UNIVERSIDAD CARLOS III DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

Planificación y diseño de un CPD de respaldo basado en la norma ANSI TIA 942

PROYECTO FIN DE CARRERA
INGENIERÍA DE TELECOMUNICACIÓN

Autor: Héctor Pérez Martín
Tutor: Julio Villena Román

Abril 2014

Título: Planificación y diseño de un CPD de respaldo basado en la norma ANSI TIA 942

Autor: Héctor Pérez Martín

Tutor: Julio Villena Román

EL TRIBUNAL

Presidente:

_____

Secretario:

_____

Vocal:

_____

Realizado el acto de defensa del Proyecto Fin de Carrera el día __ de _____ de _____ en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de:

Fdo.: Presidente Fdo.: Secretario Fdo.: Vocal

Agradecimientos

En el siglo XII, Bernardo de Chartres dijo: "Somos como enanos a los hombros de gigantes. Podemos ver más, y más lejos que ellos, no porque la agudeza de nuestra vista ni por la altura de nuestro cuerpo, sino porque somos levantados por su gran altura.". Un proyecto como este está apoyado en muchos hombros; cabe pues agradecer a algunos sin los cuales no hubiera sido posible:

A mi madre, por contagiarme la pasión por la lectura y el conocimiento, y en general por enseñarme lo que realmente importa en la vida.

A mi padre, por sus consejos, críticas y por tantas horas de conversación sobre ingeniería, sin las cuales no estaría aquí ahora mismo.

A Jorge y Marta, que me despertaron del letargo con una sana competición. A mi familia por su constante apoyo y comprensión.

A Aurora, que encontró las teclas correctas para que este proyecto no fuera una sinfonía inacabada.

A mi familia adoptiva brasileña: Ana, Santiago, Eduardo, Paula, Pipoca y Nadal; me han dado su apoyo y soportado horas de pensamientos en alto aún sin tener muy claro de qué trataba el proyecto y que me van a cobrar la paella de celebración.

A mis amigos, compañeros y colegas. Especialmente Javier, Manolo, Elsa, Jaime, Noemí y Enrique que nunca me dejaron olvidar mis tareas pendientes.

A Julio, que consiguió lo que llegué a pensar imposible, haciendo que 10.000km y un océano parecieran tan fácil como bajarse del cercanías en Leganés Central.

Y a todos aquellos que aún sin estar aquí nombrados saben de su contribución.

Espero que el resultado sea de vuestro agrado.

Resumen

Año tras año la dependencia de las organizaciones en las TIC aumenta, hasta el punto de que no se puede concebir la operación de la organización en ausencia de la infraestructura TIC. Esta dependencia significa a su vez una gran exigencia en el funcionamiento ininterrumpido de los sistemas, los profesionales y la infraestructura que los soportan, ya que cualquier fallo tiene un impacto negativo en la operación.

En este sentido las áreas de TI garantizan unos niveles de calidad del servicio, normalmente medidos en % de tiempo de disponibilidad de los sistemas individuales. Sin embargo, esta disponibilidad depende no solo del sistema individual, sino también de la plataforma TIC que la sustenta, y más específicamente, del centro de proceso de datos en la que el sistema se aloja. Es por tanto necesario analizar el centro de proceso de datos como único sistema compuesto de múltiples subsistemas complejos, identificando cuales son los posibles fallos que pueden llevar a indisponibilidad del sistema como un todo. Con estos fallos identificados es posible diseñar el centro de datos-sistema y sus componentes minimizando los riesgos de interrupciones no deseadas.

En esta tarea existen múltiples subsistemas y decisiones de diseño que deben ser tomadas en un amplio grupo de áreas de conocimiento, no sólo a nivel de diseño de redes y sistemas informáticos, sino también a nivel arquitectónico, de seguridad, infraestructura de energía o enfriamiento, entre otros. Esta tarea se ve simplificada gracias a la norma TIA-942, que establece una serie de reglas a seguir en el diseño de los diferentes subsistemas del centro de datos en función del nivel de disponibilidad deseada (diferenciando cuatro niveles o Tiers, desde Tier 1 hasta Tier 4).

Este proyecto analiza la norma, y la aplica un caso práctico siguiendo el diseño de un centro de datos para la empresa ZEREPSA, cumpliendo los requisitos de la norma para un centro Tier 4. Este centro será un centro de respaldo para el centro principal de la compañía, lo que permite abordar algunos asuntos adicionales, como racionalización de los recursos y conectividad de con el centro de datos principal y otras sedes de la compañía.

Abstract

Year by year reliance of organizations on Information Technologies keeps growing, up to not being able to foresee the organization's business operations in the absence of IT infrastructures. This reliance implies great strain on the systems, infrastructure and people supporting these systems in order to achieve uninterrupted system operation, as any fault will have negative impact on the business.

TI departments guarantee certain service levels, usually measured as individual system uptime. This uptime, however depends not only on the specific system, but also on the IT platform underneath, and explicitly on the datacenter where the system resides. So it is necessary to analyze such datacenter as an unique complex system made up by multiple and complex subsystems, identifying which points of failure could cause downtime for the whole system. By identifying these points of failure, it is possible to design the datacenter/system and its components minimizing undesired downtimes.

Into that task, multiple subsystem and design considerations must be taken care of, across many knowledge areas, not only on network and computing systems but also on architectural, security, power and cooling, for instance. The task can be simplified by using the TIA-942 standard, that establishes a set of guidelines to be followed for each subsystem based on the desired availability (classified as four Tiers, ranging from Tier 1 to Tier 4).

This project analyzes the standard, applying it into a practical case by following the design od a datacenter for the ZEREPSA company, achieving the Tier 4 datacenter requirements described in the standard. The mentioned datacenter will be a backup for the primary site, allowing the analysis of additional concepts, as resource optimization and connectivity with the primary datacenter and with other offices.

Índice

Índice de figuras

Índice de tablas

1 INTRODUCCIÓN

Con esta introducción se presenta una breve introducción al proyecto, se presenta la empresa y se plantean los principios básicos del centro de respaldo y se describe someramente la norma ANSI/TIA/EIA-942 [*1*]. Norma que resulta básica de aplicación para la realización de cualquier Centro de proceso de Datos o centro de Cómputo que se pretenda realizar.

1.1 Introducción al Proyecto

Se trata de realizar un CPD con el que se de soporte a los datos y aplicaciones que la empresa dispone en su CPD principal En definitiva se trata de establecer la salvaguarda de datos y recuperación ante desastres.

Se pretende construir un Centro de Respaldo para el Centro de Proceso de Datos de la empresa ACME, en el que se alojarán una serie de Sistemas de información calificados como de alta criticidad para la empresa y otros de baja y media criticidad que permitan el correcto funcionamiento de los sistemas en explotación en caso de que el CPD principal falle por cualquier motivo.

El proyecto se centra en la definición de este centro de respaldo, siguiendo las indicaciones de la norma TIA-942 [*1*], abordando todos los aspectos citados en la norma, tanto de infraestructura de telecomunicaciones, arquitectura, infraestructura eléctrica y elementos mecánicos.

El objetivo es, basado en las características del centro principal y en la guía de la normativa, definir los componentes del centro de respaldo, las tecnologías y características fundamentales, de forma que a partir de esta información se puedan iniciar las tareas de diseño detallado, contratación y compra de los diferentes elementos. Si bien este proyecto tendrá un detalle suficiente como para realizar un anteproyecto completo y un presupuesto de alto nivel, no es objetivo especificar con detalle todos los componentes, ya que estos variarán con las decisiones de diseño detallado y contratación.

