

2.1. ÍNDICE DE FIGURAS

2.2. ÍNDICE DE TABLAS

2.3. ÍNDICE DE GRÁFICOS

3. BIBLIOGRAFÍA

Libros de texto y proyectos

Francisco Javier García Mata. "Videovigilancia: CCTV usando videoIP". Editorial Vértice Books 2011.

Victor M. Sempere Payá y Sergio Cerdá Fernández. "Comunicaciones Industriales con Simatic S7". Editorial Universidad Politécnica de Valencia.

Aquillino Rodríguez Penin. "Sistemas Scada. Editorial Marcombo S.A". Tercera edición.

Miguel Cuadros Quesada. "Diseño, instalación y configuración de un sistema integral de seguridad corporativa". 2013.

Silvia Martí Martí. "Diseño de un sistema de televigilancia sobre IP para el edificio CRAI de la Escuela Politécnica Superior de Gandia". 2013.

Páginas Web

Universitat Politècnica de Valencia. 2012. <https://riunet.upv.es>

C3comunicaciones. 2014. <http://www.c3comunicaciones.es>

Hikvision. 2014. <http://www.hikvision.com/en/>

Web de desarrolladores de Android. 2016. <https://developer.android.com/index.html>

Wikipedia. 2016. <https://es.wikipedia.org/wiki/Control_de_acceso>

Vigicam. 2016. <http://www.vigicam.cl/fullip.htm>

4. ANEXOS

ANEXO I. PRESUPUESTO.

ANEXO II. PLANIMETRÍA.

ANEXO III. FICHAS TÉCNICAS.