



**PAC 5**  
del  
**Trabajo Final de Máster**  
**MEMORIA**

**Título del Proyecto:**

Diseño de un modelo de red domótica libre basada en componentes OpenDomo, para aplicación a un pequeño hotel

**Especialidad:** Administración de redes y sistemas operativos en entornos de Software Libre

**Autor:** Valeriano López Torres  
**Consultor:** Miguel Martín Mateo  
**Tutor de prácticas externas:** Oriol Palenzuela i Rosés  
**Fecha:** Mayo-2014

**Este trabajo se publica con la Licencia:**  
“Reconocimiento-CompartirIgual 3.0 España (CC BY-SA 3.0 ES)”  
de Creative Commons.

**Los términos de esta licencia pueden consultarse en la siguiente dirección:**  
<http://creativecommons.org/licenses/by-sa/3.0/es/>

## RESUMEN

El objeto de este proyecto es crear un *diseño tipo* de instalación domótica para un hotel de hasta unas 100 habitaciones, basada en componentes Hardware/Software diseñados y distribuidos por la empresa OpenDomo. OpenDomo es una empresa dedicada al desarrollo y comercialización de productos de control domótico, para cuyo desarrollo del software necesario se basa en los principios de software libre.

La instalación propuesta está orientada principalmente al ahorro energético y por tanto al control de los principales elementos que tienen impacto sobre el ahorro, esto es, la iluminación y la climatización; aunque pueden ampliarse y particularizarse en la etapa de diseño con aplicaciones más concretas según necesidades del cliente hotelero.

En el modelo se define una distribución tipo de componentes, la topología y redundancia de los elementos de la red, la interconexión necesaria con sensores y actuadores, así como una descripción de su comportamiento funcional. El problema se plantea como un proyecto informático de redes, con la particularidad de que al no tratarse de una aplicación a un caso concreto sino a un modelo, algunas de sus distintas fases se aplicarán a un escenario ficticio que sirva como modelo de referencia.

El sistema propuesto se apoya por un lado en la gama de productos OpenDomo, y muy particularmente en el controlador ODControl como elemento básico, y por otro en los dispositivos, tecnologías y protocolos de red abiertos de uso común en el mercado, lo cual confiere al modelo unas ventajas en diversos aspectos sobre otras tecnologías propietarias.

A continuación se presenta un diagrama básico descriptivo del sistema a desarrollar :



## Índice de contenido

1	Introducción.....	7
1.1	Contexto de la aplicación. Domótica e Inmótica.....	7
1.2	Qué es OpenDomo.....	7
1.2.1	La tecnología de OpenDomo.....	8
1.3	Motivación del Proyecto.....	8
2	Objetivos del Proyecto.....	9
3	Estudio de Viabilidad.....	11
3.1	Necesidades y requisitos del cliente.....	11
3.2	Análisis de la situación actual.....	12
3.3	Definición de requisitos del sistema.....	13
3.4	Estudio de alternativas de solución.....	14
3.4.1	Riesgos genéricos detectados que afectan a la viabilidad del sistema: .....	14
3.4.2	Conclusión sobre la viabilidad de cumplimiento de los requisitos.....	15
3.5	Alternativas de solución.....	15
3.5.1	Implantación de los ODControl en los espacios del hotel.....	15
3.5.2	Topología de la red local.....	16
3.5.3	Puesto de control.....	19
3.5.4	Ancho de banda necesario para la LAN de ODControles (en el peor caso): .....	23
3.6	Valoración y elección de las posibles soluciones.....	25
3.6.1	Revisión final de cumplimiento de requisitos para la opción elegida.....	26
3.7	Estudio de viabilidad desde el punto de vista de ahorro energético y económico..	27
3.7.1	Datos de partida del estudio.....	27
3.7.2	Cálculo del ahorro energético.....	28
3.7.3	Presupuesto de realización de la instalación.....	28
3.7.4	Cálculo del COSTE / BENEFICIO y recuperación de la inversión.....	30
3.8	Conclusiones del Estudio de Viabilidad.....	31
4	Etapas de Análisis.....	32
4.1	Definición del Sistema.....	32
4.1.1	Límites del sistema.....	33
4.1.2	Comunicación entre los subsistemas.....	34
4.1.3	Entorno tecnológico.....	35
4.2	Establecimiento de Requisitos exactos del Proyecto.....	35
4.2.1	Requisitos adicionales en fase de Análisis.....	35
4.2.2	Especificación de Casos de Uso.....	37
4.3	Definición de las interfaces de usuario.....	41
4.3.1	Identificación de perfiles de usuario de la interfaz: .....	41
4.3.2	Especificación de Principios Generales de la Interfaz.....	42
4.3.3	Esquema de la interface de usuario.....	43
4.4	Plan de Pruebas.....	44
5	Etapas de Diseño.....	45
5.1	Definición de la Arquitectura del Sistema.....	45
5.1.1	Definición de Niveles de Arquitectura .....	45
5.1.2	Especificación de Estándares y Normas de Diseño y Construcción .....	47
5.1.3	Identificación de Subsistemas de Diseño.....	47
5.1.4	Especificación del Entorno Tecnológico.....	48
5.1.5	Integración con otros sistemas.....	55
5.1.6	Seguridad y control de acceso :.....	55
5.2	Especificaciones de desarrollo y pruebas .....	58
5.2.1	Especificaciones de desarrollo .....	58

5.2.2 Especificaciones de pruebas.....	59
Especificación del Entorno de Pruebas. Entorno tecnológico.....	59
Especificación de las pruebas:.....	59
5.3 Establecimiento de Requisitos de Implantación.....	61
5.3.1 Especificación de Requisitos de Documentación de Usuario.....	61
5.3.2 Especificación de Requisitos de Implantación.....	62
6 Etapa de Desarrollo.....	63
6.1 Definición de la documentación necesaria (Manuales de Usuario).....	63
6.1.1 Documentación para el usuario normal.....	63
6.1.2 Documentación para el usuario administrador.....	64
6.2 Definición de la formación necesaria para Usuarios Finales.....	65
6.2.1 Definición del Esquema de Formación.....	65
6.2.2 Especificación de los Recursos y Entornos de Formación.....	66
7 Licencias del software y de los manuales desarrollados.....	66
8 Etapa de Implantación y Aceptación del Sistema.....	66
8.1 Establecimiento de un Plan de Implantación.....	67
8.1.1 Alcance .....	67
8.1.2 Condicionantes.....	67
8.1.3 Definición del Plan de Implantación.....	68
8.1.3.1 Especificación del Equipo de Implantación.....	69
8.1.3.2 Cronograma de implantación. Diagrama de Gantt .....	70
9 Valoración económica.....	72
10 Conclusiones.....	74
10.1 Cumplimiento de objetivos del proyecto.....	74
10.2 Propuesta para nuevas versiones de ODControles.....	75
10.3 Escalabilidad del diseño de la LAN.....	75
10.4 Posibles ampliaciones del trabajo.....	75
11 Referencias bibliográficas.....	76
ANEXO 1. Componentes OpenDomo.....	79
ODControl.....	79
Aspecto del controlador ODControl:.....	80
Conexiones e indicaciones del controlador ODControl:.....	80
Módulo AI420.....	80
Módulo AO010.....	80
OpenDomo (sistema operativo).....	80
ODNetwork.....	81
Interfaces de usuario.....	82
ANEXO 2. Viabilidad de cumplimiento de los requisitos.....	84
Viabilidad de la instalación desde el punto de vista del cumplimiento de las normativas legales.....	86
ANEXO 3. VERIFICACION FINAL CUMPLIMIENTO DE LOS REQUISITOS DEL SISTEMA POR LA OPCION ELEGIDA.....	89
ANEXO 4: Cálculo del coste del desarrollo del software.....	91
ANEXO 5. Ejemplo de plantilla de un protocolo de pruebas, proporcionada por la Metodología Métrica 3 .....	92
ANEXO 6: Esquemas de principio del control de los diversos elementos domóticos mediante el controlador ODControl.....	93
ANEXO 7. Diagramas de despliegue del sistema.....	96
ANEXO 8. Instalación de las aplicaciones.....	98
Instalación del Servidor HTTP Apache V2.....	98
Instalación del Servidor de tiempo NTP.....	99
Instalación de Unison (sincronización de réplicas de la base de datos).....	99

Instalación de OpenSSH.....	99
Instalación de Nmap.....	100
Instalación del antivirus clamav.....	100
Instalación de IPTables.....	100
Instalación de vlan.....	100
Instalación de MySQL.....	100
Instalación de NESSUS.....	101
ANEXO 9. Configuración de red en los servidores y el router-firewall.....	106
Datos previos.....	106
Configuraciones de red de cada máquina.....	107
ANEXO 10. Implementación de reglas de firewall's mediante IPTables.....	110
Reglas para los Servidores de control .....	110
Enrutado interno hacia las VLAN.....	110
Función de filtrado de paquetes (firewall).....	110
Implementación del firewall con IPTables .....	111
Carga y almacenamiento persistente de las reglas de IPTables.....	112
Reglas para el Router-firewall.....	113
Función de enrutado. Tabla de rutas del router-firewall.....	113
Activación del reenvío de paquetes (IP Forwarding).....	113
Función de filtrado de paquetes (firewall).....	114
Implementación del firewall con IPTables .....	115
ANEXO 11. Breve descripción de las comunicaciones y comandos de control del sistema OpenDomo.....	117
Comunicaciones entre los ODControl y el puesto de control.....	117
Envío de los estados de los ODControl.....	117
Envío de órdenes desde el Puesto de Control .....	117
Recepción de comandos en el ODControl por el puerto 1729/TCP.....	118
Recepción de comandos en el ODControl por el puerto 81/TCP.....	119
Autenticación de acceso a los ODControl.....	119
Seguridad de las comunicaciones.....	120
Sincronización de tiempos entre dispositivos.....	120
Interface gráfica del ordenador central (puesto de control ODNetwork).....	120
ANEXO 12. Instrucción técnica complementaria ITC-BT-51 , del Reglamento Electrotécnico de Baja Tensión, para aplicación a instalaciones domóticas.....	121
Anexo 13. Esquema de la topología de la LAN para 15 plantas.....	124
ANEXO 14. Cálculo de la tasa de bits para 480 ODcontroles.....	126

# 1 Introducción

En este trabajo se creará un diseño tipo de instalación inmótica para un hotel de pequeño tamaño, basada en un red IP y componentes hardware y software de la empresa OpenDomo. Los diferentes componentes de monitorización y control estarán interconectados a través de una red Ethernet.

Ello permitirá disponer de un modelo de instalación que podrá servir de referencia para los profesionales, arquitectos e ingenieros, que deban realizar diseños de instalaciones domóticas en el sector hotelero y que consideren las ventajas que reportarán a sus diseños la utilización de componentes sencillos, de bajo coste y de tecnologías abiertas, como son los productos de OpenDomo.

## 1.1 Contexto de la aplicación. Domótica e Inmótica

Las tecnologías de automatización, en su acepción moderna, no son algo reciente. Ya a mediados del siglo XVIII, con el inicio de la Revolución Industrial, surgió la necesidad de crear elementos de control para las máquinas, que en un principio fueron de tipo mecánico. Sin embargo, a diferencia de otros campos, la automatización de los hogares, lo que entendemos por Domótica [1], es relativamente reciente. Si bien durante todo el siglo XX hubieron diversas iniciativas y proyectos, desde el punto de vista comercial la Domótica solo empieza a despegar seriamente a partir de los años 70 del siglo pasado, y en concreto con el desarrollo de la tecnología X10 [2] ideada para el telecontrol de iluminación y dispositivos a través del cableado eléctrico de los edificios.

A diferencia de otras aplicaciones en las que se ha producido una rápida expansión, en el caso de la domótica no se ha generalizado su uso, dado que la renovación del parque de edificios es un proceso muy lento. Su implantación, en mayor o menor grado, es más significativa en grandes edificios como rascacielos o edificios públicos, donde se aprecian significativamente las ventajas de la automatización de edificios. Para este tipo de edificios, y en general aquellos utilizados en el ámbito industrial o del sector servicios, como oficinas, centros comerciales, hoteles, etc se introduce el término Inmótica [3], de mayor alcance al considerar la automatización integral del edificio. Así, la Inmótica es la aplicación de los principios de la Domótica a los grandes edificios, lo que da lugar a los llamados “edificios inteligentes”.

Entre las ventajas de la Domótica y la Inmótica tenemos el aumento del confort, el ahorro energético y la seguridad de las viviendas y edificios.

## 1.2 Qué es OpenDomo

Tal como se define en su página web “es una empresa dedicada a la investigación, desarrollo y comercialización de productos de control inteligente basados en tecnología libre” ([www.opendomo.com](http://www.opendomo.com)).

Siguiendo la filosofía del Software Libre, la empresa además cuenta con una web para la colaboración de usuarios interesados en esta tecnología abierta: <http://es.opendomo.org/>

### 1.2.1 La tecnología de OpenDomo

OpenDomo ha creado una gama de productos hardware cuyo software es de código abierto y cumple los principios del software libre. Aunque el catálogo de OpenDomo dispone de más productos, el elemento básico (e imprescindible) del sistema será el controlador ODCControl, un controlador con diferentes tipos de entradas y salidas analógicas y digitales y posibilidades de ampliación mediante módulos. Se trata de un dispositivo que combina su gran sencillez con una gran versatilidad para las aplicaciones de control, ya que al disponer de todos los diferentes tipos de entradas y salidas analógicas y digitales es adaptable a casi cualquier tipo de escenario en que se necesite alguna prestación de supervisión y control. Este controlador además puede comunicarse mediante una red IP con otros equipos de supervisión, desde móviles inteligentes para pequeñas aplicaciones hasta hosts que supervisen un gran número de ellos, como será el caso en este trabajo. Esta versatilidad trae como consecuencia añadida y de gran importancia, que el stock de recambios necesarios para el mantenimiento de la instalación se vea reducido. El aspecto de este controlador es el de la siguiente imagen:



El controlador puede funcionar de forma totalmente autónoma, lo que facilitará darle una alta disponibilidad a las funcionalidades básicas del sistema, aun incluso ante una eventual pérdida del puesto de control o de las comunicaciones en la red Ethernet.

Los restantes componentes podrán ser utilizados o no dependiendo de la arquitectura final del sistema que se adopte en la fase de diseño. Una descripción técnica de los productos OpenDomo susceptibles de ser considerados puede consultarse en el ANEXO 1.

### 1.3 Motivación del Proyecto

Existen varias motivaciones que justifican la realización de este proyecto.

Desde el punto de vista de OpenDomo, si bien la empresa ha realizado diversos proyectos en el sector hotelero, siempre ha sido desde el punto de vista de la gestión energética, controlando y monitorizando los consumos de las instalaciones en el cuadro eléctrico principal de Baja Tensión, pero sin llegar a abordar el control integral de las instalaciones del hotel, y en particular del conjunto de habitaciones. Motivo por el que le es de gran interés realizar un ejercicio como en que se plantea en este trabajo, a fin de conocer con más detalles las posibilidades, necesidades y limitaciones de una infraestructura basada en sus productos, en el escenario que se plantea.



El proyecto asimismo será un punto de partida para la toma de decisiones de los profesionales encargados del diseño y reforma de instalaciones hoteleras, haciéndose llegar sus contenidos a ingenieros y arquitectos que deban tomar decisiones en el sector hotelero. De esta forma dispondrán de un análisis demostrativo de las posibilidades de los productos OpenDomo, aplicado al sector en cuestión, así como una propuesta de arquitectura en cuanto a la infraestructura a instalar, lo cual facilitará en gran medida su toma de decisiones. Como consecuencia, ayudará a situar el producto ofertado en una posición más competitiva.

En cuanto a las motivaciones desde un punto de vista puramente técnico, se puede considerar que el uso de tecnologías abiertas, combinado con la utilización de productos de uso general, aporta una serie de ventajas. Como es sabido, en el ámbito de la Domótica existen múltiples protocolos y hardware de uso específico. Algunos de estos protocolos son propietarios, con las desventajas que ello conlleva. También existen otros abiertos, como KNX-EIB, Lonworks o X10, pero cuya especificidad, ya sea a nivel de instalación (por ejemplo X10 funciona a través de los cableados eléctricos) o su relativa complejidad a nivel protocolo, innecesaria en ciertas aplicaciones o escenarios, pueden no ser una solución totalmente satisfactoria. Así, resulta interesante la creación de una red domótica basada en componentes de infraestructura y protocolos de uso generalizado (protocolo TCP/IP, switches o routers de uso general, etc), no exclusivamente utilizables en aplicaciones domóticas, lo cual permite la integración y reutilización de componentes de diferentes sistemas. También permitirá una menor necesidad de personal especializado en un tipo de instalación domótica determinada, menores necesidades formativas, al basarse la infraestructura y protocolos de red en los de uso más extendido en el ámbito de las telecomunicaciones (en particular TCP/IP), siendo específico únicamente el controlador ODControl, cuyos comandos de control son realmente sencillos de aprender y utilizar. Y al ser una tecnología abierta y sencilla, permite una fácil implementación de reformas, mejoras, ampliaciones, etc...tanto de la infraestructura como del software de monitorización, por prácticamente cualquier tipo de empresa informática local, evitando así la dependencia tecnológica y disminuyendo los costes de mantenimiento.

Desde un punto de vista personal, este proyecto surge como una propuesta propia realizada a la empresa OpenDomo, al comprobar que sus productos tienen el potencial para crear una red para automatización conjugando varios aspectos de interés y de actualidad:

- la domótica
- el ahorro energético
- el software libre y las tecnologías abiertas.

## 2 Objetivos del Proyecto

Entre los objetivos a conseguir, tenemos los de tipo más general y otros más específicos. Entre los primeros tenemos los siguientes:

- Demostrar la viabilidad de la utilización de los productos OpenDomo como parte fundamental de la infraestructura de control inmótico de un pequeño hotel.
- Obtener un modelo de instalación de control domótico basada en componentes OpenDomo, aplicable y adaptable a pequeños hoteles.
- Diseñar una instalación domótica de bajo coste.

- Diseñar una instalación domótica fácil de mantener.
- La utilización y promoción de las tecnologías abiertas y el software libre, lo cual permitirá la independencia en su administración y mantenimiento.
- Que la calidad del servicio y confort para los clientes del hotel no se vea afectada por fallos del sistema informático domótico. Este objetivo es de importancia fundamental; deberemos tener presente que la idoneidad del diseño final propuesto va a tener un alto impacto en la calidad del servicio dado por el hotel. Puesto que las instalaciones de todas las habitaciones van a estar controladas por el sistema informático, el diseño de la instalación deberá ser tal que, aún en caso de fallo de algún componente, no haya un impacto sobre el funcionamiento global del sistema y el servicio del hotel y las instalaciones puedan seguir funcionando con normalidad.

Desde un punto de vista más técnico, nos proponemos que el diseño contemple los siguientes aspectos:

- La supervisión de todas las habitaciones del hotel.
- La integración de los controladores y actuadores con la instalación eléctrica debe ser sencilla.
- Que el sistema diseñado permita el ahorro energético, actuando sobre:
  - la iluminación y el control del consumo eléctrico.
  - control de temperaturas actuado sobre el aire acondicionado y la calefacción.
- Que el sistema diseñado permita el ahorro de agua, detectando la circulación indebida por fugas o aperturas de grifos en zonas desocupadas.
- La utilización de componentes de uso común en el mercado para la infraestructura de comunicaciones, a fin de evitar la dependencia tecnológica.
- Que el sistema sea seguro desde el punto de vista informático.
- Que sean identificados los riesgos que puede presentar la nueva instalación, desde el punto de vista de operación y calidad del servicio (análisis de riesgos).
- Que el sistema pueda operar sin interrupción, incluso ante averías. Para ello será preciso realizar un análisis de necesidades de alta disponibilidad por componentes, considerando el suministro de energía y el hardware o software redundante necesario.
- Definición de la distribución óptima de controladores en dependencias y particularmente en habitaciones y pasillos.
- Que el modelo de instalación quede bien documentado. Para lo cual deberemos considerar:
  - Diagramas de Despliegue de la red
  - Creación de esquemas-tipo de integración con el sistema a controlar (indicando sensores y actuadores necesarios)
- Que la topología y características de la red de controladores sean las más adecuadas para poder garantizar la continuidad del servicio (disponibilidad).
- Definición de la infraestructura de la red.
- Que queden concretadas las características del puesto de control en cuando a el software libre necesario, las funcionalidades del mismo para el control y supervisión de la instalación, así como la funcionalidad de la interfaz gráfica del SCADA.

### 3 Estudio de Viabilidad

Para este estudio se consideran las actividades que se describen en los siguientes subapartados.

#### 3.1 Necesidades y requisitos del cliente

En este apartado se exponen los requisitos de tipo funcional que el cliente, en este caso la gerencia del hotel, espera que cumpla la instalación domótica. Se establecen diferentes prioridades para su cumplimiento, con la siguiente escala: Muy alta, Alta, Media y Baja. Los requisitos que se fijan son los siguientes:

<b>Identificador</b>	RC-1	<b>Tipo</b>	Funcional	<b>Prioridad</b>	Muy alta
<b>Descripción</b>	El sistema será capaz de controlar un hotel de hasta 100 habitaciones				

<b>Identificador</b>	RC-2	<b>Tipo</b>	Funcional	<b>Prioridad</b>	Muy alta
<b>Descripción</b>	Se realizará el control, a efectos de ahorro energético, de la iluminación				

<b>Identificador</b>	RC-3	<b>Tipo</b>	Funcional	<b>Prioridad</b>	Muy alta
<b>Descripción</b>	Se realizará el control, a efectos de ahorro energético, de la climatización				

<b>Identificador</b>	RC-4	<b>Tipo</b>	Funcional	<b>Prioridad</b>	Alta
<b>Descripción</b>	Se realizará el control, a efectos de ahorro energético, de persianas y ventanas				

<b>Identificador</b>	RC-5	<b>Tipo</b>	Funcional	<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema gestionará alarmas técnicas de detección de fugas de agua				

<b>Identificador</b>	RC-6	<b>Tipo</b>	Técnico	<b>Prioridad</b>	Muy alta
<b>Descripción</b>	Las partes principales de la instalación cuyo posible fallo comprometa la funcionalidad de la instalación al completo, deberán ser diseñadas de tal manera que sea tolerante a más de un fallo.				

<b>Identificador</b>	RC-7	<b>Tipo</b>	Técnico	<b>Prioridad</b>	Muy alta
<b>Descripción</b>	En caso de fallo total del sistema informático, existirá un mecanismo alternativo para poder seguir dando servicio en las habitaciones. Se entenderá por "dar servicio" el poder controlar manualmente la iluminación, la climatización y las persianas.				

Identificador	RC-8	Tipo	Técnico	Prioridad	Muy alta
Descripción	La red del sistema de control será segura y aislada de otros sistemas, al menos a nivel lógico, aunque a nivel físico, dependiendo del diseño, se podrán compartir equipos con otros sistemas (WIFI, etc)				

Identificador	RC-9	Tipo	Legal	Prioridad	Muy alta
Descripción	<p>Cumplimiento de las normativas legales, de distintos ámbitos, de la instalación domótica:</p> <ul style="list-style-type: none"> <li>• Reglamento Electrotécnico de Baja Tensión (RD 842/2002 ) y sus instrucciones técnicas específicas (ICT-BT-51:“<i>instalaciones de sistemas de automatización, gestión técnica de la energía y seguridad para viviendas y edificios</i>”)</li> <li>• Directiva 2004/108/CE de Compatibilidad Electromagnética y RD1580/2006, por el que se regula la compatibilidad electromagnética de los equipos eléctricos y electrónicos</li> <li>• Código Técnico de la Edificación (RD 314/2006)</li> <li>• Reglamento de Instalaciones Térmicas de los Edificios (RITE, RD1027/2007, modificado por el RD 238/2013)</li> </ul>				

A los requisitos del cliente “Gerencia del hotel”, añadiremos el siguiente de OpenDomo:

Identificador	RC-0	Tipo	Técnico	Prioridad	Muy alta
Descripción	El desarrollo se basará en los productos HW/SW y servicios comercializados por OpenDomo				

### 3.2 Análisis de la situación actual

En esta etapa, el estudio será aplicable tanto para nuevos edificios como para aquellos previamente construidos, variando en uno u otro caso la forma de instalación.

Generalizando, podremos encontrarnos dos tipos de situaciones, atendiendo a la existencia o no de una infraestructura previa disponible. En el caso de que existiera una instalación de red previa, deberíamos considerar cuestiones como el rango de IP's utilizados y disponibles, equipos existentes y topología, velocidad actual de la red, equipos reutilizables y necesidades de nuevas adquisiciones, etc, a fin de evaluar las adaptaciones necesarias. Normalmente, si existe una infraestructura previa, será por los servicios habituales de los hoteles, como puntos de red en habitaciones o acceso WIFI. Dado que las casuísticas que se pueden encontrar son muy diferentes, nos centraremos en el otro caso, que es aquel en que se ha de adquirir e instalar toda la infraestructura de red “desde cero”.

El mismo análisis se puede hacer en caso de existir una infraestructura inmótica previa, en cuanto a aprovechamiento de actuadores y sensores. Como en el caso anterior, supondremos que no existe una instalación previa.

### 3.3 Definición de requisitos del sistema

<b>Identificador</b>	RS-1	<b>Tipo</b>	Técnico	<b>Prioridad</b>	Alta
<b>Descripción</b>	Cada habitación será controlada de forma independiente, mediante su propio controlador ODControl (requisito que proporcionará un adecuado equilibrio entre funcionalidad y coste de la instalación)				

<b>Identificador</b>	RS-2	<b>Tipo</b>	Técnico	<b>Prioridad</b>	Muy alta
<b>Descripción</b>	En cada habitación se controlará al menos: <ul style="list-style-type: none"> <li>iluminación (control de tipo ON/OFF: encendido/apagado)</li> <li>temperatura</li> </ul>				

<b>Identificador</b>	RS-3	<b>Tipo</b>	Técnico	<b>Prioridad</b>	Media
<b>Descripción</b>	En cada habitación se controlará adicionalmente: <ul style="list-style-type: none"> <li>motorización de persianas</li> <li>apertura de ventanas</li> <li>detección de fugas de agua</li> </ul>				

<b>Identificador</b>	RS-4	<b>Tipo</b>	Técnico	<b>Prioridad</b>	Muy alta
<b>Descripción</b>	Se controlará la climatización, así como la iluminación de las zonas comunes, haciendo uso de sensores de presencia				

<b>Identificador</b>	RS-5	<b>Tipo</b>	Técnico	<b>Prioridad</b>	Muy alta
<b>Descripción</b>	Los subsistemas troncales tendrán redundancia para garantizar una alta disponibilidad. En concreto: <ul style="list-style-type: none"> <li>la red local de comunicaciones dispondrá de al menos un camino alternativo</li> <li>el puesto de control estará redundado a nivel hardware y software</li> </ul>				

<b>Identificador</b>	RS-6	<b>Tipo</b>	Técnico	<b>Prioridad</b>	Muy alta
<b>Descripción</b>	El puesto de control dispondrá de algoritmos o consignas de control de dispositivos para ahorro energético (bajar persianas, apagar iluminación de plantas enteras, etc)				

<b>Identificador</b>	RS-7	<b>Tipo</b>	Técnico	<b>Prioridad</b>	Muy alta
<b>Descripción</b>	Existirá un puesto de mando en el que se controlarán, para cada habitación o zona común: <ul style="list-style-type: none"> <li>iluminación</li> <li>temperatura</li> <li>alarmas técnicas (las que se implementen)</li> </ul>				

### 3.4 Estudio de alternativas de solución

Antes de proponer las diferentes alternativas, vamos a evaluar los principales riesgos que puede presentar la instalación, así como la viabilidad de cumplimiento de cada uno de los requisitos con los productos OpenDomo que vamos a utilizar.

#### 3.4.1 Riesgos genéricos detectados que afectan a la viabilidad del sistema:

En la siguiente tabla se describen posibles riesgos que podrían comprometer seriamente la óptima funcionalidad de la instalación (independientemente de su arquitectura) y las mitigaciones que deberán considerar las diferentes alternativas. Algunos de estos riesgos ya están mitigados por los propios requisitos del cliente o del sistema. Los no contemplados, deberán ser considerados de forma particular en cada una de las alternativas de solución.

SITUACION DE RIESGO	MITIGACIONES
Pérdida de las comunicaciones con los servidores del Puesto de Control	<ul style="list-style-type: none"> <li>Rutas alternativas en la red de comunicaciones troncal.</li> <li>ODControl con funcionamiento autónomo</li> </ul>
Fallo de un servidor del Puesto de Control	Diseñar configuración de alta disponibilidad
Fallo total del Puesto de Control (fallos catastróficos, en diversas modalidades, que hagan perder ambos servidores)	<ul style="list-style-type: none"> <li>Disponer de un ordenador portátil con una versión reducida del software de supervisión y mando, conectable en un puerto de switch de la red, para poder dar las consignas básicas necesarias a cualquier ODControl de la red.</li> <li>Disponer de una versión instalada del software del control sobre una máquina virtual, de manera que en caso necesario pueda arrancarse desde cualquier equipo disponible.</li> </ul>
Fallo del equipo centralizador de una planta (router o switch)	<ul style="list-style-type: none"> <li>ODControl con funcionamiento autónomo.</li> </ul>
Fallo del suministro de energía del Puesto de Control y equipos de comunicaciones	Instalación de un SAI que alimente todos los equipos principales → tendido de líneas eléctricas de SAI, a cada planta, alimentando todos los switches o routers
Fallo de un ODControl de una habitación o dependencia en general.	<p>Alternativa no informática para mantener las funciones básicas (por ejemplo un "by-pass" eléctrico de las órdenes enviadas por el ODControl).</p> <p>Watchdog por hardware del ODControl, que lo reinicia en pocos milisegundos en caso de fallo por bloqueo del software.</p> <p>Disponer de diversas unidades de ODControl programadas en el stock de repuestos de mantenimiento, para reemplazar un ODControl averiado (aproximadamente en 10 minutos).</p>
Ataques informáticos	Énfasis en el diseño de la seguridad informática: aislar la red domótica mediante un firewall. Aislamiento físico o lógico de otras redes locales de servicios del hotel (WIFI,

	Intranet, etc). Controles de accesos a la sala técnica. Protección física de la red y equipos de comunicaciones, perfiles de usuarios según funciones, autenticación en el sistema, inhabilitar puertos hardware.
Virus informáticos	Utilización de software libre. Antivirus. Imposibilidad de instalar software por usuarios no administradores. Inhabilitar puertos físicos.
Corrupción del software	Copias de seguridad. CD's de instalación

### 3.4.2 Conclusión sobre la viabilidad de cumplimiento de los requisitos

Se ha hecho un repaso de los requisitos del proyecto, evaluando para cada uno de ellos su viabilidad y comprobando la inexistencia de posibles incompatibilidades entre ellos. Dicho análisis de requisitos está disponible en el ANEXO 2. Como resultado de ello se llega a las siguientes conclusiones:

- Todos los requisitos analizados pueden ser llevados a la práctica mediante productos OpenDomo (en particular con el elemento básico, el ODControl).
- No existen requisitos incompatibles.
- Una propuesta cumplirá todos los requisitos expuestos anteriormente si cumple:
  1. Todos los requisitos del sistema.
  2. los siguientes requisitos del cliente: RC-7, RC-8 y RC-9, dado que los demás ya quedan englobados por los requisitos del sistema.
  3. La condición, lógica por otro lado, de que la red y el puesto de control se dimensionen adecuadamente al número de ODControles instalados.

## 3.5 Alternativas de solución

Se analizarán separadamente las diferentes partes de la instalación para obtener las distintas posibilidades.

### 3.5.1 Implantación de los ODControl en los espacios del hotel

Ya se ha visto que la instalación de un solo ODControl por habitación es viable para controlar las magnitudes principales indicadas en los requisitos (ANEXO 2). Tratándose además de uno de los requisitos, todas las propuestas deben incluir un controlador por cada habitación. En cuanto a las zonas comunes, en la fase de diseño se deberá establecer para cada caso concreto el número de ODControles y los sensores/actuadores que sean necesarios para cada tipo espacio, y en especial en el caso de los pasillos, tratándose a efectos de conectividad a la red como el resto de controladores de las habitaciones.

### 3.5.2 Topología de la red local

Un parámetro a tener en cuenta es el número de puertos físicos del nodo de comunicaciones a situar en cada planta. Dado que en cada habitación se instalará un ODControl, con su propia conexión de red, previamente haremos una sencilla estimación aproximada, a efectos de estudio de viabilidad, del número máximo de habitaciones por planta que nos podemos encontrar, así como de los restantes ODControl que debemos instalar en las zonas comunes, para el control de la iluminación de los pasillos y la climatización.

- Estimación de ODControles para las habitaciones:  
 En el caso más desfavorable (hotel con muchas habitaciones por planta), podemos hacer la hipótesis de un hotel de 100 habitaciones (nº máximo según requisitos), con una planta baja (planta 0), más 4 plantas dedicadas a habitaciones (plantas 1 a 4), a 25 habitaciones por planta. Así, se requerirán 25 ODControles por cada planta de habitaciones, cada uno en una habitación.
- Estimación de ODControles para las zonas comunes de una planta:  
 En estas zonas un ODControl puede controlar series de elementos (por ejemplo, conjuntos de luminarias de un pasillo, grupos de sensores de presencia con contactos seriados, etc), de manera que no son necesarios tantos controladores. En el caso más desfavorable, de 25 habitaciones/planta, pueden haber (dependiendo de la geometría de los espacios) hasta unos 65 metros de pasillos (\*) y algunos vestíbulos, que pueden ser controlados fácilmente por 5 ODControles.

(\*) considerando una habitación de unos 20 m<sup>2</sup>. que comparta unos 5 m de pared común con el pasillo y que hayan 2 habitaciones enfrentadas.

Teniendo en cuenta que además es conveniente dejar bocas de reserva (en el switch o router), supondremos que el dispositivo de red centralizador deberá disponer de, al menos 32 bocas, y preferiblemente 48 (en un caso real se deberá ajustar al número de elementos a conectar, incluyendo la integración con otros elementos de red que se conecten al switch o router, según diseño (por ejemplo si la infraestructura se aprovecha para la instalación de puntos de acceso WIFI).

Los principales problemas que se detectan al definir la topología de la red son:

ASPECTOS BÁSICOS A CONSIDERAR	COMENTARIO
Al disponer de un ODControl por cada habitación, se requiere un elevado número de puertos del dispositivo de red centralizador ubicado en cada planta.	En cada caso de instalación real, se habrá de calcular el nº mínimo necesario de puertos físicos de conexión de red por cada planta. En el caso propuesto, el mínimo serían 32 puertos; el recomendado 48.
Limitación de los dominios de broadcast. Existen muchos ODControl conectados a la red y su modo de funcionamiento por defecto supone el envío, muy frecuente, de mensajes de broadcast. (Ver ANEXO 11 sobre las comunicaciones OpenDomo).	Cuestiones a tener en cuenta: 1. Configuración de redes virtuales (VLAN) [10] 2. Los ODControl se configurarán en "modo silencioso" (así solo envía un mensaje de broadcast de 30B cada 5 minutos, para informar que está en funcionamiento).



<p>Deben existir rutas alternativas en la red LAN (para satisfacer el requisito de disponibilidad).</p>	<p>Cuestiones a tener en cuenta:</p> <ul style="list-style-type: none"> <li>• Mallado de la red</li> <li>• Protocolo Spanning Tree [12] en los switches</li> <li>• Enlaces Etherchannel (según coste y necesidades de ancho de banda) → puertos virtuales redundantes</li> </ul>
<p>Coste de los dispositivos (routers o switches), dependiendo de su inteligencia y protocolos que soportan.</p>	<p>Los switches CISCO [8] de diversas series (por ejemplo la 2960) disponen de funcionalidades avanzadas muy interesantes para esta aplicación. En concreto el Etherchannel, que permite agrupar diversos puertos físicos para formar un único enlace Etherchannel, proporcionando a la vez redundancia e incremento del ancho de banda del enlace, de manera que si falla 1 enlace físico, los demás siguen funcionando. No obstante los precios de estos switches son sensiblemente mayores.</p>

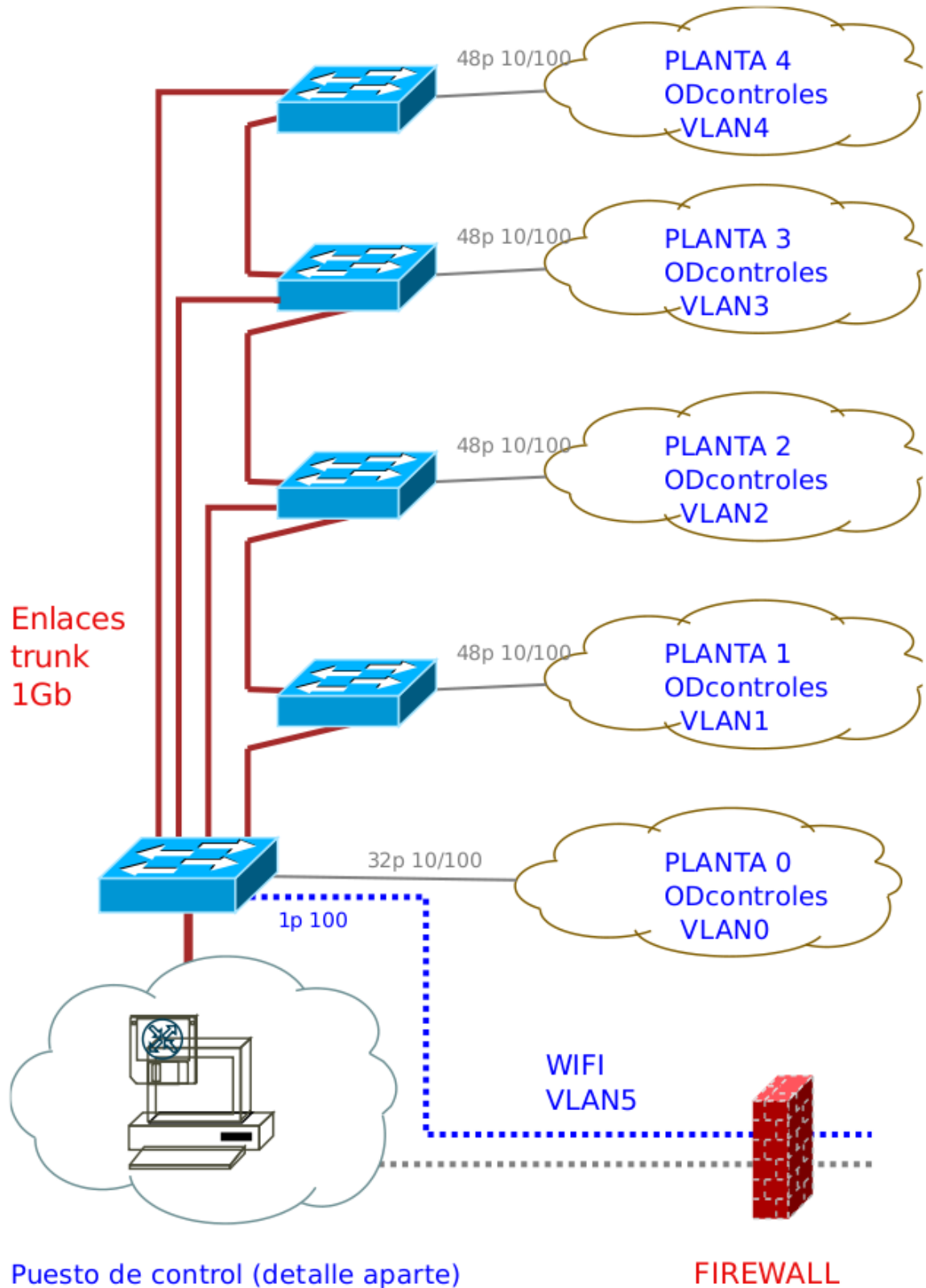
Una opción contemplada en un primer momento hubiera sido trabajar en la capa de red, dada la flexibilidad que permiten los routers para crear y configurar rutas alternativas de backup y limitar los dominios de broadcast definiendo distintas subredes, sin necesidad de utilizar dispositivos de elevadas prestaciones y por tanto alto coste (como es el caso de los switches, como luego veremos). Sin embargo es difícil encontrar routers con muchos puertos físicos Ethernet. Por ejemplo, en uno de los pocos modelos con numerosos puertos, el Cisco RV016 , solo disponemos de 13 puertos Fast Ethernet 10/100 Mbps , por lo que necesitaríamos al menos 3 routers por planta, lo que por precio y complejidad innecesaria es una solución a descartar.

Así, vamos a la solución natural para una red LAN, que es la utilización de switches. Como se adelantó en la tabla anterior, deberemos tener en cuenta lo siguiente a la hora de elegir el switch:

- deberá soportar VLAN's, para reducir los dominios de broadcast. Además, permitirá, en la fase de diseño, integrar otras aplicaciones (por ejemplo puntos de acceso WIFI).
- deberá soportar el protocolo Spanning Tree, para poder integrarse en una red mallada sin que se formen bucles con las tramas

Para reducir el cableado, entre los switches se implementarán enlaces troncales (trunk) [11] por los que se habilitarán todas las VLAN's.

Así, la topología propuesta sería la del la siguiente figura:



Aunque no se considerará un factor a tener en cuenta para determinar la viabilidad, en esta etapa, se ha incluido a efectos ilustrativos de las posibilidades de la topología, la VLAN5 para poner puntos de acceso WIFI en cada planta, aprovechando la infraestructura de switches.