1.2 Descripción de la empresa

En lo que sigue se describe someramente la empresa a la que se le va a dotar del centro de respaldo.

La importancia de la descripción es debido a que permite disponer de visibilidad sobre los mecanismos de conexión que requieren las actividades de la misma y a los que habrá que dar respaldo habida cuenta la gran responsabilidad que estos juegan en su funcionamiento. La empresa se describe a continuación.

1.2.1 Organigrama de la empresa

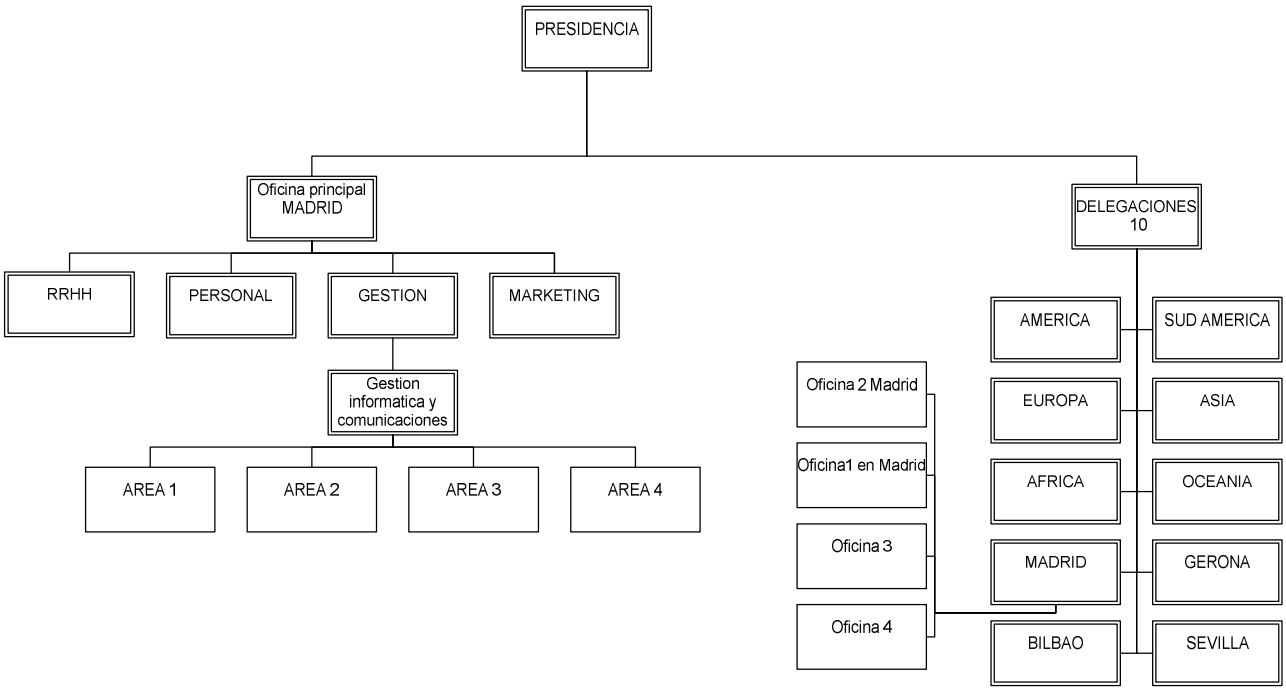


Figura 1: Organigrama de la empresa ZEREPSA

La empresa es una multinacional petrolera que tiene su sede en Madrid y diversas delegaciones por todo el mundo. Alguna de las delegaciones es en extensión mayor, incluso que la oficina de Madrid.

El CPD que se desea respaldar está ubicado en la oficina principal en Madrid.

El citado CPD es el responsable de que la totalidad de los sistemas implantados en la compañía estén en funcionamiento, así como del correcto funcionamiento de las comunicaciones y de la totalidad de los sistemas básicos sobre los que funcionan los sistemas que se hallan en las delegaciones regionales.

Algunas de las Delegaciones disponen de flotas de vehículos tanto terrestres como marítimos para el transporte de los productos. Dichos vehículos poseen sus propios sistemas de gestión de los sistemas informáticos que acarrean (sistemas propios de gestión de las plataformas móviles, como sistemas de gestión del transporte que efectúan así como del personal, y las comunicaciones a todos los niveles, incluidas las de telefonía y de correo electrónico). Todas estas plataformas móviles, se hallan también completamente vinculadas, a través de su delegación con el CPD central.

El Organigrama representa la organización a nivel de centros de proceso de datos.

Algunas sedes disponen de equipos destacados a zonas de prospección en que se dispone de torres y de equipos de extracción También el personal de estos puntos dispone de equipamiento informático que mantiene el CPD principal, tanto fijo como móvil (portátiles, PDA, sistemas de medición y control, etc.).

Desde el CPD se dan los servicios básicos de informática a todos los puestos de trabajo así como los de red y, como se ha dicho de telefonía.

Asimismo se dan los servicios de correo electrónico y de hosting y housing a todos los sistemas de la empresa ya que se hallan centralizados en el citado CPD.

De igual modo se distribuye todo el software y se mantienen las protecciones de seguridad necesarias. Se gestiona y mantiene la configuración de los sistemas tanto en cuanto al equipamiento Hardware como al Software que se ejecuta. Por ello dispone de sistemas que le permiten efectuar en forma mecanizada tales actividades.

Mantiene y da servicios de Internet centralizados en un único nodo de salida a la red, manteniendo una RPV (red privada virtual) que funciona como intranet corporativa enlazando todos los componentes de la empresa, tanto sedes como vehículos e incluso desplazados con sistemas móviles, ya que todos los directivos disponen de Smartphone y de ordenador portátil. Los equipos móviles y de prospección disponen de sistemas móviles de registro y control de parámetros que pasan vía intranet a los sistemas de control y seguimiento de la producción y de los parámetros medioambientales en que se desenvuelven.

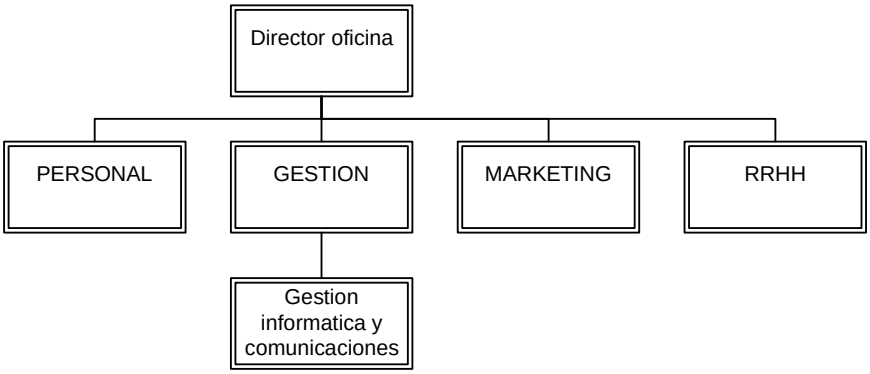


Figura 2: Organigrama de una sede tipo

Todas las oficinas disponen de una unidad dedicada a la gestión de los sistemas informáticos de la oficina y de la demarcación que esta tenga asignada y los que la empresa tenga desplegados en la demarcación así como de las comunicaciones. Esta unidad es la encargada de solicitar y de implantar sistemas particulares que sean necesarios para la oficina y que hayan sido aprobadas por el servicio de Informática de la empresa.

Igualmente son responsables de administrar los sistemas desplegados que dispone la empresa en su demarcación.

Cada oficina (ya sea de una zona o de un área de actuación), dispone de su propia red LAN que interconecta sus dispositivos y se comunica con la red general de la empresa.

1.2.2 Plataformas destacadas en cada emplazamiento

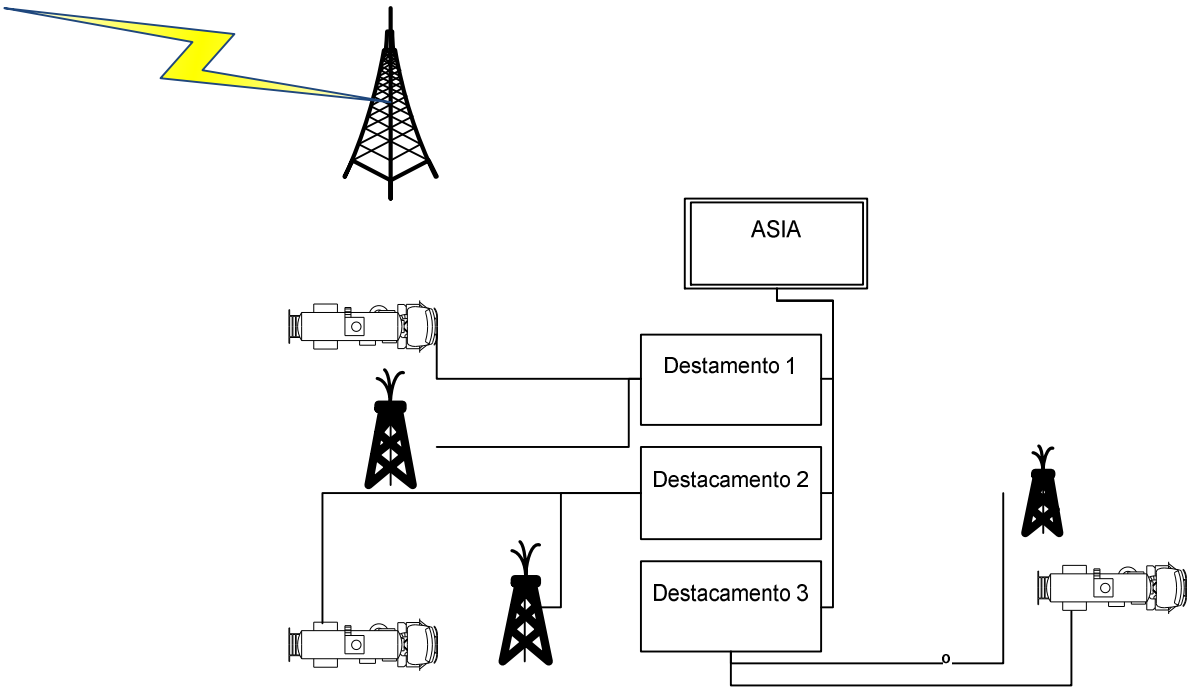


Figura 3: Organigrama de emplazamientos

Cada emplazamiento o cada zona tienen desplegados una serie de destacamentos que corresponden a los puntos de extracción. Dichos destacamentos pueden tener o no personal para la gestión de los sistemas informáticos o de información que mantenga operativos en su despliegue. No obstante todos los equipos y sistemas son atendidos, como mínimo por el equipo de informática de la oficina que les atiende. Los equipos informáticos atienden no sólo a la informática de gestión sino también a los dispositivos de obtención y manejo de la información necesaria para el trabajo como pueden ser equipos de tratamiento de la extracción y del posicionamiento o movilidad de los equipos.

Cada destacamento dispone de su propia red LAN que interconecta sus dispositivos y se comunica con la red general de la empresa.

1.2.3 Tipología de las plataformas móviles que han de conectarse

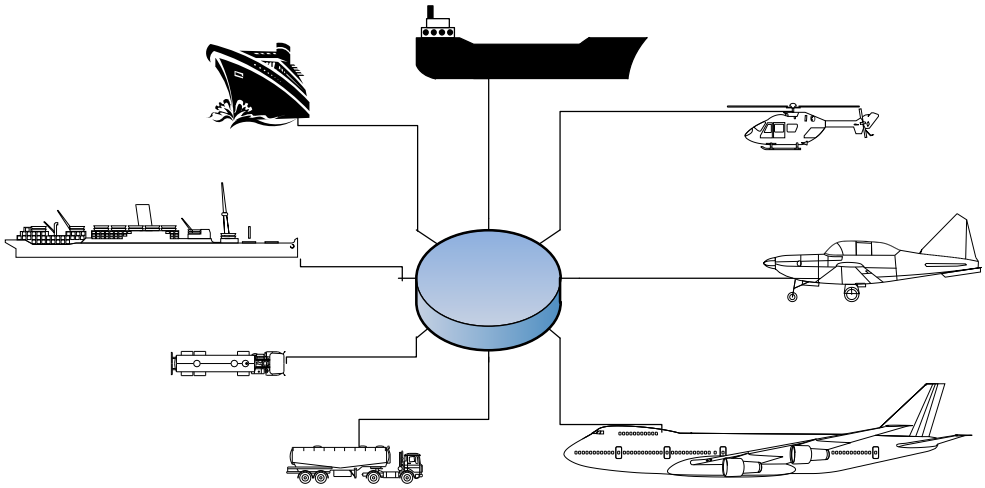


Figura 4: Diversidad de plataformas móviles

Las plataformas móviles están dotadas de sistemas GIS y GPS que les permite mantenerse continuamente conectados con los sistemas de información de la empresa así como su georeferenciamiento y localización, además de los sistemas de comunicaciones que permiten al personal tanto su conexión con otros como para asegurar su calidad de vida en las plataformas.

Los tipos de plataforma que se consideran en este apartado son sólo las móviles ya que las plataformas fijas, estén donde estén ubicadas (tanto en tierra o sobre el mar) se consideran como plataformas destacadas.

Así las plataformas móviles, suelen estar asociadas, todas ellas, con la sede central de la empresa, independientemente de la plataforma destacada de la que partan o hacia la que se dirigen, sus movimientos, posicionamiento y necesidades de información se proporcionan desde la sede central

Cada plataforma dispone de su propia red LAN que interconecta sus dispositivos y se comunica con la red general de la empresa.

Para el transporte del crudo se utiliza una flota de barcos petroleros así como para diferentes mercancías transportes de shelters. Para su distribución a los puntos de reparto se utilizan vehículos cisterna o camiones de trasporte en general para el transporte de material

También existen varios barcos de pasaje para el personal y dos aviones de transporte de personal.

Todos los vehículos cuentan con interconexión entre sí y conexión con la sede central y con las aplicaciones de la empresa.

Cuando se encuentran en tierra, la empresa dispone de muelles de atraque particulares y de hangares también particulares así como de centros de distribución y de almacenamiento en que también están conectadas con las aplicaciones de la sede central, participando de los sistemas propios como de aquellos sistemas de gestión de estos “emplazamientos” que se hallan en régimen de alquiler y que son propiedad y utilizan las organizaciones que los alquilan (AENA, puertos del estado, etc.).