### 3.5.3 Puesto de control

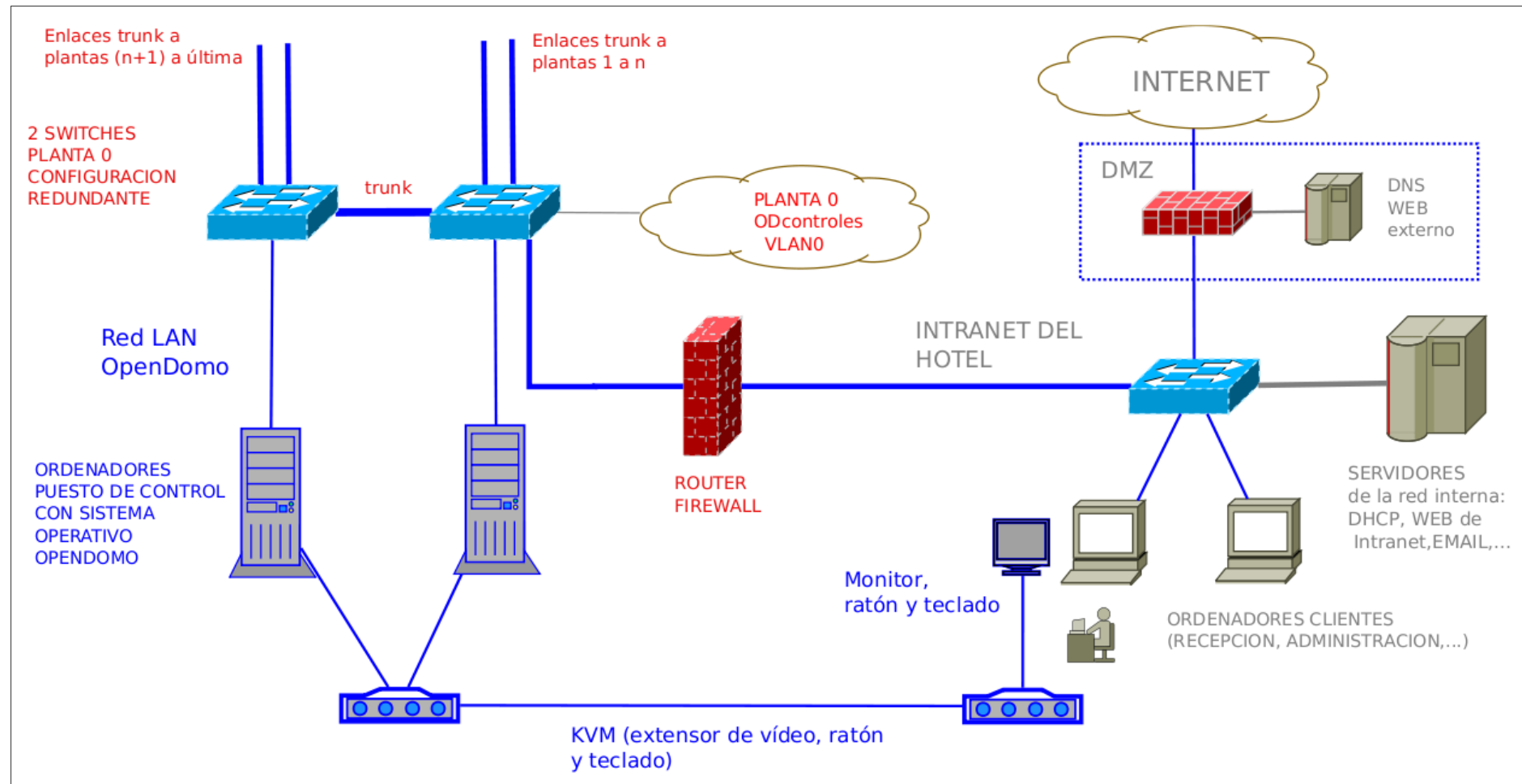
Dada la envergadura de la instalación, los equipos hardware ODNetwork (descritos en el ANEXO 1) no disponen de la potencia suficiente por sí solos para la gestión del sistema, ya que están diseñados para pequeñas instalaciones domóticas. Para la supervisión de los ODControl, se analizarán diferentes posibilidades:

- OPCION A: Ordenadores con la distribución OpenDomo instalada (ya sea sobre máquina virtual o mediante los paquetes .deb o .rpm) y sus aplicaciones standard o ligeras adaptaciones para el caso del hotel. Las interfaces de usuario se trasladan a los puestos de operación (por ejemplo la recepción del hotel) a través de extensores de vídeo, ratón y teclado (extensores KVM). Sería la extrapolación a un hotel de la arquitectura de una instalación domótica OpenDomo de tipo residencial o de oficina, pero de mayor envergadura.
- OPCION B: Ordenadores con la distribución de sistema operativo OpenDomo instalada (ANEXO 1) y sus aplicaciones standard o, como en el caso anterior, con ligeras adaptaciones. Acceso a la aplicación a través de la Intranet, desde cualquier cliente de la Intranet. Este caso es similar al anterior, pero con el acceso web.
- OPCION C: Servidores de control, con una distribución de sistema operativo GNU/Linux convencional por determinar, con un software desarrollado a medida para comunicación y control sobre los ODControles y con funcionalidades accesibles vía web por la Intranet del hotel, lo cual requerirá por tanto, adicionalmente, la instalación de un servidor web en los mismos.

Para asegurar la disponibilidad del control de la instalación, se pueden instalar además ordenadores de control redundados, tal como se ha representado en los esquemas de las figuras siguientes. Asimismo el switch de la planta 0 puede desdoblarse en 2, repartiéndose los enlaces con cada una de las plantas (plantas de la “1 a n” para un switch y de la “n+1 a la última” para el otro) y conectándolos entre ellos para mantener rutas alternativas hacia uno u otro ordenador de control, en caso de fallo del ordenador que se encuentra on-line.

En las siguientes figuras se muestra cada una de las opciones indicadas:

**OPCION A: Ordenadores con la distribución OpenDomo instalada y sus aplicaciones standard (o ligeras adaptaciones). Interfaces a través de extensores KVM.**

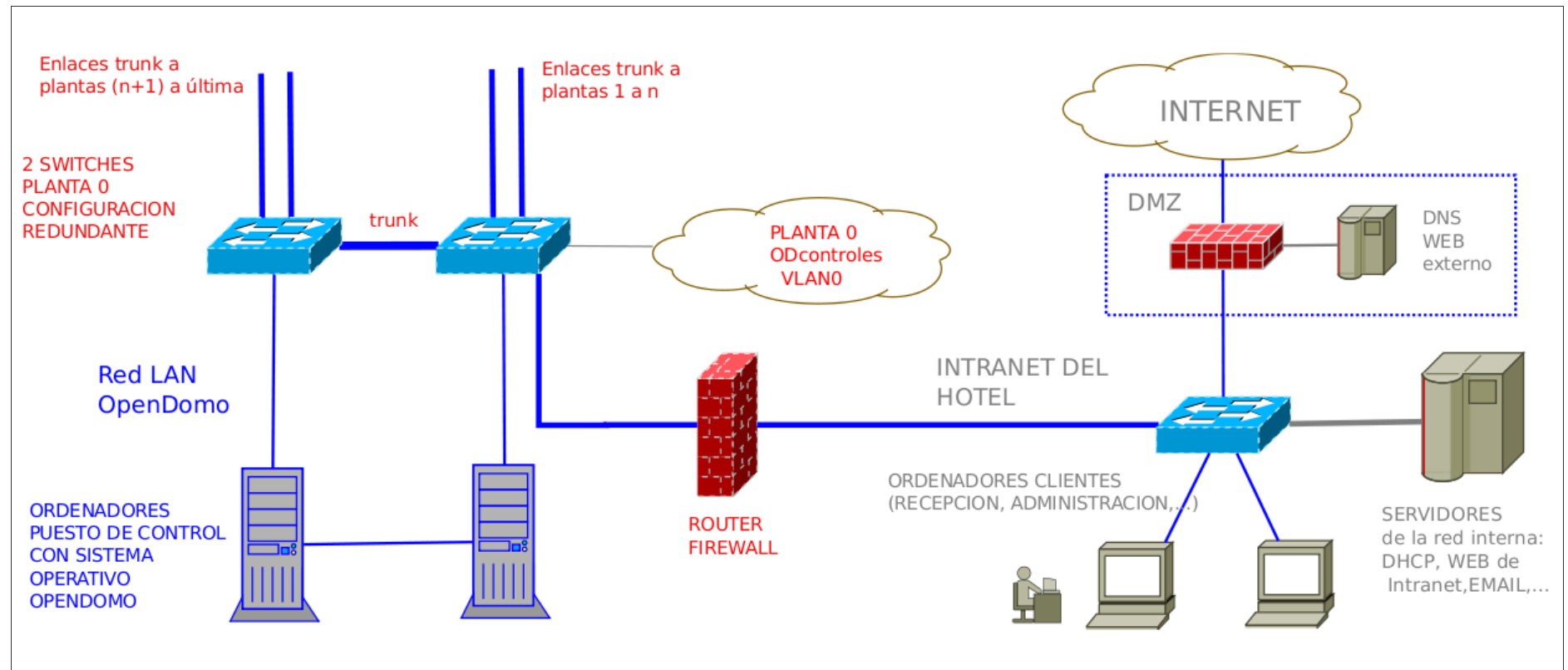


**Observaciones:**

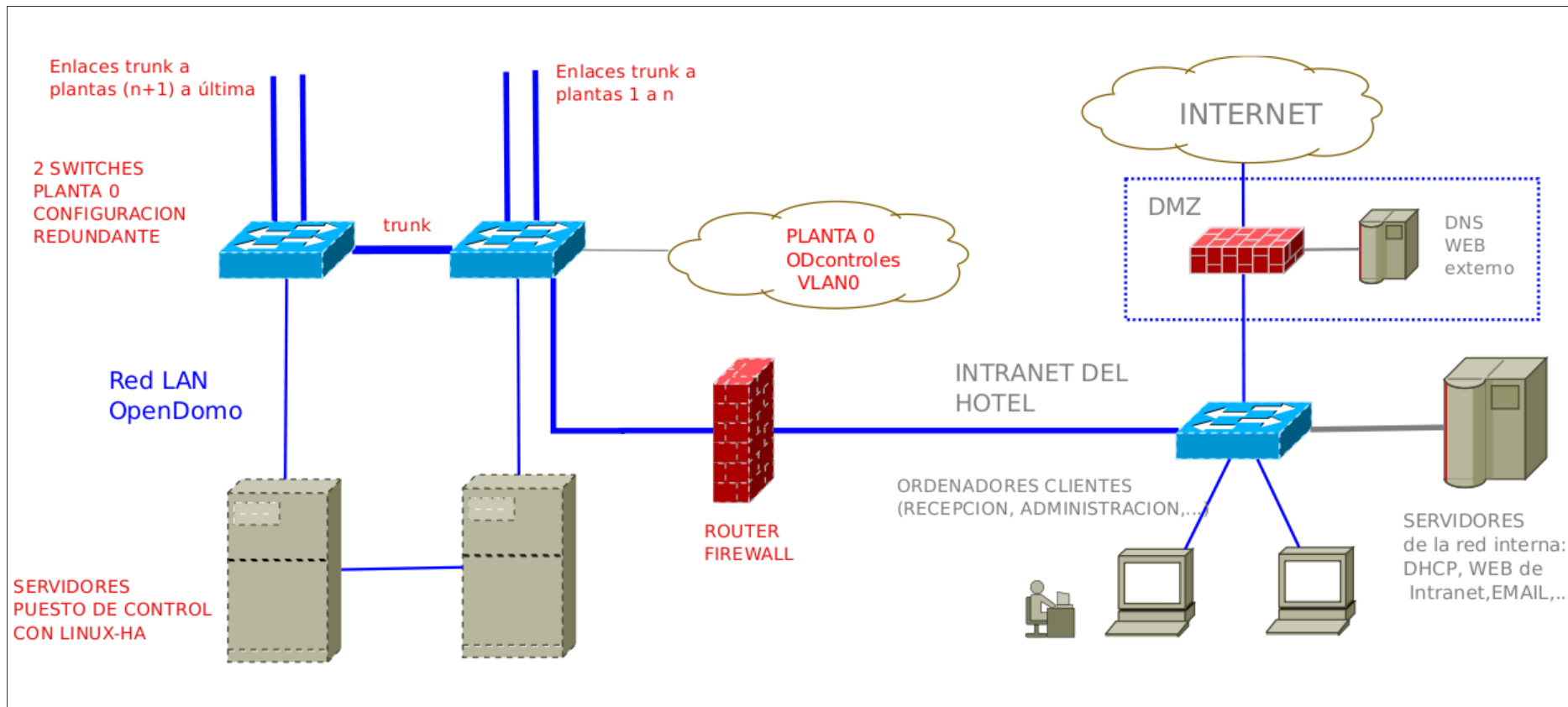
- En la planta 0 se instalan 2 switches conectados entre sí, para mayor disponibilidad.
- La configuración de la Intranet del hotel es orientativa, solo para mostrar la integración con la red OpenDomo
- El acceso a la aplicación de control se realiza directamente mediante extensores de vídeo, teclado y ratón (KVM).

**OPCION B: Ordenadores con la distribución OpenDomo instalada y sus aplicaciones standard (o ligeras adaptaciones). Acceso a**

### la aplicación a través de la Intranet.



**OPCION C: Servidores de control con funcionalidades accesibles vía web por la Intranet (servidor web instalado).**



Observaciones:

- El acceso a la aplicación de control de la red OpenDomo se realiza a vía web desde los ordenadores clientes de la Intranet

### 3.5.4 Ancho de banda necesario para la LAN de ODControles (en el peor caso):

Dado que el mayor volumen de tráfico IP se va a localizar en la conexión entre el switch de la Planta 0 y el Puesto de control (ya que envía y recibe los datagramas de todos los ODControles del edificio), a efectos de viabilidad es preciso hacer una estimación del tráfico que va a soportar. Para ello se realizará un cálculo de máximos, teniendo en cuenta siguientes premisas:

- Cantidad de ODControles instalados: 150
- Tamaño del Mensaje de solicitud de estado de puertos (enviado por el Puesto de Control): 50 bytes
- Tamaño del Mensaje de respuesta a petición de estado de puertos (enviado por el ODControl): 1024 bytes
- Tamaño de un mensaje de "heartbeat" (\*) del ODControl: 30 bytes
- Tiempo máximo del ciclo de interrogación (seg): 3 minutos
- Intervalo (periodo) medio de envío de órdenes (segundos): 5 segundos

(\*) mensaje broadcast que emite cada 5 minutos un ODControl cuando funciona en modo silencioso, para indicar que está activo.

- Protocolo HTTP: Se han supuesto unos 400 caracteres para los mensajes HTTP. En este ejercicio de máximos se ha considerado que los ODControl están funcionando mediante comandos enviados vía HTTP, aunque pueden usarse los otros protocolos menos pesados (véase ANEXO 11).
- Cabecera TCP (incluyendo campo de opciones): 24 bytes
- Cabecera IP: longitud variable de 20-60 bytes; supondremos que es de 40, como en IPv6
- Bytes de las tramas más el intervalo entre tramas Ethernet (interframe gap): 42 bytes

Detalle de bytes considerados para las tramas Ethernet:							
Preámbulo	Dir. Destino	Dir origen	Etiqueta 802.1Q(campo opcional para indicar pertenencia a una VLAN o prioridad en IEEE P802.1p)	Tipo / Longitud datos	CRC	interframe gap (intervalo entre tramas)	TOTAL
8	6	6	4	2	4	12	42
Nota: La longitud mínima de datos en el campo Payload (datos útiles) es 46 bytes. Si es menor se completa hasta los 46 bytes. Aquí en todos los casos siempre se transmiten más de 46 bytes							

Con estos datos, a través de una hoja de cálculo mostrada en la página siguiente hemos obtenido que la tasa de bits máxima que recibe la tarjeta de red del Puesto de control es de unos 20 Kbps, valor muy inferior al de la velocidad que puede soportar una LAN de ancho de banda nominal de 100 Mbps.

<b>CALCULO DE LA TASA DE BITS. ( Ejemplo: nodo mas desfavorable, la tarjeta de red del puesto de control)</b>								
<b>Cantidad de ODControl: 150</b>								
<b>EMISION DE LOS ODControl (BROADCASTS: Cada 5 minutos, envía un "heartbeat" de 30B)</b>								
	Tamaño de datos (bytes)	Bytes Cabecera HTTP	Bytes Cabecera TCP (incl. opciones)	Bytes Cabecera IP	Bytes Ethernet	TAMAÑO TOTAL PAQUETE (packet size) + INTERFRAME GAP en Bytes	Packet Rate (pps). Paquetes enviados por segundo	Tasa total de bits emitidos en conjunto (en Kbps)
Por cada ODControl	30	400	24	40	42	536	0,00333	---
Para todos los ODControl							0,50	<b>2,14</b>
<b>POLLING DEL PUESTO DE CONTROL (Interrogación a los ODControl 1 a 1 para obtener sus estados)</b>								
	segundos	minutos						
Tiempo máximo del ciclo de interrogación (seg)	180	3						
Intervalo (periodo) medio de envío de mensaje de polling (segundos)	1,2							
Mensaje de solicitud de estado de puertos (enviado por el Puesto de Control)	50	400	24	40	42	556	0,83	<b>3,71</b>
Mensaje de respuesta a petición de estado de puertos (enviado por el ODControl)	1024	400	24	40	42	1530	0,83	<b>10,2</b>
<b>ENVIO DE ORDENES ESPECÍFICAS DESDE PUESTO DE CONTROL (activar o desactivar elementos por actuación del usuario) - ESTIMACION</b>								
Intervalo (periodo) medio de envío de órdenes (segundos)	5							
Petición	50	400	24	40	42	556	0,2	<b>0,89</b>
Respuesta (ack)	1024	400	24	40	42	1530	0,2	<b>2,45</b>
						<b>TOTAL TASA DE BITS: 19,39 Kbps</b>		



### 3.6 Valoración y elección de las posibles soluciones

Para la elección de la solución a adoptar, la decisión se centra básicamente en la configuración del puesto de control, dado que la distribución de un ODControl por cada habitación es uno de los requisitos (RS-1) y la topología física de la red es común, mediante switches que permiten rutas alternativas (cumpliendo con el requisito RS-5) y la separación lógica de sistemas (cumpliendo con el requisito RC-8), en este caso mediante VLAN's. Así, centrándonos en la elección de la configuración del centro de control, en la siguiente tabla se muestran ventajas e inconvenientes de cada una de las opciones:

COMPARATIVA ENTRE LAS OPCIONES PARA EL PUESTO DE CONTROL		
OPCION A: S.O. OpenDomo y sus aplicaciones + KVM	OPCION B: S.O. OpenDomo y sus aplicaciones + acceso web por Intranet	OPCION C: Desarrollo a medida + acceso web por Intranet
Encarece el hardware, al tener que incluir los dispositivos extensores de periféricos	Se ahorra el coste de los extensores KVM	Se ahorra el coste de los extensores KVM
No existe redundancia del hardware de los periféricos. (INCUMPLE REQUISITO RS-5)	El ordenador de control puede ser accesible desde cualquier cliente habilitado de la Intranet	El ordenador de control puede ser accesible desde cualquier cliente habilitado de la Intranet
El modo de funcionamiento de los ODControl debe ser el "modo por defecto", que sobrecarga innecesariamente la red de mensajes de broadcast, dado que los modelos basados en el S.O. OpenDomo requieren sincronización de estados entre el sistema operativo y los dispositivos mediante este tipo de mensajes.	El modo de funcionamiento de los ODControl debe ser el "modo por defecto", que sobrecarga innecesariamente la red de mensajes de broadcast, dado que los modelos basados en el S.O. OpenDomo requieren sincronización de estados entre el sistema operativo y los dispositivos mediante este tipo de mensajes.	Permite total flexibilidad, pudiéndose usar el "modo silencioso", con el cual los mensajes broadcast se generan en periodos de 5 minutos, lo que reduce la carga de la red.
La implantación en un hotel requiere hacer cierto grado de adaptación para cumplir algunos de los requisitos, como por ejemplo implementación de algunos algoritmos de gestión energética o integración con la gestión de reservas.	La implantación en un hotel requiere hacer cierto grado de adaptación para cumplir algunos de los requisitos, como por ejemplo implementación de algunos algoritmos de gestión energética o integración con la gestión de reservas.	La adaptación necesaria es total (desarrollo), lo cual encarece la instalación. En contrapartida, el sistema está totalmente optimizado para las funciones que debe realizar.
La distribución OpenDomo aunque está basada en el kernel Linux, es una distribución reducida, con lo que en ella no pueden	La distribución OpenDomo aunque está basada en el kernel Linux, es una distribución reducida, con lo que en ella no pueden	Utilizando distribuciones Linux como Debian, Ubuntu, Fedora, etc permite aplicar muchas aplicaciones libres y en particular tecnologías web: por ejemplo,

<p>instalarse y correr todos los paquetes de software y aplicaciones libres que, durante la fase de diseño, se estime que puedan ser útiles en el caso de la aplicación del hotel.</p>	<p>instalarse y correr todos los paquetes de software y aplicaciones libres que, durante la fase de diseño, se estime que puedan ser útiles en el caso de la aplicación del hotel.</p>	<p>servidor web Apache [19] o Tomcat, alta disponibilidad con Heartbeat [16], etc, que puedan ser útiles para el diseño.</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------

Se ha revisado la lista de requisitos para cada una de las opciones, comprobándose que pueden ser cumplidos por las propuestas B y C, observándose no obstante que la OPCION A, además de requerir un coste adicional para la extensión de periféricos, representa una desventaja respecto a las otras 2 opciones, ya que el ordenador de control solo puede ser accedido desde un único puesto a través de los KVM, considerándose ello un incumplimiento del requisito RS-5. Por tanto esta opción queda descartada.

Para las otras 2 opciones, la diferencia básica es la idoneidad de la solución desde el punto de vista técnico: si bien la utilización de la distribución OpenDomo reporta la ventaja inicial del software de control e interfaces gráficas de usuario que ya incluye, éste no está diseñado para el control de una instalación de la envergadura de un hotel, requiriendo algunas adaptaciones y su utilización impondría una serie de limitaciones, según lo descrito en la tabla anterior, tanto a nivel de recursos del sistema utilizados como de integración y reutilización de aplicaciones libres que puedan ser de utilidad en el desarrollo de la aplicación. Debido a ello, y teniendo en cuenta que el coste de desarrollo tampoco se evita, se considera que la opción más adecuada para la implementación del puesto de control es la OPCION C: Servidores de control desarrollados a medida, con funcionalidades accesibles vía web por la Intranet.

En la etapa de diseño se definirán los paquetes de software libre y funcionalidades que deben incorporar dichos servidores.

### 3.6.1 Revisión final de cumplimiento de requisitos para la opción elegida

Recordemos que con la opción seleccionada:

- Instalaremos un ODControl en cada habitación.
- Se instalará un switch en cada planta, excepto en la planta baja donde irán 2, formando todos ellos un bucle cerrado para tener rutas alternativas.
- El puesto de control dispondrá de redundancia mediante dos servidores, con desarrollos a medida (utilizando software libre) y accesibles desde clientes de la Intranet del hotel, entre ellos al menos uno ubicado en recepción.

Una vez elegida la configuración final del sistema, se vuelve a revisar el cumplimiento de requisitos de forma más específica para la misma. El análisis realizado se encuentra en el ANEXO 3, concluyéndose que la opción elegida es capaz de cumplir cada uno de los requisitos.

## 3.7 Estudio de viabilidad desde el punto de vista de ahorro energético y económico.

Un aspecto para determinar si el sistema es viable es predecir si la inversión realizada se podrá recuperar en un plazo razonable con el ahorro energético que producirá. Para ello, a partir de datos basados en valores actuales del precio de la energía, veremos si es posible amortizar la inversión e incluso obtener beneficios, en un plazo que deberá ser inferior al ciclo de vida de la instalación.

Para este estudio nos basaremos en los datos publicados por la Agencia Valenciana de la Energía (<http://www.gva.es/aven>) de la Generalitat Valenciana, en su “Guía de Ahorro y Eficiencia Energética en Establecimientos Hoteleros de la Comunidad Valenciana” y que puede obtenerse en [http://www.magrama.gob.es/es/cambio-climatico/temas/GuiaEficienciaHoteles\\_CV\\_tcm7-293295.pdf](http://www.magrama.gob.es/es/cambio-climatico/temas/GuiaEficienciaHoteles_CV_tcm7-293295.pdf)

### 3.7.1 Datos de partida del estudio

Según los datos de esta agencia, la distribución típica de gasto en energía para hoteles de la Comunidad Valenciana es:

- Calefacción y aire acondicionado: 45%
- Iluminación: 15%
- Agua caliente sanitaria: 23%

Como vemos, la mayor parte del gasto energético se produce en la climatización, por lo que al ser la Comunidad Valenciana una zona de clima templado, el análisis será aún más favorable para aquellos hoteles ubicados en zonas de clima más extremo.

Asimismo el estudio clasifica los hoteles por su grado de eficiencia energética (pag35 del documento), con la siguiente clasificación de la eficiencia: Excelente, Buena, Pobre o Deficiente. En la tabla “Parámetros de eficiencia en hoteles” vemos que para “hoteles de 50 a 150 habitaciones, sin lavandería, con calefacción y aire acondicionado en algunas dependencias”, con clasificación de la eficiencia “Pobre”, el consumo total de energía puede oscilar entre 320 y 380 (kWh/m<sup>2</sup>-año). Para el cálculo se considerará un hotel cuya eficiencia es un término medio de los clasificados con eficiencia pobre: **350 (kWh/m<sup>2</sup>-año)**, pero se obtendría un resultado aún más favorable al estudio (un mayor ahorro) para aquellos hoteles con clasificación de eficiencia Deficiente.

Otros datos de interés que aporta el documento son los de la eficiencia debida a los sistemas de control. Así, indica que con sencillas medidas de control se puede conseguir un ahorro del 10% de consumo eléctrico en iluminación y del 20 al 30% de la energía utilizada en climatización.

En el apartado de agua caliente sanitaria los sistemas de control propuestos no tienen tanto impacto en el ahorro respecto a otras medidas de ahorro, por lo que lo omitiremos en el cálculo.

En los subapartados siguientes calcularemos el ahorro energético obtenido con la instalación (en euros), el coste de realización de la misma y finalmente haremos un “ANALISIS COSTE/BENEFICIO” considerando el IPC y el valor actualizado de los beneficios futuros que reporte el ahorro energético.

### 3.7.2 Cálculo del ahorro energético

Dependerá de la superficie climatizada de cada hotel en concreto, pero podemos hacer una aproximación con unos sencillos cálculos, aplicados a una superficie estimada para un hotel de 100 habitaciones. El modelo se basará en los siguientes datos:

- N° de Plantas : 5 ( 4 de habitaciones + planta baja (comedores, bar, etc))
- N° de habitaciones: 100 (ubicadas en plantas 1ª a 4ª. 25 habitaciones por cada planta)
- Superficie de las habitaciones: 20 m<sup>2</sup>
- Superficie de pasillos en cada planta: 100 m<sup>2</sup>
- Superficie de vestíbulos en plantas 1ª a 4ª: 20 m<sup>2</sup> (por planta)

Con estos datos, la superficie por cada planta es de unos 620 m<sup>2</sup> , y la superficie total del hotel son **3100 m<sup>2</sup>**:

En la siguiente hoja de cálculo, a partir de los datos anteriores y los de la Agencia Valenciana de la Energía, obtendremos el ahorro total en energía de iluminación y climatización para el hotel, a lo largo de un año, que resulta ser de 20.751 euros.

ESTIMACION DEL AHORRO ENERGETICO POR LA IMPLANTACION DEL SISTEMA DE CONTROL		
SUPERFICIE TOTAL INTERIOR DEL HOTEL (m2)	3100	
CONSUMO ENERGETICO DE UN HOTEL TAMAÑO MEDIO, en kwh /(m2*año) (*) :	350	
CONSUMO ENERGETICO DEL HOTEL EN 1 AÑO (kwh /año):	1085000	
PRECIO DEL kwh (euros/kwh)	0,15	
COSTE ECONOMICO EN EUROS DE LA ENERGIA CONSUMIDA	162750	euros / año
De los cuales corresponde a iluminación un 15% (*):	24413	euros / año
Y a climatización un 45% (*):	73238	euros / año
AHORRO EN EUROS MEDIANTE LOS SISTEMAS DE CONTROL:		
10% del consumo eléctrico en iluminación (*):	2441	euros / año
25 % de la energía utilizada en climatización (*):	18309	euros / año
<b>TOTAL AHORRO EN ENERGIA (Iluminación + climatización)</b>	<b>20751</b>	<b>euros / año</b>
(*) valores según documento de la Agencia Valenciana de la Energía		

### 3.7.3 Presupuesto de realización de la instalación

Por otra parte, en una primera aproximación al presupuesto de realización de la instalación, para un hotel de 100 habitaciones y 5 plantas (según los esquemas realizados), el coste total asciende a unos 88.000 euros, según se muestra en el presupuesto siguiente:

**Presupuesto para un hotel de 100 habitaciones (5 plantas):**

ODControles instalados:		<b>130</b>		
Habitaciones:		<b>100</b>		
DESCRIPCION	UNIDADES	PRECIO	TOTAL	OBSERVACIONES
<b>CONTROLADORES, SENSORES Y ACTUADORES</b>				
Controlador ODControl	130	200	26000	
motores de persianas y sus accesorios	100	150	15000	1 por cada habitación
sensores de presencia	50	10	500	1 cada 2 habitaciones aprox
Termostatos	100	12	1200	1 por cada habitación
Relé 10 A montaje en carril de 35 mm (EN 60715)	300	25	7500	3 por habitación
<b>ELEMENTOS DE RED</b>				
Switches	5	350	1750	Ej: Mod. D-Link DGS-1210-52 52-Port 10/100/1000Mbps
Ordenadores	3	500	1500	(incluido 1 cliente)
cables UTP cat 5 (cableado horizontal)	900	0,15	135	(5 m por pared frontal de habitación + 3 m interior ) * 25 habitac /planta * 4 plantas + planta baja
cables UTP cat 5 (cableado vertical)	210	0,15	31,5	aprox. 15 m por cada cable "trunk" entre plantas
conectores RJ-45	298	0,3	89,4	min: 2 conectores ODControl ↔ switch + 2 conectores PC ↔ switch + 2 conectores switch ↔ switch cableado vertical (32 unid)
Bandeja de cables blanca dim. 100x100 marca Qu	700	11,24	7868	125m por 4 plantas de 25 habitaciones + planta baja + 100 m cableado vertical
Canaleta blanca de cables 30x25 - (m)	390	2,54	990,6	3 m aprox. por derivación a cada ODControl
ARMARIO MURAL 19" 4U 520X450X240MM	5	76,13	380,65	1 armario por cada switch
PATCH PANEL 19" CAT.6 24 PUERTOS UTP	5	36,72	183,6	1 armario por cada armario de switch
Cable red latiguillo RJ45 CAT.5E UTP 25 cm	149	0,5	74,5	1 por cada elemento conectado al switch
<b>INSTALACION ELECTRICA</b>				
SAI	1	2000	2000	
Cable eléctrico 230 v para SAI (metros)	200	0,16	32	alimentacion switches y ordenadores desde SAI
Tiras de regleta de empalme 12 bornas	3	0,6	1,8	alimentacion switches y ordenadores desde SAI
Caja de empalmes eléctrica 80x80 estanca	10	1,09	10,9	alimentacion switches y ordenadores desde SAI
Magnetotérmicos para armarios del switch	5	5	25	alimentacion switches desde SAI
<b>MANO DE OBRA DE INSTALACIONES Y DESARROLLO DE SOFTWARE</b>				
Instalador electricista -horas	80	25	2000	2 personas / 1 semana / 40 horas por semana
Instalador LAN -horas	320	25	8000	2 personas / 4 semanas / 40 horas por semana
Desarrollo/configuración de software	1	12423	12423	segun modelo COCOMO básico: 2 personas en 2,3 meses
<b>COSTE TOTAL DE LA INSTALACION:</b>			<b>87696</b>	

Observaciones:

- Para el cálculo del Desarrollo de software se ha utilizado el modelo COCOMO, según cálculos reflejados en el ANEXO 4

### 3.7.4 Cálculo del COSTE / BENEFICIO y recuperación de la inversión

Con los costes de la inversión y el ahorro calculado, obtenemos el tiempo de recuperación de la inversión (entre el 4º y 5º año) y el ahorro económico total (116662 euros), para el ciclo de vida de la instalación, que estimamos en 10 años. Hay que tener en cuenta además que el análisis ha sido conservador, ya que no hemos considerado los casos más desfavorables (hoteles de clasificación Ineficiente, todas las medidas de ahorro,..):

ANALISIS COSTE / BENEFICIO					
DATOS INICIALES					
	<b>Coste del Proyecto (Co) =</b>	88000	(inversión inicial)	<b>AHORRO ENERGIA 1º AÑO =</b>	20571
	r=	2	(tipo de interés "r" del dinero en %)		
	IPC =	3	(en %)		
AÑO	COSTE (1)	BENEFICIO (2)	BENEFICIO NETO ACTUALIZADO (3)	SUMA BENEFICIOS ACTUALIZADOS ACUMULADOS	
0	<b>88000</b>				
1	600	20571	19579		
2	618	21188	19771	39351	
3	637	21824	19965	59316	
4	656	22478	20161	79477	
5	675	23153	20359	99836	← RETORNO DE LA INVERSION Y BENEFICIOS
6	696	23847	20558	120394	
7	716	24563	20760	141153	
8	738	25300	20963	162117	
9	760	26059	21169	183286	
10	783	26840	21376	204662	
		<b>AHORRO EN 10 AÑOS (ACTUALIZADO):</b>		<b>116662</b>	<b>EUROS</b>
	<b>Observaciones:</b>				
	(1)	<i>Inversión inicial + costes de mantenimiento y formación en años sucesivos (incrementados con el IPC)</i>			
	(2)	<i>Beneficios debidos al ahorro energético (se incrementan según aumento del coste de la energía)</i>			
		<i>Supongamos que aumentan según el IPC</i>			
	(3)	<i>Valor del capital (beneficios) si se actualizara a día de hoy, para compararlo con la inversión inicial</i>			

### 3.8 Conclusiones del Estudio de Viabilidad

En este estudio se ha comprobado que:

- Todos los requisitos de prioridad Alta o Muy Alta pueden ser cumplidos con un diseño basado en los productos OpenDomo y en particular con su controlador ODControl.
- Se han identificado los riesgos que puede presentar un sistema como el propuesto y se han propuesto las mitigaciones necesarias.
- Se ha comprobado que uno de los factores que en un principio presentaban más dudas en cuanto a la viabilidad del sistema dado el elevado número de controladores a instalar, el ancho de banda necesario, es muy inferior al que soporta una red LAN convencional de hoy en día, por lo que no supone ningún problema.
- Se han evaluado varias opciones técnicas, ajustándose a los requisitos, seleccionándose una de ellas.
- La opción elegida permite cumplir todos los requisitos del cliente y del sistema.
- Para aquellos hoteles clasificados como de eficiencia pobre o deficiente, se consigue un ahorro energético, y como consecuencia de ello un ahorro económico, que permite recuperar la inversión inicial en un plazo razonable de unos 5 años (inferior al ciclo de vida del sistema), obteniéndose un sustancial ahorro económico a lo largo del ciclo de vida de la instalación.

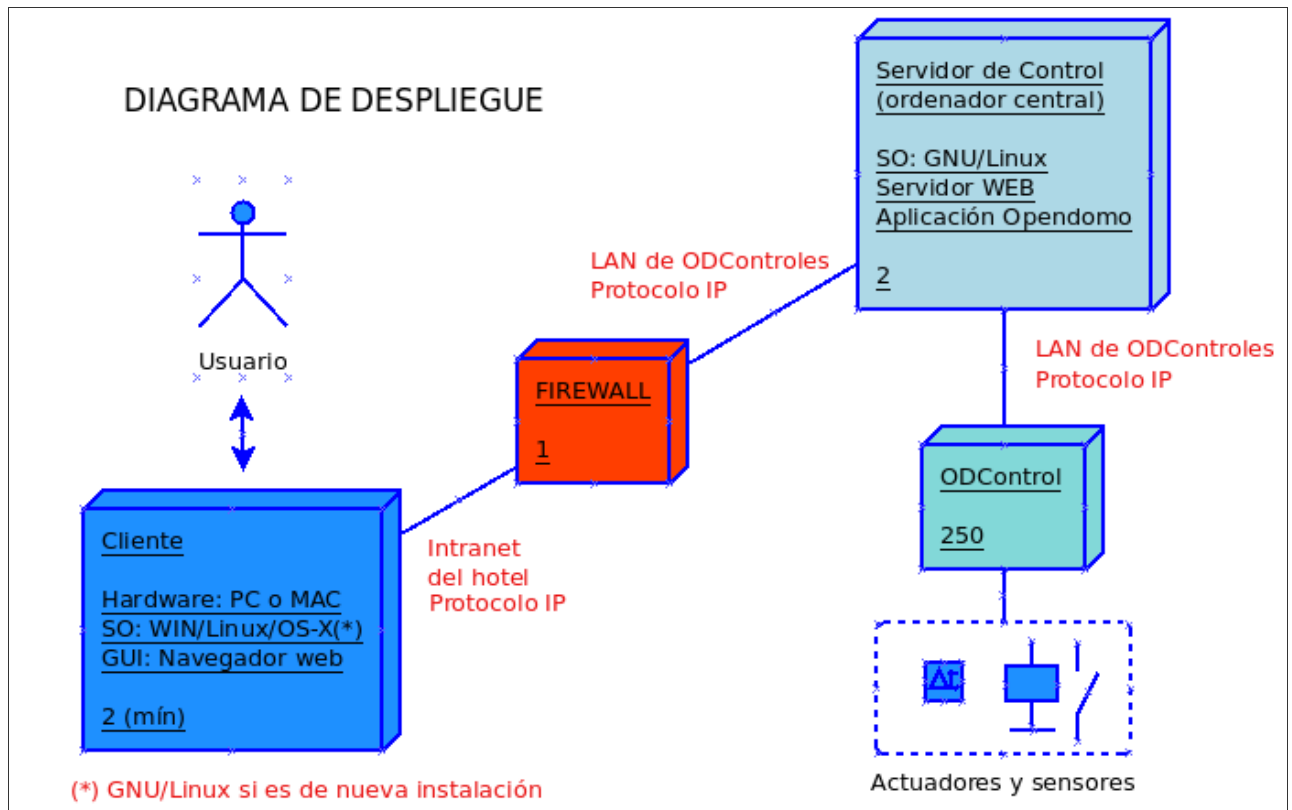
Por tanto se considera que el proyecto es VIABLE.

## 4 Etapa de Análisis

En la Etapa de Análisis se va a especificar con más detalle la solución propuesta en el Estudio de Viabilidad.

### 4.1 Definición del Sistema

El sistema a implementar tiene por misión gestionar el consumo energético y recursos del hotel relacionados, controlando y actuando sobre otros sistemas como son la climatización, persianas, iluminación y la red de tuberías de agua sanitaria, a fin de optimizar los consumos. También tiene por misión facilitar al personal del hotel su interacción con el sistema de control y avisar de las anomalías que se puedan producir. El sistema está formado por varios subsistemas interconectados por una red LAN. El diagrama de despliegue del sistema propuesto es el siguiente:



Las funciones y usuarios de los subsistemas principales se resumen en la siguiente tabla:



Funciones y usuarios de los subsistemas			
SUBSISTEMA →	Ordenador Cliente (típicamente en recepción del hotel)	Servidor de Control (*)	Controlador ODControl
<b>FUNCION</b>	<p><b>Permitir al personal de recepción:</b></p> <ul style="list-style-type: none"> <li>* Visualizar las alarmas técnicas y del sistema</li> <li>* Anular el modo automático cuando un cliente lo solicite</li> <li>* Ver el estado de las habitaciones</li> <li>* Enviar secuencias de órdenes</li> </ul> <p><b>Permitir al administrador:</b></p> <ul style="list-style-type: none"> <li>* Fijar las consignas de temperatura</li> <li>* Crear escenarios y secuencias de órdenes</li> <li>* Gestionar usuarios</li> </ul>	<ul style="list-style-type: none"> <li>* Comunicarse con el sistema de reservas para identificar las habitaciones ocupadas</li> <li>* Atender las peticiones del "ordenador cliente"</li> <li>* Informar a cada controlador cuándo una habitación pasa a estado de "reservada"</li> <li>* Solicitar periódicamente a los ODControl sus estados</li> <li>* Enviar a cada ODControl las nuevas consignas de temperatura</li> <li>* Enviar a cada ODControl los nuevos escenarios</li> </ul>	<ul style="list-style-type: none"> <li>* Actuar autónomamente sobre climatización, luces y persianas de la dependencia que controla para ahorrar recursos, en función del estado de sus entradas y salidas analógicas y digitales y las consignas que reciba.</li> <li>* Enviar al servidor de control sus estados</li> </ul>
<b>USUARIO HABITUAL</b>	Personal de recepción	no requiere (autónomo)	no requiere (autónomo)
<b>USUARIO RESPONSABLE</b>	Administrador del sistema	Administrador del sistema	Administrador del sistema

(\*) aunque realizará otras funciones más allá del concepto de "servidor", lo denominaremos así para identificar este equipo sin posible confusión.

#### 4.1.1 Límites del sistema

Este apartado es importante, por ejemplo, para definir el ámbito de actuación del personal de mantenimiento, según su perfil, contratos de mantenimiento, etc.

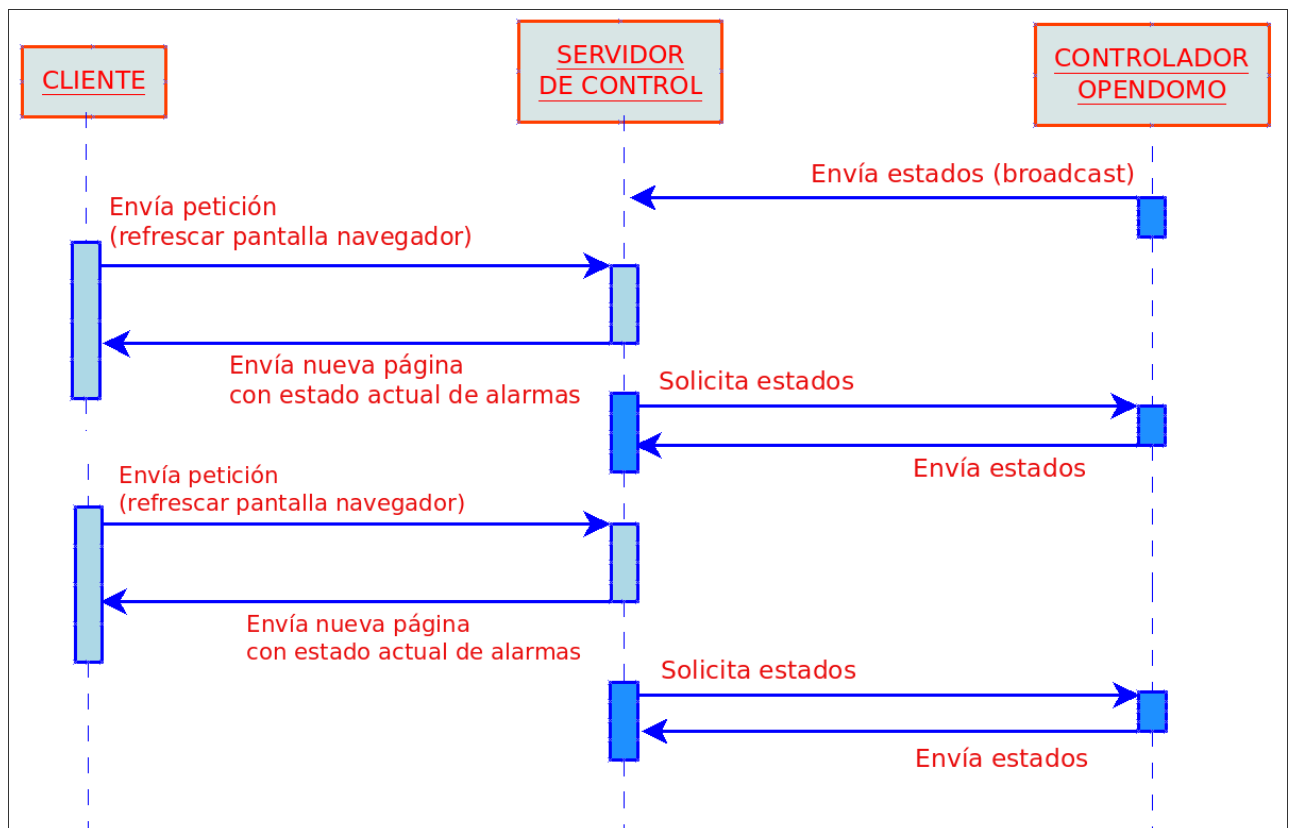
El sistema de control propiamente dicho está constituido por:

- Los clientes (incluyendo el nuevo hardware, o solo el software si están físicamente instalados en hardware existente (PC's) de otra red LAN (por ejemplo la Intranet).
- El firewall que protege la LAN de ODControles.
- El servidor del puesto de control.
- La red LAN de ODControles: switches, cableados, armarios, etc.
- Los ODControles y todos sus sensores.
- En cuanto a los actuadores, sólo se consideran incluidos los elementos directamente conectados al ODControl, pero no los elementos finales. Por ejemplo, en el caso de una electroválvula, es parte del sistema el relé accionado directamente por el ODControl, pero no el actuador de la propia electroválvula (que funciona dentro de la instalación de Baja Tensión) ni la válvula (del sistema de climatización).

La infraestructura de la LAN de ODControles, o una parte de ella, puede ser compartida para aprovechamiento de la infraestructura por otros sistemas (Wifi, videovigilancia IP, etc), pero éstos tampoco se consideran parte del sistema de control.

#### 4.1.2 Comunicación entre los subsistemas

Los 3 subsistemas se comunican entre sí a través de la red LAN. Todas las comunicaciones se establecen a través del servidor de control, no habiendo comunicación directa entre los PC's clientes y los controladores. El siguiente diagrama de interacción resume el caso de comunicación típico, cuando ningún usuario realiza acción alguna:



El diagrama que ilustra la comunicación variará dependiendo de los diferentes casos de uso que se describen más adelante. Los controladores funcionarán en “modo silencioso” (una de las formas de funcionamiento del ODControl), atendiendo asimismo las peticiones de estados que periódicamente les envíe el servidor de control.

Además, el sistema de reservas se comunica con el servidor de control, para informarle del estado de ocupación de las habitaciones.

### 4.1.3 Entorno tecnológico

En el diseño se tendrá en cuenta que:

- Se utilizará software libre:
  - Sistema operativo: GNU/Linux (alguna de sus distribuciones)
  - Gestor de base de datos, de ser necesario: MySQL [17] o PostgreSQL
  - Servidor web Apache HTTP Server.
  - (Se considerará el uso de infraestructura basada en LAMP [25] )
- Utilización de estándares abiertos de uso extendido y en particular comunicaciones basadas en TCP/IP o UDP/IP
- Lenguajes de programación: PHP o Python (para web) y scripts del sistema.
- El hardware de red será el de uso común (switches, hubs, etc), no instalándose otros dispositivos de adquisición de datos o control que no sean los propios ODControls, a fin de conseguir una instalación homogénea.
- Las GUI serán basadas en navegador web (por ejemplo Firefox).

## 4.2 Establecimiento de Requisitos exactos del Proyecto

### 4.2.1 Requisitos adicionales en fase de Análisis

Todos los requisitos considerados en el Estudio de Viabilidad son aplicables, y en esta etapa se amplían con los siguientes:

<b>Identificador</b>	RA-1	<b>Tipo</b>	Funcional	<b>Prioridad</b>	Alta
<b>Descripción</b>	Las funcionalidades de control del sistema, para habitaciones y zonas comunes, serán las resumidas en las TABLAS 1 y 2 (ver página siguiente)				

<b>Identificador</b>	RA-2	<b>Tipo</b>	Funcional	<b>Prioridad</b>	Alta
<b>Descripción</b>	<p>El sistema permitirá la programación de diferentes “escenas” (*) que se ejecutarán automáticamente según hora del día y fecha, es decir, según cambian los diferentes escenarios a controlar. La ejecución final de las escenas además podrá ser condicionada según sea la temperatura exterior, el nivel de insolación real en el exterior y en función de si la habitación se encuentra ocupada o libre.</p> <p>(*) Tal como se define en la documentación web de OpenDomo, una “escena” es una instantánea de la situación en que se encuentran un grupo de elementos de la instalación. Por ejemplo, se puede definir una <i>escena</i> en que todas las persianas de habitaciones desocupadas orientadas entre el este y el sur se bajen a partir de las 11h, durante los meses de julio y agosto. En el ejemplo:  <b>Escena</b> → bajadas todas las persianas de habitaciones desocupadas orientadas entre este y sur  <b>Escenario</b> → meses calurosos (julio y agosto)</p>				

**TABLA 1: FUNCIONALIDAD de supervisión y control para cada habitación**

ESTADO DE LA HABITACION	TARJETA LLAVE ENTREGADA AL CLIENTE	CALEFACCION y AIRE ACONDICIONADO	ILUMINACION	PERSIANAS MOTORIZADAS	APERTURA DE VENTANAS	DETECCION DE FUGAS DE AGUA (sensor de inundación)	DETECCION DE CAUDAL DE AGUA (sensor de caudal)
HABITACION RESERVADA	Consigna "habitación reservada" a OControl +  TARJETA LLAVE INSERTADA	controlar temperatura según termostato a gusto del cliente	Permitir encendido de lámparas a gusto del cliente	Permitir subir / bajar a gusto del cliente	Apagar climatización (incluso sin temperatura de mantenimiento)	Enviar una alarma de "fuga de agua en habitación" al Puesto de Control.	No hacer nada
	Consigna "habitación reservada" a OControl +  TARJETA LLAVE NO INSERTADA	bajar temperatura a mínimo de mantenimiento (configurable, por ej. 19º)	Apagar todo	ODControl la sube o baja según temperatura exterior y nivel de insolación en la fachada (aplicación de escenarios)	Apagar climatización (incluso sin temperatura de mantenimiento) y bajar persianas motorizadas	Enviar una alarma de "fuga de agua en habitación" al Puesto de Control.	Enviar una alarma de "consumo de agua en habitación desocupada" al Puesto de Control
HABITACION SIN RESERVA	Consigna "habitación No reservada" a OControl	Apagado total	Apagar todo	ODControl la sube o baja según temperatura exterior y nivel de insolación en la fachada (aplicación de escenarios)	<ul style="list-style-type: none"> <li>Apagar climatización y bajar persianas motorizadas.</li> <li>Enviar una alarma de "ventana abierta en habitación no reservada" al Puesto de Control.</li> </ul>	Enviar una alarma de "fuga de agua en habitación" al Puesto de Control.	Enviar una alarma de "consumo de agua en habitación desocupada" al Puesto de Control.

**TABLA 2: FUNCIONALIDAD de supervisión y control para las zonas comunes**

	CALEFACCION y AIRE ACONDICIONADO	ILUMINACION	PERSIANAS MOTORIZADAS (donde se requiera)	APERTURA DE VENTANAS (donde se requiera)
FUNCIONALIDAD DEL ODCONTROL EN UNA PLANTA CON CLIENTES	controlar temperatura a temperatura fija de confort preestablecida (p.e. 21º)	Al tener una entrada activa de un sensor de presencia, encender selectivamente el alumbrado de zona del pasillo controlada	ODControl la sube o baja según temperatura exterior y nivel de insolación en la fachada (aplicación de escenarios)	Enviar una alarma de "ventana abierta en zonas comunes" al Puesto de Control.
FUNCIONALIDAD DEL ODCONTROL EN UNA PLANTA DESHABITADA	Mantener temperatura a un valor mínimo de mantenimiento (p.e. 15º)	Apagar todo	ODControl la sube o baja según temperatura exterior y nivel de insolación en la fachada (aplicación de escenarios)	Enviar una alarma de "ventana abierta en zonas comunes" al Puesto de Control.

### 4.2.2 Especificación de Casos de Uso

Los actores identificados que interactuarán con el sistema informático de control son:

- el subsistema de reservas (*El subsistema de reservas no forma parte del sistema de control. Le debe informar de la ocupación y desocupación de habitaciones*).
- el usuario no autenticado (cualquier usuario).
- el usuario normal autenticado (típicamente el personal de recepción).
- el usuario con perfil de administrador (mantenedor del sistema).

Los clientes del hotel interactúan únicamente mediante la inserción de tarjetas-llave, lo cual es tratado mediante los ODControles como una variable controlada más (una entrada digital), por lo que no se consideran actores que interactúan con una interfaz compleja del sistema informático.

Los casos de uso de alto nivel que al menos deberá contemplar el sistema son:

CU-0	Iniciar la Interfaz de usuario y visualizar alarmas técnicas y del sistema
Precondición	<b>Cualquier usuario</b> , sin necesidad de autenticarse, lanza o maximiza la aplicación.
Secuencia normal	1-El usuario no autenticado lanza la aplicación desde el ordenador cliente. 2-El sistema mostrará una pantalla con las alarmas activas y las opciones del “usuario normal” (que requerirán autenticación para usarlas) 3-El usuario se autentica para acceder como usuario normal o administrador, según su identificador.
Postcondición	El usuario se ha autenticado y accede a los menús correspondientes a su perfil de usuario.
Excepciones	Paso 3: el usuario puede finalizar la aplicación cerrando el navegador.
Comentarios	Al acceder el administrador, le aparecen sus opciones adicionales.

CU-1	Informar al servidor de control de la reserva de una habitación (habitación ocupada)
Precondición	Ninguna
Secuencia normal	1- <b>El subsistema de reservas</b> informa al servidor de control de la nueva ocupación
Postcondición	El servidor de control ha registrado el estado “ocupado” de la habitación
Excepciones	---
Comentarios	El Recepcionista interactúa con el subsistema de reservas y es éste quien conecta con el servidor de control. El servidor de control comunica con el ODControl de la habitación y le informa de “habitación en estado de ocupada”. El ODControl de la habitación establece los nuevos ajustes de climatización y habilita la iluminación (según se describe en las tablas del requisito RA-1)

CU-2	Informar al servidor de control de la finalización de reserva de una habitación
Precondición	Ninguna
Secuencia normal	1- <b>El subsistema de reservas</b> informa al servidor de control de la desocupación de la habitación
Postcondición	El servidor de control ha registrado el estado “libre” de la habitación
Excepciones	---
Comentarios	El servidor de control comunica con el ODControl de la habitación y le informa de

	“habitación en estado de desocupada”. El ODControl de la habitación establece los nuevos ajustes de climatización y deshabilita la iluminación
CU-3	Establecer una nueva consigna de <i>temperatura inicial de confort para habitaciones (p.e. 21º), para zonas comunes (p.e. 21º), la de mínimo de mantenimiento de habitaciones (p.e.18º) o la de mínimo de mantenimiento en zonas comunes deshabitadas (p.e. 15º)</i>
Precondición	El <b>usuario administrador</b> se ha autenticado como tal en el sistema
Secuencia normal	1-El administrador selecciona una de las opciones disponibles en “configurar temperaturas de climatización” 2-El sistema mostrará una pantalla indicando la temperatura de consigna que se va a modificar y una opción con todos los valores de temperatura posibles 3-El administrador selecciona un valor y acepta 4-el sistema informa mediante una pantalla de la modificación a la nueva consigna 5-El administrador “acepta” 6-El sistema devuelve a la pantalla de inicio
Postcondición	La consigna de temperatura del tipo elegido ha sido modificada en el sistema
Excepciones	---
Comentarios	El sistema no le permitirá seleccionar la consigna actual ni valores fuera de rango admisible. La temperatura inicial de confort podrá ser posteriormente cambiada a voluntad por cada cliente mediante el termostato de la habitación.
CU-4	Reconocer una alarma (ventanas abiertas, fugas de agua, inundación)
Precondición	El <b>usuario normal (repcionista)</b> se ha autenticado en el sistema La interface gráfica (navegador) ha actualizado automáticamente su estado
Secuencia normal	1-El sistema envía una nueva alarma (al refrescarse automáticamente el navegador) 2- El recepcionista reconoce la alarma (click sobre el objeto mostrado) 3- El sistema muestra el mensaje “Reconocida alarma X”.
Postcondición	El sistema deja de mostrar la alarma y registra el reconocimiento de la alarma
Excepciones	---
Comentarios	El ODControl informa al servidor de control de la nueva alarma. El servidor de control la registra y se la muestra al cliente cuando el navegador hace una nueva petición
CU-5	Envío de consignas de control pre-programadas (escenarios)
Precondición	El <b>usuario administrador</b> se ha autenticado como tal en el sistema
Secuencia normal	1-El administrador accederá en el menú a la opción “Activar escenario” 2-El sistema mostrará una pantalla con los distintos escenarios pre-programados 3-El administrador selecciona uno y acepta 4-el sistema devuelve una pantalla informando del éxito de la operación. 5-El administrador “acepta” 6-El sistema devuelve a la pantalla de inicio
Postcondición	El Servidor de Control envía automáticamente a los ODControles, según fecha y hora, las nuevas consignas establecidas para ese escenario.
Excepciones	----
Comentarios	----
CU-6	Crear o modificar escenarios.
Precondición	El <b>usuario administrador</b> se ha autenticado como tal en el sistema
Secuencia normal	1-El administrador accederá en el menú a la opción “Crear o modificar escenario”

	2-El sistema mostrará una pantalla con los distintas opciones y operaciones necesarias para crear escenarios 3-El administrador selecciona las opciones y operaciones y acepta 4-el sistema devuelve una pantalla informando del éxito de la operación. 5-El administrador "acepta" 6-El sistema devuelve a la pantalla de inicio
Postcondición	El Servidor de Control registra y muestra el nuevo escenario cuando se accede al menú "Activar Escenario"
Excepciones	----
Comentarios	Un escenario puede definirse mediante opciones y operaciones como en el siguiente ejemplo: <i>IF [ ( f1 &lt; fecha &lt; f2) AND (hora &gt; h1) AND (orientación=Este) AND (estadoHabitacion=libre) AND (nivel insolación &gt; S) AND (temp &gt; temp_ref) ] → (Enviar al ODControl de la habitación X la orden de bajar persiana)</i>

CU-7	Crear o modificar secuencias de órdenes
Precondición	El <b>usuario administrador</b> se ha autenticado como tal en el sistema
Secuencia normal	1-El administrador accederá en el menú a la opción "Crear o modificar secuencias" 2-El sistema mostrará una pantalla con los distintas opciones y operaciones necesarias para crear secuencias 3-El administrador selecciona las opciones y acepta 4-el sistema devuelve una pantalla informando del éxito de la operación. 5-El administrador "acepta" 6-El sistema devuelve a la pantalla de inicio
Postcondición	El Servidor de Control registra y muestra la nueva secuencia cuando se accede al menú "Lanzar secuencia"
Excepciones	----
Comentarios	---

CU-8	Lanzar una secuencia de órdenes
Precondición	El <b>usuario normal (repcionista)</b> se ha autenticado en el sistema
Secuencia normal	1-El <b>usuario normal</b> accederá en el menú a la opción "Lanzar secuencia" 2-El sistema mostrará una pantalla con los distintas secuencias posibles. 3-El usuario selecciona una y acepta. 4-el sistema devuelve una pantalla informando del éxito de la operación. 5-El usuario "acepta" 6-El sistema devuelve a la pantalla de inicio
Postcondición	Los ODControles ejecutan las órdenes recibidas
Excepciones	---
Comentarios	---

CU-9	Conectar/desconectar el modo AUTO para una habitación.
Precondición	El <b>usuario normal (repcionista)</b> se ha autenticado en el sistema
Secuencia normal	1-El <b>usuario normal</b> accederá en el menú "MODO AUTO/MANUAL" a la opción deseada. 2-El sistema mostrará una pantalla con la lista de habitaciones. 3-El usuario selecciona una y acepta. 4-el sistema devuelve una pantalla informando del éxito de la operación. 5-El usuario "acepta" 6-El sistema devuelve a la pantalla de inicio
Postcondición	El ODControl de la habitación pasa el control al nuevo modo para la iluminación y la climatización.

Excepciones	---
Comentarios	Se permite la desconexión de una habitación, por ejemplo para permitir la regulación manual por el cliente en caso de avería de un componente (un relé, etc)

CU-10	Listar habitaciones que se encuentran en modo MANUAL
Precondición	El <b>usuario normal (repcionista)</b> se ha autenticado en el sistema
Secuencia normal	1-El <b>usuario normal</b> accederá en el menú "MODO AUTO/MANUAL" a la opción "Listar habitaciones en modo manual". 2-El sistema mostrará una pantalla con la lista de habitaciones en modo manual. 3-El usuario "acepta" 4-El sistema devuelve a la pantalla de inicio
Postcondición	---
Excepciones	---
Comentarios	---

CU-11	Listar habitaciones que se encuentran reservadas
Precondición	El <b>usuario normal (repcionista)</b> se ha autenticado en el sistema
Secuencia normal	1-El <b>usuario normal</b> accederá en el menú "ESTADO DE HABITACIONES" a la opción "Visualizar reservadas". 2-El sistema mostrará una pantalla con la lista de habitaciones reservadas. 3-El usuario "acepta" 4-El sistema devuelve a la pantalla de inicio
Postcondición	---
Excepciones	---
Comentarios	---

CU-12	Listar el histórico de alarmas
Precondición	---
Secuencia normal	1- <b>Cualquier usuario</b> , sin necesidad de autenticarse, accede a la opción "Ver Histórico de Alarmas". 2-El sistema mostrará una pantalla con la lista de las últimas alarmas. 3-El usuario "acepta" 4-El sistema devuelve a la pantalla de inicio
Postcondición	---
Excepciones	---
Comentarios	Para cada alarma se incluye el tipo, la fecha/hora en que se reconoció y el usuario.

CU-13	Crear usuarios
Precondición	El <b>usuario administrador</b> se ha autenticado como tal en el sistema
Secuencia normal	1-El administrador accederá en el menú "USUARIOS" a la opción "Crear". 2-El sistema solicitará al administrador crear un identificador de usuario. 3-El administrador introduce la información solicitada y acepta. 4-el sistema crea el nuevo usuario y una contraseña provisional y devuelve una pantalla informando del éxito de la operación. 5-El administrador "acepta" 6-El sistema devuelve a la pantalla de inicio
Postcondición	Se crea un nuevo registro en la base de datos (BD) (con identificador usuario + hash de contraseña )
Excepciones	Si el identificador ya existe, el sistema informa y retorna al paso 2.



Comentarios	El usuario deberá acceder con la nueva contraseña que le remita el administrador y modificarla mediante la opción "Modificar contraseña"
-------------	------------------------------------------------------------------------------------------------------------------------------------------

CU-14	Dar de baja usuarios
Precondición	El <b>usuario administrador</b> se ha autenticado como tal en el sistema
Secuencia normal	1-El administrador accederá en el menú "USUARIOS" a la opción "Dar de baja usuarios". 2-El sistema listará los usuarios y permitirá seleccionar uno o varios. 3-El administrador selecciona los usuarios que desea y acepta. 4-El sistema devuelve a la pantalla de inicio
Postcondición	Se borran de la BD los registros de los usuarios seleccionados
Excepciones	En los pasos 2 y 3 el administrador puede elegir la opción "Cancelar" y continúa en el paso 4. En todo momento al cerrar la ventana se cancela la operación.
Comentarios	---

CU-15	Modificar contraseña
Precondición	El <b>usuario normal o administrador</b> <b>clica</b> el hipervínculo "Modificar contraseña"
Secuencia normal	1-El sistema le devuelve una página que le solicita: identificador de usuario, contraseña actual, contraseña nueva y repetir contraseña nueva. 2-El usuario introduce los datos solicitados y acepta. 3-el sistema devuelve una pantalla informando del éxito de la operación. 4-El usuario "acepta" 5-El sistema devuelve a la pantalla de inicio
Postcondición	Se modifica la contraseña del usuario (se graba hash md5 en la base de datos (BD))
Excepciones	En el paso 1 el usuario puede elegir la opción "Cancelar", que le devuelve a la página de inicio.
Comentarios	---

### 4.3 Definición de las interfaces de usuario

Este apartado hace referencia a las interfaces de usuario para interactuar con el Servidor de Control desde un PC de supervisión y mando.

#### 4.3.1 Identificación de perfiles de usuario de la interfaz:

A efectos de diseño de la interfaz, se identifican 2 perfiles:

1. el usuario normal (principalmente los recepcionistas del hotel).
2. el usuario administrador (mantenedor del sistema).

El primer tipo de usuario puede ser un usuario más o menos habituado a interactuar con aplicaciones de tipo gráfico en su ámbito privado, y en particular con las aplicaciones web.

En el caso del usuario administrador, se trata de un perfil técnico, aunque se ha de tener en cuenta que en algunos casos puede tratarse de personal que realiza el mantenimiento de instalaciones diversas del hotel y entre ellas algunas tareas administrativas del sistema informático, como gestión de usuarios, establecer consignas de temperatura, etc, por lo que no tiene porqué ser un técnico puramente informático ni estar acostumbrado a las aplicaciones en modo consola de comandos (aunque para una administración integral serán necesarias las propias del sistema operativo).

### 4.3.2 Especificación de Principios Generales de la Interfaz

La aplicación de monitorización y control del sistema desde el PC de supervisión y mando, tendrá las siguientes características:

- Para ambos casos de perfiles de usuario, se considera que las interfaces más adecuadas serán las de tipo gráfico.
- Las interfaces de usuario serán de tipo web, debiendo ser compatibles con los navegadores de mayor difusión.
- La aplicación será accesible mediante un icono ubicado en el escritorio de un PC, que abrirá el navegador direccionando la URL del servidor WEB ubicado en el servidor de control. La configuración de este navegador no deberá poder ser modificada por usuarios no administradores del PC cliente.
- La página de inicio del navegador mostrará las alarmas técnicas existentes y las no reconocidas, sin que se requiera autenticación para ello.
- Para poder enviar órdenes y reconocer alarmas, el sistema pedirá al usuario que se autentique.
- La selección de opciones se realizará mediante objetos como menús desplegables, botones de selección, listas, etc, que incluyan todas las opciones disponibles para cada acción y sin que el usuario deba introducir datos manualmente, siempre que sea evitable.
- En cada pantalla existirá una breve instrucción de la acción que debe realizar el usuario y del resultado producido por las opciones disponibles.
- Las opciones seleccionadas que no se realicen con éxito, devolverán una pantalla con una explicación del error producido y la opción de volver a la pantalla anterior, a la pantalla de inicio o a ambas, según el caso.
- Existirá una opción de ayuda más detallada que abrirá una nueva página sin abandonar la anterior.
- La interfaz se refrescará automáticamente para mostrar las alarmas técnicas actualizadas.
- Se generará un sonido de aviso cuando se produzca una nueva alarma.

### 4.3.3 Esquema de la interface de usuario

La interfaz estará estructurada según el siguiente esquema:

LOGO DEL HOTEL	Ver Histórico de Alarmas	Ayuda	LOGO OPENDOMO
<p><b>OPCIONES USUARIO NORMAL</b></p> <p><b>MODO AUTO / MANUAL</b></p> <ul style="list-style-type: none"> <li>Inhabilitar modo automático para una habitación</li> <li>Conectar modo automático para una habitación</li> <li>Listar habitaciones en modo manual.</li> </ul> <p><b>SECUENCIAS DE ÓRDENES</b></p> <ul style="list-style-type: none"> <li>Lanzar secuencia</li> </ul> <p><b>ESTADO DE HABITACIONES</b></p> <ul style="list-style-type: none"> <li>Visualizar reservadas</li> </ul>	<p><b>ZONA DE MENSAJES DE ALARMAS TECNICAS Y DEL SISTEMA</b></p> <p>(alarmas inundación, grifos abiertos, ventanas abiertas, ODControl no comunica, etc)</p>	<p>Identificador de usuario</p> <div style="background-color: #ffff00; height: 20px; width: 100%;"></div> <p>Contraseña</p> <div style="background-color: #ffffff; height: 20px; width: 100%;"></div> <p>Modificar contraseña</p>	
<p><b>OPCIONES ADICIONALES</b></p> <p><b>SOLO USUARIO ADMINISTRADOR</b></p> <p><b>CONFIGURAR TEMPERATURAS DE CLIMATIZACIÓN</b> (establecer consignas globales):</p> <ul style="list-style-type: none"> <li>temperatura confort para habitaciones</li> <li>temperatura confort para zonas comunes</li> <li>temperatura mínima de mantenimiento para habitaciones</li> <li>temperatura mínima de mantenimiento para zonas deshabitadas</li> </ul> <p><b>ESCENARIOS:</b></p> <ul style="list-style-type: none"> <li>Activar escenario</li> <li>Crear o modificar</li> </ul> <p><b>SECUENCIAS DE ÓRDENES</b></p> <ul style="list-style-type: none"> <li>Crear o modificar</li> </ul> <p><b>USUARIOS</b></p> <ul style="list-style-type: none"> <li>Crear</li> <li>Dar de baja</li> </ul>	<p>Opción “Mostrar todas las plantas (alzado)”      Opción “Mostrar dependencias de una planta”</p> <p style="text-align: center;"><b>AREA DE VISUALIZACION DE PLANOS DEL HOTEL</b></p> <p style="text-align: center;">(selección geográfica de ubicaciones para ejecución de comandos)</p>		

## 4.4 Plan de Pruebas

Durante las fases de desarrollo e implantación, se deberán realizar diversas pruebas encuadradas en diversas categorías, definidas brevemente como sigue:

En la fase de desarrollo:

- Pruebas unitarias: las de componentes aislados del sistema.
- Pruebas de integración: las de grupos de componentes.
- Pruebas del sistema: las de integración del sistema al completo.

En la fase de Implantación:

- Pruebas de implantación: las del sistema completo en el entorno de operación real.
- Pruebas de aceptación: comprobar cumplimiento de requisitos para aprobación del cliente.

Estas últimas serán las acordadas con cada cliente para comprobar el cumplimiento de requisitos. En la etapa de diseño se definirán las pruebas necesarias a realizar en cada fase y su horizonte: criterios de aceptación de la prueba, entorno de pruebas, etc. La metodología *Métrica versión 3* (\*) [5], en su actividad “*DSI 10: Especificación técnica del Plan de Pruebas*” proporciona un modelo de conceptos a considerar, tareas y participantes, que debidamente adaptado sirve de referencia para elaborar las pruebas en fase de diseño. También resulta de interés las plantillas y aspectos a considerar en cada uno de los tipos de pruebas, que se definen en las Técnicas de Métrica 3, donde, a título de ejemplo, podemos encontrar un modelo de plantilla para un protocolo de pruebas unitarias (mostrada en el ANEXO 5).

(\*) La Metodología Métrica V3 puede ser utilizada libremente con el único requisito de citar su propiedad intelectual, el Ministerio de Hacienda y Administraciones Públicas de España. En este trabajo se consideran algunos conceptos o actividades que aparecen en ella, adaptados al caso concreto según convenga.

La definición de los diversos protocolos de pruebas, actores que intervienen en cada una de ellas, el orden de ejecución, requisitos previos y los criterios de superación de las pruebas determinarán el avance del proyecto en las fases de desarrollo e implantación.

## 5 Etapa de Diseño

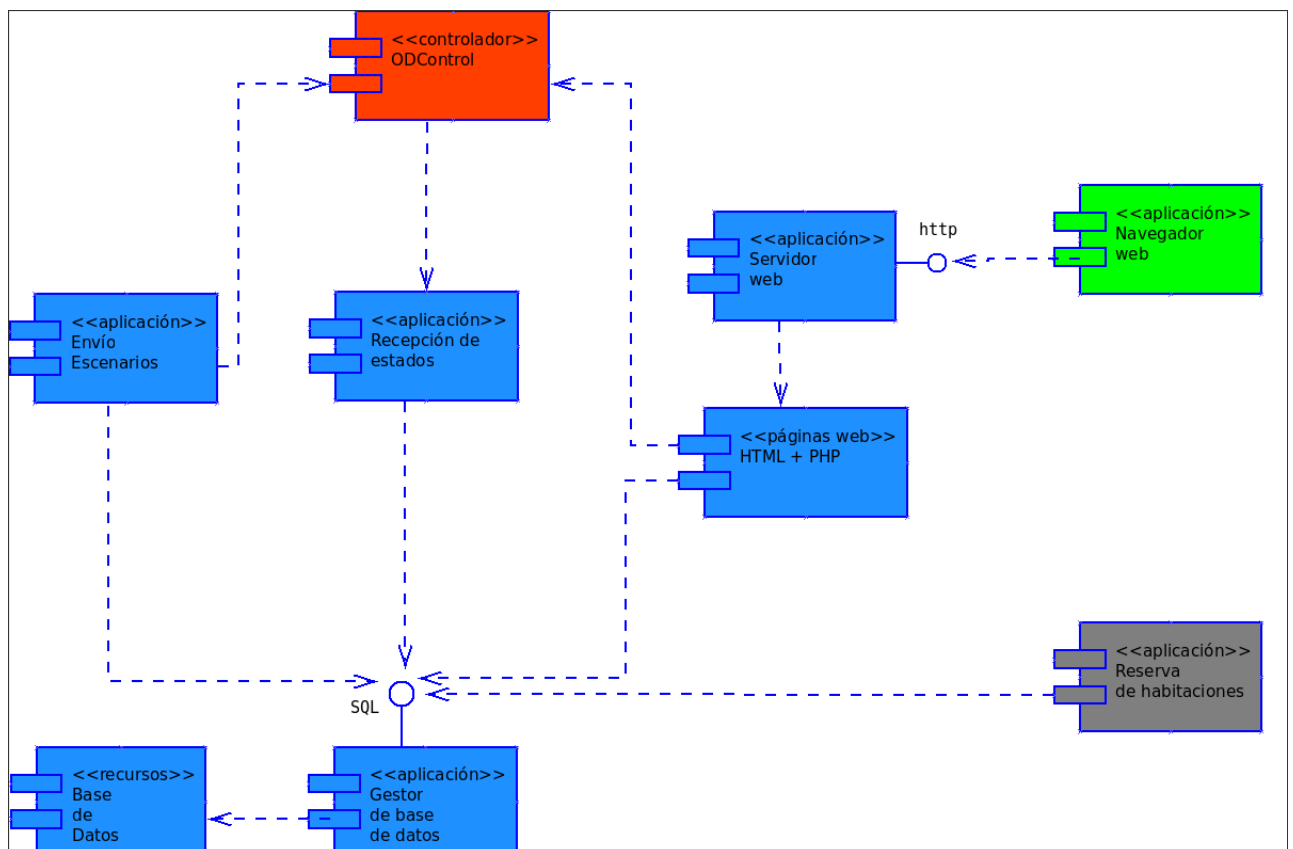
Al no ser objeto del proyecto el desarrollo de software, sino definir la arquitectura y funcionalidad general del sistema, en esta etapa se consideran los siguientes apartados, seleccionados de las actividades “DSI1:Definición de la Arquitectura del Sistema” y “DSI 11: Establecimiento de Requisitos de Implantación”, tomando como referencia la metodología Métrica v3.

### 5.1 Definición de la Arquitectura del Sistema

Tal como se define en Métrica v3, el objeto de esta actividad es definir la arquitectura general del sistema, identificando las particiones físicas (nodos), la descomposición lógica en subsistemas y concretando la infraestructura tecnológica.

#### 5.1.1 Definición de Niveles de Arquitectura

Los componentes del mismo color se ubican en la misma máquina. En color azul los ubicados en el servidor de control:



A continuación se detallan mediante tarjetas CRC (Class Responsibility Collaborator) la función y relaciones de los componentes anteriores que requieren hacer un desarrollo de software a medida:

HTML + PHP (+ javascript)	
FUNCIONES O DATOS DEL COMPONENTE	RELACIONES (depende de..)
Enviar a los ODControles: <ul style="list-style-type: none"> <li>• secuencias de órdenes</li> <li>• conectar/desconectar modo automático para una habitación</li> </ul> Los scripts PHP acceden a la base de datos para: <ul style="list-style-type: none"> <li>- Leer habitaciones en estado “reservadas” y en “modo manual”</li> <li>- Leer consignas de temperatura</li> <li>- Escribir en Base de datos:                             <ul style="list-style-type: none"> <li>• nuevas consignas de temperatura</li> <li>• condiciones de las secuencias y de los escenarios y asignarles un estado (activo/inactivo)</li> <li>• crear o borrar usuarios</li> </ul> </li> <li>-Listar el histórico de alarmas</li> <li>- Crear usuarios y sus contraseñas en la Base de datos, modificar contraseñas y dar de baja usuarios</li> </ul>	Gestor de base de datos  ODControles

Envío de escenarios	
FUNCIONES O DATOS DEL COMPONENTE	RELACIONES (depende de..)
Funcionando como un daemon realiza: <ul style="list-style-type: none"> <li>• Periódicamente lee de la BD las condiciones y estado (activado/desactivado) de los escenarios</li> <li>• Envía órdenes debidas a escenarios en el momento oportuno</li> </ul>	Gestor de base de datos  ODControl

Recepción de estados	
FUNCIONES O DATOS DEL COMPONENTE	RELACIONES (depende de..)
Interroga secuencialmente a cada uno de los ODControles, con el comando “Ist” para obtener el estado de los puertos y “upt ” (uptime) Está a la escucha de las respuestas que envían los ODControl y actualiza la base de datos con estados y alarmas	Gestor de base de datos

Base de datos	
FUNCIONES O DATOS DEL COMPONENTE	RELACIONES (depende de..)
<p><b>Tabla “habitaciones”:</b> nº de habitación (o dependencia), dirección IP asignada a su ODControl, estado (libre/ocupada), Modo(manual/auto), orientación geográfica.</p> <p><b>Tabla “Estados”:</b> temperaturas, estado del alumbrado, puertas, ventanas, etc por dependencia (información recibida del ODControl)</p> <p><b>Tabla “Temperaturas de consigna”:</b> “temp.confort para habitaciones”, “temp.confort para zonas comunes”, “temp.mínima de mantenimiento para habitaciones”, “temp.mínima de mantenimiento para zonas deshabitadas”</p> <p><b>Tabla “Escenarios”:</b> parámetros y operaciones definición del escenario , periodo de aplicación, estado (habilitado/deshabilitado)</p> <p><b>Tabla “secuencias:</b> lista de órdenes</p> <p><b>Tabla “Histórico de alarmas”:</b> fecha/hora, descripción, estado(activa/reconocida), usuario que la reconoce</p> <p><b>Tabla “usuarios”:</b> identificador del usuario, contraseña cifrada (en md5), tipo de usuario (normal o administrador)</p>	-----

### 5.1.2 Especificación de Estándares y Normas de Diseño y Construcción

Dado que la elección concreta dependerá de cada caso de proyecto real, en este apartado se indican las directrices a tener en cuenta en el proyecto y se realiza una propuesta.

Se deberán definir, para la documentación, los formatos, plantillas, idioma, notación y herramientas a utilizar para generar los documentos. Se proponen los siguientes formatos:

Con la herramienta OpenOffice:

1. Documentación general y de diseño: formatos OpenDocument (.odt, .ods, etc)
2. Documentación para distribución: formato PDF
3. Documentación técnica: formato DocBook



Herramienta "Dia" (software libre de GNOME) para diagramas (formato .dia) :

1. Documentación del software, utilizando notación UML
2. Diagramas y esquemas en general (red, eléctricos, etc)



Todos los documentos generados deben contener la siguiente información: título, código o nº de documento, persona o departamento responsable del mismo, control de cambios indicando autor del cambio, fecha y motivo de la modificación. Los documentos relevantes además incluirán las firmas: creado, revisado, aprobado.

### 5.1.3 Identificación de Subsistemas de Diseño

Se identifican los siguientes subsistemas;

1. Subsistemas específicos (funcionalidades propias del sistema de control): consideraremos que son todos los representados en el diagrama de componentes anterior (incluiremos también, aunque no es parte del sistema, el de Gestión de reservas, que puede requerir una adaptación).
2. Subsistemas de soporte (servicios comunes, transparentes para la funcionalidad) :
  - Servidor de tiempo NTP [13], para sincronización de los nodos de red.
  - Seguridad y control de acceso : firewalls, autenticación.
  - Servicios de infraestructura de clúster (comunicación y pertenencia) y gestor de recursos del clúster (CRM).
  - Administración de dispositivos de infraestructura de red: dependiendo del hardware de red adquirido, consistirá en software diverso como interfaces para configuración (usualmente un navegador web).
  - Sincronización de ficheros del clúster: dado que por redundancia vamos a mantener 2 máquinas, y una de ellas off-line, la base de datos debe estar sincronizada.
  - Herramientas de administración del sistema y seguridad: comandos del sistema, antivirus, escaners de vulnerabilidades y auditoría de seguridad.

### 5.1.4 Especificación del Entorno Tecnológico

- **CONTROLADORES ODCONTROL**

Dado que el ODControl es un producto acabado, en este apartado sólo se ha de definir la asignación de entradas y salidas analógicas o digitales a utilizar en cada caso y el tipo de sensor o actuador (lector de tarjeta, relé, etc). Para ello en este proyecto se han debido diseñar también las interfaces necesarias con los sistemas controlados (esquemas eléctricos del ANEXO 6). Ello permite definir un prototipo de controlador con una asignación concreta de entradas y salidas, las cuales pueden ser usadas para cada instalación en función de las necesidades. En los planos del ANEXO 6 se puede ver el tipo de sensor o actuador correspondiente a cada I/O. Las asignaciones de I/O propuestas para cada zona son:

TABLA 2: ASIGNACION DE ENTRADAS Y SALIDAS DE UN ODCONTROL DE HABITACIONES		
	TIPO Y NUMERO	FUNCION
Selección modo Manual/AUTO	1 salida digital	Conmutar modo Manual/AUTO
LECTOR DE TARJETA-LLAVE	1 entrada digital	Detectar tarjeta insertada
ILUMINACION Y ENCHUFES	1 salida digital	Conexión y apagado de luces y enchufes.
	2 salidas analógicas	Opcional para regulación de luminosidad
	1 entrada analógica	Sensor de nivel luminoso (si hay regulación de luminosidad)
CLIMATIZACION (un Fan-Coil)	3 salidas digitales	Regulación de potencia de climatización del Fan-Coil (ver TABLA 4)
	2 entradas analógicas	Sensor de temperatura ambiente Ajuste de temperatura deseada por el cliente
SENSORES DE VENTANAS ABIERTAS	1 entrada digital	Para actuar sobre la climatización
PERSIANAS MOTORIZADAS (una persiana)	2 salidas digitales	órdenes de “subir persiana” y “bajar persiana”
	1 entrada digital	Detener movimiento persiana (parada emerg.)
SENSOR DE INUNDACIÓN	1 entrada digital	Detectar fugas de agua
SENSORES DE CIRCULACIÓN DE AGUA EN TUBERIAS	1 entrada digital	Detectar circulación indebida de agua en habitación desocupada
SENSOR DE PRESENCIA	1 entrada digital	Opcional en aplicaciones de control de iluminación, junto apertura de puerta
SENSOR DE PUERTA ABIERTA	1 entrada digital	Opcional en aplicaciones de control de iluminación, junto sensor de presencia
<b>TOTALES</b>	<b>7 salidas digitales, 7 entradas digitales, 2 salidas analógicas y 3 entradas analógicas</b>	

Las asignaciones de I/O en los ODControl de zonas comunes pueden variar según los dispositivos a controlar en cada zona. Se propone la siguiente distribución tipo (aunque a adaptar a cada caso concreto):



TABLA 3: ASIGNACION DE ENTRADAS Y SALIDAS DE UN ODCONTROL DE ZONAS COMUNES		
	TIPO Y NUMERO	FUNCION
Selección modo Manual/AUTO	1 salida digital	Conmutar modo Manual/AUTO
LECTOR DE TARJETA-LLAVE	No aplica	
ILUMINACION Y ENCHUFES (nota 1)	2 salidas digitales	Conexión y apagado de 2 grupos de lámparas independientes
	2 salidas analógicas (+3 con módulo ACC-AO)	Opcional para regulación de luminosidad
	1 entrada analógica (+3 si hay un ACC-AO)	Opcional para regulación de luminosidad
CLIMATIZACION (un Fan-Coil) [ 4 ]	3 salidas digitales	Regulación de potencia de climatización del Fan-Coil (ver TABLA 4)
	2 entradas analógicas	Sensor de temperatura Ajuste de temperatura
SENSORES DE VENTANAS ABIERTAS	1 entrada digital	Para actuar sobre la climatización
PERSIANAS MOTORIZADAS (una persiana)	2 salidas digitales	órdenes de “subir persiana” y “bajar persiana”
	1 entrada digital	Detener movimiento persiana (parada emerg.)
SENSOR DE INUNDACIÓN	1 entrada digital	En cocina, lavandería, etc
SENSORES DE CIRCULACIÓN DE AGUA EN TUBERIAS	1 entrada digital	En cocina, lavandería, etc
SENSOR DE PRESENCIA	2 entradas digitales	Control de iluminación (nota 2)
SENSOR DE PUERTA ABIERTA	No aplica	
TOTALES	<b>8 salidas digitales, 6 entradas digitales, 2 (+3) salidas analógicas y 3 (+3) entradas analógicas</b>	

**Observaciones:**

(nota 1): Se conecta/desconecta selectivamente el alumbrado por zonas, en concordancia con los detectores de presencia.