1.3 Descripción del problema (necesidad de respaldo)

La empresa ZEREPSA es una empresa española con una sede central y varias sedes locales, así como varias sedes off-shore. Para dar soporte a los distintos sistemas de negocio, la empresa dispone de un centro de proceso de datos principal, ubicado en las instalaciones de la sede central. Este centro principal también da el servicio de web corporativa y extranet, así como de telefonía corporativa. Asimismo dispone de una serie de sistemas que operan en modo distribuido, debiendo dar cobertura de soporte a dichos sistemas tanto la parte integrada en el CPD principal como aquellas partes que se hallan en localizaciones externas.

Para dar servicios de telefonía, ZEREPSA tiene contratados servicios de telefonía fija y telefonía móvil.

La empresa dispone de un Contact Center (basado en telefonía IP) que da servicio al centro de atención al usuario (CAU) referente a las aplicaciones IT de la empresa. La sede central dispone de telefonía IP, pero las distintas subsedes están en proceso de migración.

Dado la creciente dependencia de estos sistemas, ZEREPSA se plantea dotar de redundancia a los sistemas, para lo que decide disponer de un centro de respaldo que en caso de fallo del centro principal permita a la empresa seguir realizando sus operaciones sin grandes disrupciones.

El esquema de interconexionado de la empresa es el que se muestra en la figura siguiente.

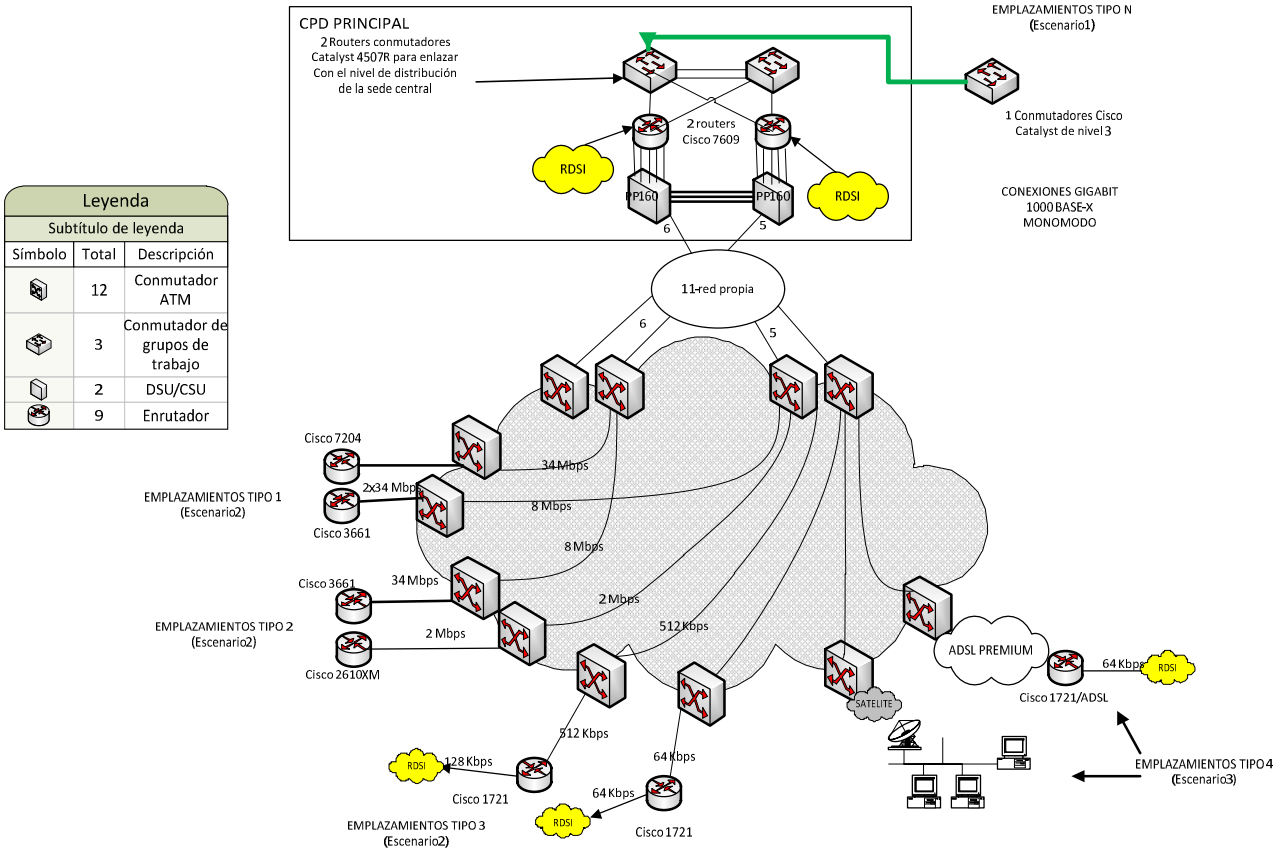


Figura 5: Esquema general de red ZEREPSA

Actualmente, la seguridad frente a fallos y malfuncionamiento se garantiza mediante el empleo de sistemas redundantes 2N+1 de tal forma que todos se duplican. Esto implica el balanceo de los sistemas que, a su vez implica la presencia de software para su gestión, que complica y ralentiza la red. Pero la garantía de seguridad es elevada 99,95%.

El hecho de requerir un centro de respaldo es motivado por el deseo de alcanzar una disponibilidad superior al 99,99%, además de permitir la supervivencia de los sistemas en caso de fallo catastrófico en el centro principal.

1.4 Guías generales

Se analizaron identificaron tres modelos de respaldo existentes en el mercado.

- **Modelo dedicado (in-house)**, gestionado por la propia empresa, en el que el centro de respaldo forma parte de la infraestructura propia de la empresa, siendo esta la responsable por su explotación. Dentro de este modelo se puede optar por una estrategia **centralizada** (un único centro que alberga todo el respaldo) o **distribuida** (varios centros que se encargan del respaldo de diferentes elementos).
- **Modelo on demand (outsourced)**, en el que la empresa alquila a un tercero el espacio y equipos, ubicados en un centro de respaldo compartido con otros clientes, permitiendo aumentar los recursos conforme sea necesario. En este modelo parte de la gestión del centro recae sobre el proveedor y parte sobre la propia empresa.
- **Modelo virtual (Iaas, infrastructure as a service)**, en el que la empresa contrata un pool de recursos en la nube, ofrecidos por un tercero.

Se descarta el uso de un modelo de respaldo on-demand, virtual o distribuido, ya que se desea tener un control completo del centro, incluyendo la explotación de la infraestructura y la seguridad de las redes. Se fija el proyecto en un centro de respaldo completo y dedicado, gestionado por la propia empresa.

Se hará una descripción de alto nivel de la relación del Centro de Respaldo con el centro principal, y una justificación de la necesidad del punto neutro de red en el centro de respaldo para la interconexión con diferentes ISPs (Intenet Service Providers) así como con distintos NSPs (Network Service Providers) y en general los diferentes proveedores de telefonía que pudieran darse, para de este modo poder atender sin problemas los posibles cambios de suministradores de servicios de red, de internet o de telefonía.

Se han clasificado las aplicaciones y sistemas en función de su criticidad con el fin de atender a las necesidades de respaldo y recuperación de las mismas. Con ello hemos podido determinar los dos parámetros básicos a la hora de definir el tipo de solución técnica de respaldo que tendrán los sistemas que albergan la aplicación.

  - Objetivo de Tiempo de Respuesta: El tiempo máximo requerido para que una aplicación esté disponible después de una contingencia.
  - Objetivo de Pérdida de Datos: Determina la pérdida de datos que puede permitirse una aplicación. En algunos casos se pueden llegar a recuperar por algún procedimiento manual. Esto es fundamental para determinar por ejemplo si la copia de datos entre cabinas puede ser síncrona (no existe pérdida) o asíncrona (puede haber pérdida de datos pero permite cualquier distancia).

Para obtener estos datos se hizo un inventario de las aplicaciones en servicio y se evaluó para cada una de ellas su criticidad en función de su responsabilidad ante el negocio (BIA, Business Impact Analysis).

Los parámetros que se han empleado como fundamentales han sido los siguientes: distancia, tiempo de respuesta y perdida de datos, pero se han tenido en cuenta, también otros factores a la hora de determinar la solución:

  - Selección de Soluciones Homogéneas para todo el CPD: con el fin de que los recursos puestos en juego en la atención a los sistemas de soporte no difieran de los que ya existen en el CPD principal. Tanto en lo referente a tecnologías como a lo referente al personal de operación.

- Aprovechamiento de los recursos para servicios no críticos: Se han tenido en cuenta que ciertos entornos no críticos pueden servir de apoyo a otros más críticos para la puesta en operación y recuperación de esos y más tarde entrar en operación cuando todos los servicios considerados críticos lo han hecho.

1.5 Estructura del documento

Este documento se compone de tres secciones principales bien diferenciadas. En la sección "Análisis de requisitos" se presenta el problema a resolver, detallando la norma TIA 942, y pasando a detallar los elementos TIC deberán respaldarse, así como su priorización. Finalmente se resumen los requisitos mínimos que la solución deberá cumplir.

En la sección "Solución propuesta - Infraestructura de soporte y seguridad física" se describen los elementos de infraestructura física y eléctrica del centro de respaldo. Si bien se presta especial atención a las características relacionadas con la Sala técnica y zonas relacionadas con las TIC, se repasan también otros elementos mencionados en la norma.

En la sección "Solución propuesta - Infraestructura informática y de comunicaciones" se describen los elementos de la solución referentes a los elementos de red y servidores. En esta sección se presentan las estrategias para atender las necesidades de respaldo, y se describen las guías para definir las redes y elementos de electrónica de red, si bien se omite el detalle de estos elementos.

Finalmente, se presentan los presupuestos, historia del proyecto y las conclusiones y trabajos futuros relacionados con el centro de respaldo y su evolución.

2 ANÁLISIS DE REQUISITOS

En este apartado se describe detalladamente la estructura de sistemas de información y comunicación de la empresa ZEREPSA, ya que dar respaldo a esa estructura es el objetivo del proyecto. Esta fase de análisis por tanto concluye con las especificaciones a cumplir por el centro de respaldo.

2.1 Requisitos previos

Antes de establecer un plan para el centro de respaldo, se lleva a cabo un análisis de la situación de los sistemas de información y comunicación de la empresa, la importancia de estos para el desempeño de su línea de negocio y a partir de estos se establecen los requisitos que tendrá que cumplir el centro de respaldo.

2.1.1 Análisis de impacto en negocio

Este análisis, llamado "Análisis de Impacto en Negocio" (*Business Impact Analysis*, *BIA*) [*2*] es una actividad que se ha realizado a nivel de la organización, y ha tenido en cuenta todos los departamentos y ámbitos de la empresa. Este análisis de impacto ha sido ya realizado en la empresa ZEREPSA, como parte de otros estudios (como parte de un plan de calidad), y formará el núcleo de actividad del proyecto de centro de respaldo.

Durante el proceso de análisis se han definido:

1. Los **departamentos y procesos** generales de la empresa, recogidos en el Anexo A - Áreas y procesos.
2. Los **procesos**, **servicios**, **actividades** y **funciones** que las TIC desempeñan y prestan en la empresa. Estos procesos son los procesos de TI que dan soporte y apoyan a los procesos de negocio que la empresa desarrolla y que si bien no son objeto del estudio, serán estos los que permitan priorizar la disponibilidad de aquellos que constituyen la infraestructura y el conjunto de las aplicaciones de TI, y permiten valorar cada elemento en función de la importancia dentro de los procesos de la empresa. La lista de sistemas a respaldar se encuentran en el Anexo B - Censo y priorización de aplicaciones.
3. Los **recursos** necesarios para llevar a cabo cada proceso desempeñado. Aunque estos recursos son tanto humanos así como de conocimiento, tecnológicos y económicos, nosotros para el problema que nos ocupa nos hemos centrado en los recursos de TI: las aplicaciones, la plataforma tecnológica y la plataforma física. Estos recursos tecnológicos son los que pretendemos respaldar.
4. Las **interrelaciones** entre los procesos y/o departamentos. Desde nuestro punto de vista estas interrelaciones se han considerado ya que ha sido necesario censar las aplicaciones, y cada departamento ha tenido que indicar las aplicaciones que utiliza.
5. La **criticidad de cada proceso**: Este aspecto ya ha sido elaborado para toda la organización. En el sentido de los recursos de TI se ha tenido en cuenta el impacto de estos recursos sobre

el desarrollo de cada proceso de la empresa.

Para cada proceso de negocio, se ha decidido un "Objetivo de Tiempo de Recuperación" (*Recovery Time Objective, RTO*), que es el tiempo máximo deseable para recuperar el proceso en caso de caída, y un "Objetivo de Punto de Recuperación" (*Recovery Point Objective, RPO*), que es el retraso máximo en el proceso tras su recuperación (relacionado con la pérdida de datos en los pasos intermedios del proceso).

La relación de los procesos del negocio, sus aplicaciones relacionadas, los recursos usados, la criticidad de los mismos así como los tiempos de recuperación se consideran en el Anexo B - Censo y priorización de aplicaciones. Las diferentes áreas han sido consideradas en función de los aplicativos o sistemas afectados así como por la ubicación en que se explotan, de tal modo que hay áreas o aplicativos en ciertas áreas que afectan a la totalidad de la empresa mientras que otras son puntuales en alguna determinada dependencia o unidad.

2.1.2 Análisis de riesgos

Los tipos típicos de riesgo y su porcentaje de incidencias en instalaciones de CPDs se exponen en la siguiente tabla.

Causa	**% Ocurrencias**
Caídas de Alimentación de energía	27,7%
Daños por descargas eléctricas (tormentas)	11,7%
Diversas causas (no identificadas)	10,1%
Inundaciones	9,6%
Explosiones (bombas)	7,2%
Errores de HW	7,7%
Huracanes	6,3%
Incendios	5,6%
Energía mal regulada (picos y caídas o microcortes)	5,1%
Terremotos	4,9%
Caídas en las redes de comunicaciones	2,1%
Errores Humanos	2,0%

Tabla 1 Causas más comunes de indisponibilidad *[**3**] [**3**]*

Otros tipos incluyen fallos del aire acondicionado, error de software, sabotajes, rotura de tuberías, agua en general, contaminación, revueltas, accidentes de transporte, etc.