(nota 2): una agrupación de sensores, con sus contactos seriados, comparten una entrada digital.

En el desarrollo del software y en concreto de los comandos y programación de puertos del ODControl, se deberá tener en cuenta el tipo de interfaces que controla (relés, dimmers, etc), según los esquemas eléctricos adjuntos en el ANEXO 6, así como las entradas y valores que considerará para actuar sobre un elemento controlado. Requiere mención especial el control de la climatización (basada en ventilosconvectores [4], también llamados “fan-coils”, muy habitual en los hoteles), por ser el más complejo y de mayor impacto en el ahorro energético. De acuerdo a los esquemas eléctricos del ANEXO 6, la programación del ODControl se deberá ajustar a la siguiente funcionalidad:

TABLA 4: LOGICA DE LA FUNCIONALIDAD DEL VENTILOCONVECTOR				
Relé Ro (selector MANUAL/AUTO)	Relé R1	Relé R2	Relé R3 (control de la electroválvula)	FUNCIONALIDAD
excitado ↑	reposito ↓	reposito ↓	excitado ↑	Desconecta totalmente el Fan-Coil, sin abandonarse el modo automático. El ventilador se para y no circula fluido por él intercambiador de frío/calor al cerrar la electroválvula.
excitado ↑	reposito ↓	reposito ↓	reposito ↓	Para el motor en modo automático. El Fan-Coil no transfiere apenas frío o calor a la dependencia, pero sigue preparado para actuar de nuevo cuando la temperatura ambiente salga del rango de consigna de temperatura.
excitado ↑	excitado ↑	reposito ↓	reposito ↓	Motor a velocidad 1 (potencia mínima). Transferencia baja de frío o calor
excitado ↑	reposito ↓	excitado ↑	reposito ↓	Motor a velocidad 2 (potencia media). Transferencia media de frío o calor
excitado ↑	excitado ↑	excitado ↑	reposito ↓	Motor a velocidad 3 (potencia máxima). Transferencia máxima de frío o calor
reposito ↓	indistinto	indistinto	reposito ↓	Funcionamiento Manual alternativo (p.e. fallo en la alimentación del ODCControl)

Cumpliendo con el requisito RC-7, dichos esquemas eléctricos están diseñados para que en caso de fallo del sistema informático (por ejemplo avería del ODCControl), automáticamente exista una alternativa no informática (el modo manual) de funcionamiento de la iluminación, la climatización y las persianas, que permita seguir usando la habitación (ello se consigue mediante el relé R0: Manual/Auto, que al desexcitarse permite la operación manual).

- **DISEÑO DE LA RED LAN**

**Diseño Lógico:**

1) Topología: es la definida en la Etapa de Análisis para la opción elegida, según los diagramas de despliegue del ANEXO 7.

2) Protocolos y estándares principales de referencia para este diseño:

- Redes Ethernet (IEEE 802.3)
- Redes virtuales o VLAN's (IEEE 802.1Q )
- Protocolo Spanning Tree (IEEE 802.1D), para la gestión de rutas alternativas y supresión de bucles.

3) Plan de direccionamiento IP. Dado el elevado número de nodos de red y que la asignación de direcciones de los ODControl se realiza de forma manual durante su montaje físico (no DHCP), para facilitar el mantenimiento es conveniente usar un criterio lógico al asignar las direcciones IP. En este caso se propone que para los ODControles una parte de la dirección IP designe la planta y otra parte a la habitación o dependencia:

Equipos	Dirección IP			Máscara
Servidor Control (mínimo una IP por cada VLAN, implementada con interfaces virtuales)	192.168.	0 1 nn	2-3-4 2 2	255.255.255.0
ODControles Planta 0 (VLAN_0)	192.168.	0	5-254	255.255.255.0
ODControles Planta 1 (VLAN_1)	192.168.	1	3-254	255.255.255.0
ODControles Planta n (VLAN_n)	192.168.	nn	3-254	255.255.255.0
Administración switches (VLAN_ADM)	10.115.	0	2-20	255.255.255.0
WIFI, u otros sistemas (VLAN_x)	10.115.	xx	2-254	255.255.255.0
Router-firewall (una IP , con interfaces virtuales, por cada VLAN que reciba)	192.168. 10.115. 10.115.	0 0 x	1 1 1	255.255.255.0

Observaciones:

- La división en VLAN's se ha hecho únicamente para limitar, en la capa 2 (enlace de datos) los dominios de broadcast. Cada servidor se conecta a un puerto trunk de un switch por donde recibe las tramas de todas las VLAN de ODControles. Además los servidores se deben conectar directamente entre ellos mediante un cable cruzado (en un puerto serie o de red) para la supervisión de disponibilidad mediante Heartbeat.
- Al servidor se le reservan 3 IP's en una de las VLAN: una para cada máquina física y otra, común a ambas, que será la IP del clúster Se les debe enrutar el resto de VLANS.

### Diseño físico

#### 1) Tecnologías

- 100BaseTX, para enlaces en cableado horizontal (permite 100 Mbit/s con un máximo de 100m).
- 1000BaseT (Gigabit Ethernet) , para los enlaces en cableado vertical (1GB/s hasta 100m)

#### 2) Dispositivos de red

- Switch: La elección se realizará considerando el nº de puertos necesarios, según el nº de habitaciones por planta. Para 25 habitaciones por planta, se recomendaron 48 puertos. El modelo elegido es: D-LINK DGS-1210-48 (48 puertos 10/100/1000 Mbps + 4 puertos combo SFP. [9])



Características destacadas:

- 48 puertos compatibles con 100BASE-TX Fast Ethernet y 1000BASE-T Gigabit Ethernet
- VLAN ( 802.1Q ), Quality of Service (802.1p ) y Spanning Tree Protocol (802.1D )
- Altura en el rack: 1U
- Opción de disponer de switches de idénticas características de 8,16 ó 24 puertos.

- Precio: 430 euros.
- Router-firewall: se implementará con un ordenador con GNU/Linux, 2 tarjetas de red e IPTables. Puede ser el mismo modelo que los servidores.

### 3) Cableados

Por razones económicas se evitan los enlaces de fibra. En consonancia con los puertos del modelo de switch elegido serán:

- Cableado horizontal (conexión switch ↔ ODControl): Par trenzado UTP categoría 5
- Cableado vertical (conexión switch ↔ switch o router ): UTP categoría 6. Para conexiones entre plantas extremas (más de 100m) poner un repetidor de 2 puertos (operando solo en la capa física del modelo OSI). Otra alternativa, pero que requeriría tendido de fibra óptica, sería utilizar uno de los 4 puertos combo del switch con un módulo transceptor D-LINK DEM-311GT (alcance 550 metros).

### 4) Armarios y accesorios

Se instalará un armario en cada planta para alojar un switch (o varios si se comparte con servicios como IPTV, etc). Los elementos necesarios son:

- ARMARIO MURAL 19" dimensiones: 4U 520x450mm. Ref.: AR1904U520X450D1. Precio 40,95 € (o de más unidades de altura dependiendo de si van más equipos).
- BANDEJA EXTENSIBLE 19" 1U. Ref.: ARABE1U45- Precio 15,43 €
- Alimentación eléctrica: REGLETA ENRACABLE 19" con 6 tomas SCHUKO CON MAGNETO-TERMICO 4000W 16A. Ref: REG6SCHMAG. Precio 35,08 €. (precios y referencias de <http://armariosrack.es>)

No se considera necesario instalar patch panels, ya que los ODControl se pueden conectar directamente al switch y no se han de hacer cambios posteriores.

#### • ALTA DISPONIBILIDAD. ALIMENTACIÓN ELÉCTRICA.

Los switches, el firewall, el servidor de control y al menos un puesto cliente deben estar alimentados de un SAI, que se ubicará en un cuarto técnico debidamente acondicionado para equipos informáticos. Para los equipos ubicados fuera del cuarto técnico, se deberá tender una línea eléctrica dedicada:

- Desde el cuarto técnico al puesto cliente (si no está alimentado de otro SAI)
- Desde el cuarto técnico a cada uno de los armarios de los switch en cada planta (una línea con derivaciones en cada planta)

Cálculo de la potencia del SAI requerida: aunque la potencia de los switches no es significativa en el cómputo total, se ha considerado un caso desfavorable en que el hotel tiene hasta 8 plantas. La potencia total consumida es de 1,42 KVA (1,28 KVA con 6 switches):

	Nº de equipos instalados	Potencia por unidad (vatios)	Potencia Vatios	Corrección factor de potencia	Potencia KVA
<b>Servidor</b>	2	250	500	0,9	0,56
<b>PC cliente</b>	1	250	250	0,9	0,28
<b>Firewall</b>	1	200	200	0,9	0,22
<b>Switch</b>	10	33	330	0,9	0,37
		<b>TOTAL</b>	<b>1280</b>		<b>1,42</b>

Se elige el modelo de SAI SPS ADVANCE RT de Salicrú (<http://catalogo.salicru.com>).

No es conveniente elegir la potencia del SAI muy ajustada y además para una misma carga la autonomía aumenta a mayor potencia de SAI. El modelo de 1,5 KVA queda muy justo, por lo que se elige el de 2 KVA, que permitirá una autonomía de más de 10 minutos. (PRECIO: 550 euros)

La autonomía puede ser aumentada con SAI's más grandes, pero aumenta mucho el coste sin suponer grandes mejoras en autonomía, por lo que, donde existan previamente (debido también a su coste de instalación), pueden contemplarse otras soluciones complementarias más eficaces en términos de disponibilidad, como son el uso de grupos electrógenos o disponer de 2 acometidas independientes de alimentación de energía eléctrica.

- **SERVIDOR DE CONTROL**

1. Estimación de los requisitos de Hardware:

1º criterio. Mínimos de instalación del software: básicamente el software a instalar se trata de una infraestructura LAMP, instalable mediante los paquetes de Debian [15]. Los requisitos mínimos de instalación de Debian GNU/Linux 7.0 son: un Pentium 4 a 1 GHz ; RAM: 512 Megabytes (si es con entorno gráfico) y disco duro de 5 Gigabytes. El volumen de páginas web a desarrollar, así como los 2 procesos independientes, también será pequeño (máximo unas decenas de MB), por lo que vemos que los mínimos necesarios están muy lejos de los valores de las maquinas actuales. Ref: <http://www.debian.org/releases/stable/i386/ch03s04.html.es>  
<http://www.debian.org/releases/wheezy/amd64/install.pdf.es>

2º criterio. Determinación del perfil de uso: en la elección se han tenido en cuenta que la carga (medida en kB/s y número de peticiones) demandada al servidor web es realmente baja y normalmente será sin peticiones concurrentes (habitualmente una sola página web, de unos 200 KB, servida cada varios segundos). Por otra parte, la carga debida a la comunicación con los ODControles es incluso inferior, ya que por ejemplo si establecemos que todo el ciclo de polling se complete en 10 segundos (admisibile para el tipo de parámetros a monitorizar), tendremos que para 150 ODControles resulta una tasa de bits de 256 Kbits/s (según el modelo de cálculo del estudio de viabilidad), frente a los algo más de 850 Kbits/seg que supone el refresco cada 2 segundos de la página web antes mencionada. El hipotético cuello de botella se podría encontrar en los accesos a la base de datos, donde pueden concurrir, además de la copia periódica de la réplica, simultáneamente 4 transacciones: la de la aplicación de reserva de habitaciones (ocasional), la del módulo "envío de escenarios" (ocasional), del de "recepción de estados" (periodicidad del orden de segundos, almacenado estados en memoria para reducir escrituras en la BD) y una consulta de las páginas web (periodicidad del orden de segundos). Aun concurriendo todos en el intervalo de 1 segundo (tiempo de respuesta bueno para esta aplicación) y suponiendo que al encolarse utilizan el mismo tiempo en realizar la transacción, cada uno de ellos dispondría de 200 mseg para realizarla, mientras que el tiempo medio de acceso de un disco duro moderno es menos de 10 mseg y su tasa de transferencia de más de 10 MB/seg (datos muy conservadores), con lo que en los restantes 190 milisegundos se pueden leer/escribir hasta 1,9 MB, valor muy superior al necesario en las transacciones a realizar en cada momento (que por otra parte se producirán solo en caso de que existan cambios).

Ref: <http://dev.mysql.com/doc/refman/5.1/en/optimize-overview.html>  
[http://es.wikipedia.org/wiki/Tiempo\\_de\\_acceso](http://es.wikipedia.org/wiki/Tiempo_de_acceso)  
[http://es.wikipedia.org/wiki/Tiempo\\_de\\_b%C3%BAsqueda](http://es.wikipedia.org/wiki/Tiempo_de_b%C3%BAsqueda)

Por ello los requisitos de hardware son muy poco exigentes, siendo suficiente un servidor de bajas prestaciones. El modelo de equipo elegido es el DELL PowerEdgeTM R210 II . Sus características son:

- Procesador Intel® Core™ Processor I3-3220, 2C/4T, 3.30GHz, 3M cache
- 4GB Memory (1x4GB), 1600Mhz
- Disco duro: 500GB, SATA, 3.5-in, 7.2K RPM
- Tarjeta de red: Broadcom NetXtreme II 5709 Dual Port 1GbE
- Montaje en rack de 19" (altura 1U)
- Precio : 844,00 € . Con descuento (enero-2014): 487,00 €

2. Software: Los paquetes de Software Libre seleccionados para instalar son:

SOFTWARE	VERSION	FUNCION
<b>Debian</b>	<b>7 (Wheezy)</b>	<b>Sistema operativo</b>
Apache2	2.2.22-13	Servidor HTTP Apache V2
ntp (paquete de utilidades)	1:4.2.6.p5+dfsg-2	Servidor de tiempo NTP
Heartbeat (Linux-HA project)	1:3.0.5-3	Subsistema para alta disponibilidad de Linux
Unison	2.40.65-2	Sincronización de réplicas de la BD
OpenSSH	1:6.0p1-4	Para administración remota del servidor y sincronización remota de las BD con Unison
Nmap ("Network Mapper")	6.00-0.3+deb7u1	Exploración de red y auditoría de seguridad
Nessus	2.2.11-2	Escáner de vulnerabilidades
ClamAV	0.97.8+dfsg-1	Antivirus
IPtables	1.4.14-3.1	Firewall
vlan	1.9-3	paquete para habilitar VLAN's a interface de red
MySQL	5.5	Gestor de base de datos (varios paquetes: servidor, cliente, interfaces gráficas,...)

Todos los paquetes de software necesario se encuentran incluidos en la distribución Debian. Las versiones indicadas son las estables a 4/1/2013, pero en todo momento las últimas se pueden instalar y actualizar automáticamente de los repositorios Debian mediante el Gestor de Paquetes, que además instala sus dependencias (otros paquetes necesarios). La elección de esta distribución se ha basado en su reconocida estabilidad y seguridad, el software disponible y un buen soporte de la comunidad.

Ref:

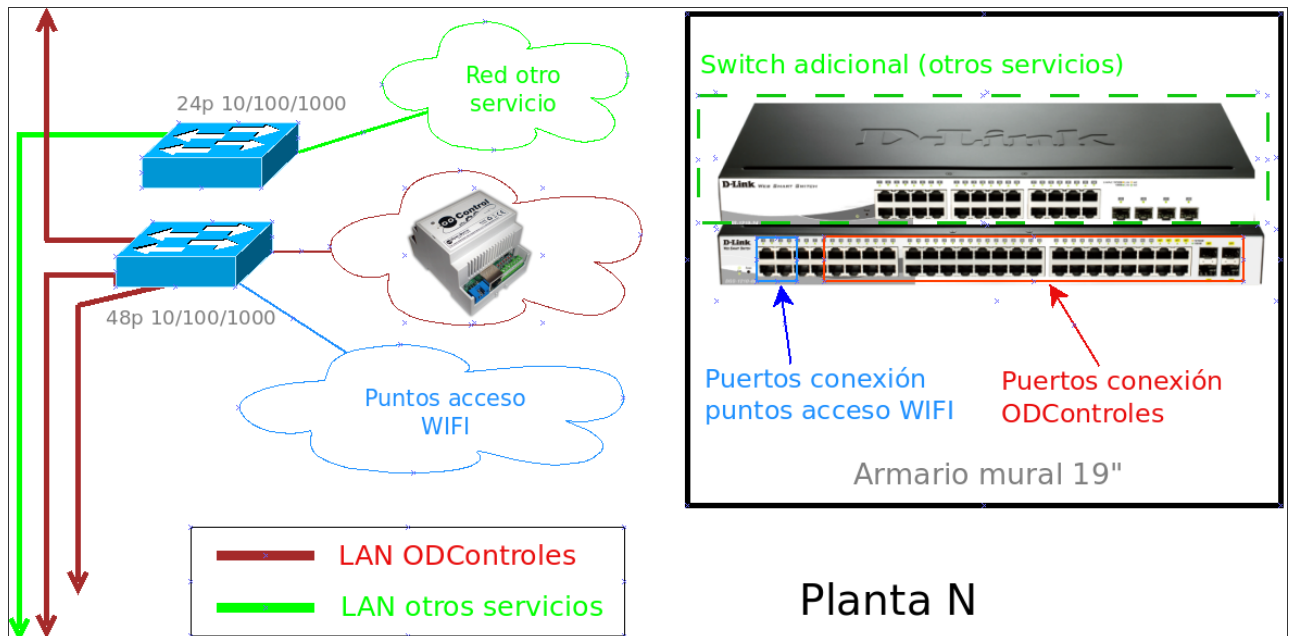
Debian: <http://www.debian.org>

Nessus: <http://www.tenable.com/products/nessus/select-your-operating-system>

### 5.1.5 Integración con otros sistemas

Dado que no se requiere instalar un gran número (1 ó 2, dependiendo del área a cubrir), en cada planta se pueden instalar varios puntos de acceso WIFI conectándolos a puertos libres del switch y asignándoles un VLAN específica. No obstante se deberá garantizar un ancho de banda disponible óptimo para los ODControles (En los menús de configuración del switch D-LINK: *Opciones QoS > Bandwidth Control* , limitar el ancho de banda en el puerto del punto Wifi), así como asignar la máxima prioridad a los puertos de los ODControles (en menú QoS > 802.1p).

Para las otras aplicaciones (como IPTV y telefonía IP) el número de puertos adicionales necesarios sería significativo, además de consumir un gran ancho de banda, por lo que en caso de quererse instalar estos servicios la mejor opción es la instalación de switches adicionales y cableados dedicados aprovechando los racks de 19" instalados en cada planta. En la imagen siguiente se muestra la instalación para una Planta, añadiendo un switch adicional, en este caso de 24 puertos.



### 5.1.6 Seguridad y control de acceso :

**SEGURIDAD FÍSICA:** aspectos que se deben tener en cuenta en la instalación:

- 1) Accesos físicos restringidos: los armarios de los switches deben situarse en dependencias inaccesibles al público y personal no autorizado. Asimismo deben ser inaccesibles los cables de red y de alimentación de energía a lo largo de su trazado.
- 2) Protección contra factores ambientales, inundaciones e incendio: la sala de servidores debe tener controlada la temperatura, la humedad y estar libre de polvo. Debe ubicarse en un lugar donde no exista riesgo de inundación y disponer de medidas contra incendios (alarmas, extintores de CO2, etc según dispongan las normativas).
- 3) La BIOS de los servidores y el router-firewall deben estar correctamente configuradas:
  - las secuencias de arranque deben ser: 1º el disco duro y luego los dispositivos

externos.

- debe estar protegida por contraseña.

**AUTENTICACIÓN:**

- Las autenticaciones en los servidores y el router-firewall se apoyarán en los módulos PAM del sistema Linux. En la configuración se deberá forzar una longitud mínima de contraseña de 8 caracteres.
- La autenticación de usuarios a través de la interface gráfica de la aplicación de control será, tal como se indicó, contra la base de datos MySQL (tabla “usuarios”), donde se almacenarán las contraseñas cifradas con el algoritmo de hash md5 (o el SHA-1).

**FIREWALL:** Dispone de 2 interfaces de red, una conectada a un switch de la LAN de ODControles y otra a la Intranet del hotel (donde se ubican los PC's clientes). Al igual que los servidores, debe soportar VLAN (instalando el paquete vlan y configurando la interface de red conectada al switch). El software mínimo a instalar es:

SOFTWARE	VERSION	FUNCION
Debian	7 (Wheezy)	Sistema operativo
IPtables	1.4.14-3.1	Firewall
vlan	1.9-3	paquete para habilitar VLAN's a interface de red

- **Diseño de reglas del firewall:** Si las distintas subredes son:  
 10.30.0.0/24 -> Intranet del hotel  
 192.168.x.0/24 -> VLAN's de ODControles (x= 0,1,2,...)

Y suponemos, a modo de ejemplo, que además están instalados varios Puntos WIFI conectados a los switches, cuya red es 10.115.1.0/24, las reglas serán:

Nota previa:

- El “\*” indica “cualquier valor”
- 192.168.x.x debe entenderse como cualquiera de las VLAN de ODControles
- Las direcciones acabadas en “0” se refieren a toda la subred (Se omite la máscara de subred).

ROUTER-FIREWALL que protege la LAN de ODControles							
TRAFICO ENTRANTE							
REGLA	ACCION	ORIGEN	PUERTO ORIGEN	DESTINO	PUERTO DESTINO	PROTOC.	DESCRIPCION
1	permite	10.30.0.0	*	192.168.0.2	80	TCP	Permite peticiones http al servidor de control (IP común)
2	permite	10.30.0.0	*	192.168.0.2	443	TCP	Permite peticiones https al servidor de control (IP común)
3	permite	10.30.0.0	*	192.168.0.3	22	TCP	SSH. Conexión a servidor 1 para uso de administrador
4	permite	10.30.0.0	*	192.168.0.4	22	TCP	SSH. Conexión a servidor 2 para uso de administrador
5	permite	10.30.0.0	*	10.115.0.0	80	TCP	Admin. switches interface web



6	rechaza	*	*	*	*	*	RECHAZA las demás conexiones
TRAFICO SALIENTE							
REGLA	ACCION	ORIGEN	PUERTO ORIGEN	DESTINO	PUERTO DESTINO	PROTOC.	DESCRIPCION
7	permite	10.115.1.0	*	*	53	*	Clientes WIFI. Consulta DNS
8	permite	10.115.1.0	*	*	143	TCP	Clientes WIFI. Protocolo IMAP Saliente
9	permite	10.115.1.0	*	*	110	TCP	Clientes WIFI. protocolo POP3 Saliente
10	permite	10.115.1.0	*	*	25	TCP	Clientes WIFI. protocolo SMTP Saliente
11	permite	10.115.1.0	*	*	80	TCP	Clientes WIFI. HTTP (navegación web)
12	permite	10.115.1.0	*	*	443	TCP	Clientes WIFI. HTTPS (nav. web segura)
13	permite	192.168.0.2	*	*	53	*	Consulta DNS de los servidores de control
14	rechaza	*	*	*	*	*	RECHAZA las demás conexiones

Además el firewall debe enrutar las conexiones con origen en la red 10.115.1.0 a un portal cautivo para autenticación de los usuarios del hotel para poder usar el WIFI. Las peticiones DNS de los servidores de control (si no existe DNS local), necesarias para la actualización automática del software del S.O. Debian, las debe dirigir al gateway de acceso a Internet.

Asimismo podemos implementar un firewall en cada servidor con las siguientes reglas:

FIREWALL DE SERVIDOR							
TRAFICO ENTRANTE							
REGLA	ACCION	ORIGEN	PUERTO ORIGEN	DESTINO	PUERTO DESTINO	PROTOC.	DESCRIPCION
1	permite	192.168.x.x	*	*	1729	*	Recepción de estados ODControl
2	permite	192.168.x.x	*	*	123	UDP	NTP
3	permite	192.168.0.0	*	*	9122	TCP	Sincronización de réplica de la BD
4	permite	*	*	*	22	TCP	SSH, para uso de administrador
5	rechaza	*	*	*	*	*	RECHAZA las demás conexiones
TRAFICO SALIENTE							
REGLA	ACCION	ORIGEN	PUERTO ORIGEN	DESTINO	PUERTO DESTINO	PROTOC.	DESCRIPCION
6	permite	*	*	192.168.x.x	1729	TCP	envío de comandos a ODControl
7	permite	*	*	192.168.x.x	123	UDP	NTP
8	permite	*	*	192.168.x.x	81	TCP	envío de comandos a ODControl por http (*)
9	permite	*	*	192.168.x.x	80	TCP	GUI web del ODControl (nota 1)
10	permite	*	*	(IP DNS)	53	*	Consulta DNS de los servidores de control

11	permite	*	*	192.168.0.0	9122	TCP	Sincronización de réplica de la BD
12	permite	*	*	10.115.0.0	80	TCP	Admin. switches interface web
13	rechaza	*	*	*	*	*	RECHAZA las demás conexiones

Nota 1: disponible para tareas de administración

## 5.2 Especificaciones de desarrollo y pruebas

### 5.2.1 Especificaciones de desarrollo

Durante el desarrollo de deberán efectuar las siguientes actividades:

1) Instalación de la distribución Debian 7 en un servidor de pruebas DELL PowerEdge™ R210 II realizando su configuración general: alta de usuarios, resolución de pantalla, etc.

2) Con el Gestor de Paquetes se realizarán las instalaciones de paquetes de software definidos anteriormente para los servidores. Tras examen de la documentación de cada paquete (referencias indicadas a continuación), se estudiarán y definirán los parámetros, reglas o directivas de configuración a aplicar para cada paquete según cada caso (servidor o router-firewall):

- IPtables [18] y desarrollo de las reglas del firewall según tablas anteriores (<http://www.netfilter.org/documentation/index.html>)
- Servidor de tiempo NTP (<https://wiki.debian.org/es/NTP>)
- Unison (<http://www.cis.upenn.edu/~bcpierce/unison/docs.html>)
- ClamAV (antivirus) (<http://www.clamav.net/lang/en/doc/>)
- OpenSSH (<http://www.openssh.com/manual.html>)
- Nmap ("Network Mapper") (<http://nmap.org/book/man.html>)
- vlan (<https://wiki.debian.org/NetworkConfiguration>  
([http://www.microhowto.info/howto/configure\\_an\\_ethernet\\_interface\\_as\\_a\\_vlan\\_trunk\\_on\\_debian.html](http://www.microhowto.info/howto/configure_an_ethernet_interface_as_a_vlan_trunk_on_debian.html)))
- MySQL (<http://dev.mysql.com/doc/>)
- Heartbeat ([http://www.linux-ha.org/wiki/Main\\_Page](http://www.linux-ha.org/wiki/Main_Page))
- Nessus (<http://www.tenable.com/products/nessus>)
- Apache2 (<http://httpd.apache.org/docs/>)

3) Definición de las configuraciones de los switches para implementar las VLAN: asignación de puertos, tipo (tagged/untagged), etc (Ref: DGS-1210-16 D-Link Web Smart Switch User Manual vers.4.0)

4) Definición de los comandos de control de cada ODCControl a aplicar en cada caso: órdenes, escenarios, etc.

5) Desarrollo de las diferentes tablas de la base de datos MySQL. Inserción de los datos de aplicación en cada tabla.

6) Desarrollo de las aplicaciones de recepción de estados y escenarios y las páginas web con HTML, PHP y Javascript para la interface web de usuario. Las aplicaciones no web en servidor también se realizarán usando PHP, y si fuera necesario apoyándose en

comandos o herramientas del sistema (cron, netcat, etc). El entorno de desarrollo a utilizar será Eclipse con el plugin PHP de EasyEclipse (<http://www.eclipse.org/> ; <http://www.easyeclipse.org/site/home/>).

7) Modificación necesaria en la aplicación de reservas para que actualice la base de datos MySQL.

### 5.2.2 Especificaciones de pruebas

Tal como establece el Plan de Pruebas, se realizarán diversas pruebas en las fases de Desarrollo e Implantación. El Plan de Pruebas inicial se debe actualizar con las pruebas indicadas en la fase de diseño, que se describirán a continuación junto con el entorno tecnológico necesario:

- **Especificación del Entorno de Pruebas. Entorno tecnológico.**

1. Hardware, software y comunicaciones.
  - Los dos servidores con Debian y todos los paquetes preinstalados, incluyendo un Front-end para MySQL y la configuración de red con todas las VLAN de la instalación real.
  - PC con navegador web y entorno de desarrollo Eclipse + EasyEclipse
  - Varios ODControls, cada uno asignado a una VLAN distinta.
  - Una LAN de pruebas con conexión a Internet (normalmente deshabilitada) a la que se conectan mediante un switch configurado cada uno de los equipos anteriores a su correspondiente VLAN.
  
2. Requisitos de operación y seguridad del entorno de pruebas  
 La LAN de pruebas será específica para pruebas (no puede ser una LAN con equipos en producción). No se conectará a Internet, excepto para descargar actualizaciones Debian, previa configuración de la seguridad.
  
3. Procedimientos de emergencia, recuperación, y de vuelta atrás.  
 Una vez finalizada la instalación y configuración definitiva de aplicaciones de los servidores, se obtendrá una imagen del disco duro y se realizará también una instalación en una máquina virtual.

- **Especificación de las pruebas:**

A continuación se hace una descripción genérica de las pruebas a efectuar, que deberán ser desarrolladas extensamente con los casos de prueba específicos de cada instalación real:

PRUEBAS UNITARIAS	
Nombre de la prueba	BASE DE DATOS: LECTURA Y MODIFICACIÓN DE REGISTROS
Casos de prueba que incluirá	Ejecución de las sentencias SQL previstas para cada una de las tablas: Habitaciones, Estados, Escenarios, etc

Criterios de aceptación	Los datos leídos o escritos en los registros de la BD son los esperados para cada sentencia.
Nombre de la prueba	FUNCIONAMIENTO DEL SERVIDOR WEB Y DISEÑO DE PÁGINAS WEB
Casos de prueba que incluirá	<ul style="list-style-type: none"> <li>• conexión al servidor y comprobación de opciones y seguimiento de hipervínculos</li> <li>• Comprobación visual del diseño de la página en los 3 navegadores más populares</li> </ul>
Criterios de aceptación	Están todas las opciones y funcionan todos los enlaces. La presentación es correcta en los 3 navegadores.
Nombre de la prueba	ANÁLISIS DE SEGURIDAD DE LOS PAQUETES DE SOFTWARE
Casos de prueba que incluirá	Identificación con Nessus de las posibles vulnerabilidades de los paquetes de software instalados en los servidores y el router-firewall
Criterios de aceptación	No hay vulnerabilidades calificadas con riesgos bajo a crítico

PRUEBAS DE INTEGRACIÓN	
Nombre de la prueba	RECEPCIÓN DE ESTADOS DE ODCONTROLES
Casos de prueba que incluirá	<ul style="list-style-type: none"> <li>• Comprobar que la aplicación "Recepción de estados" interroga secuencialmente a cada uno de los ODControles de pruebas.</li> <li>• Comprobar que actualiza la base de datos</li> </ul>
Criterios de aceptación	Comunica con los ODControles, éstos envían sus estados y la base de datos se actualiza de forma coherente con estados de los ODControles.
Nombre de la prueba	ENVÍO DE ESCENARIOS
Casos de prueba que incluirá	Configurar un escenario en la BD. Acortando el tiempo de ejecución del escenario, ejecutar la aplicación "Envío de escenarios"
Criterios de aceptación	Envía las órdenes a los ODControles y éstos las ejecutan se acuerdo a lo programado en el escenario. Repetir con varios escenarios distintos.
Nombre de la prueba	INTEGRACIÓN CLIENTE WEB-SERVIDOR-ODCONTROLES-BASE DE DATOS
Casos de prueba que incluirá	<ul style="list-style-type: none"> <li>• Enviar desde la interface web todas las órdenes y ver que se ejecutan Parametrizando previamente diversos casos en la base de datos, comprobar: <ul style="list-style-type: none"> <li>• Autenticación con todos los perfiles de usuario</li> <li>• Visualizar habitaciones en estado "reservadas" y en "modo manual"</li> <li>• Leer consignas de temperatura (visualizadas en cliente web)</li> </ul> </li> </ul> <p>Escribir en Base de datos:</p> <ul style="list-style-type: none"> <li>• Nuevas consignas de temperatura</li> <li>• condiciones de las secuencias y escenarios y asignarles un estado (activo/inactivo)</li> <li>• Crear y dar de baja usuarios</li> <li>• Listar el histórico de alarmas</li> <li>• Comprobar que los datos de la interface gráfica se actualizan periódicamente de forma correcta.</li> </ul>
Criterios de aceptación	Cada una de las pruebas se supera correctamente.
Nombre de la prueba	Comprobación de configuraciones de paquetes instalados en S.O. Linux
Casos de prueba que incluirá	Check-list de las configuraciones de todos los servicios instalados: Heartbeat , Unison, SSH, MySQL,... comprobando los ficheros de directorios como "/etc" ,...)
Criterios de aceptación	Cada una de las pruebas se supera correctamente.

Las pruebas del sistema se realizarán sobre la instalación real (pruebas de implantación):

PRUEBAS DE IMPLANTACION	
Nombre de la prueba	CONECTIVIDAD ENTRE EQUIPOS Y FUNCIONALIDAD DE CONTROL
Casos de prueba que incluirá	* Con toda la instalación eléctrica, sensores, etc, instalados: Probar para cada ODControl, que éste recibe correctamente órdenes (subir/bajar persianas, etc), que se reciben sus alarmas en la interface gráfica y comprobando que se ajusta, según corresponda, a: - la TABLA 1: "Funcionalidad de supervisión y control para cada habitación" - la TABLA 2: "Funcionalidad de supervisión y control para las zonas comunes"
Criterios de aceptación	Todas las órdenes y comprobaciones se ejecutan y reciben correctamente y la funcionalidad es correcta.
Nombre de la prueba	INTEGRACIÓN CON SISTEMA DE RESERVAS
Casos de prueba que incluirá	Desde el sistema de reservas, reservar diversas habitaciones y comprobar que en la interface web del sistema de control aparecen en estado "reservada"
Criterios de aceptación	Cada una de las reservas realizadas se muestra correctamente en la interface.
Nombre de la prueba	ANALISIS DE SEGURIDAD DEL SISTEMA
Casos de prueba que incluirá	Pruebas del firewall de los servidores y del router-firewall: comprobar mediante un escaner de puertos (Nmap) que están cerrados todos excepto los permitidos y para las IP's permitidas. Se deben probar las tablas de diseño de los firewall.
Criterios de aceptación	El resultado de las pruebas se debe ajustar a las tablas del diseño del firewall
Nombre de la prueba	DISPONIBILIDAD DEL SISTEMA
Casos de prueba que incluirá	<ul style="list-style-type: none"> <li>Desconectar la tensión de entrada del SAI y comprobar que los equipos siguen funcionando con el SAI durante el tiempo previsto.</li> <li>Comprobar que la réplica de la BD se va actualizando correctamente en el otro servidor, cuando se producen cambios en el servidor activo.</li> <li>Desconectar el cable de red del servidor activo y comprobar que el sistema sigue funcionando con el otro servidor. Repetir la prueba, volviendo a conectar el cable de red y desconectando el del último que estaba activo.</li> <li>Desconectar el enlace trunk de cada switch y comprobar que las comunicaciones se establecen por otra ruta (los ODControles de esa planta siguen comunicando)</li> </ul>
Criterios de aceptación	Cada una de las pruebas se supera correctamente.

## 5.3 Establecimiento de Requisitos de Implantación

### 5.3.1 Especificación de Requisitos de Documentación de Usuario

Previo a la Implantación, se debe disponer de los siguientes documentos:

\* Para el *usuario normal* (repcionistas): Manual de la interface de usuario (incluyendo una breve descripción del sistema y sus funciones)

\* Para el *usuario administrador*:

- Manual de la interface de usuario.
- Documento de la descripción del sistema, incluyendo diagramas de despliegue, etc
- Documentos de las configuraciones aplicadas al software (sistema operativo y paquetes instalados en cada equipo), configuraciones de switches, manuales y especificaciones técnicas de equipos de red, ODControles, SAI, etc
- Manual de administración del sistema informático
- Manual de Políticas de Seguridad del sistema.

- Plan de Mantenimiento.
- Manuales para la formación de usuarios normales.

Todos los documentos mencionados estarán en formato pdf, llevarán control de versiones y seguirán un formato homogéneo.

### 5.3.2 Especificación de Requisitos de Implantación

Los requisitos para poder iniciar la Fase de Implantación serán:

- 1) Requisitos de documentación: habrá sido generada y entregada la documentación definida en el apartado anterior.
- 2) Requisitos de formación:
  - Deben haber sido elaborados los manuales de formación para los usuarios normales y los usuarios administradores.
  - Los usuarios normales y los administradores deberán haber recibido previamente la formación que les permita usar y administrar el sistema, según corresponda, y dispondrán de las herramientas necesarias.
- 3) Requisitos tecnológicos:
  - Haber concluido satisfactoriamente las pruebas unitarias y de integración.
  - Las instalaciones (cableados, etc) deberán estar preinstaladas.
  - El hardware necesario (ODControles, switches, etc) habrá sido acopiado.
  - El sistema debe estar totalmente configurado: la base de datos (usuarios, escenarios, consignas de temperatura, etc), los servidores, switches, firewall, etc.
- 4) Requisitos de gestión:
  - Se deberán definir previamente las responsabilidades del personal que interactuará con el sistema. En particular deberá existir la figura del responsable de administración y seguridad del sistema y los administradores necesarios.
  - En caso de no haber personal experto, se deberá tener contratado un servicio de mantenimiento externo.
  - Se deberán especificar los procedimientos de comunicación de incidencias del sistema.
  - Deberá estar definido un Plan de Implantación y un Cronograma de Implantación.
  - Aceptación del Plan de Implantación y del Cronograma por la Gerencia del hotel.

## 6 Etapa de Desarrollo

Durante la Etapa de Desarrollo de una instalación real se deberán realizar diversas actividades, que deberán ser planificadas previamente y son:

- 1) Elección de la licencia del software desarrollado.
- 2) Concretar las versiones del software (paquetes, módulos, etc).
- 3) Preparar el entorno de desarrollo.
- 4) Desarrollar, instalar y configurar componentes y servicios del sistema.
- 5) Realizar las Pruebas Unitarias.
- 6) Realizar las Pruebas de Integración y del sistema.
- 7) Realizar la documentación.
- 8) Planificar la formación a los usuarios del sistema.
- 9) Validar y aprobar el sistema.

Siguiendo la planificación del TFM, en esta etapa se definen los manuales de usuario y la formación necesaria para el modelo de instalación domótica. Estas actividades también forman parte de la Etapa de Desarrollo y siguen el esquema propuesto en la metodología Métrica v3 para esta Etapa. Asimismo se ha incluido, en forma de anexos (ANEXOS 8 a 10), la parte del desarrollo correspondiente a:

- La instalación de las aplicaciones en Debian 7
- Las configuraciones de red de los servidores y del router-firewall
- La implementación de los firewall mediante reglas de IPTables

### 6.1 Definición de la documentación necesaria (Manuales de Usuario)

Este apartado hace referencia a la estructura y contenido de la documentación necesaria para la explotación y el mantenimiento del sistema, teniendo en cuenta los formatos definidos en la fase de Diseño. Para ello se deben considerar los dos perfiles de usuario identificados:

- el usuario normal (repcionista), encargado de la explotación del sistema.
- el usuario administrador, encargado del mantenimiento del sistema.

Los apartados que debe contener y deben ser desarrollados para cada manual de cada proyecto son los que se describirán en los subapartados siguientes.

#### 6.1.1 Documentación para el usuario normal

Dispondrá de un manual que describirá a grandes rasgos la funcionalidad del sistema y en detalle la interface gráfica para su perfil y sus funciones.

Manual del Usuario del Sistema de Control Domótico del Hotel	
Tabla de contenidos	
Capítulo 1. Introducción: Objeto del documento	
Capítulo 2. Descripción general del sistema domótico.	
2.1. descripción textual: arquitectura del sistema, explicación de elementos controlados: iluminación, climatización, persianas, etc	

2.2. Diagrama de bloques del sistema
Capítulo 3: Descripción de la interface gráfica y funciones (con imágenes de pantalla).