Los riesgos se han evaluado teniendo en cuenta los diferentes enfoques que se presentan en los diferentes conceptos relativos a los mismos.

Se ha evaluado la potencial probabilidad de pérdida de datos y malfuncionamiento o fallo de los sistemas (en su totalidad, contemplados como hardware, software e infraestructura que los soporta).

Por otro lado se ha evaluado la probabilidad de accesos indeseados y agresiones externas a dichos datos y sistemas.

Los riesgos potenciales frente a agresión de los sistemas TI fueron evaluados y valorados de acuerdo a la metodología Magerit [4] del Ministerio de Hacienda y Administraciones Públicas de España. Para su evaluación se ha empleado los criterios contemplados en las herramientas que a tales efectos ha desarrollado el CCN (EAR/PILAR [5]).

El análisis de Riesgos del Centro principal nos ha servido para desarrollar un plan de prevención de riesgos en el Centro de Respaldo que se propone. En cuanto a los riesgos de mal funcionamiento se ha tenido en cuenta que se desea un CPD Tier III preparado para Tier IV. Además como primera aproximación el análisis de riesgos de los sistemas en explotación se ha realizado teniendo en cuenta los datos de priorización (disponibilidad necesaria del sistema) y los niveles de servicio con que se ofrecen dichos sistemas a sus usuarios o explotadores así como de sus cumplimientos. De este modo el documento base para dicho análisis lo constituye en su apartado de análisis de riesgos en la explotación de los sistemas. Y de cuya aplicación se obtuvieron los Sistemas críticos a respaldar y las máquinas relacionadas así como los procesos del CPD que debían ejecutarse en el respaldo junto al personal que los desempeñaba, de este modo se pudieron definir las áreas del Centro de respaldo que eran necesarias y las superficies necesarias en cada área para dar servicio a dichos procesos.

2.2 Requisitos generales de la solución

En cuanto a la solución propuesta, se han considerado dos partes claramente diferenciadas:

- La arquitectónica
- La de los Sistemas de Información y Comunicaciones.

Para el correcto funcionamiento del edificio que albergue al Centro será obligatorio (por ser exigencia normativa) todo lo que indique el Código Técnico de la Edificación [***6***].

Las siguientes son las características principales a tener en cuenta para el centro.

Subdivisión "X" / "Y" (en cuadrículas) de las instalaciones desatendidas y de alta concentración de equipos de TI.

- Áreas de CPU / DASD [1]/ Server
- Áreas de Red
- Áreas de sistemas de Servicios del edificio que se requieren para mantener los servicios TI interrumpidamente
- Conexión directa a redes de suministro (electricidad, fibra óptica, etc.)

[1] DASD: Direct Access Storage Device

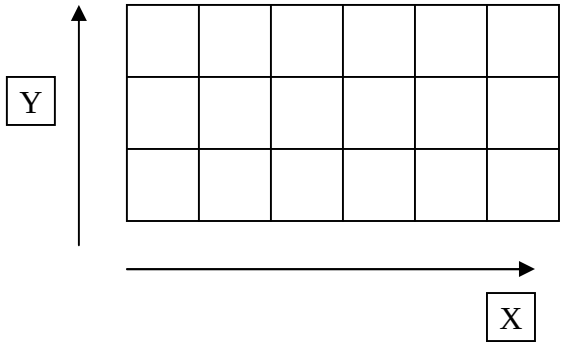


Figura 6 Subdivisión X/Y de equipos de TI

Instalaciones de almacenamiento de datos desatendidas.

- Almacenes de datos acordes a UNE-EN 1047 [7] [7] [8] [8]
- Áreas de sistemas de Servicios del edificio que se requieren para mantener los servicios TI interrumpidamente
- Conexión directa a redes de utilidades (electricidad, fibra óptica)

Garantía de una operación continua de las TI y los sistemas de red por medio de un apropiado diseño de los sistemas de servicio del edificio

- 7 x 24 h / 365 días
- Disponibilidad > 99,9 %
- No se permiten ventanas de mantenimiento
- No se permiten cortes programados
- Se aplicará la filosofía n+1 / n+2 a todos los componentes importantes de los sistemas de servicios del edificio (enfriamiento en salas técnicas, AA de vida, energía eléctrica y otros)

Proporcionar un núcleo para futuros cambios en la tecnología

- Disposición de suelo técnico abierto (accesible)
- Estructura modular
- Matrices de múltiples áreas de IT
- Diseño modular de los componentes de los sistemas de servicios al edificio

Reconciliar objetivos conflictivos

- Proporcionar flexibilidad para permitir cambios futuros y desconocidos
- Proporcionar un control de seguridad física sólida al entorno físico del CPD de respaldo

Equilibrio entre la accesibilidad y la seguridad

- Aplicación de los modelos de zona segura/línea de seguridad
- Integración de las áreas de servicios y sistemas del área de CPD en el conjunto de la seguridad del edificio.

Proporcionar condiciones favorables tanto a los empleados como a los visitantes

- Entorno de trabajo cálido y confortable
- Manteniendo precauciones de seguridad eficientemente.

Mantenimiento de los principios de desarrollo sostenible

- Diseño y materiales beneficiosos medioambientalmente
- Reutilización de instalaciones
- Aplicación de tecnologías energéticamente eficientes (por ejemplo cogeneración).

2.2.1 Descripción de la norma ANSI TIA 942

En todo el diseño se seguirá la metodología propuesta por la norma ANSI TIA 942 [***1***]. El estándar TIA-942 nació con la intención de unificar criterios en el diseño de áreas de tecnología de la Información y comunicaciones. Este estándar que en sus orígenes se basa en una serie de especificaciones para comunicaciones y cableado estructurado, avanza sobre los subsistemas de infraestructura y los subsistemas de redes, indicando los criterios mínimos que se deben cumplir para clasificar estos subsistemas en función de los distintos grados de disponibilidad que se pretende alcanzar para los mismos.

La norma TIA-942 es un estándar que describe los requerimientos que deberían ser considerados para implementar la infraestructura de un data center.

Basado en recomendaciones del Uptime Institute, establece cuatro niveles (Tiers) en función de la redundancia necesaria para alcanzar niveles de disponibilidad de hasta el 99.995%. Cada uno de los cuatro Tiers que plantea el estándar se corresponden con cuatro niveles de disponibilidad, teniendo que a mayor número de Tier mayor disponibilidad, lo que implica también mayores costes constructivos y de mantenimiento.

El más simple es un centro de nivel 1 (Tier 1), que es básicamente una sala de servidores siguiendo las directivas básicas para la instalación de sistemas informáticos. El nivel más estricto es el 4 (Tier 4), que está diseñado para albergar los sistemas informáticos más críticos. Otra consideración es la ubicación del centro de datos en un entorno capaz de garantizar la seguridad de los datos, así como las condiciones ambientales necesarias para el correcto funcionamiento de las infraestructuras, como por ejemplo la refrigeración.

La norma exige las condiciones de redundancia correspondientes a cada Tier tanto para los sistemas de la infraestructura (energía, enfriamiento, ventilación, contraincendios, etc.) como para la infraestructura eléctrica y electrónica (redes equipos, etc.) como para los sistemas de información (aplicaciones, etc.).