### 6.1.2 Documentación para el usuario administrador

La documentación para este perfil de usuario estará formada por varios manuales:

Manual de Administrador del Sistema de Control Domótico del Hotel
Tabla de contenidos
Capítulo 1. Introducción: Objeto del documento
Capítulo 2. Descripción general del sistema domótico. 2.1. descripción textual: arquitectura del sistema, explicación de elementos controlados: iluminación, climatización, persianas, etc 2.2. Descripción funcional detallada del sistema 2.3. Diagrama de bloques del sistema
Capítulo 3: Descripción de la interface gráfica y funciones.
Capítulo 4: Descripción de la interface gráfica: opciones adicionales de administrador.
Capítulo 5: Descripción de la red LAN 5.1. Topología y diagrama de despliegue 5.2. Dispositivos de red y características 5.3. Plan de direccionamiento IP
Capítulo 6: Configuraciones de los clientes web.
Capítulo 7: Instalación y configuración de las aplicaciones de los servidores. 7.1. Configuración general para Debian Wheezy 7.2. Servidor de tiempo NTP 7.3. Unison 7.4. OpenSSH 7.5. Nmap 7.6. Paquete vlan 7.7. MySQL 7.8. Heartbeat 7.9. Servidor web Apache2
Capítulo 8: configuraciones de seguridad. 8.1. Antivirus ClamAV 8.2. Reglas IPtables de los firewall 8.3. Nessus
Capítulo 9: Configuraciones de los dispositivos de red.
Capítulo 10: configuraciones individualizadas de los controladores ODControl.
ANEXOS: ficheros y pantallas de configuración originales de las aplicaciones A1: Ajustes de configuración inicial de los navegadores clientes A2: Software de los servidores: path's y contenidos de los ficheros de configuración A2: Ajustes de configuración inicial de los switches A4: Ajustes de configuración inicial del software del router-firewall A5: Listado de entradas/salidas de los ODControl y asignación de sensores y actuadores

MANUALES y DOCUMENTACION DEL HARDWARE
Manual de usuario del controlador ODControl
Manual de usuario del switch D- LINK DGS-1210-48
Manual de usuario del SAI SPS ADVANCE RT de Salicrú.



Esquemas de cableados de red
Esquemas de despliegue de ODControles y dispositivos de red
Planos de conexionado de los controladores ODControl con sensores y actuadores

OTROS DOCUMENTOS
Manual de Política de Seguridad del sistema
Plan de Mantenimiento

Tal como se definió en la Etapa de Diseño, uno de los requisitos para el inicio de la implantación es haber generado y entregado la documentación especificada en dicha etapa. Algunos de los documentos definidos en la etapa de Diseño quedan integrados dentro en un único Manual de Administrador.

## 6.2 Definición de la formación necesaria para Usuarios Finales

En esta actividad se definirá el esquema de formación y los contenidos necesarios para el usuario final (repcionistas y administradores).

### 6.2.1 Definición del Esquema de Formación

En esta tarea se define el contenido de la formación y su duración, por cada perfil de usuario.

ESQUEMA DE FORMACION para el USUARIO NORMAL	
<b>Objetivo:</b> el usuario (repcionista) deberá conocer todas las opciones disponibles para su perfil (según caso de uso) y su efecto sobre el sistema domótico, así como saber interpretar los mensajes y alarmas mostradas en la interface.	
Contenidos formativos	Duración
Exposición de los temas contenidos en el Manual de Usuario	6 horas
Prácticas sobre la interface web	2 horas

ESQUEMA DE FORMACION para el USUARIO ADMINISTRADOR	
<b>Objetivo:</b> el administrador deberá conocer todas las opciones disponibles para su perfil (según caso de uso) y su efecto sobre el sistema domótico, así como saber interpretar los mensajes y alarmas mostradas en la interface. Conocer la arquitectura global del sistema, poder sustituir y configurar sus componentes.	
Contenidos formativos	Duración
Exposición de los temas contenidos en el Manual de Administrador	16 horas
Prácticas sobre la interface web	2 horas
Explicación del controlador ODControl e interpretación de conexionados	3 horas
Configuración del switch D- LINK DGS-1210-48	3 horas

### 6.2.2 Especificación de los Recursos y Entornos de Formación

En este subapartado se detallan los recursos que se requieren para impartir la formación a cada perfil de usuario (aulas, ordenadores, etc):

PERFIL DE USUARIO: USUARIO NORMAL	
<b>Entorno de formación:</b> un aula que disponga de un proyector o monitor grande donde mostrar una presentación OpenOffice o PowerPoint y la pantalla de un ordenador, así como un ordenador con navegador web, conectado a la LAN por cada asistente.	
<b>Materiales:</b> Un Manual de Usuario por asistente. Una presentación que resuma los contenidos del manual, como guía para el profesor	
PERFIL DE USUARIO: USUARIO ADMINISTRADOR	
<b>Entorno de formación:</b> un aula que disponga de un proyector o monitor grande donde mostrar una presentación OpenOffice o PowerPoint y la pantalla de un ordenador, así como un ordenador con navegador web, conectado a la LAN por cada asistente. También debe permitir conexiones SSH a los servidores y a un switch D-LINK de pruebas (para hacer demostraciones de configuraciones durante la explicación)	
<b>Materiales:</b> Un Manual de Administrador, del ODControl y del switch por cada asistente Una presentación que resuma los contenidos formativos, como guía para el profesor	

## 7 Licencias del software y de los manuales desarrollados

El software a desarrollar es relativamente sencillo y solo toma verdadero valor integrado con el resto de la instalación. Por ello, no es un aspecto crucial la elección de una licencia, aunque se recomienda una licencia libre permisiva, como puede ser BSD de 3 cláusulas (3-clause BSD) [7], ya que permite más flexibilidad a la hora de integrar con otro software y es compatible con la distribución Debian. En cuanto a la documentación, también es específica para cada proyecto y no para distribución, por lo que no es necesario licenciar. Aunque si el instalador genera manuales genéricos, una licencia adecuada puede ser la *Creative Commons Atribución-CompartirIgual 3.0 Unported* (<http://creativecommons.org/licenses/by-sa/3.0/deed.es>).

## 8 Etapa de Implantación y Aceptación del Sistema

Esta etapa viene marcada por la tipología de proyecto, tratándose en este caso de un proyecto mixto de Desarrollo/Instalación de Software así como de instalación de Infraestructura. Esta última tiene un gran peso en esta fase, en la que se deberán desarrollar diversas actividades, que de forma resumida son:

- Establecer un Plan de Implantación.
- Impartir la formación para los usuarios del sistema
- Instalación de toda la infraestructura.
- Realizar las pruebas de implantación y las de aceptación del sistema
- Por último, se realizará su Aprobación y paso a Producción.

Todo ello quedará concretado en el Cronograma definido para el Plan de Implantación.

## 8.1 Establecimiento de un Plan de Implantación

### 8.1.1 Alcance

- Alcance de los trabajos de implantación:
  1. Gestión de suministros: ODControles, servidores, cableados, SAI, canalizaciones, switches, etc.
  2. Instalación de canalizaciones, cableados y equipos y su integración.
  3. Impartir la formación para los usuarios del sistema.
  4. Realizar las Pruebas de Implantación (sistema completo en entorno real).
  5. Realizar con el cliente las Pruebas de Aceptación del sistema (comprobar cumplimiento de requisitos para aprobación del cliente).

### 8.1.2 Condicionantes

Desde un punto de vista de instalación, se van a distinguir los siguientes subsistemas y sus dependencias respecto a otros proyectos o instalaciones:

Identificación de subsistemas involucrados	Dependencia de otros proyectos o instalaciones (condicionantes)
Dependencias o espacios técnicos	Deben haberse reservado y adecuado previamente espacios para: -instalación de armarios de red en cada planta -adecuación dependencia técnica para ubicar: <ul style="list-style-type: none"> <li>• Rack 19" con 2 servidores + 1 router-firewall</li> <li>• SAI</li> <li>• Aire acondicionado (si no existe)</li> <li>• Cuadro eléctrico</li> </ul>
Servidores de control	Adecuación de espacios previa
Alimentación de Energía (SAI, acometidas)	Finalización previa de instalación y acometidas eléctricas
Router-firewall	Adecuación de espacios Asignar IP e integrar en LAN del HOTEL
Cliente web	Integrar en LAN del HOTEL (asignación de IP si el hardware es nuevo)
Subsistema de ODControles	Instalación de cableados eléctricos y actuadores
LAN de ODControles: cableados de red, switches,...	-----
Sistema de reservas	Requiere modificación por equipo externo para integración con el sistema de control

### 8.1.3 Definición del Plan de Implantación

El plan de implantación, y en especial el cronograma, dependerá de si se trata de un hotel de nueva construcción o bien uno ya en funcionamiento, siendo éste último el caso más complejo, dado que se ha de compatibilizar la puesta en marcha de la instalación con la continuidad del servicio a los clientes del hotel. Vamos a considerar esta situación por ser la más compleja (aunque el plan de implantación y el cronograma podrían ser aplicados también a un edificio nuevo).

Un enfoque adecuado sería realizar los trabajos de instalación de ODControles, canalizaciones, sensores, actuadores, etc, de forma sucesiva por zonas del hotel desocupadas, e irlos conectando a la LAN de ODControles con los servidores de control ya operativos. El Plan de Implantación constará de varias fases, y cada una de ellas aplicada sucesivamente a distintas zonas del hotel ocupado.

Por simplicidad, en este caso supondremos que cada zona es una planta del hotel, a las que se aplicará de forma sucesiva una parte del mismo Plan de Implantación (aunque se podría extrapolar a otras áreas). El Plan de Implantación tendrá las siguientes fases y tareas:

FASES DEL PLAN DE IMPLANTACION
<p><b>FASE 0 : IMPARTIR LA FORMACIÓN a los Usuarios Finales.</b></p> <ul style="list-style-type: none"> <li>• Formación de administradores</li> <li>• Formación de recepcionistas</li> </ul>
<p><b>FASE 1: INSTALACION SERVIDORES Y LAN PLANTA 0.</b></p> <p>Adecuación sala de servidores (si no existiera ya) e instalación de:</p> <ul style="list-style-type: none"> <li>• Instalación interior de bandejas de cables</li> <li>• Instalación de cableados de energía</li> <li>• Instalación de cuadro eléctrico y SAI</li> <li>• Instalación de armarios de 19"</li> <li>• Instalación de aire acondicionado (si no existe)</li> <li>• Instalación de cableados de red</li> <li>• Instalación switches planta 0</li> <li>• Instalación de servidores y router-firewall</li> </ul> <p>Instalación/configuración PC cliente web en recepción                      Conectar en red todos los equipos, configuraciones finales y puesta en marcha                      Pruebas (parciales) de Implantación del Sistema</p>
<p><b>FASE 2: INSTALACION SWITCHES Y CABLEADO VERTICAL</b></p> <ul style="list-style-type: none"> <li>• Instalación de bandejas, cableado vertical de red y rack de 19" en cada planta</li> <li>• Instalación y puesta en marcha de switches preconfigurados para cada planta</li> </ul>
<p><b>FASE 3: INSTALACION ODControles Y CABLEADO HORIZONTAL</b></p> <p>(aplicada sucesivamente a zona o PLANTA 0, 1, 2, 3, etc)</p> <p>Instalación de bandejas y cableado horizontal de red</p> <p>Instalación ODControles en habitaciones y dependencias:</p> <ul style="list-style-type: none"> <li>• Instalación cuadros de ODControles y sus módulos y relés de control.</li> <li>• instalación y cableado de sensores y mandos manuales aire acondicionado</li> <li>• recablear alimentación 230V de ventiloconvectores a través de relés de control</li> <li>• recablear alimentación 230V de iluminación y enchufes a través de relés de control</li> </ul>

<ul style="list-style-type: none"> <li>• instalar motores de persianas, sus pulsadores y alimentación 230V a través de relés de control</li> </ul> <p>Conexión de todos los ODControls a la red LAN (switch de la planta)</p> <p>Pruebas (parciales) de Implantación del Sistema</p> <p>Realización de las Pruebas parciales de Aceptación del Sistema (parte instalada)</p> <p>Evaluación del Resultado de las Pruebas de Aceptación (parte instalada)</p> <p>PUESTA EN SERVICIO de la parte de la instalación</p>
<p>FASE 4, FASE 5, FASE 6:</p> <p><i>( Para cada planta o zona seleccionada se repiten las actividades de la FASE 3 hasta completar la totalidad del hotel)</i></p>
<p>FASE 7: Aceptación Total del sistema</p> <ul style="list-style-type: none"> <li>• Revisión de los documentos parciales de Aceptación y firma</li> <li>• Formalización de la Aceptación</li> </ul>

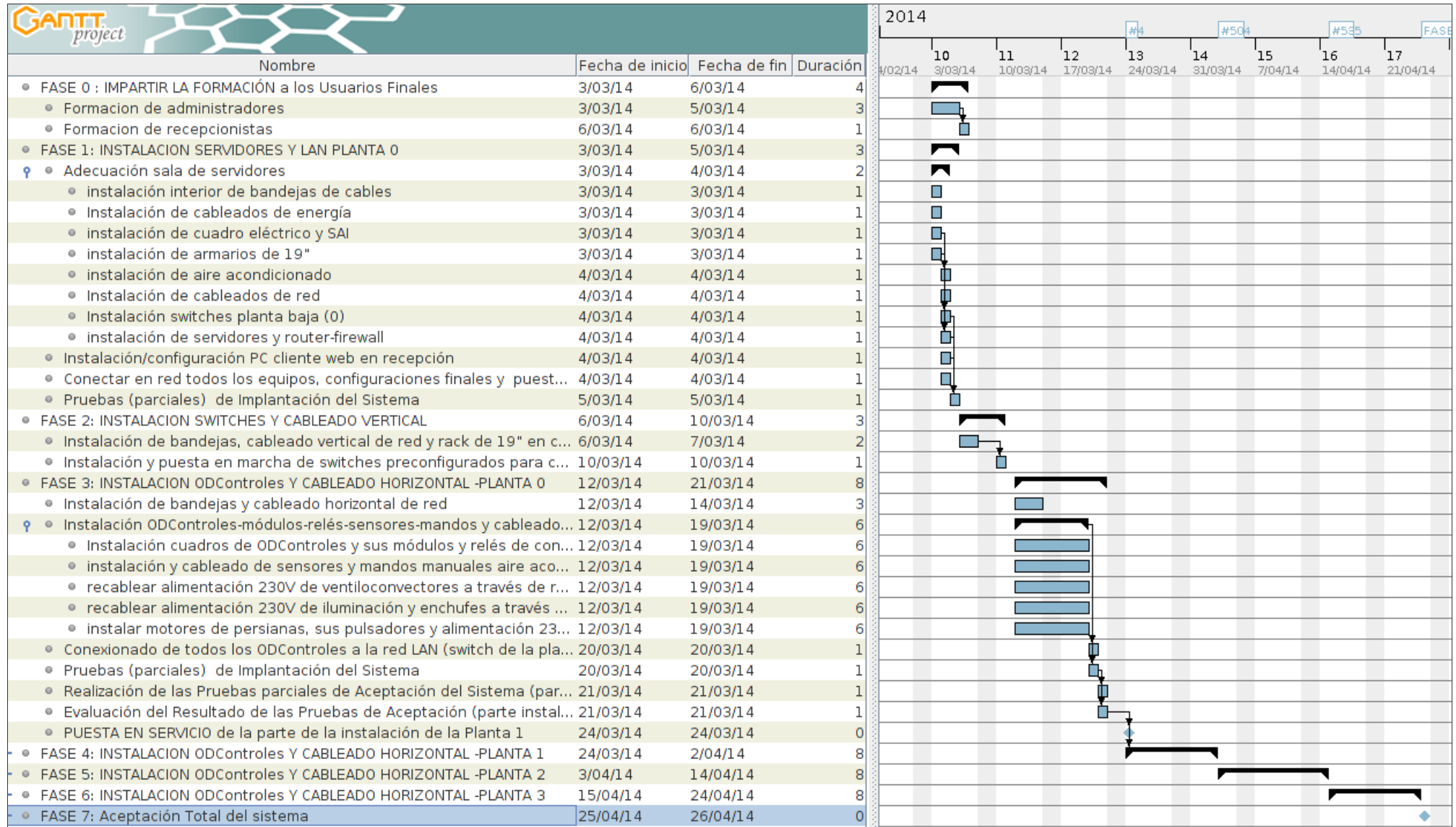
### 8.1.3.1 Especificación del Equipo de Implantación

La implantación y aceptación del sistema será efectuada por los siguientes equipos, cuyas fechas de participación quedarán definidas en el cronograma:

Equipo de implantación	Constituyentes
Etapa de instalación y pruebas de implantación	Un administrador de sistemas
	Instalador LAN
	Técnico instalador (ODControls)
	Instalador electricista 1
	Instalador electricista 2
	Instalador aire acondicionado
Etapa de Aceptación	Un Jefe de Proyecto
	Gerente del hotel (o delegado)
	Usuario en pruebas (perfil administrador)

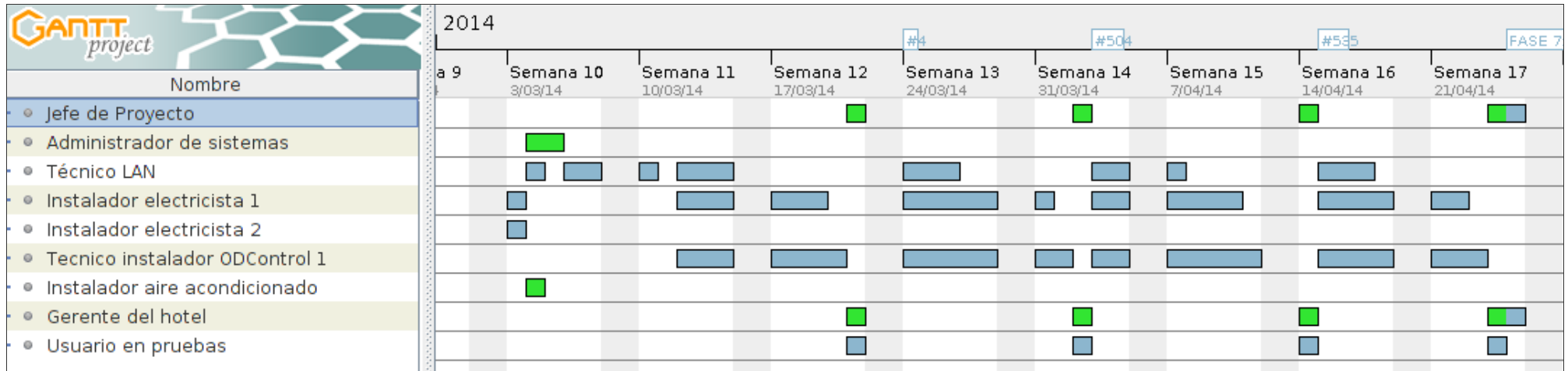
### 8.1.3.2 Cronograma de implantación. Diagrama de Gantt

Basándose en las actividades y tareas anteriores, el diagrama de Gantt completo del proyecto, para una instalación realizada sucesivamente en varias plantas, es el siguiente:



(Nota: en las fases 4, 5 y 6 no se han desplegado las tareas, ya que son idénticas a las de la FASE 3).

Los recursos asignados en la fase de implantación se muestran en el siguiente diagrama:



Con lo que resulta el siguiente cómputo de horas en la fase de Implantación, para el presupuesto:

	FASE1	FASE2	FASE3	FASE4	FASE5	FASE6	FASE7	Total horas de trabajo
Jefe de Proyecto			4	4	4	4	2	18
Administrador de sistemas	9							9
Instalador LAN	8	24	24	24	24	24		128
Instalador electricista 1	8		32	32	32	32		136
Instalador electricista 2	8							8
Técnico instalador ODControl			32	32	32	32		128
Instalador aire acondicionado	4							4
					<b>TOTAL HORAS</b>			<b>431</b>

## 9 Valoración económica

A partir del diseño realizado, se ha elaborado un presupuesto para una instalación de hotel del 100 habitaciones (modelo de partida), en el cual se han incluido también los costes de formación del personal (administradores y recepcionistas). El presupuesto asciende a 113.665 euros, tal como se refleja en la página siguiente:



ODControles instalados: <b>130</b>		Habitaciones: <b>100</b>		
DESCRIPCION	UNIDADES	PRECIO	TOTAL	OBSERVACIONES
<b>CONTROLADORES, SENSORES Y ACTUADORES</b>				
Controlador ODControl	130	200	26000	1 por habitación + zonas comunes
Motores de persianas y sus accesorios	100	150	15000	1 por cada habitación
Sensores de presencia	50	10	500	1 cada 2 habitaciones aprox (para pasillos)
Potenciómetro ajuste de temperatura	100	5	500	1 por cada habitación
Sensor de temperatura ambiente	130	5	650	1 por cada habitación y zonas comunes (basado en semiconductor LM35, TMP35 o similar)
Mando manual Fan-coil 3 velocidades + ON/OFF	130	28	3640	1 por cada habitación y zonas comunes
Relé 10 A montaje en carril de 35 mm (EN 60715)	700	25	17500	7 por habitación: control ventiloincubador, iluminación ON/OFF y persianas)
Contactos magnéticos montaje en superficie	130	3	390	1 por habitación + zonas comunes (detección ventanas abiertas)
Interruptor de tarjeta	100	8	800	1 por habitación
Interruptor doble para persiana	100	5	500	1 por habitación
Pulsador parada motor persiana	100	3	300	1 por habitación
<b>ELEMENTOS DE RED</b>				
Switches	5	430	2150	Mod. D-LINK DGS-1210-48
Servidores	3	844	2532	2 servidores DELL + 1 para el router-firewall
Ordenador cliente	1	500	500	
Cables UTP cat 5 (cableado horizontal)	900	0,15	135	(5 m por pared frontal de habitación + 3 m interior ) * 25 habitac /planta * 4 plantas + planta baja
Cables UTP cat 6 (cableado vertical)	210	0,24	50,4	aprox. 15 m por cada cable "trunk" entre plantas
Conectores RJ-45	298	0,3	89,4	min: 2 conectores ODControl ↔ switch + 2 conectores PC ↔ switch + 2 conectores switch ↔ switch cableado vertical (32 unid)
Bandeja de cables blanca dim. 100x100 marca Quin>	700	11,24	7868	125m por 4 plantas de 25 habitaciones + planta baja + 100 m cableado vertical
Canaleta blanca de cables 30x25 - (m)	390	2,54	990,6	3 m aprox. por derivación a cada ODControl
ARMARIO MURAL 19" 4U 520X450X240MM	5	40,95	204,75	1 armario por cada switch (Ref.: AR1904U520X450D1)
Bandeja extensible 19" 1U	5	15,43	77,15	1 bandeja por cada armario de switch Ref.: ARABE1U45)
Regleta enracable 19"	5	35,08	175,4	de 6 tomas SCHUKO + MAGNETO-TERMICO 4000W 16A (Ref: REG6SCHMAG)
<b>INSTALACION ELECTRICA</b>				
SAI	1	550	550	SAI SPS ADVANCE RT de Salicrú
Cable eléctrico 230 v para SAI (metros)	200	0,16	32	alimentacion switches y ordenadores desde SAI
Tiras de regleta de empalme 12 bornas	3	0,6	1,8	alimentacion switches y ordenadores desde SAI
Caja de empalmes eléctrica 80x80 estanca	10	1,09	10,9	alimentacion switches y ordenadores desde SAI
<b>MANO DE OBRA DE INSTALACIONES Y DESARROLLO DE SOFTWARE</b>				
<u>Etapa Diseño y Desarrollo</u>				
Diseño eléctrico de la instalación	1	6000	6000	
Desarrollo/configuración de software	1	12423	12423	segun modelo COCOMO básico: 2 personas en 2,3 meses
<u>Etapa Implantación</u>				
Total costes de la mano de obra	431	25	10775	horas totales trabajadas * precio/hora
<b>GASTOS DE FORMACION</b>				
Recepcionistas (horas totales)	48	25	1200	6 recepcionistas * 8 horas (costes de personal-horas no trabajadas)
Administradores (horas totales)	48	25	1200	2 administradores * 24 horas (costes de personal-horas no trabajadas)
Profesorado (horas totales impartidas)	32	25	800	
Materiales cursos	12	10	120	12 manuales
<b>COSTE TOTAL DE LA INSTALACION:</b>			<b>113665</b>	

## 10 Conclusiones

### 10.1 Cumplimiento de objetivos del proyecto

En la etapa de Estudio de Viabilidad se analizó el cumplimiento de requisitos para el modelo propuesto, viéndose que los podía cumplir. En esta última etapa se repasa el cumplimiento de los objetivos del Proyecto.

Los objetivos planteados inicialmente se habían dividido en los de carácter general y otros más técnicos. Respecto a los primeros, se puede decir que se han cumplido en su totalidad, dado que:

- hemos desarrollado un modelo viable de instalación domótica para un hotel de hasta 100 habitaciones, cuyo componente esencial es un producto OpenDomo, el controlador ODControl y que es parte fundamental de la instalación.
- Se ha diseñado una instalación domótica de bajo coste y fácil de mantener, dado que se basa en componentes usuales del mercado y tecnologías abiertas, incluyendo el software libre.
- En el diseño se han tomado varias medidas para que la calidad del servicio y confort para los clientes del hotel no se vea afectada por fallos del sistema informático (redundancia SW/HW y modo de funcionamiento manual).

Respecto a los objetivos técnicos que se plantearon:

- El sistema puede supervisar todas las habitaciones del hotel y las zonas comunes.
- Se han elaborado esquemas tipo sencillos para integrar el sistema con la instalación eléctrica (luces, climatización y persianas). Esto está en consonancia con otro de los objetivos: que el sistema permita el ahorro actuando sobre iluminación y la climatización.
- El sistema es adaptable según los requisitos del promotor hotelero, por lo que puede incluir sensores de circulación de fluido para detectar circulaciones y fugas de agua en estancias desocupadas.
- El sistema puede integrarse con otros sistemas del hotel (Intranet y Wifi), si bien manteniendo una separación lógica, en ambos casos para aprovechar la infraestructura existente o instalada. Para otros sistemas no se ha considerado conveniente, dado que significaría sobredimensionar la instalación para aplicaciones diferentes al objetivo de esta instalación, sin aportar ningún beneficio.
- Se han identificado los riesgos que presenta la nueva instalación, desde el punto de vista de operación y calidad del servicio (análisis de riesgos), tomándose diversas medidas para paliarlos: medidas de seguridad informática, operación ininterrumpida incluso con averías del sistema informático, topología de red con rutas alternativas, etc.
- Se ha concretado la arquitectura del puesto de control y el software libre necesario.
- Se han utilizado componentes de uso común en el mercado para la infraestructura de comunicaciones, a fin de evitar la dependencia tecnológica. Asimismo, se ha propuesto modelos concretos, como ejemplo.

Todos estos objetivos se han cumplido. Asimismo, la ligera desviación del coste previsto en el Estudio de Viabilidad no tiene apenas impacto en la rentabilidad desde el punto de vista de ahorro energético.

Por otra parte, el Plan de Implantación, tal como se ha definido, permite compatibilizar la ejecución de la instalación con la continuidad del servicio del hotel. También permite aplicarlo, con ligeras adaptaciones, por zonas o por plantas, según las necesidades y características del hotel.

Todo ello hace que el modelo propuesto puede darse como válido y crear proyectos de instalaciones viables a partir de él, tanto en hoteles de nueva construcción como reformados.

## 10.2 Propuesta para nuevas versiones de ODControles

Desde el punto de vista técnico, uno de los aspectos que complican la instalación ha sido el tener que reducir los dominios de broadcast. Si bien el tráfico generado en modo silencioso por los ODControles no es muy alto, el intentar reducirlos ha supuesto tener que utilizar switches más sofisticados que soporten VLAN's, configuraciones de red y reglas de firewall más complejas.

En este sentido, decir que puede ser interesante en nuevas versiones de ODControl permitir un nuevo modo de funcionamiento en el que no se envíen los broadcast y que el ODControl solo responda a peticiones de un puesto de control. Ello sería de utilidad en instalaciones con un elevado número de ODControles, como es el caso del hotel, de manera que todos podrían integrarse en una única subred.

## 10.3 Escalabilidad del diseño de la LAN

Aunque va más allá de los requisitos iniciales (hotel de hasta 100 habitaciones), a petición de OpenDomo se ha hecho un pequeño análisis de las posibilidades de escalar este diseño para un hotel de 15 plantas a 25 habitaciones por planta, más la planta baja. Partiendo del mismo análisis expuesto para el caso de 100 habitaciones, en el que se habían previsto un máximo de 30 ODControles por planta (en el caso más desfavorable), hemos de considerar la instalación adicional de 330 ODControles (en total 480). El diseño de la red propuesto sigue siendo válido dado que:

- El número de enlaces troncales (es decir, desde el switch de cada planta a la planta donde se ubican los servidores) aumenta en 11, que es asumible por los modelos de switches propuestos (de hasta 48 puertos 10/100/1000 Mbps) y en caso de ser necesario incluso se podría añadir un switch adicional para los ODControles de la planta baja, tratándose a nivel de instalación hardware como una planta más, con su switch independiente. En el ANEXO 13 se observa que el esquema de la topología de la LAN para 15 plantas es idéntico.
- Asimismo se observa en la hoja de cálculo del ANEXO 14 que el ancho de banda necesario en el punto de mayor congestión sigue estando dentro de valores admisibles ( 55 Kbps) para los 480 ODControles instalados.

## 10.4 Posibles ampliaciones del trabajo

Conforme se ha ido avanzando y profundizando en los aspectos del proyecto, se ha ido viendo la envergadura que puede ir tomando cada uno de los temas para llegar a implementar un proyecto sobre una instalación de un hotel real.

Cuestiones con las que se puede ampliar este trabajo, desde el punto de vista informático, son la aplicación a una instalación real. Para ello se requiere:

- Desarrollar el software del servidor de control y la interface gráfica.
- Ajustar la configuración de las aplicaciones instaladas y de los switches.
- Elaborar los contenidos de los manuales de formación de la instalación.
- Elaborar los planes de mantenimiento de la instalación.

## 11 Referencias bibliográficas

<b>TEMAS GENERALES:</b>		
[1]	Domótica	<a href="http://es.wikipedia.org/wiki/Domótica">http://es.wikipedia.org/wiki/Domótica</a>
[2]	X10	<a href="http://es.wikipedia.org/wiki/X10">http://es.wikipedia.org/wiki/X10</a>
[3]	Inmótica	<a href="http://es.wikipedia.org/wiki/Inmótica">http://es.wikipedia.org/wiki/Inmótica</a>
[4]	Ventiloconvector o FAN-COIL	<a href="http://es.wikipedia.org/wiki/Ventiloconvector">http://es.wikipedia.org/wiki/Ventiloconvector</a>
[5]	Métrica V.3 (metodología)	<a href="http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Metrica_v3.html#.U1gkYNdCXFQ">http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Metrica_v3.html#.U1gkYNdCXFQ</a>
[6]	<b>OPENDOMO:</b> Web corporativa  Comunidad de usuarios  Documentación  Lista de comandos del ODControl	<a href="http://www.opendomo.es/">http://www.opendomo.es/</a>  <a href="http://es.opendomo.org/">http://es.opendomo.org/</a>  <a href="http://opendomo.com/wiki">http://opendomo.com/wiki</a>  <a href="http://www.opendomo.com/wiki/index.php/Comandos_de_ODControl">http://www.opendomo.com/wiki/index.php/Comandos_de_ODControl</a>
[7]	Licencia BSD de 3 cláusulas (3-clause BSD)	<a href="http://opensource.org/licenses/BSD-3-Clause">http://opensource.org/licenses/BSD-3-Clause</a>  <a href="http://es.wikipedia.org/wiki/Licencia_BSD">http://es.wikipedia.org/wiki/Licencia_BSD</a>
<b>NETWORKING :</b>		
[8]	Cisco (Routers y switches)	<a href="http://www.cisco.com/">http://www.cisco.com/</a>
[9]	D-Link (Routers y switches)	<a href="http://www.dlink.com/es/es">http://www.dlink.com/es/es</a>  <a href="http://www.dlink.com/">http://www.dlink.com/</a>
[10]	VLAN	<a href="http://es.wikipedia.org/wiki/VLAN">http://es.wikipedia.org/wiki/VLAN</a>  <a href="http://www.redespracticas.com/conmutacion/switching/vlan">http://www.redespracticas.com/conmutacion/switching/vlan</a>
[11]	Trunking	<a href="http://standards.ieee.org/findstds/standard/802.1Q-2011.html">http://standards.ieee.org/findstds/standard/802.1Q-2011.html</a>  <a href="http://es.wikipedia.org/wiki/IEEE_802.1Q">http://es.wikipedia.org/wiki/IEEE_802.1Q</a>  <a href="http://publib.boulder.ibm.com/infocenter/">http://publib.boulder.ibm.com/infocenter/</a>  <a href="http://www.cisco.com/cisco/es/19180/Cisco_Technology/09/09_09_01a.html">Cisco. Trunking: Configuring Access and Trunk Interfaces</a>
[12]	Spanning Tree Protocol (STP)	<a href="http://standards.ieee.org/getieee802/download/802.1D-2004.pdf">http://standards.ieee.org/getieee802/download/802.1D-2004.pdf</a>  <a href="http://es.wikipedia.org/wiki/Spanning_Tree_Protocol">http://es.wikipedia.org/wiki/Spanning_Tree_Protocol</a>  <a href="http://es.wikipedia.org/wiki/IEEE_802.1D">http://es.wikipedia.org/wiki/IEEE_802.1D</a>

		<a href="http://www.cisco.com/c/en/us/tech/lan-switching/spanning-tree-protocol/index.html">http://www.cisco.com/c/en/us/tech/lan-switching/spanning-tree-protocol/index.html</a>
[13]	<b>Network Time Protocol (NTP)</b>	<a href="http://tools.ietf.org/html/rfc1305">http://tools.ietf.org/html/rfc1305</a> <a href="http://es.wikipedia.org/wiki/Network_Time_Protocol">http://es.wikipedia.org/wiki/Network_Time_Protocol</a>
[14]	<b>Configuración Ethernet como enlace VLAN trunk 802.1q en sistemas GNU/Linux</b>	<a href="http://tuxjm.net/docs/Configurando_una_interfaz_Ethernetcomo_enlace_VLAN_trunk_802.1q_en_sistemas_GNU_Linux">http://tuxjm.net/docs/Configurando una interfaz Ethernet como enlace VLAN trunk 802.1q en sistemas GNU Linux</a> <a href="https://wiki.debian.org/NetworkConfiguration#Howto_use_vlan_.28dot1q.2C_802.1q.2C_trunk.29_.28Etch.2C_Lenny.29">https://wiki.debian.org/NetworkConfiguration#Howto_use_vlan .28dot1q.2C_802.1q.2C_trunk.29 .28Etch.2C_Lenny.29</a>
<b>SOFTWARE:</b>		
[15]	<b>Debian Handbook</b>  <b>Paquetes</b>  <b>Configuración de red</b>	<a href="http://debian-handbook.info/browse/stable/">The Debian Administrator's Handbook http://debian-handbook.info/browse/stable/</a>  <a href="https://www.debian.org/distrib/packages">https://www.debian.org/distrib/packages</a>  <a href="https://wiki.debian.org/NetworkConfiguration">https://wiki.debian.org/NetworkConfiguration</a>
[16]	<b>LINUX-HA (Heartbeat)</b>	<a href="http://www.linux-ha.org">http://www.linux-ha.org</a>  <a href="http://linux-ha.org/wiki/Documentation">http://linux-ha.org/wiki/Documentation</a>  <a href="http://linux-ha.org/wiki/Haresources">http://linux-ha.org/wiki/Haresources</a>
[17]	<b>MySQL</b>	<a href="http://dev.mysql.com/doc">http://dev.mysql.com/doc</a>  <a href="http://es.wikipedia.org/wiki/MySQL">http://es.wikipedia.org/wiki/MySQL</a>
[18]	<b>IPTABLES</b>	<a href="http://www.netfilter.org/projects/iptables/">http://www.netfilter.org/projects/iptables/</a>  <a href="http://es.wikipedia.org/wiki/Iptables">http://es.wikipedia.org/wiki/Iptables</a>
[19]	<b>Apache HTTP Server</b>	<a href="http://httpd.apache.org/">http://httpd.apache.org/</a>  <a href="http://es.wikipedia.org/wiki/Apache_HTTP_Server">http://es.wikipedia.org/wiki/Apache_HTTP_Server</a>
[20]	<b>Nessus</b>	<a href="http://www.tenable.com">http://www.tenable.com</a>  <a href="http://es.wikipedia.org/wiki/Nessus">http://es.wikipedia.org/wiki/Nessus</a>
[21]	<b>UNISON</b>	<a href="http://www.cis.upenn.edu/~bcpierce/unison/">http://www.cis.upenn.edu/~bcpierce/unison/</a>  <a href="http://en.wikipedia.org/wiki/Unison_(file_synchronizer)">http://en.wikipedia.org/wiki/Unison_(file_synchronizer)</a>
[22]	<b>OpenSSH</b>	<a href="http://www.openssh.com/">http://www.openssh.com/</a>  <a href="http://es.wikipedia.org/wiki/OpenSSH">http://es.wikipedia.org/wiki/OpenSSH</a>
[23]	<b>NMAP</b>	<a href="http://nmap.org/">http://nmap.org/</a>  <a href="http://es.wikipedia.org/wiki/Nmap">http://es.wikipedia.org/wiki/Nmap</a>
[24]	<b>CLAMAV (antivirus)</b>	<a href="http://www.clamav.net">http://www.clamav.net</a>  <a href="http://es.wikipedia.org/wiki/ClamAV">http://es.wikipedia.org/wiki/ClamAV</a>
[25]	<b>LAMP</b>	<a href="http://es.wikipedia.org/wiki/LAMP">http://es.wikipedia.org/wiki/LAMP</a>

# ANEXOS

## ANEXO 1. Componentes OpenDomo

Productos hardware y software de OpenDomo susceptibles de ser considerados inicialmente en el diseño, y descripción de sus principales características:

- **ODControl**

Se trata de un controlador IP que dispone de toda la lógica de control necesaria para gobernar los elementos que se les ha encomendado a cada uno de ellos. Una vez programados mediante una interface gráfica disponible en la distribución OpenDomo, pueden funcionar autónomamente, incluso si se pierde la comunicación con los ODNetwork o el ordenador central de supervisión. De esta manera, pueden instalarse tantos ODControl como sean necesarios para el control de la instalación. El número de dispositivos a instalar dependerá exclusivamente de la envergadura del sistema a controlar.

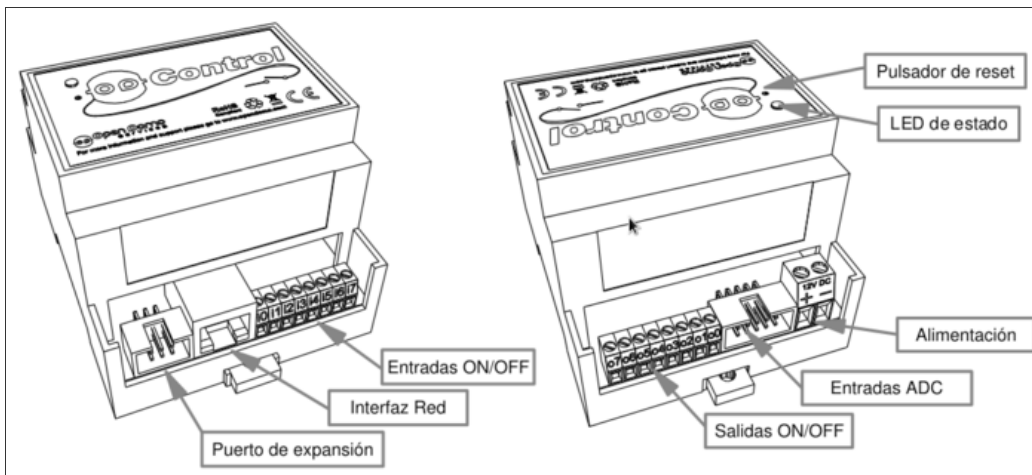
Tienen las siguientes características:

- 8 salidas digitales
- 8 entradas digitales
- 8 entradas analógicas
- 1 puerto Ethernet RJ45
- Puertos de expansión 1 int. + 1 ext
- Protocolos soportados: UDP, HTTP, netcat
- Puertos virtuales: 48
- Enlaces: 32
- Configuración con interfaces gráficas o con comandos:
  1. mediante aplicación on-line (Configurator 2.0)
  2. con la biblioteca de plantillas disponibles
  3. mediante comandos, por el puerto 1729 (con telnet o netcat)
  4. mediante interface gráfica desde un ODNetwork
- Modos de operación: esta característica va a ser muy importante a la hora de definir la arquitectura de nuestra red, ya que ODControl es capaz de funcionar de forma autónoma. Los modos que permite son:
  1. manual: mediante una sencilla interfaz web que incorpora.
  2. autónomo, aislado de la red de datos
  3. integrado con OpenDomo: controlado desde ordenador central, por ejemplo un ODNetwork
- Instalable sobre carril DIN (ocupa 4U)
- Dimensiones (mm): 78x93x56

▪ Aspecto del controlador ODControl:



▪ Conexiones e indicaciones del controlador ODControl:



○ **Módulo AI420**

Este módulo se puede agregar, opcionalmente, al controlador ODControl. Dispone de 8 entradas analógicas para sensores del tipo 4-20mA.

○ **Módulo AO010**

Se trata de un módulo de 3 salidas analógicas de tipo seleccionable: 0..10V, 1..10V, 0..20mA ó 4..20mA, con 256 niveles (8bits). Se añade, opcionalmente, al ODControl Aplicaciones: controles analógicos de niveles de luz, caudal de fluidos, etc.

○ **OpenDomo (sistema operativo)**

Se trata del sistema operativo instalado en el ODNetwork (o en una máquina virtual), el cual está basado en el núcleo de Linux. Consta de las siguientes capas:



1. Núcleo Linux
2. Busybox: una serie de herramientas básicas para administración, incluyendo un intérprete de comandos, que admite scripts.
3. Paquetes OpenDomo: capa de aplicación con diversas funcionalidades.

```

Starting SYSLOG ... [ OK ]
Initializing random number generator... [ OK ]
Loading storage modules... [ OK ]
Mounting drives...(sr0=iso9660) [ OK ]
Loading network drivers... (pcnet32) [ OK ]
Starting network (looking for a DHCP server)... [ OK ]
Loading remote configuration ... [SKIPD]
Script not found S49nfsd [SKIPD]
Mounting network drives... [ OK ]
Starting 1 TCP services... [ OK ]
Installing packages ...(kernel)(kernel_sound)(kernel_video)(odai)(odcgi)(odcommo
n)(odcontrol)(odcontrol_arduino)(odcontrol_micropik)(odcontrol_x10)(oddiscovery)
(odevents)(odpkg)(odspeech)(odvideo) [ OK ]
Script not found S63cherokee [SKIPD]
Script not found S64cherokee-ssl [SKIPD]
Starting sshd: (generating rsa key...)(generating dsa key...) [ OK ]
Loading extra modules... [SKIPD]
Starting Universal Identification ... [ OK ]
Starting OpenDomo Network ... [ OK ]
Starting controllers... [ OK ]
Starting CRON [ OK ]
Starting sound system ... [ OK ]

Welcome to OpenDomo
od0800273C3AB7 login: _
    
```

Una forma habitual de instalación de OpenDomo en entornos empresariales es corriendo en una máquina virtual. El número de ODControles que se pueden controlar con esta configuración solo dependerá de la potencia de la máquina, y en particular de la memoria asignada a la máquina virtual.

También existe la posibilidad de instalarlo directamente sobre un ordenador con alguna distribución Linux, mediante paquetes (.deb o .rpm) que proporcionan las funcionalidades equivalentes al sistema OpenDomo.

- **ODNetwork**

Se trata de un ordenador de muy reducidas dimensiones y bajo consumo. Puede controlar fácilmente una docena de ODControles. Lleva preinstalada la distribución OpenDomo e incluye las siguientes funcionalidades domóticas:

- Escenas: grabación del estado de un grupo de elementos determinado de la instalación, para su accionamiento conjunto.
- Secuencias: sucesión de instrucciones prefijadas para actuar sobre dispositivos.
- Condiciones: se ejecutan acciones cuando se cumple determinada condición.

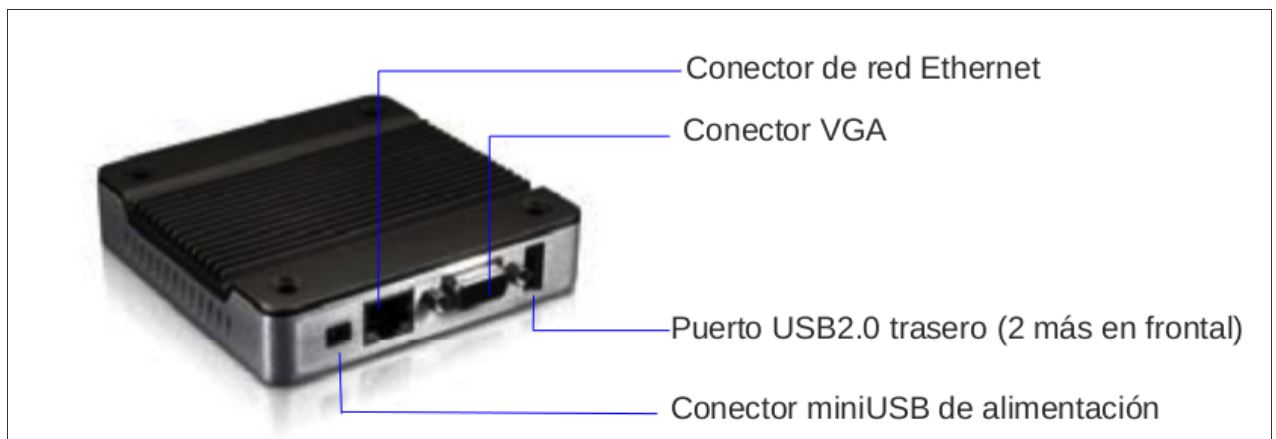
- Estados: similar al “runlevel” de un sistema operativo, aunque aquí se habilitan o no servicios domóticos: videovigilancia, hilo musical,... en función del perfil de servicios que interese. Por ejemplo, para horario diurno, de descanso, ausencias, etc.

Funciones adicionales, mediante módulos instalables:

- Sintetizador de voz: para notificación de eventos mediante voz
- Hilo musical: en desarrollo

Características del hardware (vers. 2012)

- Procesador: 1 GHz
- Memoria RAM: 512 MByte DDR2
- Tarjeta gráfica: 32MB, resolución máxima 1920 x 1200
- Tarjeta de sonido: compatible AC97 v2.2
- Red: 10/100 Mbps
- USB 2.0: 3 puertos
- Dimensiones: 90 x 90 x 20 mm
- Memoria no volátil para almacenaje: tarjeta SD 2GB



### • Interfaces de usuario

Existen diferentes tipos de interfaces de usuario, a aplicar cada una dependiendo del tamaño de la instalación. Se dispone desde interfaces para teléfonos móviles inteligentes, hasta una interfaz tipo SCADA para la supervisión de un número muy elevado de elementos en entornos profesionales. A modo de ejemplo, la siguiente es la interfaz instalada en el software del ODNetwork, en concreto la que permite la configuración de los controladores ODControl:



**Control**   **Zonas**   **Herramientas**   **Configurar**

---

**Requisitos**

hora 19 00

**Eliminar requisitos**   **Ayuda**

**Si todos los requisitos se cumplen**

Ejecutar acción o secuencia   Actualizar paquetes instalados

**Guardar**   **Volver al listado**   **Ayuda**

**Añadir requisito**

...

**Añadir**   **Ayuda**

       OpenDomo © 2006-2013

## ANEXO 2. Viabilidad de cumplimiento de los requisitos

Para que las alternativas de solución sean viables, deberán cumplir cada uno de los requisitos, o en su defecto aquellos relevantes (con prioridad alta o muy alta) que permitan dar unos mínimos válidos de las funcionalidades deseadas. Pero previamente a la elaboración de la propuesta debemos tener en cuenta la identificación de posibles requisitos incompatibles o contradictorios (por ejemplo, si es posible controlar todos los parámetros solicitados (requisitos RS-2 y RS-3) con un solo controlador por habitación (requisito RS-1):

CUMPLIMIENTO DE LOS REQUISITOS DEL SISTEMA			
Id	Descripción	Requisitos incompatibles	RESULTADO (Viabilidad)
RS-1	Cada habitación será controlada de forma independiente, mediante su propio controlador ODControl	NINGUNO	VIABLE, dado que cada ODControl dispone de: <ul style="list-style-type: none"> <li>• 8 salidas digitales</li> <li>• 8 entradas digitales</li> <li>• 8 entradas analógicas</li> </ul> Condicionado a dimensionar adecuadamente la red local y el puesto de control, dado el elevado número de controladores que se instalarán.
RS-2	En cada habitación se controlará al menos: <ul style="list-style-type: none"> <li>• iluminación</li> <li>• temperatura</li> </ul>	NINGUNO	VIABLE, pues se disponen de suficientes E/S en cada ODControl
RS-3	En cada habitación se controlará adicionalmente: <ul style="list-style-type: none"> <li>• motorización de persianas</li> <li>• detección de apertura de ventanas</li> <li>• detección de fugas de agua</li> </ul>	NINGUNO	VIABLE Condicionado al diseño de las interfaces con actuadores en cuanto a necesidades de E/S en cada ODControl
RS-4	Se controlará la climatización, así como la iluminación de las zonas comunes, haciendo uso de sensores de presencia	NINGUNO,	VIABLE, instalando los ODControl necesarios con sus correspondientes sensores y actuadores en cada zona a controlar Condicionado a dimensionar adecuadamente la red local y el puesto de control.
RS-5	Los subsistemas troncales tendrán redundancia para garantizar una alta disponibilidad. En concreto: <ul style="list-style-type: none"> <li>• la red local de comunicaciones dispondrá de al menos un camino alternativo</li> <li>• el puesto de control estará redundado a nivel hardware y software</li> </ul>	NINGUNO	VIABLE
RS-6	El puesto de control dispondrá de algoritmos o consignas de control de dispositivos para ahorro energético (bajar persianas, apagar iluminación de plantas enteras, etc)	NINGUNO	VIABLE
RS-7	Existirá un puesto de mando en el	NINGUNO	VIABLE

	que se controlarán, para cada habitación o zona común: <ul style="list-style-type: none"> <li>• iluminación</li> <li>• temperatura</li> <li>• alarmas técnicas (las que se implementen)</li> </ul>		Actualmente ya existen productos y experiencia en OpenDomo para el control de un gran número de dispositivos. Condicionado a dimensionar adecuadamente la red local y el puesto de control.
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Los siguientes requisitos del cliente son cumplidos si se cumplen simultáneamente los requisitos técnicos que se indican a continuación:

CUMPLIMIENTO DE REQUISITOS DEL CLIENTE		
Id	Descripción	Requisitos técnicos del sistema que lo suplen
<b>Requisitos de cliente que pueden ser suplidos por requisitos del sistema</b>		
RC-1	El sistema será capaz de controlar un hotel de hasta 100 habitaciones	RS-1: Cada habitación será controlada de forma independiente, mediante su propio controlador ODControl. Al ser de funcionamiento autónomo, el nº de ODControles que se pueden instalar es ilimitado. CONDICION ADICIONAL: la red y el puesto de control deben dimensionarse adecuadamente al número de ODControl.
RC-2	Se realizará el control, a efectos de ahorro energético, de la iluminación	RS-2: En cada habitación se controlará al menos: <ul style="list-style-type: none"> <li>• iluminación</li> <li>• temperatura</li> </ul> RS-4: Se controlará la climatización, así como la iluminación de las zonas comunes, haciendo uso de sensores de presencia
RC-3	Se realizará el control, a efectos de ahorro energético, de la climatización	RS-2: En cada habitación se controlará al menos: <ul style="list-style-type: none"> <li>• iluminación</li> <li>• temperatura</li> </ul> RS-4: Se controlará la climatización, así como la iluminación de las zonas comunes, haciendo uso de sensores de presencia
RC-4	Se realizará el control, a efectos de ahorro energético, de persianas y ventanas	RS-3: En cada habitación se controlará adicionalmente: <ul style="list-style-type: none"> <li>• motorización de persianas</li> <li>• apertura de ventanas</li> <li>• detección de fugas de agua</li> </ul>
RC-5	El sistema gestionará alarmas técnicas de detección de fugas de agua	RS-3: En cada habitación se controlará adicionalmente: <ul style="list-style-type: none"> <li>• motorización de persianas</li> <li>• apertura de ventanas</li> <li>• detección de fugas de agua</li> </ul>
RC-6	Las partes principales de la instalación cuyo posible fallo comprometa la funcionalidad de la instalación al completo, deberán ser de diseñadas de tal manera que sea tolerante a más de un fallo.	RS-5: Los subsistemas troncales tendrán redundancia para garantizar una alta disponibilidad. En concreto: <ul style="list-style-type: none"> <li>• la red local de comunicaciones dispondrá de al menos un camino alternativo</li> <li>• el puesto de control estará redundado a nivel hardware y software</li> </ul>
RC-0	El desarrollo se basará en los productos HW/SW y servicios comercializados por OpenDomo	RS-1: Cada habitación será controlada de forma independiente, mediante su propio controlador ODControl RS-4: Se controlará la climatización, así como la iluminación de las zonas comunes, haciendo uso de sensores de presencia Con ello se cumple que la mayor parte de la instalación (si exceptuamos la infraestructura de red) se basa en productos OpenDomo

Requisitos de cliente no recogidos en los del sistema	
RC-7	En caso de fallo total del sistema informático, existirá un mecanismo alternativo para poder seguir dando servicio en las habitaciones
RC-8	La red del sistema de control será segura y aislada de otros sistemas, al menos a nivel lógico, aunque a nivel físico, dependiendo del diseño, se podrán compartir
RC-9	Cumplimiento de las normativas legales, de distintos ámbitos, de la instalación domótica

Respecto a estos últimos, comentar que:

- No se detectan, para los requisitos RC-7, RC-8 y RC-9 incompatibilidades con otros requisitos.
- El requisito RC-7 puede cumplirse mediante conexiones/desconexiones manuales de la iluminación, climatización y persianas. Por ejemplo con el uso de circuitos eléctricos paralelos a los contactos de conexión/desconexión del ODControl.
- El requisito RC-8 se reduce a una cuestión de diseño de la red local.
- En cuanto al requisito RC-9, de cumplimiento de las normativas legales, se trata tal vez del más importante de todos, ya que de nada serviría diseñar una instalación que pueda satisfacer todos los demás, si legalmente no se puede llevar a la práctica. Por ello, dado que estamos desarrollando un modelo de instalación domótica, vamos a darle un tratamiento más extenso.

### Viabilidad de la instalación desde el punto de vista del cumplimiento de las normativas legales

A continuación se indican las normativas y los puntos de afectación de las mismas:

Directiva 2004/108/CE de Compatibilidad Electromagnética y REAL DECRETO 1580/2006, de 22 de diciembre, por el que se regula la compatibilidad electromagnética de los equipos eléctricos y electrónicos
Los controladores ODControl cumplen la directiva europea de Compatibilidad Electromagnética. El resto de componentes son los de uso habitual en redes y sistemas informáticos, por lo que no existirán problemas de cumplimiento en este sentido.
Código Técnico de la Edificación (RD 314/2006)
En el ámbito tratado es de aplicación el Artículo 15 - Exigencias básicas de ahorro de energía (HE): 15.2 Exigencia básica HE 2: Rendimiento de las instalaciones térmicas. Los edificios dispondrán de instalaciones térmicas apropiadas destinadas a proporcionar el bienestar térmico de sus ocupantes, <b>regulando el rendimiento de las mismas y de sus equipos</b> . Esta exigencia se desarrolla en Reglamento de Instalaciones Térmicas en los Edificios (RITE )  15.3 Exigencia básica HE 3: Eficiencia energética de las instalaciones de iluminación: los edificios dispondrán de instalaciones de iluminación adecuadas a las necesidades de sus usuarios y a la vez eficaces energéticamente <b>disponiendo de un sistema de control que permita ajustar el encendido a la ocupación real de la zona</b> , así como de un sistema de regulación que optimice el aprovechamiento de la luz natural, en las zonas que reúnan unas determinadas condiciones.

## Reglamento de Instalaciones Térmicas en los Edificios

En las Disposiciones Generales se indica:

Artículo 2. **Ámbito de aplicación:** El RITE se aplicará a las instalaciones térmicas en los edificios de nueva construcción y a las instalaciones térmicas en los edificios construidos, en lo relativo a su reforma, mantenimiento, uso e inspección, con las limitaciones que en el mismo se determinan.

Artículo 12: **Eficiencia energética, punto 3. Regulación y control:** las instalaciones estarán dotadas de los sistemas de regulación y control necesarios para que se puedan mantener las condiciones de diseño previstas en los locales climatizados, ajustando, al mismo tiempo, los consumos de energía a las variaciones de la demanda térmica, así como interrumpir el servicio.”

También afecta directamente la instrucción técnica IT.1.2.4.3-Control, en varios subapartados:

IT.1.2.4.3.1 - Control de las instalaciones de climatización, que indica en su punto 2:

2. El empleo de controles de tipo todo-nada está limitado a las siguientes aplicaciones:

- límites de seguridad de temperatura y presión.
- regulación de la velocidad de ventiladores de unidades terminales.
- control de la emisión térmica de generadores de instalaciones individuales.
- control de la temperatura de ambientes servidos por aparatos unitarios, siempre que la potencia térmica nominal total del sistema no sea mayor que 70 kW.
- control del funcionamiento de la ventilación de salas de máquinas con ventilación forzada.

IT.1.2.4.3.4 - Control de instalaciones centralizadas de ACS:

El equipamiento mínimo del control de las instalaciones centralizadas de preparación de ACS será el siguiente:

- Control de la temperatura de acumulación
- Control de la temperatura del agua de la red de tuberías en el punto hidráulico más lejano del acumulador;
- Control para efectuar el tratamiento de choque térmico
- Control de funcionamiento de tipo diferencial en la circulación forzada del primario de las instalaciones de energía solar térmica. Alternativamente al control diferencial se podrán emplear sistemas de control accionados en función de la radiación solar
- Control de seguridad para los usuarios.

### Reglamento Electrotécnico de Baja Tensión (ICT-BT-51:“*instalaciones de sistemas de automatización, gestión técnica de la energía y seguridad para viviendas y edificios*”)

En el ANEXO 12 se puede encontrar dicha Instrucción Técnica completa. De la clasificación de instalaciones domóticas que indica, este caso se incluye dentro de los “*Sistemas que usan en todo o en parte señales transmitidas por cables específicos para dicha función, tales como cables de pares trenzados, paralelo, coaxial, fibra óptica*”. Para estos sistemas son de aplicación los siguientes preceptos (extractos aplicables de la instrucción):

**REQUISITOS GENERALES DE LA INSTALACIÓN:** Todos los nodos, actuadores y dispositivos de entrada que se instalen en el sistema, deberán incorporar instrucciones o referencias a las condiciones de instalación y uso que deban cumplirse para garantizar la seguridad y compatibilidad electromagnética de la instalación, como por ejemplo, tipos de cable a utilizar, aislamiento mínimo,

apantallamientos, filtros y otras informaciones relevantes para realizar la instalación. En el caso de que no se requieran condiciones especiales de instalación, esta circunstancia deberá indicarse expresamente en las instrucciones. Dichas instrucciones se incorporarán en el proyecto o memoria técnica de diseño, según lo establecido en la ITC-BT-04. [...]. Cuando el sistema domótico esté alimentado por muy baja tensión o la interconexión entre nodos y dispositivos de entrada este realizada en muy baja tensión, las instalaciones e interconexiones entre dichos elementos seguirán lo indicado en la ITC-BT-36 (instalaciones a muy Baja Tensión).

CONDICIONES PARTICULARES DE INSTALACIÓN: Requisitos para sistemas que usan señales transmitidas por cables específicos para dicha función: Sin perjuicio de los requisitos que los fabricantes de nodos, actuadores o dispositivos de entrada establezcan para la instalación, cuando el circuito que transmite la señal transcurra por la misma canalización que otro de baja tensión, el nivel de aislamiento de los cables del circuito de señal será equivalente a la de los cables del circuito de baja tensión adyacente, bien en un único o en varios aislamientos. Los cables coaxiales y los pares trenzados usados en la instalación deberán cumplir con las normas de la serie EN 61.196 y CEI 60.189 -2.

Se observa que algunos preceptos legales son muy genéricos mientras que en los aspectos más concretos no se observa nada que pueda ser problemático en relación a la instalación que se va a diseñar. Simplemente se deberá prestar atención en el diseño, en particular en relación a las Instrucciones técnicas del RITE y del REBT. Por ello se considera que el cumplimiento de los requisitos legales es VIABLE.



## ANEXO 3. VERIFICACION FINAL CUMPLIMIENTO DE LOS REQUISITOS DEL SISTEMA POR LA OPCION ELEGIDA

VERIFICACION FINAL CUMPLIMIENTO DE LOS REQUISITOS DEL SISTEMA POR LA OPCION ELEGIDA			
Id	Descripción	SE CUMPLE	Observaciones
RS-1	Cada habitación será controlada de forma independiente, mediante su propio controlador ODControl	SI	Se ha comprobado que la red local puede soportar el elevado número de controladores que se deben instalar, para un hotel de hasta 100 habitaciones
RS-2	En cada habitación se controlará al menos: <ul style="list-style-type: none"> <li>iluminación</li> <li>temperatura</li> </ul>	SI	<ul style="list-style-type: none"> <li>La capacidad del ODControl lo permite.</li> <li>Se ha comprobado que la red local puede soportar el elevado número de informaciones de estados enviadas</li> </ul>
RS-3	En cada habitación se controlará adicionalmente: <ul style="list-style-type: none"> <li>motorización de persianas</li> <li>apertura de ventanas</li> <li>detección de fugas de agua</li> </ul>	SI	Mismo comentario que el requisito anterior.
RS-4	Se controlará la climatización, así como la iluminación de las zonas comunes, haciendo uso de sensores de presencia	SI	Mismo comentario que el requisito RS-2.
RS-5	Los subsistemas troncales tendrán redundancia para garantizar una alta disponibilidad. En concreto: <ul style="list-style-type: none"> <li>la red local de comunicaciones dispondrá de al menos un camino alternativo</li> <li>el puesto de control estará redundado a nivel hardware y software</li> </ul>	SI	<ul style="list-style-type: none"> <li>Las conexiones entre los switches disponen de rutas alternativas.</li> <li>Se instalan dos ordenadores en el puesto de control, en configuración de alta disponibilidad</li> </ul>
RS-6	El puesto de control dispondrá de algoritmos o consignas de control de dispositivos para ahorro energético (bajar persianas, apagar iluminación de plantas enteras, etc)	SI	El desarrollo a medida lo permite
RS-7	Existirá un puesto de mando en el que se controlarán, para cada habitación o zona común: <ul style="list-style-type: none"> <li>iluminación</li> <li>temperatura</li> <li>alarmas técnicas (las que se implementen)</li> </ul>	SI	
<b>Requisitos de cliente no recogidos en los del sistema</b>			
RC-7	En caso de fallo total del sistema informático, existirá un mecanismo alternativo para poder seguir dando servicio en las habitaciones	SI	<ul style="list-style-type: none"> <li>El ODControl puede funcionar de forma independiente.</li> <li>Alternativamente, conexión/desconexión manual de la iluminación, climatización y persianas</li> </ul>
RC-8	La red del sistema de control será segura y aislada de otros sistemas, al menos a nivel	SI	<ul style="list-style-type: none"> <li>Utilización de VLAN's</li> <li>Plan de direccionamiento IP</li> </ul>

	lógico, aunque a nivel físico, dependiendo del diseño, se podrán compartir		propio • Firewall
RC-9	Cumplimiento de las normativas legales, de distintos ámbitos, de la instalación domótica	SI	

## ANEXO 4: Cálculo del coste del desarrollo del software

Se ha utilizado el modelo COCOMO básico. Se ha considerado que el desarrollo no es complejo, por lo que se trataría, según este modelo, de un proyecto de tipo "orgánico". Los datos usados y coste obtenido son los mostrados en la siguiente hoja de cálculo:

Líneas de código (en miles)	KI =	2	miles de líneas
Salario medio mensual entre los programadores y analistas	S =	2500	euros / mes brutos
E = esfuerzo requerido en "personas * mes": $E = a*(KI)^b$	(Personas necesarias para realizar el proyecto si el plazo fuera de 1 mes)		
	E =	4,97	personas * mes
Tiempo en meses de desarrollo del proyecto ( $T_{dev}$ ) = $c*(E)^d$	Tdev =	4,60	meses
Personas necesarias para realizar el proyecto $P = E/T_{dev}$	P =	1,08	personas
<b>Coste total del proyecto (Coste) = <math>P * T_{dev} * S</math></b>	<b>Coste =</b>	<b>12423,18</b>	<b>euros</b>

MODO	a	b	c	d
Orgánico	2,4	1,05	2,5	0,38
Semilibre	3	1,12	2,5	0,35
Rígido	3,6	1,2	2,5	0,32

Nota:

En Wikipedia se encuentran definidos los tipos de proyectos de la siguiente manera (Ref: <http://es.wikipedia.org/wiki/COCOMO>):

“ cada submodelo también se divide en **modos** que representan el tipo de proyecto, y puede ser:

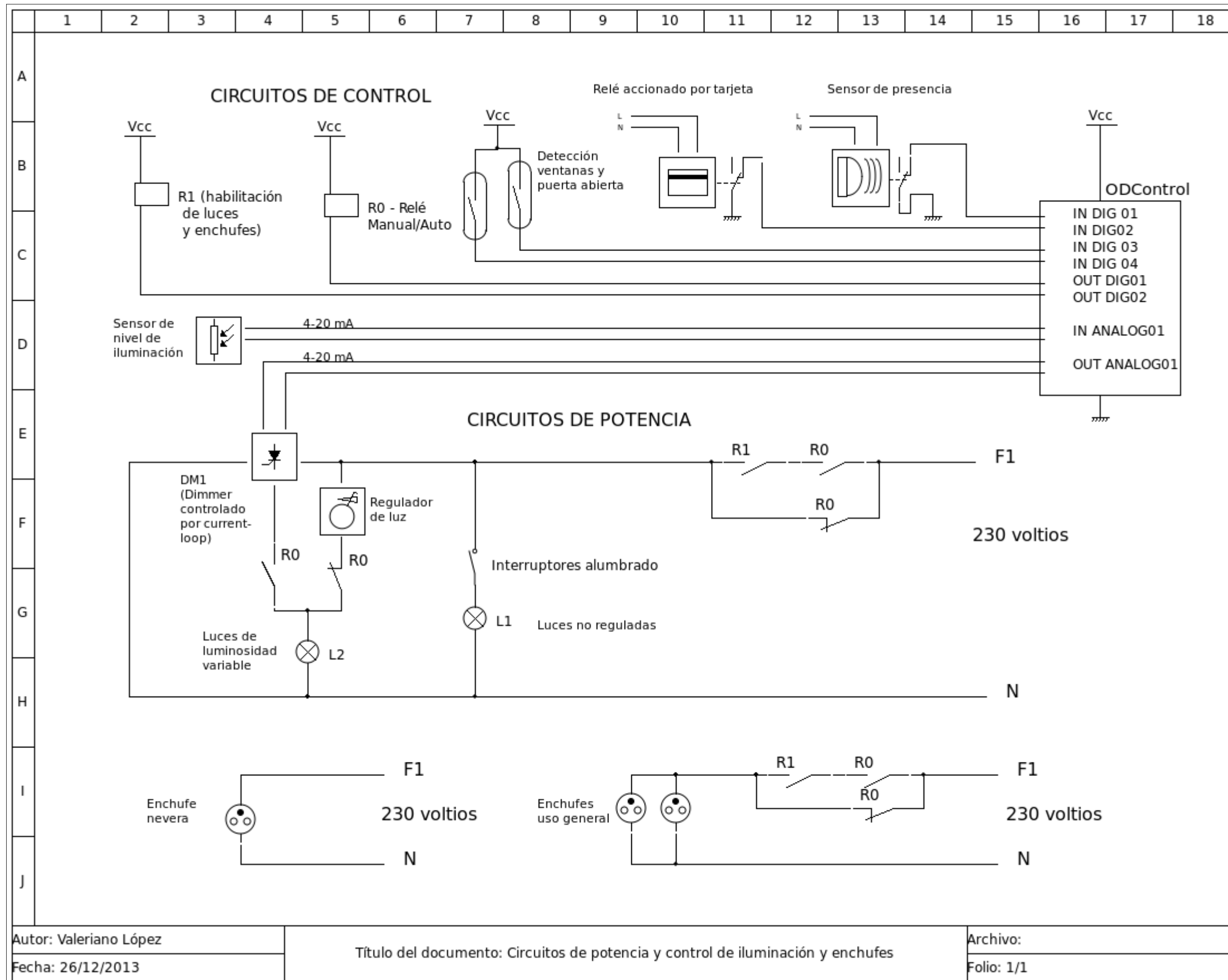
- **modo orgánico:** un pequeño grupo de programadores experimentados desarrollan software en un entorno familiar. El tamaño del software varía desde unos pocos miles de líneas (tamaño pequeño) a unas decenas de miles (medio).
- **modo semilibre o semiencajado:** corresponde a un esquema intermedio entre el orgánico y el rígido; el grupo de desarrollo puede incluir una mezcla de personas experimentadas y no experimentadas.
- **modo rígido o empotrado:** el proyecto tiene fuertes restricciones, que pueden estar relacionadas con la funcionalidad y/o pueden ser técnicas. El problema a resolver es único y es difícil basarse en la experiencia, puesto que puede no haberla. “

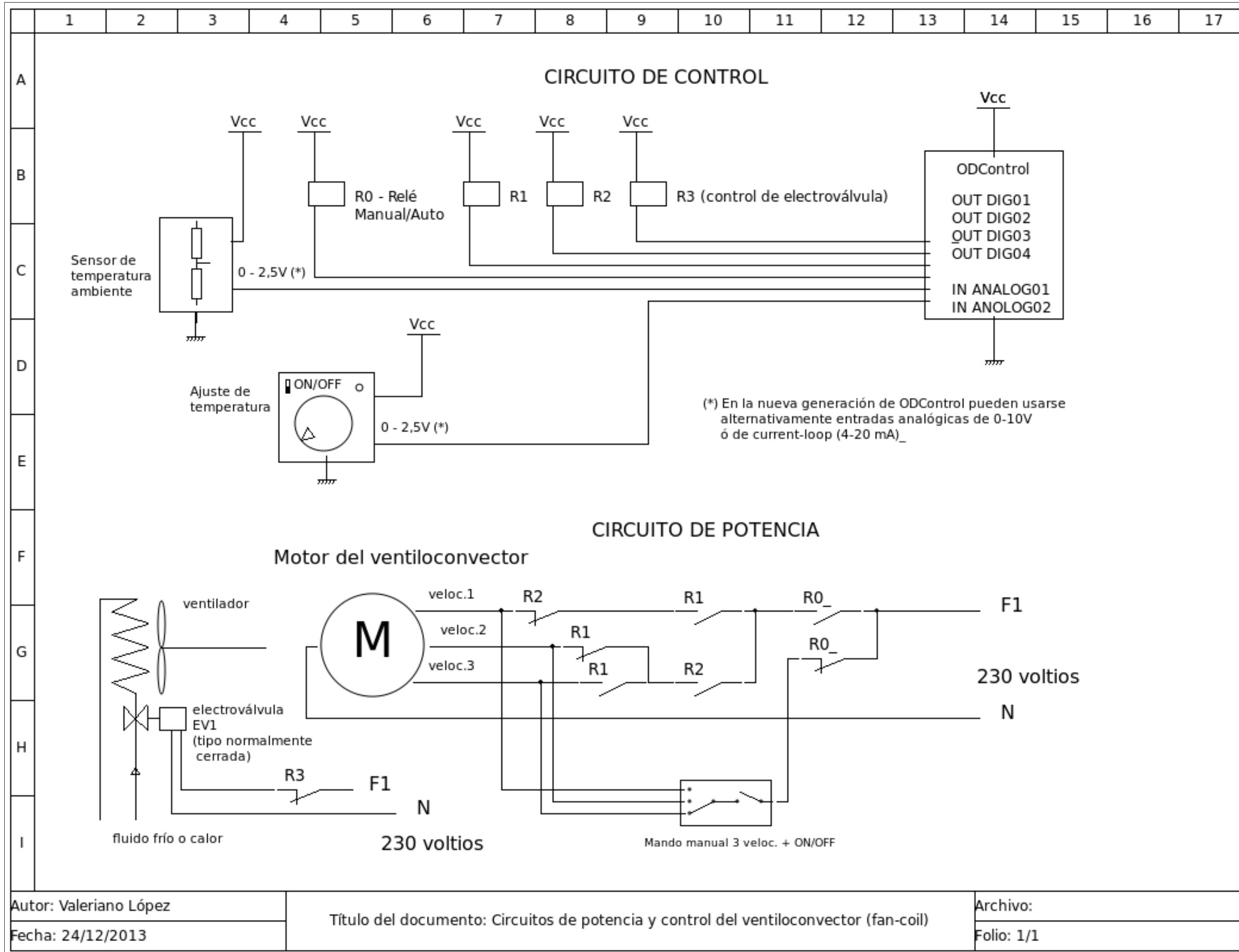
## ANEXO 5. Ejemplo de plantilla de un protocolo de pruebas, proporcionada por la Metodología Métrica 3

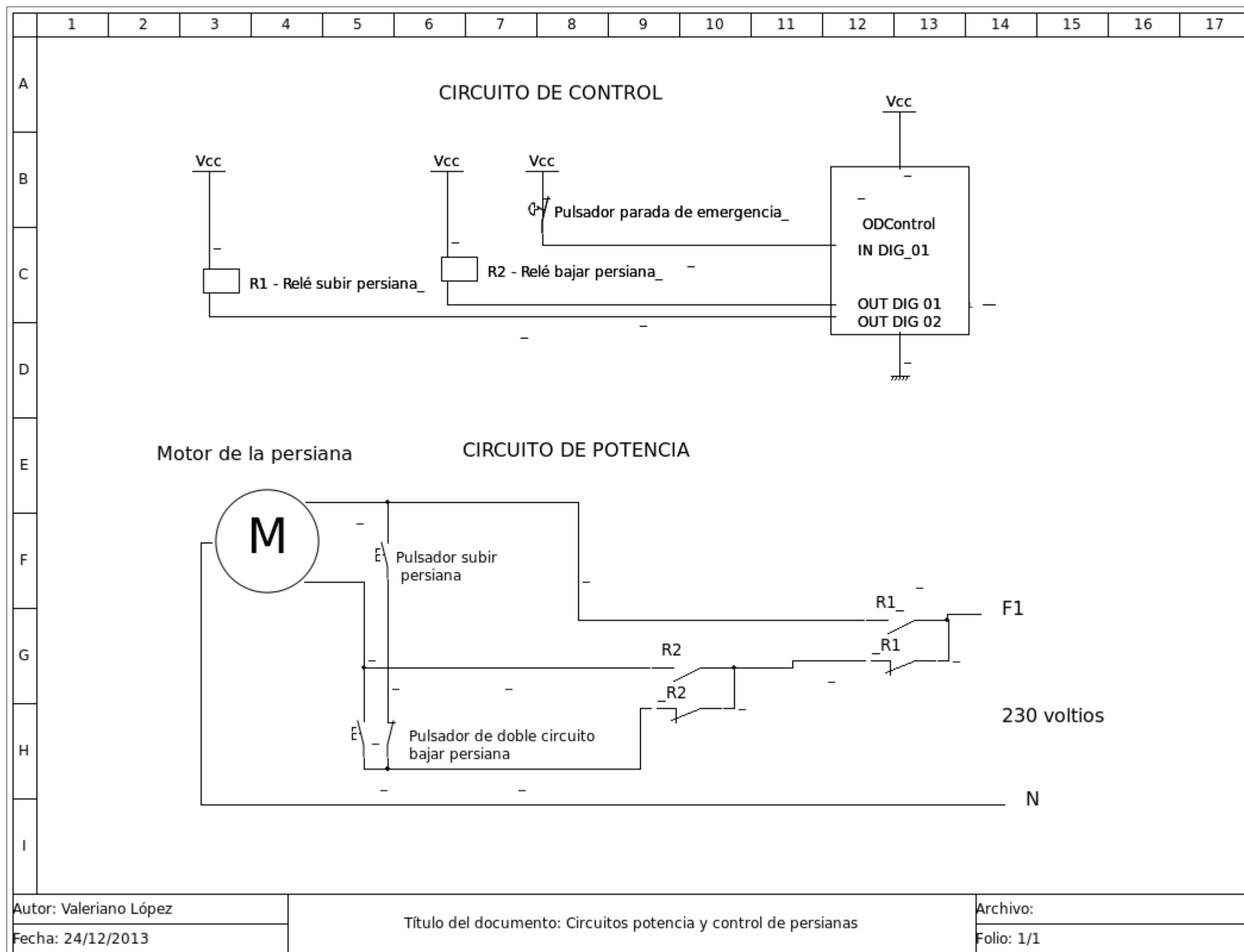
(FUENTE: Ministerio de Hacienda y Administraciones Públicas de España)

<b>PRUEBAS UNITARIAS</b>									
<b>INFORME DE PRUEBA</b>									
<b>CODIGO:</b> 001	<b>ELEMENTO DE PRUEBA:</b> <i>Clase "Búsquedas"</i>					<b>TIPO DE PRUEBA:</b> <i>Unitaria</i>			
<b>PARTICIPANTES:</b> <i>Programador</i>					<b>FECHA:</b> <i>01-10-2001</i>				
<b>DESCRIPCION</b>									
<p><i>El objetivo es comprobar el correcto funcionamiento del método "Buscar" de la clase "Búsquedas", mediante 2 casos de prueba:</i></p> <p><i>1º caso de prueba.- Comprobación de la correcta detección de ausencia de libros de un autor que no existe en la colección dentro el método Buscar de la clase Búsquedas.</i></p> <p><i>2º caso de prueba.- Comprobación de la correcta devolución de una colección de libros del autor especificado siempre y cuando el stock sea mayor que 0.</i></p>									
<b>DATOS DE ENSAYO</b>									
<i>Se han incluido en la base de datos los siguientes datos:</i>									
<u>Idbn.</u>	<u>Autor</u>	<u>Título</u>	<u>IdEdit.</u>	<u>NúmPag.</u>	<u>FechaPub.</u>	<u>Ventas</u>	<u>Precio</u>	<u>Dias</u>	<u>Stock</u>
1-1	Arturo P. Reverte	La piel del tambor	1	1500	1990	10.000	9.500	2	5
1-3	Arturo P. Reverte	El maestro de esgrima	1	250	1995	5.000	6.500	2	3
1-9	Arturo P. Reverte	Territorio comanche	1	500	1995	6.000	5.500	10	0
<b>RESULTADOS DE LA PRUEBA</b>									
<b>ESPERADOS</b>					<b>OBTENIDOS</b>				
<p><i>1º Caso de prueba:</i>                      ENTRADA: Autor = "XXXXX"                      SALIDA: "No hay libros para el autor solicitado"</p> <p><i>2º caso de prueba:</i>                      ENTRADA: Autor = "Arturo P. Reverte"                      SALIDA:                      - La piel del tambor                      - El maestro de esgrima</p>					<p><i>1º Caso de prueba:</i>                      ENTRADA: Autor = XXXXX                      SALIDA: "No hay libros para el autor solicitado"</p> <p><i>2º caso de prueba:</i>                      ENTRADA: Autor = Arturo P. Reverte                      SALIDA:                      - La piel del tambor                      - El maestro de esgrima                      - Territorio comanche</p>				
<b>INCIDENCIAS</b>									
<i>Se ha obtenido un libro cuyo stock era igual a cero. El error ha sido corregido.</i>									

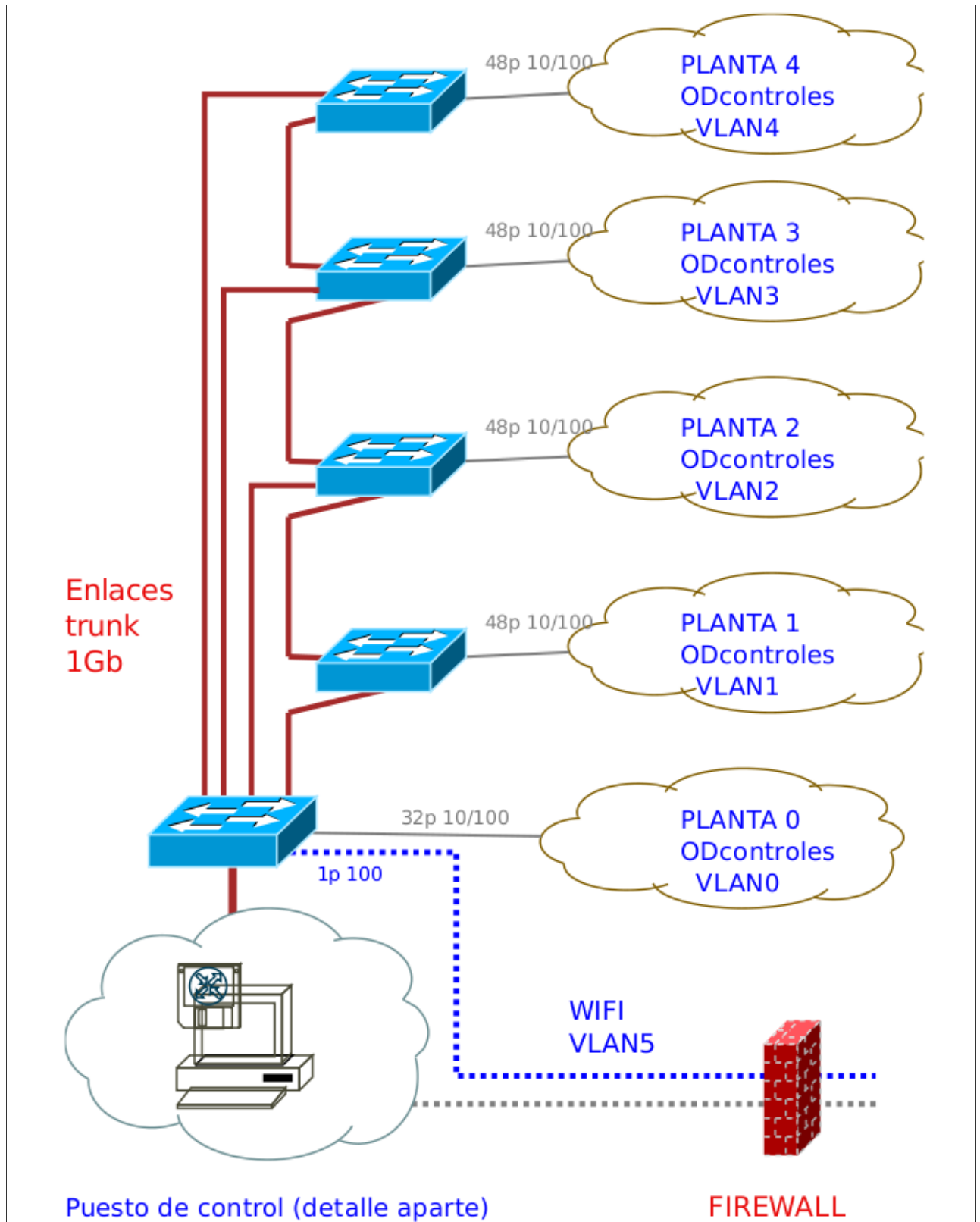
### ANEXO 6: Esquemas de principio del control de los diversos elementos domóticos mediante el controlador ODControl



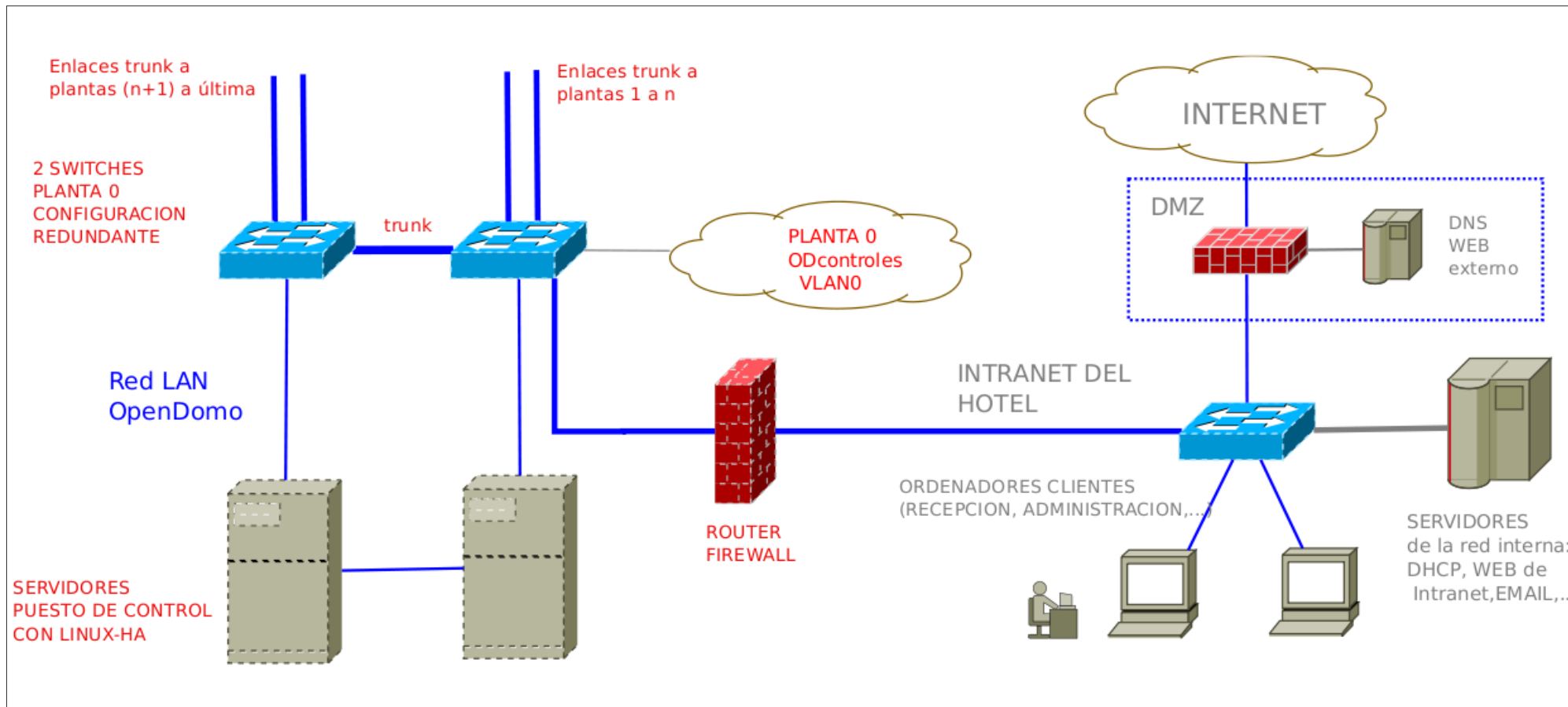




## ANEXO 7. Diagramas de despliegue del sistema







## ANEXO 8. Instalación de las aplicaciones

A continuación se detallan los comandos u operaciones a realizar para la instalación de los diferentes paquetes de software indicados en la Etapa de Diseño, para la distribución Debian Wheezy. Los paquetes en cuestión eran los siguientes:

SOFTWARE	FUNCION
Apache2	Servidor HTTP Apache V2
ntp (paquete de utilidades)	Servidor de tiempo NTP
Heartbeat	Subsistema para alta disponibilidad de Linux ((Linux-HA project)
Unison	Sincronización de réplicas de la BD
OpenSSH	Para administración remota del servidor y sincronización remota de las BD con Unison
Nmap ("Network Mapper")	Exploración de red y auditoría de seguridad
Nessus	Escáner de vulnerabilidades
ClamAV	Antivirus
IPtables	Firewall
vlan	paquete para habilitar VLAN's a interface de red
MySQL	Gestor de base de datos (varios paquetes: servidor, cliente, interfaces gráficas,...)

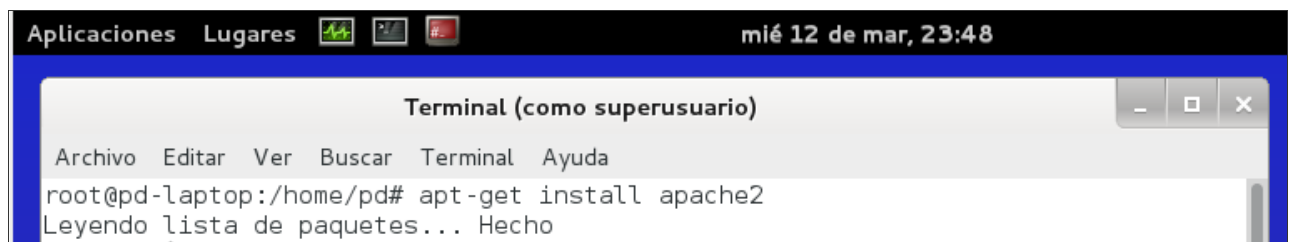
Las aplicaciones deben instalarse en ambos servidores de control, así como las que correspondan en el router-firewall.

La instalación puede realizarse mediante distintas herramientas, ya sea gráficas (como el gestor de paquetes Synaptic) o de consola, como por ejemplo el comando "apt" cuando el software está disponible en los repositorios de Debian Wheezy. Si no es el caso, otro sistema es mediante la descarga de un paquete ".deb" desde la página web del desarrollador del software (es así por ejemplo para instalar Nessus).

*Observación previa : todas las instalaciones mediante consola las debemos realizar como usuario "root"*

- **Instalación del Servidor HTTP Apache V2**

Lo podemos instalar mediante el comando **apt-get install apache2**, tal como se muestra en la consola de la siguiente imagen:



- **Instalación del Servidor de tiempo NTP**

De forma análoga al caso anterior, mediante el comando **apt-get install ntp** :

```
root@pd-laptop:/home/pd# apt-get install ntp
Leyendo lista de paquetes... Hecho
```

- **Instalación de Unison (sincronización de réplicas de la base de datos)**

Comando: **apt-get install unison**

```
Terminal (como superusuario)
Archivo Editar Ver Buscar Terminal Ayuda
root@pd-laptop:/home/pd# apt-get install unison
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

- **Instalación de OpenSSH**

Se divide en varios paquetes según su función. En este caso instalaremos el servidor ssh, pero también el cliente, que ya suele venir instalado por defecto, por si es necesaria una conexión con otro servidor SSH. Ambos paquetes se instalan con comandos distintos, que son:

Para el servidor: **apt-get install openssh-server**

```
Terminal (como superusuario)
Archivo Editar Ver Buscar Terminal Ayuda
root@pd-laptop:/home/pd# apt-get install openssh-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

Para el cliente: **apt-get install openssh-client**

```
Terminal (como superusuario)
Archivo Editar Ver Buscar Terminal Ayuda
root@pd-laptop:/home/pd# apt-get install openssh-client
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
openssh-client ya está en su versión más reciente.
```

- **Instalación de Nmap**

Comando: **apt-get install Nmap**

```

Terminal (como superusuario)
Archivo Editar Ver Buscar Terminal Ayuda
root@pd-laptop:/home/pd# apt-get install nmap
Leyendo lista de paquetes... Hecho
    
```

- **Instalación del antivirus clamav**

Se pueden instalar varios paquetes con funciones diferentes:

- clamav : es la interface para consola del antivirus
- clamav-docs : paquete que contiene documentación del antivirus
- clamav-daemon : es el daemon para escaneo de archivos
- clamav-freshclam : es un daemon para la actualización de firmas de virus
- clamtk : es una interface gráfica de configuración del antivirus

Comando: **apt-get install clamav clamav-docs clamav-daemon \ clamav-freshclam clamtk**

```

Terminal (como superusuario)
Archivo Editar Ver Buscar Terminal Ayuda
root@pd-laptop:/home/pd# apt-get install clamav clamav-docs clamav-daemon clamav
-freshclam clamtk
Leyendo lista de paquetes... Hecho
    
```

- **Instalación de IPTables**

Comando: **apt-get install iptables**

```

Terminal (como superusuario)
Archivo Editar Ver Buscar Terminal Ayuda
root@pd-laptop:/home/pd# apt-get install iptables
Leyendo lista de paquetes... Hecho
    
```

- **Instalación de vlan**

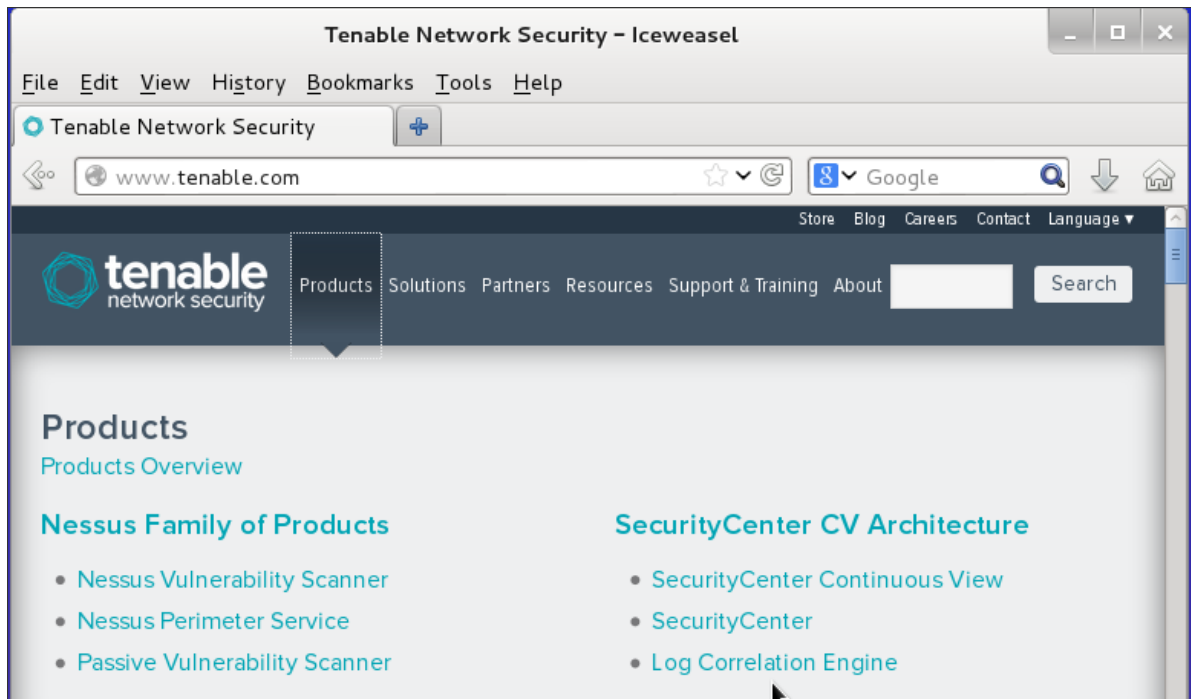
Comando: **apt-get install vlan**

- **Instalación de MySQL**

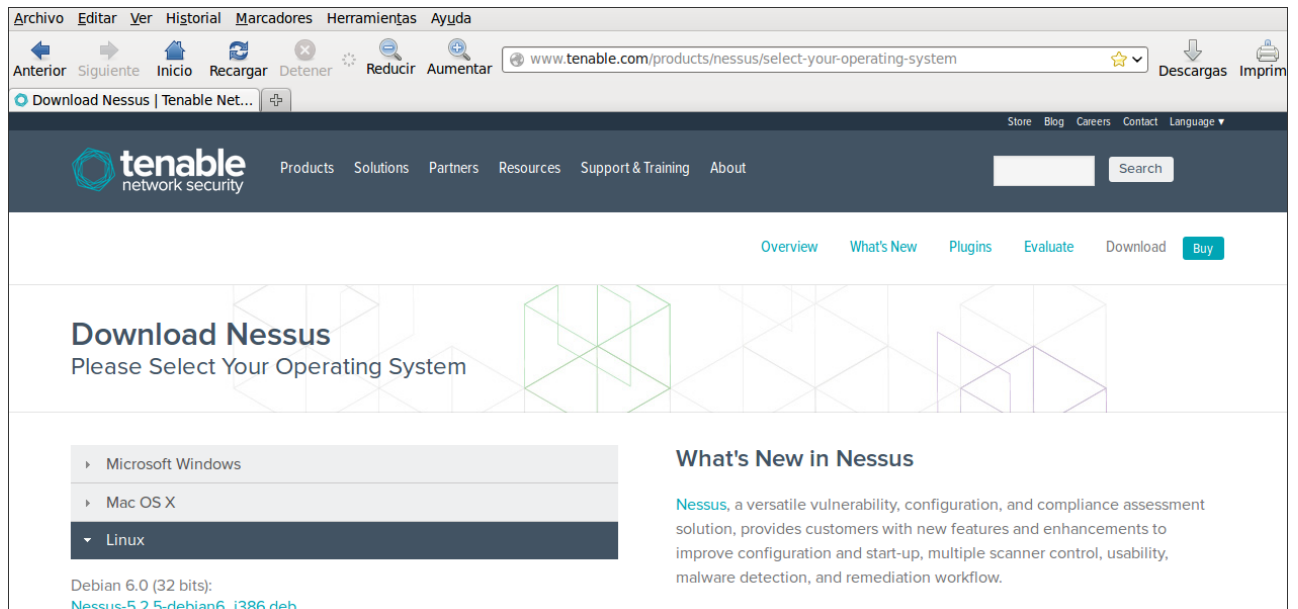
Comando: **apt-get install mysql-server mysql-client**

○ **Instalación de NNESSUS**

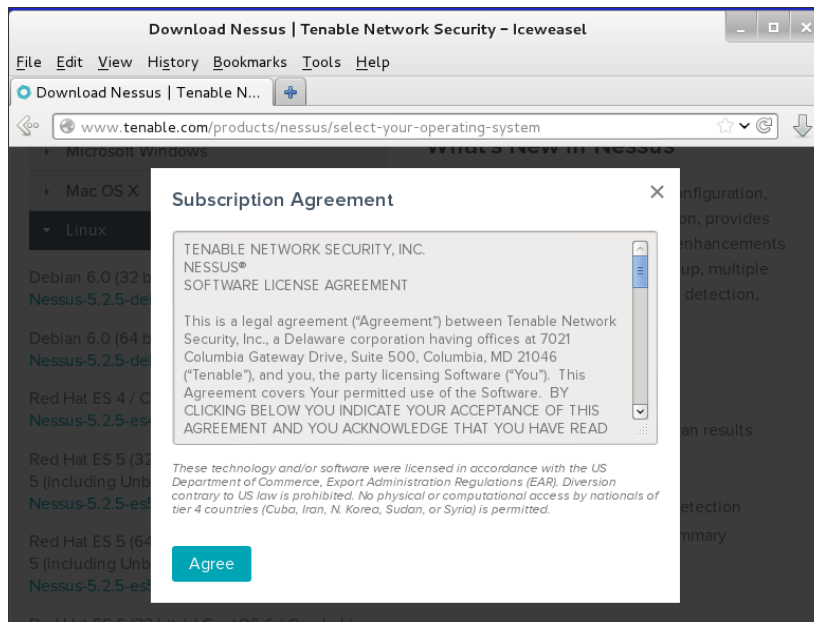
Este es el paquete más complejo de instalar, ya que no se encuentra en los repositorios Debian y lo deberemos descargar desde la página web de Tenable ([www.tenable.com](http://www.tenable.com)):



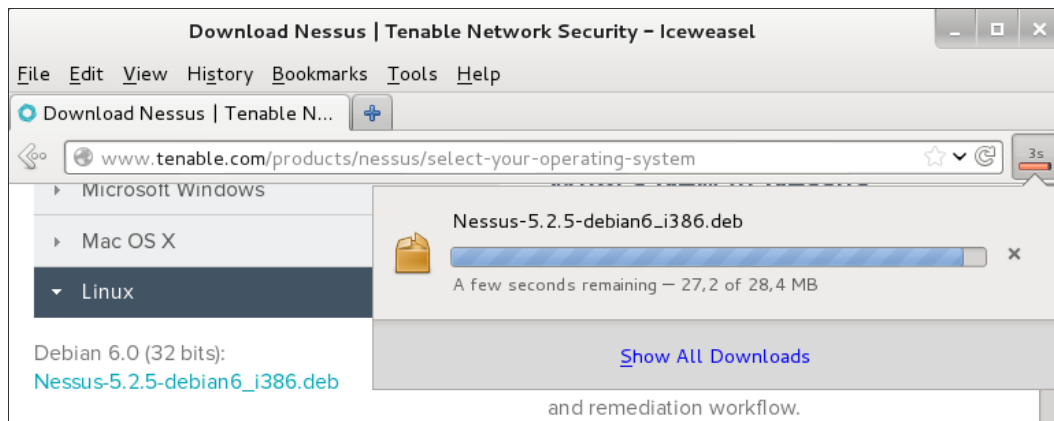
Luego en la opción “Products”, clicamos en “Nessus Vulnerability Scanner”, lo cual nos dirige a la página de descarga según sistema operativo (<http://www.tenable.com/products/nessus/select-your-operating-system> )



Seleccionamos el sistema operativo y la distribución y aceptamos el acuerdo de suscripción:



Con lo que ya podremos realizar la descarga del paquete .deb que contiene el software de Nessus:



Una vez completada la descarga, hacemos click con el ratón sobre el paquete .deb descargado y el sistema realiza su instalación. No obstante en esta etapa aún no es utilizable, ya que debemos introducir un código de activación y crear al menos un usuario de Nessus, con perfil administrador. Para obtener el código de activación nos dirigimos de nuevo a la página web de Tenable, a la dirección:

<http://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code>

y rellenamos los datos que nos solicita, entre ellos una dirección de email en la que recibiremos el código:

**De:** Nessus Registration <noreply@nessus.org>  
**Para:** mi@mail.com  
**Asunto:** Tenable Nessus Home Activation Code  
**Fecha:** 16/03/14 20:55:21

(.....)  
 Your activation code for the Nessus Home is  
 26CD-6E39-067F-3891-E2FF  
 (.....)

La activación del programa se realiza mediante la línea de comandos, en el directorio **/opt/nessus/bin**, mediante el comando **nessus-fetch** y el parámetro **--register** seguido del código de activación, como sigue:

```

Terminal (como superusuario)
Archivo Editar Ver Buscar Terminal Ayuda
root@pd-laptop:/opt/nessus/bin# ./nessus-fetch --register 26CD-6E39-067F-3891-E2FF
Your Activation Code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...
Your Nessus installation is now up-to-date.
If auto_update is set to 'yes' in nessusd.conf, Nessus will
update the plugins by itself.
root@pd-laptop:/opt/nessus/bin#

```

Ahora creamos el usuario con perfil administrador de Nessus. Para ello primero cambiamos al directorio **/opt/nessus/sbin** y ejecutamos el comando **nessus-adduser**, completando diversas opciones que se van mostrando, y ejecutando finalmente el servidor de Nessus (nessusd) mediante el comando **/etc/init.d/nessusd start**, tal como se muestra en las siguientes capturas de pantalla:

```

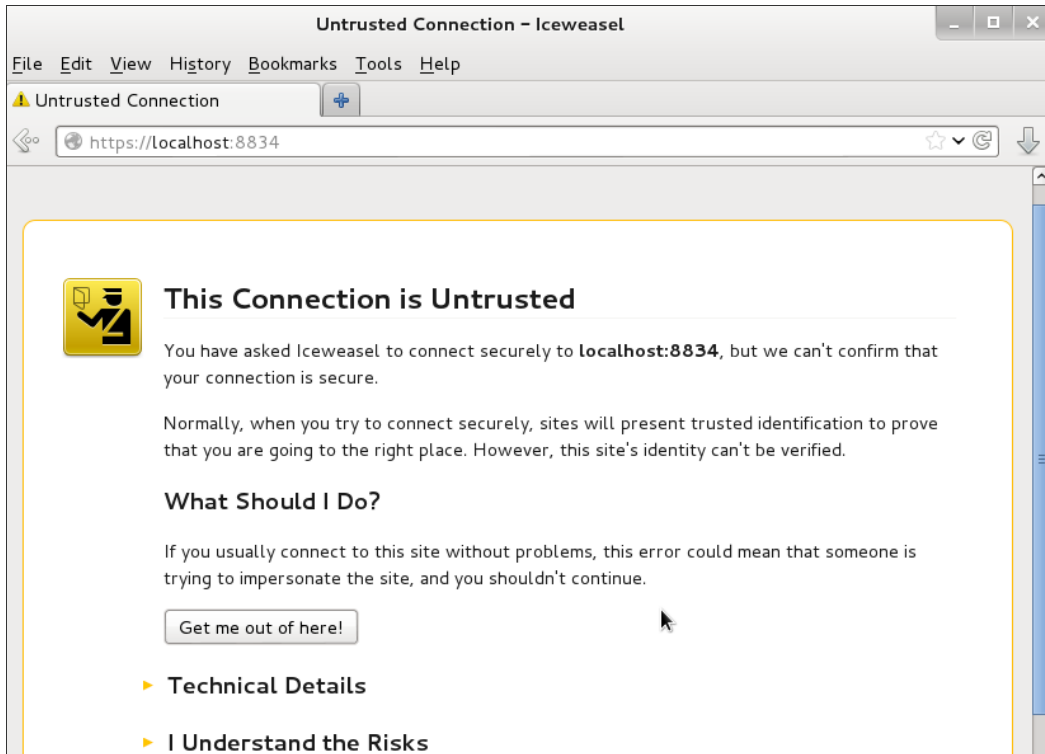
Terminal (como superusuario)
Archivo Editar Ver Buscar Terminal Ayuda
root@pd-laptop:/opt/nessus/bin# cd /opt/nessus/sbin
root@pd-laptop:/opt/nessus/sbin# ls
nessus-adduser      nessus-chpasswd    nessus-mkcert      nessus-service
nessus-admin        nessusd            nessus-mkcert-client  nessus-update-plugins
nessus-check-signature  nessus-fix        nessus-rmuser
root@pd-laptop:/opt/nessus/sbin# ./nessus-adduser
Login : TFM-vale
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc...) (y/n)
[n]: y
User rules
-----
nessusd has a rules system which allows you to restrict the hosts
that TFM-vale has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

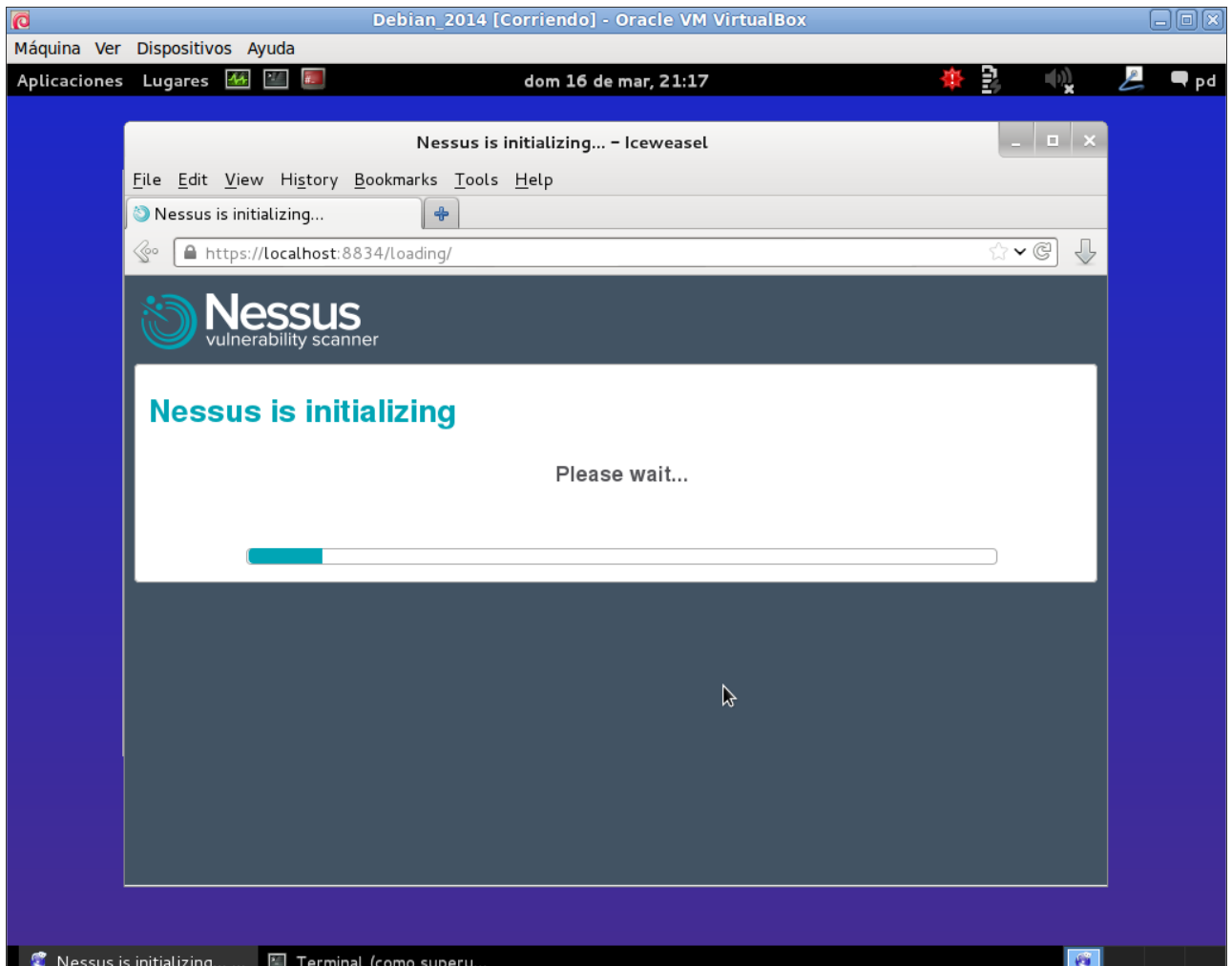
Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)

```

El servidor ya está corriendo, aunque la instalación aún no está concluida. Para completarla debemos conectarnos al servidor mediante una interface web, en el puerto 8834. Localmente podemos conectarnos en la url **https://localhost:8834**. Al conectarnos el navegador indicará que la conexión no es confiable; no obstante podemos hacer una excepción de seguridad dado que estamos seguros de la identidad del servidor:

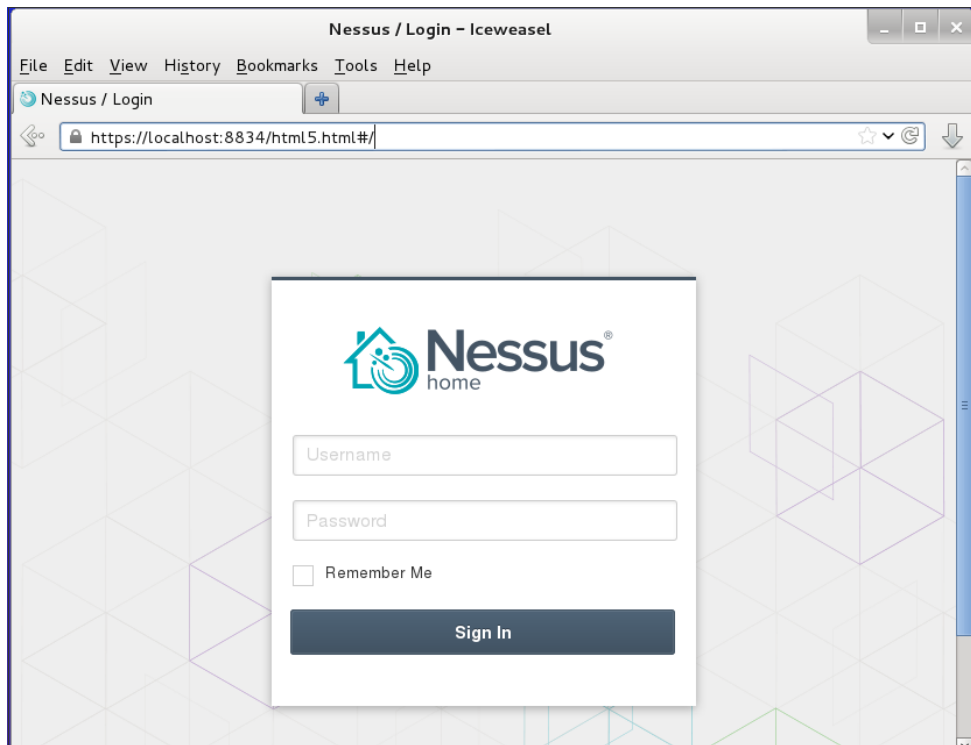


A continuación Nessus empieza a inicializarse, tardando bastante tiempo en completar esta operación:

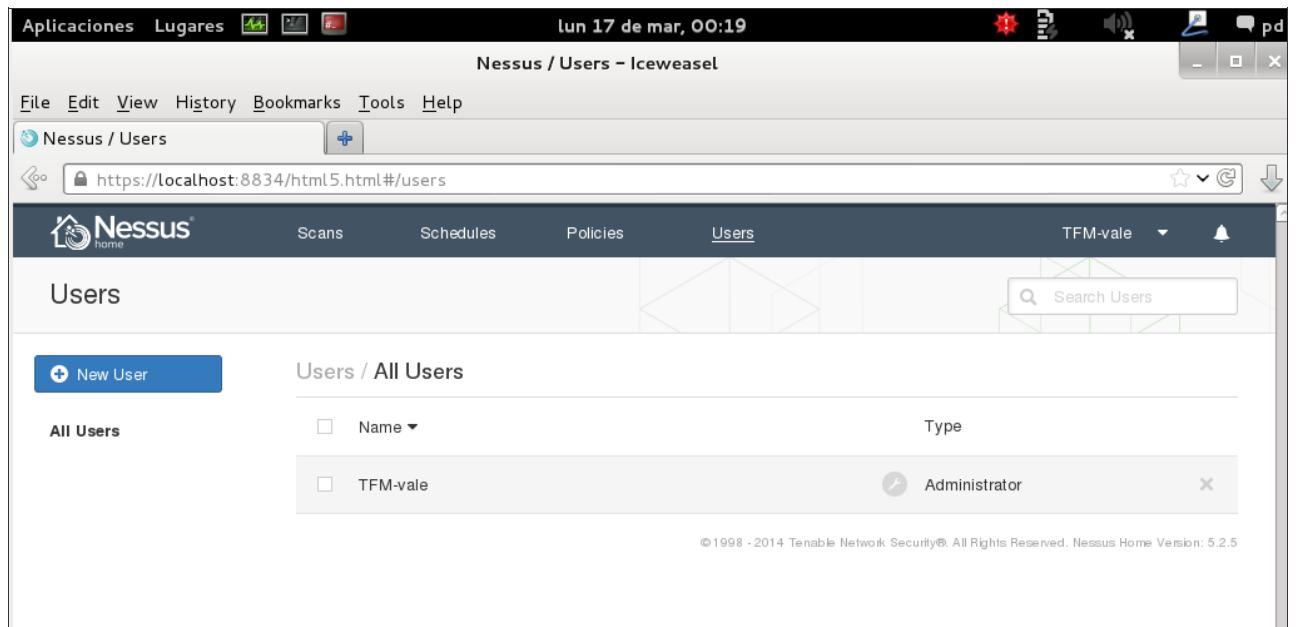




Una vez finalizada la inicialización de Nessus, nos aparecerá una pantalla de login:



Con el usuario que habíamos creado (TFM-vale) y su contraseña, ya podremos entrar en la aplicación y podremos empezar a realizar auditorías de seguridad mediante las distintas opciones disponibles:



## ANEXO 9. Configuración de red en los servidores y el router-firewall

En ambos casos la configuración es la propia de las distribuciones Debian.

- **Datos previos**

Recordemos previamente el plan de direccionamiento resumido, definido en la Fase de Diseño:

Equipos	Dirección IP			Máscara
Servidor Control (mínimo una IP por cada VLAN, implementada con interfaces virtuales)	192.168.	0 1 nn	2-3-4 2 2	255.255.255.0
ODControles Planta 0 (VLAN_0)	192.168.	0	5-254	255.255.255.0
ODControles Planta 1 (VLAN_1)	192.168.	1	3-254	255.255.255.0
ODControles Planta n (VLAN_n)	192.168.	nn	3-254	255.255.255.0
Administración switches (VLAN_ADM)	10.115.	0	2-20	255.255.255.0
WIFI, u otros sistemas (VLAN_x)	10.115.	xx	2-254	255.255.255.0
Router-firewall (una IP , con interfaces virtuales, por cada VLAN que reciba)	192.168. 10.115. 10.115.	0 0 x	1 1 1	255.255.255.0

A partir de él asignamos las siguientes IP's a cada interface de red:

DATOS PREVIOS				
Direcciones IP	Interfaces de red	Tipo interface	IP	Observaciones
ROUTER - FIREWALL	<b>eth0</b>	<b>física</b>		lado red ODControles
	VLAN_0	lógica	192.168.0.1	Red ODControles planta 0
	VLAN_ADM	lógica	10.115.0.1	Administración de switches
	VLAN_99	lógica	10.115.99.1	Red clientes WIFI
	<b>eth1</b>	<b>física</b>	10.30.0.20	lado Intranet del hotel
SERVIDOR CONTROL 1	<b>eth0</b>	<b>física</b>	192.168.0.3 192.168.0.2	La IP 192.168.0.2 es la común para ambos servidores, gestionada por Heartbeat
	VLAN_0	lógica	192.168.0.3	Red ODControles planta 0
	VLAN_1	lógica	192.168.1.2	Red ODControles planta 1
	VLAN_2	lógica	192.168.2.2	Red ODControles planta 2
	VLAN_3	lógica	192.168.3.2	Red ODControles planta 3
	<b>eth1</b>	<b>física</b>	192.168.100.1	interface dedicada para detectar SERVIDOR 2 operativo con Heartbeat
SERVIDOR CONTROL 2	<b>eth0</b>	<b>física</b>	192.168.0.4 192.168.0.2	La IP 192.168.0.2 es la común para ambos

				servidores, gestionada por Heartbeat
	VLAN_0	lógica	192.168.0.4	Red ODControles planta 0
	VLAN_1	lógica	192.168.1.2	Red ODControles planta 1
	VLAN_2	lógica	192.168.2.2	Red ODControles planta 2
	VLAN_3	lógica	192.168.3.2	Red ODControles planta 3
	<b>eth1</b>	<b>física</b>	192.168.100.2	interface dedicada para detectar SERVIDOR 1 operativo con Heartbeat

Se observa que el router-firewall, por seguridad, solo da acceso a la VLAN de los servidores de control, pero no a las diferentes VLAN de los ODControles. De esta manera no se puede acceder directamente a los puertos de configuración de los ODControl desde algún cliente de la Intranet.

- **Configuraciones de red de cada máquina**

Se detallan las configuraciones definidas en el fichero ***/etc/network/interfaces*** de cada máquina:

```

ROUTER - FIREWALL: fichero /etc/network/interfaces

auto lo eth0 eth1
iface lo inet loopback

# INTERFAZ eth0 VLAN 802.1Q (TRUNK)
iface eth0 inet manual

# Interfaz VLAN_0 - Red ODControles planta 0
auto VLAN_0
iface VLAN_0 inet static
address 192.168.0.1
netmask 255.255.255.0
broadcast 192.168.0.255
vlan_raw_device eth0

# Interfaz VLAN_ADM - Administración de switches
auto VLAN_ADM
iface VLAN_ADM inet static
address 10.115.0.1
netmask 255.255.255.0
vlan_raw_device eth0

# Interfaz VLAN_99 - Red clientes WIFI
auto VLAN_99
iface VLAN_99 inet static
address 10.115.99.1
netmask 255.255.255.0
vlan_raw_device eth0

# Interfaz eth1 - lado Intranet del hotel
iface eth1 inet static
address 10.30.0.20
netmask 255.255.255.0

pre-up iptables-restore < /etc/iptables.rules

```

**SERVIDOR DE CONTROL 1:** fichero /etc/network/interfaces

```

auto lo eth0 eth1
iface lo inet loopback

# INTERFAZ eth0 VLAN 802.1Q (TRUNK)
iface eth0 inet manual

    # Interfaz VLAN_0 - Red ODControles planta 0
    auto VLAN_0
    iface VLAN_0 inet static
    address 192.168.0.3
    netmask 255.255.255.0
    broadcast 192.168.0.255
    gateway 192.168.0.1
    vlan_raw_device eth0

    # Interfaz VLAN_1 - Red ODControles planta 1
    auto VLAN_1
    iface VLAN_1 inet static
    address 192.168.1.2
    netmask 255.255.255.0
    vlan_raw_device eth0

    # Interfaz VLAN_2 - Red ODControles planta 2
    auto VLAN_2
    iface VLAN_2 inet static
    address 192.168.2.2
    netmask 255.255.255.0
    vlan_raw_device eth0

    # Interfaz VLAN_3 - Red ODControles planta 3
    auto VLAN_3
    iface VLAN_3 inet static
    address 192.168.3.2
    netmask 255.255.255.0
    vlan_raw_device eth0

# Interfaz eth1 - Heartbeat
iface eth1 inet static
address 192.168.100.1
netmask 255.255.255.0

```

**pre-up iptables-restore < /etc/iptables.rules**

**SERVIDOR DE CONTROL 2:** fichero /etc/network/interfaces

```

auto lo eth0 eth1
iface lo inet loopback

# INTERFAZ eth0 VLAN 802.1Q (TRUNK)
iface eth0 inet manual

# Interfaz VLAN_0 - Red ODControles planta 0
auto VLAN_0
iface VLAN_0 inet static
address 192.168.0.4
netmask 255.255.255.0
broadcast 192.168.0.255
gateway 192.168.0.1

```

```

vlan_raw_device eth0

# Interfaz VLAN_1 - Red ODControles planta 1
auto VLAN_1
iface VLAN_1 inet static
address 192.168.1.2
netmask 255.255.255.0
vlan_raw_device eth0

# Interfaz VLAN_2 - Red ODControles planta 2
auto VLAN_2
iface VLAN_2 inet static
address 192.168.2.2
netmask 255.255.255.0
vlan_raw_device eth0

# Interfaz VLAN_3 - Red ODControles planta 3
auto VLAN_3
iface VLAN_3 inet static
address 192.168.3.2
netmask 255.255.255.0
vlan_raw_device eth0

# Interfaz eth1 - Heartbeat
iface eth1 inet static
address 192.168.100.2
netmask 255.255.255.0

pre-up iptables-restore < /etc/iptables.rules

```

La línea “**pre-up iptables-restore < /etc/iptables.rules**” realiza la carga de las reglas IPTables del firewall en cada equipo.

## ANEXO 10. Implementación de reglas de firewall's mediante IPTables

- Reglas para los Servidores de control

- Enrutado interno hacia las VLAN

En la configuración de las interfaces de red se definieron varias VLAN. En la siguiente tabla se aprecia con más claridad las interfaces de salida correspondientes para los paquetes de cada subred:

Destino	Pasarela	Genmask	Interfaz	Comentarios
192.168.0.0	*	255.255.255.0	VLAN_0	Hacia los ODControl de la VLAN 0
192.168.1.0	*	255.255.255.0	VLAN_1	Hacia los ODControl de la VLAN 1
192.168.2.0	*	255.255.255.0	VLAN_2	Hacia los ODControl de la VLAN 2
192.168.3.0	*	255.255.255.0	VLAN_3	Hacia los ODControl de la VLAN 3
default	192.168.0.1	0.0.0.0	VLAN_0	Hacia el router-firewall

- Función de filtrado de paquetes (firewall)

En la Etapa de Diseño se definieron las siguientes reglas para el firewall:

FIREWALL DE SERVIDOR							
TRAFICO ENTRANTE							
REGLA	ACCION	ORIGEN	PUERTO ORIGEN	DESTINO	PUERTO DESTINO	PROTOC.	DESCRIPCION
1	permite	192.168.x.x	*	*	1729	*	Recepción de estados ODControl
2	permite	192.168.x.x	*	*	123	UDP	NTP
3	permite	192.168.0.0	*	*	9122	TCP	Sincronización de réplica de la BD
4	permite	*	*	*	22	TCP	SSH, para uso de administrador
5	permite	10.30.0.0	*	*	80	TCP	Servidor web Apache (http)
6	permite	10.30.0.0	*	*	443	TCP	Servidor web Apache (https)
7	permite	10.30.0.10	*	*	3306	TCP	conexión a MySQL desde Gestor de Reservas (IP=10.30.0.10)
8	rechaza	*	*	*	*	*	RECHAZA las demás conexiones
TRAFICO SALIENTE							
REGLA	ACCION	ORIGEN	PUERTO ORIGEN	DESTINO	PUERTO DESTINO	PROTOC.	DESCRIPCION
9	permite	*	*	192.168.x.x	1729	TCP	envío de comandos a ODControl
10	permite	*	*	192.168.x.x	123	UDP	NTP
11	permite	*	*	192.168.x.x	81	TCP	envío de comandos a ODControl por http (*)
12	permite	*	*	192.168.x.x	80	TCP	GUI web del ODControl (nota 1) Nota 1: disponible para tareas de administración
13	permite	*	*	(IP DNS)	53	*	Consulta DNS de los servidores

							de control
14	permite	*	*	192.168.0.0	9122	TCP	Sincronización de réplica de la BD
15	permite	*	*	10.115.0.0	80	TCP	Admin. switches interface web
16	rechaza	*	*	*	*	*	RECHAZA las demás conexiones

### • Implementación del firewall con IPTables

Una implementación mediante IPTables puede ser la siguiente (válida para ambos servidores):

```
#!/bin/bash
```

```
# INICIALIZACION DEL FIREWALL-BORRAR REGLAS PREEXISTENTES
```

```
iptables -F # borrar reglas de la tabla FILTER (tabla por defecto si no se indica "-t")
```

```
iptables -t nat -F # borrar reglas de la tabla NAT
```

```
iptables -X # borrar cadenas de usuario
```

```
iptables -Z # poner a cero los contadores de paquetes
```

```
## Establecemos política por defecto en DROP (descartar paquetes/datagramas silenciosamente)
```

```
# para entradas (INPUT), salidas (OUTPUT) y reenvíos (FORWARD)
```

```
iptables -P INPUT DROP
```

```
iptables -P OUTPUT DROP
```

```
iptables -P FORWARD DROP
```

```
## SNAT DE SALIDAS hacia ODControls. PONE COMO IP de ORIGEN LA IP COMUN 192.168.0.2
```

```
## dado que Heartbeat solo dispondrá una IP común del clúster (192.168.0.2). Los ODControls
```

```
## de cualquier VLAN siempre responderán a la IP común del clúster
```

```
iptables -t nat -A POSTROUTING -s 192.168.0.3 -o VLAN_0 -j SNAT --to 192.168.0.2 # para servidor 1
```

```
iptables -t nat -A POSTROUTING -s 192.168.0.4 -o VLAN_0 -j SNAT --to 192.168.0.2 # para servidor 2
```

```
iptables -t nat -A POSTROUTING -s 192.168.1.2 -o VLAN_1 -j SNAT --to 192.168.0.2
```

```
iptables -t nat -A POSTROUTING -s 192.168.2.2 -o VLAN_2 -j SNAT --to 192.168.0.2
```

```
iptables -t nat -A POSTROUTING -s 192.168.3.2 -o VLAN_3 -j SNAT --to 192.168.0.2
```

```
### ACCESO LOCAL AL EQUIPO
```

```
# Permitimos todo en la interfaz localhost (entrada y salida)
```

```
iptables -A INPUT -i lo -j ACCEPT
```

```
iptables -A OUTPUT -o lo -j ACCEPT
```

```
#### PERMITIR RESPONDER A CONEXIONES PREVIAS RELATIVAS O ESTABLECIDAS
```

```
#### SOLO SE PUEDEN TRASPASAR PUERTOS EN "DROP" COMO RESPUESTA
```

```
#### A CONEXIONES RECIBIDAS O SI LA NUEVA CONEXIÓN ESTA RELACIONADA
```

```
## PERMITIR RESPONDER A CONEXIONES ENTRANTES
```

```
iptables -A OUTPUT -p tcp -m tcp --sport 1729 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p udp -m udp --sport 1729 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p udp -m udp --sport 123 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p tcp -m tcp --sport 9122 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p tcp -m tcp --sport 22 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p tcp -m tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p tcp -m tcp --sport 443 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p tcp -m tcp --sport 3306 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
## PERMITIR LAS RESPUESTAS A LAS CONEXIONES SALIENTES
```

```
iptables -A INPUT -p tcp -m tcp --sport 1729 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A INPUT -p udp -m udp --sport 123 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A INPUT -p tcp -m tcp --sport 81 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A INPUT -p tcp -m tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -m tcp --sport 53 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp -m udp --sport 53 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -m tcp --sport 9122 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
#####TRAFICO ENTRANTE#####
iptables -A INPUT -s 192.168.0.0/16 -p tcp --dport 1729 -j ACCEPT # Rx estados ODControl
iptables -A INPUT -s 192.168.0.0/16 -p udp --dport 1729 -j ACCEPT # Rx estados ODControl
iptables -A INPUT -s 192.168.0.0/16 -p udp --dport 123 -j ACCEPT # NTP
iptables -A INPUT -s 192.168.0.0/24 -p tcp --dport 9122 -j ACCEPT # Unison
iptables -A INPUT -p tcp --dport 22 -j ACCEPT # SSH
iptables -A INPUT -s 10.30.0.0/16 -p tcp --dport 80 -j ACCEPT # Servidor web Apache -http
iptables -A INPUT -s 10.30.0.0/16 -p tcp --dport 443 -j ACCEPT # Servidor web Apache -https
iptables -A INPUT -s 10.30.0.10 -p tcp --dport 3306 -j ACCEPT # Conexión a MySQL desde 10.30.0.10

#####TRAFICO SALIENTE #####
iptables -A OUTPUT -d 192.168.0.0/16 -p tcp --dport 1729 -j ACCEPT # Comandos a ODControl
iptables -A OUTPUT -d 192.168.0.0/16 -p udp --dport 123 -j ACCEPT # NTP
iptables -A OUTPUT -d 192.168.0.0/16 -p tcp --dport 81 -j ACCEPT # Comandos HTTP a ODControl
iptables -A OUTPUT -d 192.168.0.0/16 -p tcp --dport 80 -j ACCEPT # GUI del ODControl
iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT ## acceso a DNS
iptables -A OUTPUT -p udp --dport 53 -j ACCEPT ## acceso a DNS
iptables -A OUTPUT -d 192.168.0.0/24 -p tcp --dport 9122 -j ACCEPT # Unison
iptables -A OUTPUT -d 10.115.0.0/16 -p tcp --dport 80 -j ACCEPT # GUI admin. switches
### si el paquete no ha cumplido ninguna de las reglas anteriores, será DESCARTADO
### silenciosamente, dado que la POLITICA POR DEFECTO ES DROP
```

### ▪ Carga y almacenamiento persistente de las reglas de IPtables

Las reglas anteriores las editamos directamente sobre un fichero de texto, que posteriormente ejecutaremos como script. Si por ejemplo le damos el nombre “reglasIPtables.sh” y lo ejecutamos en la consola de comandos, las reglas incluidas en el fichero se cargarán en el núcleo del sistema operativo:

```
# ./reglasIPtables.sh
```

A continuación, se ejecuta el comando iptables-save, que permite guardar en el fichero /etc/iptables.rules las nuevas reglas cargadas en el kernel del sistema:

```
# iptables-save > /etc/iptables.rules
```

Luego es preciso incluir la siguiente línea en el fichero de configuración de red /etc/network/interfaces, para que las reglas de IPtables contenidas en el fichero /etc/iptables.rules se carguen automáticamente en el kernel en cada inicio del sistema:

```
pre-up iptables-restore < /etc/iptables.rules
```

Este procedimiento será aplicable también para el router-firewall.



○ Reglas para el Router-firewall

▪ Función de enrutado. Tabla de rutas del router-firewall

Antes de filtrar los paquetes con IPtables, se realiza el enrutado de los mismos. Para ello es preciso definir la tabla de rutas, que en este caso puede ser una tabla estática como la siguiente:

Destino	Pasarela	Genmask	Interfaz	Comentarios
10.30.0.0	*	255.255.255.0	eth1	Hacia la Intranet del hotel
192.168.0.2	*	255.255.255.255	VLAN_0	Hacia los servidores de control
10.115.0.0	*	255.255.255.0	VLAN_ADM	Administración de switches
10.115.99.0	*	255.255.255.0	VLAN_99	Hacia los clientes WIFI
default	10.30.0.1	0.0.0.0	eth1	Enlace a Internet para los clientes WIFI

Nota:

**eth0:** es la interface física de red con la LAN de ODControles, en la que se definen varias interfaces virtuales VLAN\_XX (requiere instalar el paquete vlan). En Debian, estas VLAN se deben definir en el fichero de configuración de red /etc/network/interfaces

**eth1:** es la interface de red con la Intranet del hotel.

**Activación del reenvío de paquetes (IP Forwarding)**

En el caso del router-firewall, es necesario activar el IP Forwarding para que reenvíe paquetes entre las 2 interfaces de red y funcione correctamente. Podemos comprobar que está habilitado ejecutando en la consola el comando

**cat /proc/sys/net/ipv4/ip\_forward** . El valor devuelto debe ser "1" :

```
~# cat /proc/sys/net/ipv4/ip_forward
1
```

Si no estuviera habilitado, puede hacerse con el comando:

```
~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

No obstante para que el IP Forwarding sea persistente frente a reinicios del sistema, debemos modificar la configuración del fichero **/etc/sysctl.conf**. Para ello se buscará en él las líneas siguientes:

```
# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1
```

y se descomentará la segunda, quedando de la siguiente manera:

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

▪ **Función de filtrado de paquetes (firewall)**

En la Etapa de Diseño se definieron las siguientes reglas para el firewall:

ROUTER-FIREWALL que protege la LAN de ODControles							
TRAFICO ENTRANTE							
REGLA	ACCION	ORIGEN	PUERTO ORIGEN	DESTINO	PUERTO DESTINO	PROTOC.	DESCRIPCION
1	permite	10.30.0.0	*	192.168.0.2	80	TCP	Permite peticiones http al servidor de control (IP común)
2	permite	10.30.0.0	*	192.168.0.2	443	TCP	Permite peticiones https al servidor de control (IP común)
3	permite	10.30.0.0	*	192.168.0.3	22	TCP	SSH. Conexión a servidor 1 para uso de administrador
4	permite	10.30.0.0	*	192.168.0.4	22	TCP	SSH. Conexión a servidor 2 para uso de administrador
5	permite	10.30.0.0	*	10.115.0.0	80	TCP	Admin. switches interface web
6	permite	10.30.0.10	*	192.168.0.2	3306	TCP	conexión a MySQL desde Gestor de Reservas (IP=10.30.0.10)
7	rechaza	*	*	*	*	*	RECHAZA las demás conexiones
TRAFICO SALIENTE							
REGLA	ACCION	ORIGEN	PUERTO ORIGEN	DESTINO	PUERTO DESTINO	PROTOC.	DESCRIPCION
8	permite	10.115.1.0	*	*	53	*	Clientes WIFI. Consulta DNS
9	permite	10.115.1.0	*	*	143	TCP	Clientes WIFI. Protocolo IMAP Saliente
10	permite	10.115.1.0	*	*	110	TCP	Clientes WIFI. protocolo POP3 Saliente
11	permite	10.115.1.0	*	*	25	TCP	Clientes WIFI. protocolo SMTP Saliente
12	permite	10.115.1.0	*	*	80	TCP	Clientes WIFI. HTTP (navegación web)
13	permite	10.115.1.0	*	*	443	TCP	Clientes WIFI. HTTPS (nav. web segura)
14	permite	192.168.0.2	*	*	53	*	Consulta DNS de los servidores de control
15	rechaza	*	*	*	*	*	RECHAZA las demás conexiones

- **Implementación del firewall con IPTables**

Una implementación mediante IPTables puede ser la siguiente:

```
#!/bin/bash

# INICIALIZACION DEL FIREWALL-BORRAR REGLAS PREEXISTENTES
iptables -F      # borrar reglas de la tabla FILTER (tabla por defecto si no se indica "-t" )
iptables -t nat -F      # borrar reglas de la tabla NAT
iptables -X      # borrar cadenas de usuario
iptables -Z      # poner a cero los contadores de paquetes

## Establecemos política por defecto en DROP (descartar paquetes/datagramas silenciosamente)
# para entradas (INPUT), salidas (OUTPUT) y reenvíos (FORWARD)
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# # # ACCESO LOCAL AL EQUIPO
# Permitimos todo en la interfaz localhost (entrada y salida)
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

#### PERMITIR RESPONDER A CONEXIONES PREVIAS RELATIVAS O ESTABLECIDAS
#### SOLO SE PUEDEN TRASPASAR PUERTOS EN "DROP" COMO RESPUESTA
#### A CONEXIONES RECIBIDAS O SI LA NUEVA CONEXIÓN ESTA RELACIONADA

## se requiere IP FORWARDING ACTIVADO
## PERMITIR RESPONDER A CONEXIONES ENTRANTES
# permite que los servidores de control respondan a las peticiones que reciben desde la Intranet
iptables -A FORWARD -p tcp -m tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -p tcp -m tcp --sport 443 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -p tcp -m tcp --sport 22 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -p tcp -m tcp --sport 3306 -m state --state RELATED,ESTABLISHED -j ACCEPT

## PERMITIR LAS RESPUESTAS A LAS CONEXIONES SALIENTES
# Respuestas de los DNS para WIFI y servidores de control
iptables -A FORWARD -p tcp -m tcp --sport 53 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -p udp -m udp --sport 53 -m state --state RELATED,ESTABLISHED -j ACCEPT
# Respuestas para los clientes WIFI
iptables -A FORWARD -p tcp -m tcp --sport 143 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -p tcp -m tcp --sport 110 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -p tcp -m tcp --sport 25 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -p tcp -m tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -p tcp -m tcp --sport 443 -m state --state RELATED,ESTABLISHED -j ACCEPT

# BLOQUEAR CONEXIONES DESDE CLIENTES WIFI A REDES INTERNAS
iptables -A FORWARD -s 10.115.1.0/24 -d 192.168.0.0/16 -j DROP # bloquea hacia red ODControles
iptables -A FORWARD -s 10.115.1.0/24 -d 10.30.0.0/16 -j DROP # bloquea hacia la Intranet
iptables -A FORWARD -s 10.115.1.0/24 -d 10.115.0.0/16 -j DROP # bloquea hacia otros clientes WIFI
#y hacia administración de switches

#####TRAFICO ENTRANTE A LA RED DE ODCONTROLES#####
# desde la Intranet del Hotel a los servidores de la red de ODControles
iptables -A FORWARD -s 10.30.0.0/16 -d 192.168.0.2 -p tcp --dport 80 -j ACCEPT #http
iptables -A FORWARD -s 10.30.0.0/16 -d 192.168.0.2 -p tcp --dport 443 -j ACCEPT #https
iptables -A FORWARD -s 10.30.0.0/16 -d 192.168.0.3 -p tcp --dport 22 -j ACCEPT #SSH
iptables -A FORWARD -s 10.30.0.0/16 -d 192.168.0.4 -p tcp --dport 22 -j ACCEPT #SSH
iptables -A FORWARD -s 10.30.0.10 -d 192.168.0.2 -p tcp --dport 3306 -j ACCEPT #MySQL
# Admin. switches interface web
iptables -A FORWARD -s 10.30.0.0/16 -d 10.115.0.0/16 -p tcp --dport 80 -j ACCEPT
```

```
#####TRAFICO SALIENTE DE LA RED DE ODCONTROLES O WIFI#####
# DNS para los servidores de control
iptables -A FORWARD -s 192.168.0.2 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -s 192.168.0.2 -p udp --dport 53 -j ACCEPT
# CONEXIONES PERMITIDAS A LOS CLIENTES WIFI
# Puertos habilitados para los clientes WIFI
iptables -A FORWARD -s 10.115.1.0/24 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -s 10.115.1.0/24 -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -s 10.115.1.0/24 -p tcp --dport 143 -j ACCEPT
iptables -A FORWARD -s 10.115.1.0/24 -p tcp --dport 110 -j ACCEPT
iptables -A FORWARD -s 10.115.1.0/24 -p tcp --dport 25 -j ACCEPT
iptables -A FORWARD -s 10.115.1.0/24 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -s 10.115.1.0/24 -p tcp --dport 443 -j ACCEPT

### si el paquete no ha cumplido ninguna de las reglas anteriores, será DESCARTADO
### silenciosamente, dado que la POLITICA POR DEFECTO ES DROP
```

## ANEXO 11. Breve descripción de las comunicaciones y comandos de control del sistema OpenDomo

Los dispositivos ODControl, ODNetwork y en general los sistemas con la distribución OpenDomo, están diseñados para comunicarse entre ellos mediante protocolo de red IP. Además se soportan otros protocolos para permitir la integración con otro tipo de dispositivos domóticos (por ejemplo el standard X10). No obstante, para mantener un sistema de características homogéneas y basado en tecnologías abiertas, en el diseño realizado en este trabajo se prescinde de estos otros protocolos.

- **Comunicaciones entre los ODControl y el puesto de control**

- **Envío de los estados de los ODControl**

En su configuración por defecto, los ODControl propagan mediante un paquete de broadcast, los cambios de estado producidos en sus entradas, enviando un máximo de 1024 Bytes cada 5 segundos. Los datagramas con los estados enviados por los ODControl son recibidos por el puerto 1729 de los equipos que se encuentren a la escucha (es decir, el mismo que se utiliza para enviar comandos al ODControl, pero en sentido inverso)

Existe otro modo de funcionamiento, el “modo silencioso”, en que el ODControl no envía los cambios, aunque se pueden consultar sus estados mediante una petición. Para informar de que el ODControl está operativo, en modo silencioso envía cada 5 minutos un mensaje de 30 Bytes en broadcast.

El puesto de control está permanentemente a la escucha de los mensajes de broadcast recibidos desde los ODControl para, así, poder conocer en todo momento los cambios de estado que se produzcan en los puertos (entendidos en el contexto de entradas y salidas de campo) de los ODControl. De esta manera puede representar en la interface gráfica de usuario (HMI) el estado de cada elemento controlado en la instalación domótica.

Ello también permite que los ODControl conectados a la red sean dados de alta de forma automática en el ordenador central (como un ODNetwork), sin necesidad de configuraciones manuales.

- **Envío de órdenes desde el Puesto de Control**

A su vez, el puesto de control puede enviar órdenes a los ODControl. En la configuración por defecto, esto siempre se realiza a iniciativa del usuario, es decir, cuando éste realiza alguna acción sobre el HMI del puesto de control (por ejemplo ordenar el encendido o apagado de alumbrado, subir o bajar persianas, etc), no enviándose ningún mensaje mientras el HMI esté inactivo.

Esta característica de funcionamiento y el hecho de que la lógica de control resida en los ODControl, hace que una eventual caída del puesto de control únicamente afecte a las funciones dadas por la interfaz del usuario, o a aquellas que se ejecuten automáticamente mediante scripts, pero no a la caída del sistema en su conjunto.

A nivel protocolo, el envío de órdenes a los ODControl se realiza mediante determinados comandos específicos del sistema OpenDomo. Ejemplos de comandos serían los siguientes:

COMANDO OPENDOMO	Explicación
lst	<p>devuelve un listado con el estado de los puertos del ODControl En este contexto, por puertos se entienden las entradas analógicas (AI), salidas analógicas (AO), entradas digitales (DI), salidas digitales (DO) y puertos virtuales (DV ). Ejemplo:</p> <pre>lst DO:do000::OFF DO:do001:OFF DO:do002:OFF DO:do003:OFF DO:do004:OFF DO:do005:OFF DO:do006:OFF DO:do007:OFF DI:di000:OFF DI:di001:OFF DI:di002:OFF DI:di003:OFF DI:di004:OFF DI:di005:OFF DI:di006:OFF DI:di007:OFF AI:ai000:+0051.0000 AI:ai001:+0034.0000  (etc)</pre> <p>donde la primera palabra de cada línea indica el tipo de puerto, la segunda el nombre del puerto o su alias y la tercera su estado.</p>
set	<p>asigna un valor a un puerto de salida o a un puerto virtual. Ejemplo: el siguiente comando activa la salida del puerto digital do000:</p> <pre>set do000 on</pre>

El juego de comandos OpenDomo está formado por varias decenas de ellos, cuya explicación detallada puede encontrarse en el wiki del proyecto OpenDomo, en [http://www.opendomo.com/wiki/index.php/Comandos\\_de\\_ODControl](http://www.opendomo.com/wiki/index.php/Comandos_de_ODControl)

Los dispositivos ODControl se mantienen a la escucha por dos puertos distintos, pudiendo recibir los comandos por cualquiera de ellos:

- **Recepción de comandos en el ODControl por el puerto 1729/TCP**

Los ODControl se mantienen a la escucha por el puerto 1729 e interpretan los comandos que van recibiendo. Dichos comandos pueden enviarse mediante cualquier herramienta que permita enviar datos a un puerto, tal como telnet o netcat, un script del sistema o una aplicación desarrollada con algún lenguaje de programación que permita establecer la conexión con el puerto 1729 y enviar los caracteres de los comandos. El siguiente ejemplo ilustra lo explicado:

Envío de una orden que muestra la versión del ODControl, mediante una consola del sistema operativo:	
Comandos / Respuestas en consola	Explicación
\$ nc 192.168.1.177 1729	← mediante netcat se establece una conexión con el puerto 1729 de un controlador ODControl cuya IP es 192.168.1.177
ver	← enviamos un comando "ver", que muestra la versión
odctl versn 1.6.0 17:35:01 Apr 2 2013	← respuesta del ODControl

▪ **Recepción de comandos en el ODControl por el puerto 81/TCP**

A partir de la versión de firmware 1.5 de ODControl, además del puerto 1729, se dispone del puerto 81 /TCP , en el cual se pueden recibir los comandos vía protocolo http y se dispone de una interface web de configuración. El mismo ejemplo anterior, enviando el comando a través de este puerto, sería:

Petición http / Respuesta	Explicación
http://192.168.1.177:81/ver+	← petición http al puerto 81 de un ODControl cuya IP es 192.168.1.177 , solicitando la versión
odctl versn 1.6.0 17:35:01 Apr 2 2013 DONE	← respuesta devuelta por el ODControl

• **Autenticación de acceso a los ODControl**

El ODControl dispone de 2 puertos http:

- el puerto 81, ya mencionado, que facilita la interface web de configuración.
- el puerto 80, que facilita al usuario una interface web de control que le permite activar o desactivar salidas del ODControl desde un PC o un smartphone.

El acceso al ODControl por cualquiera de ellos requiere autenticación. La gestión de los passwords se realiza mediante los siguientes comandos OpenDomo:

Comando	Explicación
sec webui (password )	← establecer contraseña de la interface web de control
sec webcf (password )	← establecer contraseña de la interface web de configuración. Esta segunda contraseña permite que solo un usuario administrador pueda realizar cambios de la configuración.

En el caso del puerto 1729, no se dispone de un mecanismo de autenticación, por lo que este puerto en ningún caso debe ser público.

- **Seguridad de las comunicaciones**

En el caso de los 2 puertos HTTP, para el envío de peticiones desde entornos no controlados, como es Internet, dado que sus datos no van cifrados, es necesario cifrarlos mediante un protocolo de nivel superior.

En el caso del puerto 1729, a partir de la versión de firmware 1.6 se dispone de un mecanismo propio de cifrado, mediante el comando “sec proto”:

Comando	Explicación
sec proto (password )	← activa el cifrado y establece la clave para el cifrado

- **Sincronización de tiempos entre dispositivos**

Los ODControl soportan el protocolo NTP para su sincronización. El puerto utilizado es el estándar del protocolo (123/UDP)

- **Interface gráfica del ordenador central (puesto de control ODNetwork)**

Se accede a ella mediante http, por el puerto 80, ya sea localmente (http://localhost) o desde otro equipo (http://direccion\_IP\_ordenador\_central)



# ANEXO 12. Instrucción técnica complementaria ITC-BT-51 , del Reglamento Electrotécnico de Baja Tensión, para aplicación a instalaciones domóticas

## INSTALACIONES DE SISTEMAS DE AUTOMATIZACIÓN, GESTIÓN TÉCNICA DE LA ENERGÍA Y SEGURIDAD PARA VIVIENDAS Y EDIFICIOS.

### ÍNDICE

1. OBJETO Y CAMPO DE APLICACIÓN.
2. TERMINOLOGÍA.
3. TIPOS DE SISTEMAS.
4. REQUISITOS GENERALES DE LA INSTALACIÓN.
5. CONDICIONES PARTICULARES DE INSTALACIÓN.
  - 5.1 Requisitos para sistemas que usan señales que se acoplan y transmiten por la instalación eléctrica de baja tensión.
  - 5.2 Requisitos para sistemas que usan señales transmitidas por cables específicos para dicha función.
  - 5.3 Requisitos para sistemas que usan señales radiadas.

### 1. OBJETO Y CAMPO DE APLICACIÓN.

Esta Instrucción establece los requisitos específicos de la instalación de los sistemas de automatización, gestión técnica de la energía y seguridad para viviendas y edificios, también conocidos como sistemas domóticos.

El campo de aplicación comprende las instalaciones de aquellos sistemas que realizan una función de automatización para diversos fines, como gestión de la energía, control y accionamiento de receptores de forma centralizada o remota, sistemas de emergencia y seguridad en edificios, entre otros, con excepción de aquellos sistemas independientes e instalados como tales, que puedan ser considerados en su conjunto como aparatos, por ejemplo, los sistemas automáticos de elevación de puertas, persianas, toldos, cierres comerciales, sistemas de regulación de climatización, redes privadas independientes para transmisión de datos exclusivamente y otros aparatos, que tienen requisitos específicos recogidos en las Directivas europeas aplicables conforme a lo establecido en el artículo 6 del Reglamento Electrotécnico para Baja Tensión.

Quedan excluidas también las instalaciones de redes comunes de telecomunicaciones en el interior de los edificios y la instalación de equipos y sistemas de telecomunicaciones a los que se refiere el Reglamento de Infraestructura Común de Telecomunicaciones (I.C.T.), aprobado por el R.D. 279/1999.

Igualmente están excluidos los sistemas de seguridad reglamentados por el Ministerio del Interior y Sistemas de Protección contra Incendios, reglamentados por el Ministerio de Fomento (NBE-CPI) y el Ministerio de Industria y Energía (RIPCI).

No obstante, a las instalaciones excluidas anteriormente, cuando formen parte de un sistema más complejo de automatización, gestión de la energía o seguridad de viviendas o edificios, se les aplicarán los requisitos de la presente Instrucción además los requisitos específicos reglamentarios correspondientes.

## 2. TERMINOLOGÍA.

### **Sistemas de Automatización, Gestión de la Energía y Seguridad para Viviendas y Edificios:**

Son aquellos sistemas centralizados o descentralizados, capaces de recoger información proveniente de unos entradas (sensores o mandos), procesarla y emitir ordenes a unos actuadores o salidas, con el objeto de conseguir confort, gestión de la energía o la protección de personas animales y bienes.

Estos sistemas pueden tener la posibilidad de accesos a redes exteriores de comunicación, información o servicios, como por ejemplo, red telefónica conmutada, servicios INTERNET, etc.

**Nodo:** Cada una de las unidades del sistema capaces de recibir y procesar información comunicando, cuando proceda con otras unidades o nodos, dentro del mismo sistema.

**Actuador:** Es el dispositivo encargado de realizar el control de algún elemento del Sistema, como por ejemplo, electroválvulas (suministro de agua, gas, etc.), motores (persianas, puertas, etc.), sirenas de alarma, reguladores de luz, etc.

#### **Dispositivo de entrada:**

Sensor, mando a distancia, teclado u otro dispositivo que envía información al nodo.

Los elementos definidos anteriormente pueden ser independientes o estar combinados en una o varias unidades distribuidas.

**Sistemas centralizados:** Sistema en el cual todos los componentes se unen a un nodo central que dispone de funciones de control y mando.

**Sistema descentralizado:** Sistema en que todos sus componentes comparten la misma línea de comunicación, disponiendo cada uno de ellos de funciones de control y mando.

## 3. TIPOS DE SISTEMAS.

Los sistemas de Automatización, Gestión de la energía y Seguridad considerados en la presente instrucción, se clasifican en los siguientes grupos:

- Sistemas que usan en todo o en parte señales que se acoplan y transmiten por la instalación eléctrica de Baja Tensión, tales como sistemas de corrientes portadoras.
- Sistemas que usan en todo o en parte señales transmitidas por cables específicos para dicha función, tales como cables de pares trenzados, paralelo, coaxial, fibra óptica.
- Sistemas que usan señales radiadas, tales como ondas de infrarrojo, radiofrecuencia, ultrasonidos, o sistemas que se conectan a la red de telecomunicaciones.

Un sistema domótico puede combinar varios de los sistemas anteriores, debiendo cumplir los requisitos aplicables en cada parte del sistema. La topología de la instalación puede ser de distintos tipos, tales como, anillo, árbol, bus o lineal, estrella o combinaciones de éstas.

## 4. REQUISITOS GENERALES DE LA INSTALACIÓN.

Todos los nodos, actuadores y dispositivos de entrada deben cumplir, una vez instalados, los requisitos de Seguridad y Compatibilidad Electromagnética que le sean de aplicación, conforme a lo establecido en la legislación nacional que desarrolla la Directiva de Baja Tensión (73/23/CEE) y la Directiva de Compatibilidad Electromagnética (89/336/CEE). En el caso de que estén incorporados en otros aparatos se atenderán, en lo que sea aplicable, a los requisitos establecidos para el producto o productos en los que vayan a ser integrados.

Todos los nodos, actuadores y dispositivos de entrada que se instalen en el sistema, deberán incorporar instrucciones o referencias a las condiciones de instalación y uso que deban cumplirse para garantizar la seguridad y compatibilidad electromagnética de la instalación, como por ejemplo, tipos de cable a utilizar, aislamiento mínimo, apantallamientos, filtros y otras informaciones relevantes para realizar la instalación. En el caso de que no se requieran condiciones especiales de instalación, esta circunstancia deberá indicarse expresamente en las instrucciones.

Dichas instrucciones se incorporarán en el proyecto o memoria técnica de diseño, según lo establecido en la ITC-BT-04.

Toda instalación nueva, modificada o ampliada de un sistema de automatización, gestión de la energía y seguridad deberá realizarse conforme a lo establecido en la presente Instrucción y lo especificado en las instrucciones del fabricante, anteriormente citadas.

En lo relativo a la Compatibilidad Electromagnética, las emisiones voluntarias de señal, conducidas o radiadas, producidas por las instalaciones domóticas para su funcionamiento, serán conformes a las normas armonizadas aplicables y, en ausencia de tales normas, las señales voluntarias emitidas en ningún caso superarán los niveles de inmunidad establecidos en las normas aplicables a los aparatos que se prevea puedan ser instalados en el entorno del sistema, según el ambiente electromagnético previsto.

Cuando el sistema domótico esté alimentado por muy baja tensión o la interconexión entre nodos y dispositivos de entrada este realizada en muy baja tensión, las instalaciones e interconexiones entre dichos elementos seguirán lo indicado en la ITC-BT-36.

Para el resto de los casos, se seguirán los requisitos de instalación aplicables a las tensiones ordinarias.

## **5. CONDICIONES PARTICULARES DE INSTALACIÓN.**

Además de las condiciones generales establecidas en el apartado anterior, se establecen los siguientes requisitos particulares.

### **5.1. Requisitos para sistemas que usan señales que se acoplan y transmiten por la instalación eléctrica de baja tensión.**

Los nodos que inyectan en la instalación de baja tensión señales de 3 kHz hasta 148,5 kHz cumplirán lo establecido en la norma UNE-EN 50.065 -1 en lo relativo a compatibilidad electromagnética. Para el resto de frecuencias se aplicará la norma armonizada en vigor y en su defecto se aplicará lo establecido en el apartado 4.

### **5.2. Requisitos para sistemas que usan señales transmitidas por cables específicos para dicha función.**

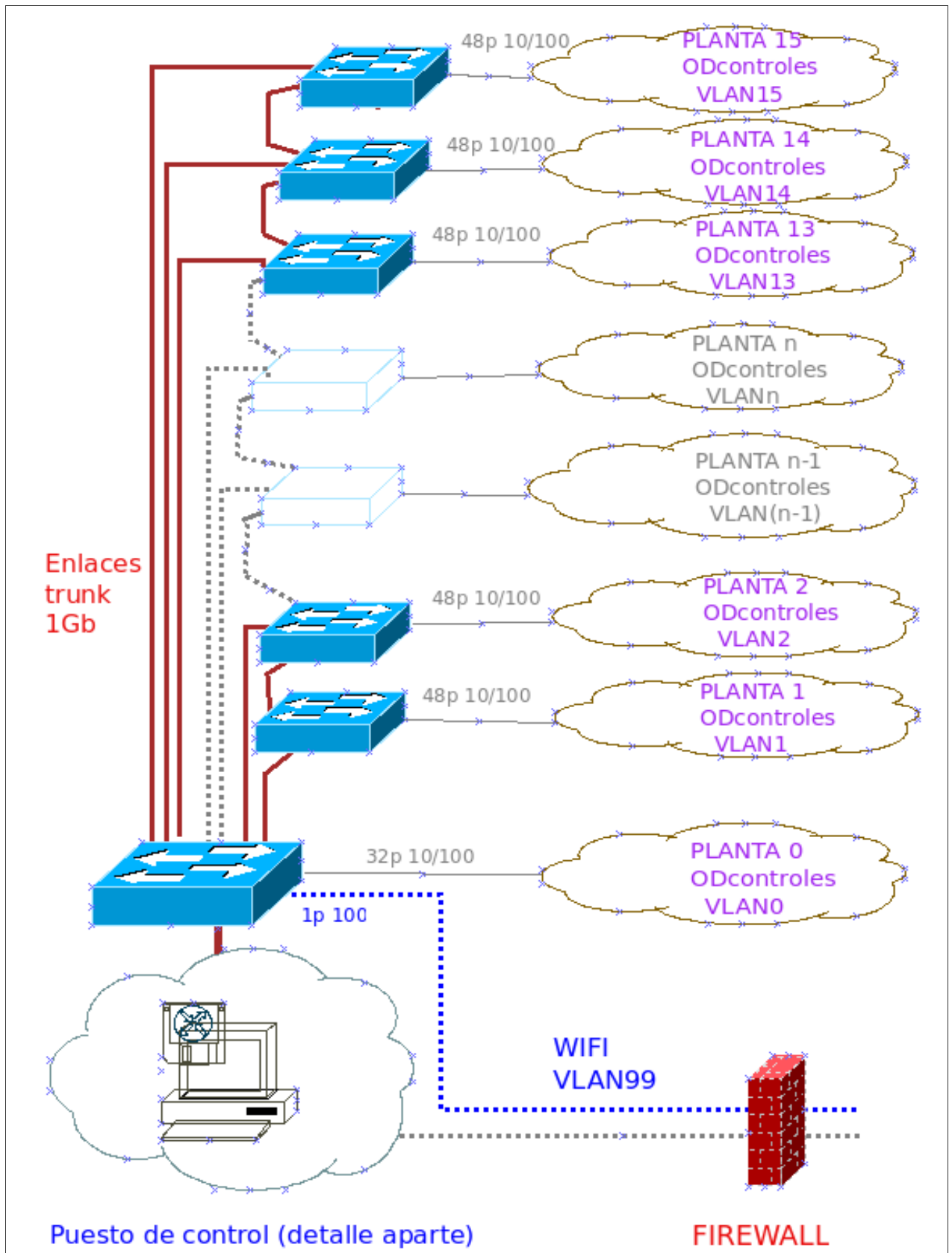
Sin perjuicio de los requisitos que los fabricantes de nodos, actuadores o dispositivos de entrada establezcan para la instalación, cuando el circuito que transmite la señal transcurra por la misma canalización que otro de baja tensión, el nivel de aislamiento de los cables del circuito de señal será equivalente a la de los cables del circuito de baja tensión adyacente, bien en un único o en varios aislamientos.

Los cables coaxiales y los pares trenzados usados en la instalación deberán cumplir con las normas de la serie EN 61.196 y CEI 60.189 -2.

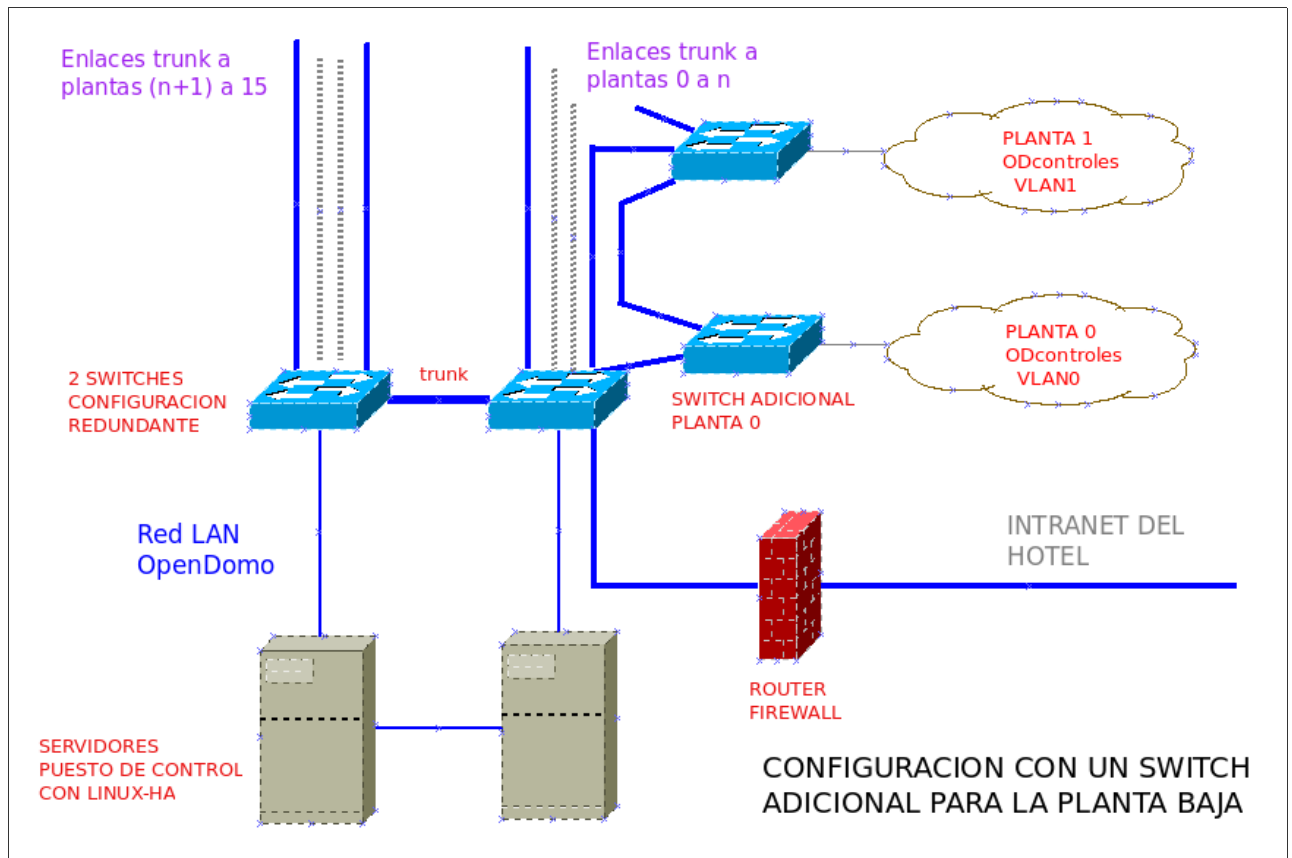
### **5.3. Requisitos para sistemas que usan señales radiadas.**

Adicionalmente, los emisores de los sistemas que usan señales de radiofrecuencia o señales de telecomunicación, deberán cumplir la legislación nacional vigente del "Cuadro Nacional de Atribución de Frecuencias de Ordenación de las Telecomunicaciones".

### Anexo 13. Esquema de la topología de la LAN para 15 plantas



**\* DETALLE DEL PUESTO DE CONTROL PARA 15 PLANTAS:**



## ANEXO 14. Cálculo de la tasa de bits para 480 ODcontroles

CALCULO DE LA TASA DE BITS. ( Ejemplo: nodo mas desfavorable, la tarjeta de red del puesto de control)								
Cantidad de ODControles:		480						
EMISION DE LOS ODControl (BROADCASTS: Cada 5 minutos, envía un "heartbeat" de 30B)								
	Tamaño de datos (bytes)	Bytes Cabecera HTTP	Bytes Cabecera TCP (incl. opciones)	Bytes Cabecera IP	Bytes Ethernet	TAMANO TOTAL PAQUETE (packet size) + INTERFRAM E GAP en Bytes	Packet Rate (pps), Paquetes enviados por segundo	Tasa total de bits emitidos en conjunto (en Kbps)
Por cada ODControl	30	400	24	40	42	536	0,00333	---
Para todos los ODControl							1,60	<b>6,86</b>
POLLING DEL PUESTO DE CONTROL (interrogación a los ODControles 1 a 1 para obtener sus estados)								
	segundos	minutos						
Tiempo máximo del ciclo de interrogación (seg)	180	3						
Intervalo (periodo) medio de envío de mensaje de polling (segundos)	0,38							
Mensaje de solicitud de estado de puertos (enviado por el Puesto de Control)	50	400	24	40	42	556	2,67	<b>11,86</b>
Mensaje de respuesta a petición de estado de puertos (enviado por el ODControl)	1024	400	24	40	42	1530	2,67	<b>32,64</b>
ENVIO DE ORDENES ESPECÍFICAS DESDE PUESTO DE CONTROL (activar o desactivar elementos por actuación del usuario) - ESTIMACION								
Intervalo (periodo) medio de envío de órdenes (segundos)	5							
Petición	50	400	24	40	42	556	0,2	<b>0,89</b>
Respuesta (ack)	1024	400	24	40	42	1530	0,2	<b>2,45</b>
<b>Celdas en verde: datos de los ODControl</b>						<b>TOTAL TASA DE BITS: 54,70 Kbps</b>		
<b>Celdas blancas: datos que se pueden modificar</b>								