2.2.1.1 Tier I: CPD (Centro de Proceso de Datos) básico.

Un CPD (Centro de Proceso de Datos) Tier I puede ser susceptible a interrupciones tanto planeadas como no planeadas. Cuenta con sistemas de aire acondicionado y distribución de energía; pero puede o no tener piso técnico, UPS o generador eléctrico; si los posee pueden no tener redundancia y existir varios puntos únicos de fallo. La carga máxima de los sistemas en situaciones críticas es del 100%. La infraestructura del CPD (Centro de Proceso de Datos) deberá estar fuera de servicio al menos una vez al año por razones de mantenimiento y/o reparaciones. Situaciones de urgencia pueden motivar paradas más frecuentes y errores de operación o fallos en los componentes de su infraestructura causarán la parada del CPD (Centro de Proceso de Datos). La tasa de disponibilidad máxima del CPD (Centro de Proceso de Datos) (1-1/365)*100 =99,726% admitiendo el supuesto

de NO PERDIDAS DE DATOS NO CAIDAS PUNTUALES.

2.2.1.2 Tier II: componentes redundantes.

Los CPD con componentes redundantes son ligeramente menos susceptibles a interrupciones, tanto planeadas como las no planeadas. Estos CPDs cuentan con piso falso, UPS y generadores eléctricos, pero están conectados a una sola línea de distribución eléctrica. Su diseño es "lo necesario más uno" (N+1), lo que significa que existe al menos un duplicado de cada componente de la infraestructura. La carga máxima de los sistemas en situaciones críticas es del 100%. El mantenimiento en la línea de distribución eléctrica o en otros componentes de la infraestructura puede causar una interrupción del procesamiento. La tasa de disponibilidad máxima del CPD es 99.749% del tiempo. Para este supuesto la norma admite una pérdida total de 3/4 de día al año, Resultando una disponibilidad de (1-0,75/365)*100 = 99,794%

2.2.1.3 Tier III: mantenimiento concurrente.

Las capacidades de un CPD de este tipo le permiten realizar cualquier actividad planeada sobre cualquier componente de la infraestructura sin interrupciones en la operación. Actividades planeadas incluyen mantenimiento preventivo y programado, reparaciones o reemplazo de componentes, agregar o eliminar elementos y realizar pruebas de componentes o sistemas, entre otros. Para infraestructuras que utilizan sistemas de enfriamiento por agua significa doble conjunto de tuberías. Debe existir suficiente capacidad y doble línea de distribución de los componentes, de forma tal que sea posible realizar mantenimiento o pruebas en una línea, mientras que la otra atiende la totalidad de la carga. En este Tier, actividades no planeadas como errores de operación o fallos espontáneos en la infraestructura pueden todavía causar una interrupción del CPD La carga máxima en los sistemas en situaciones críticas es de 90%. Muchos CPDs Tier III son diseñados para poder actualizarse a Tier IV, cuando los requerimientos del negocio justifiquen el costo. La tasa de disponibilidad máxima del CPD es 99.982% del tiempo. La Norma admite una caída total de hora y media al año con lo que resulta una disponibilidad de (1-1,5/24*365)*100 Resultando así un 99,982% de disponibilidad.

2.2.1.4 Tier IV: tolerante a fallos.

Este CPD provee capacidad para realizar cualquier actividad planeada sin interrupciones en las cargas críticas, pero además la funcionalidad tolerante a fallos le permite a la infraestructura continuar operando aun ante un evento crítico no planeado. Esto requiere dos líneas de distribución simultáneamente activas, típicamente en una configuración system + system; eléctricamente esto significa dos sistemas de UPS independientes, cada sistema con un nivel de redundancia N+1.

La carga máxima de los sistemas en situaciones críticas es de 90% y persiste un nivel de exposición a fallos, por el inicio una alarma de incendio o porque una persona inicie un procedimiento de apagado de emergencia o Emergency Power Off (EPO), los cuales deben existir para cumplir con los códigos de seguridad contra incendios o eléctricos. La tasa de disponibilidad máxima del CPD es 99.995% del tiempo. La norma prevé para este caso un máximo de indisponibilidad de media hora al año. Resultando así una disponibilidad de (1-0,5/24*365). Resultando un 99,995% de disponibilidad.

A su vez divide la infraestructura soporte de un CPD en cuatro subsistemas a saber:

- Telecomunicaciones
- Arquitectura
- Sistema eléctrico
- Sistema Mecánico

Dentro de cada subsistema el estándar desarrolla una serie de ítems como los del siguiente cuadro.

Telecomunicaciones	**Arquitectura**	**Eléctrica**	**Mecánica**
Cableado de racks	Selección del sitio	Cantidad de accesos	Sistemas de climatización
Accesos redundantes	Tipo de construcción	Puntos únicos de fallo	Presión positiva
Cuarto de entrada	Protección ignífuga	Cargas críticas	Cañerías y drenajes
Área de distribución	Requerimientos NFPA 75	Redundancia de UPS	Chillers
Backbone	Barrera de vapor	Topología de UPS	CRACs y condensadores
Cableado horizontal	Techos y pisos	PDUs	Control de HVAC
Elementos activos redundantes	Área de oficinas	Puesta a tierra	Detección de incendio
Alimentación redundante	NOC	EPO (Emergency Power Off)	Sprinklers (Rociadores)
Patch pannels	Sala de UPS y baterías	Baterías	Extinción por agente limpio (NFPA 2001)
Patch cords	Sala de generador	Monitoreo	Detección por aspiración (ASD)
Documentación	Control de acceso	Generadores	Detección de líquidos
	CCTV Transfer	switch	

Tabla 2 Subsistemas y componentes descritos en la norma TIA-942

La estructura general se describe en la siguiente figura:

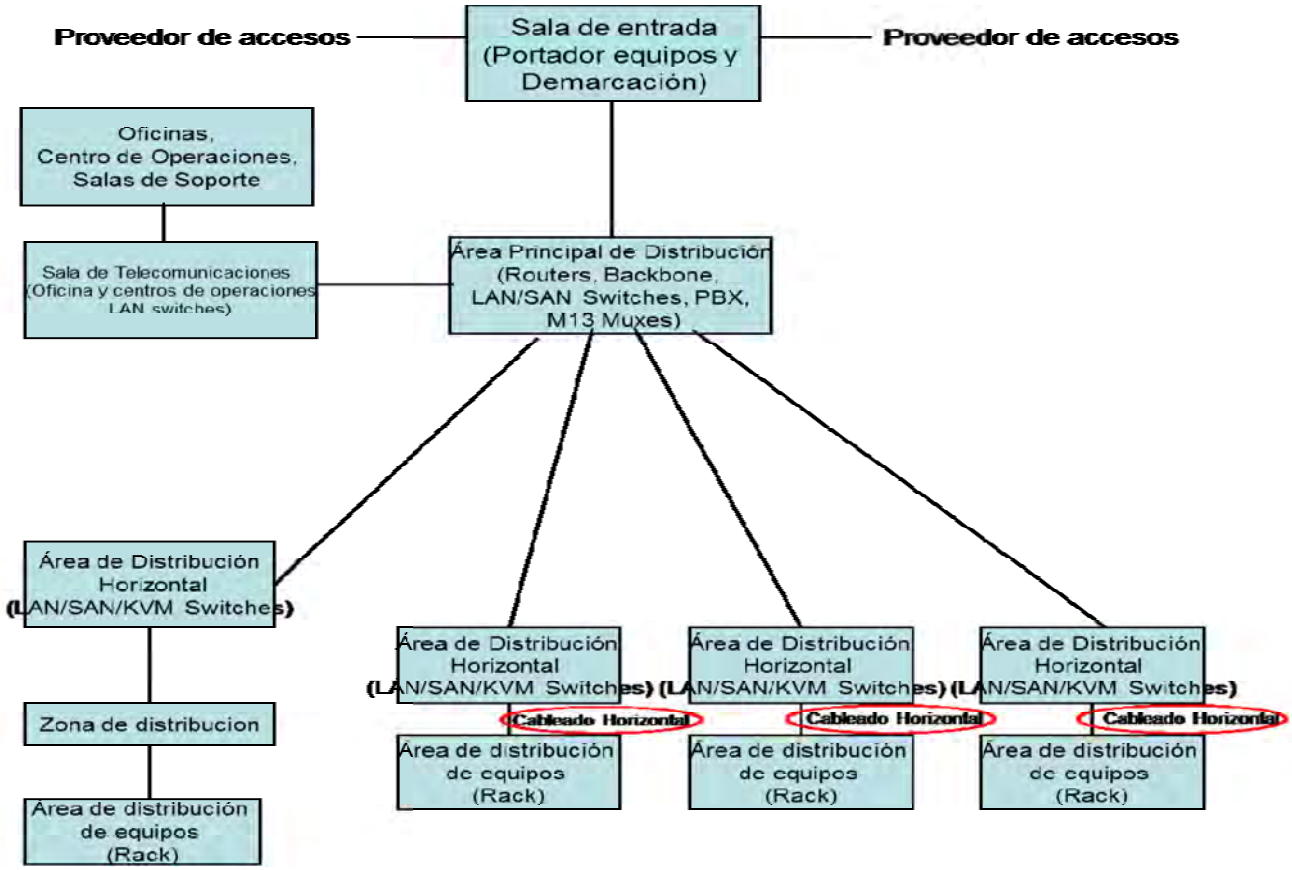


Figura 7: Nomenclatura de espacios conforme ANSI TIA 942

2.3 Estructura geográfica de la empresa, servicios y conexión de centros

La empresa ZEREPSA tiene una sede central en Madrid, en la que está situado el Centro Principal, que da soporte a todas las aplicaciones corporativas y a los servicios de telefonía.

Servicios de comunicaciones: La sede central dispone de una LAN interna y se comunica con varias sedes también en Madrid a través de una WAN de una empresa proveedora, y con las diversas sedes regionales en España a través de una VPN suministrada y servida por un único proveedor de comunicaciones. La empresa tiene también varias delegaciones internacionales que se conectan o bien mediante de VPN a través de Internet o que acceden únicamente a las aplicaciones corporativas de la empresa a través de navegador Web con protocolos SSL.

En la figura siguiente se presenta la interconexión entre sedes de la empresa mediante un esquema de conexionado y distribución de la empresa con sus sedes en Madrid, con las nacionales y con las internacionales:

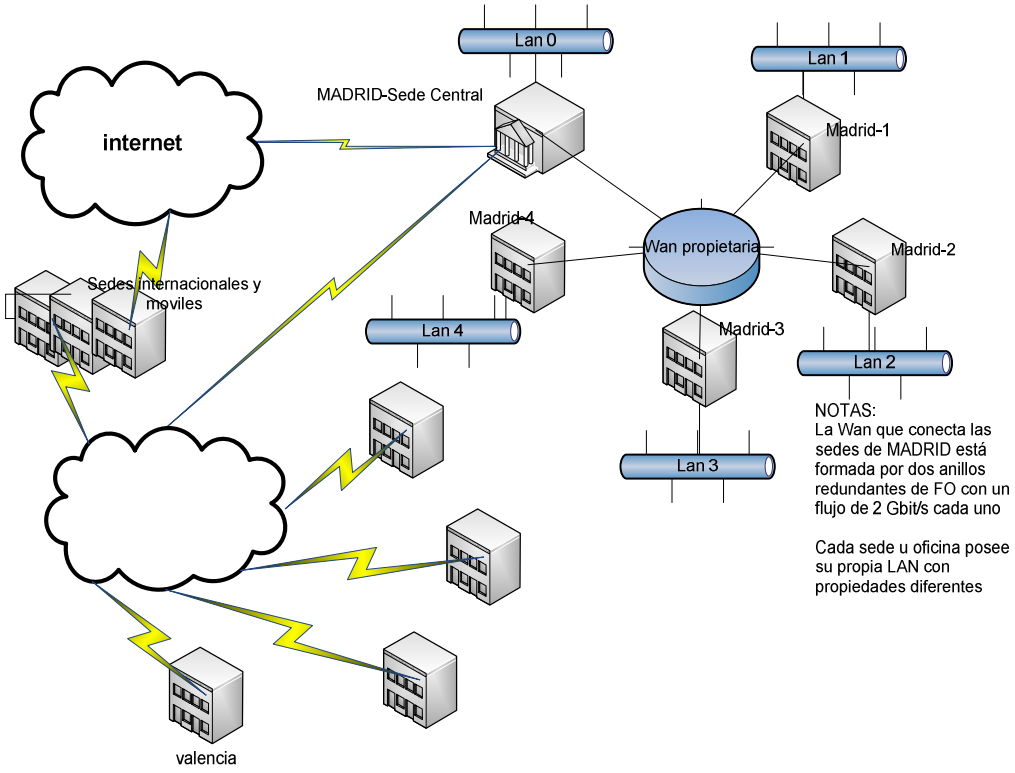


Figura 8 Visión macro de conexiones de red ZEREPSA

Servicios de telefonía: La sede central está dotada con telefonía IP, y se prevé que las distintas sedes nacionales vayan migrando hacia este sistema, pero mientras tanto disponen de centralitas locales (*Private Branch eXchange, PBX*). La telefonía fija tradicional a nivel nacional la suministra un único proveedor de telefonía, que además dota a la empresa de una réplica del sistema de facturación que se aloja en el centro principal, de forma que ZEREPSA pueda acceder a la facturación de sus empleados. Este sistema de facturación se aloja en el centro principal.

Servicios de telefonía móvil y satélite: ZEREPSA dispone también de servicios de telefonía móvil corporativa, que permiten además de los servicios de voz, la conexión a través de GPRS al centro principal para acceso a correo electrónico y a determinadas aplicaciones corporativas. ZEREPSA tiene desplegados terminales móviles (Smartphones, tablets) que permiten establecer conexiones a la VPN de modo seguro. Al igual que en el caso de la telefonía fija, el proveedor de telefonía dota a la empresa con una réplica del sistema de facturación.

Servicio de vigilancia y control: De igual modo ZEREPSA cuenta con un sistema de Seguimiento de incidencias y averías, así como de medición de ciertos parámetros de red que le permiten mantener visible el cumplimiento de los ANS (acuerdos de nivel de servicio) contratados con la empresa. Tanto para las telefonías y comunicaciones satélite como para los de red.

Servicios compartidos o con terceros: Finalmente, el proveedor de telefonía dota a ZEREPSA con varias conexiones RDSI disponibles para el acceso remoto a sistemas específicos para terceros (por ejemplo, subcontratas de servicios, mantenimientos remotos, etc.).

En la figura siguiente se presenta el esquema general de las conexiones de red.

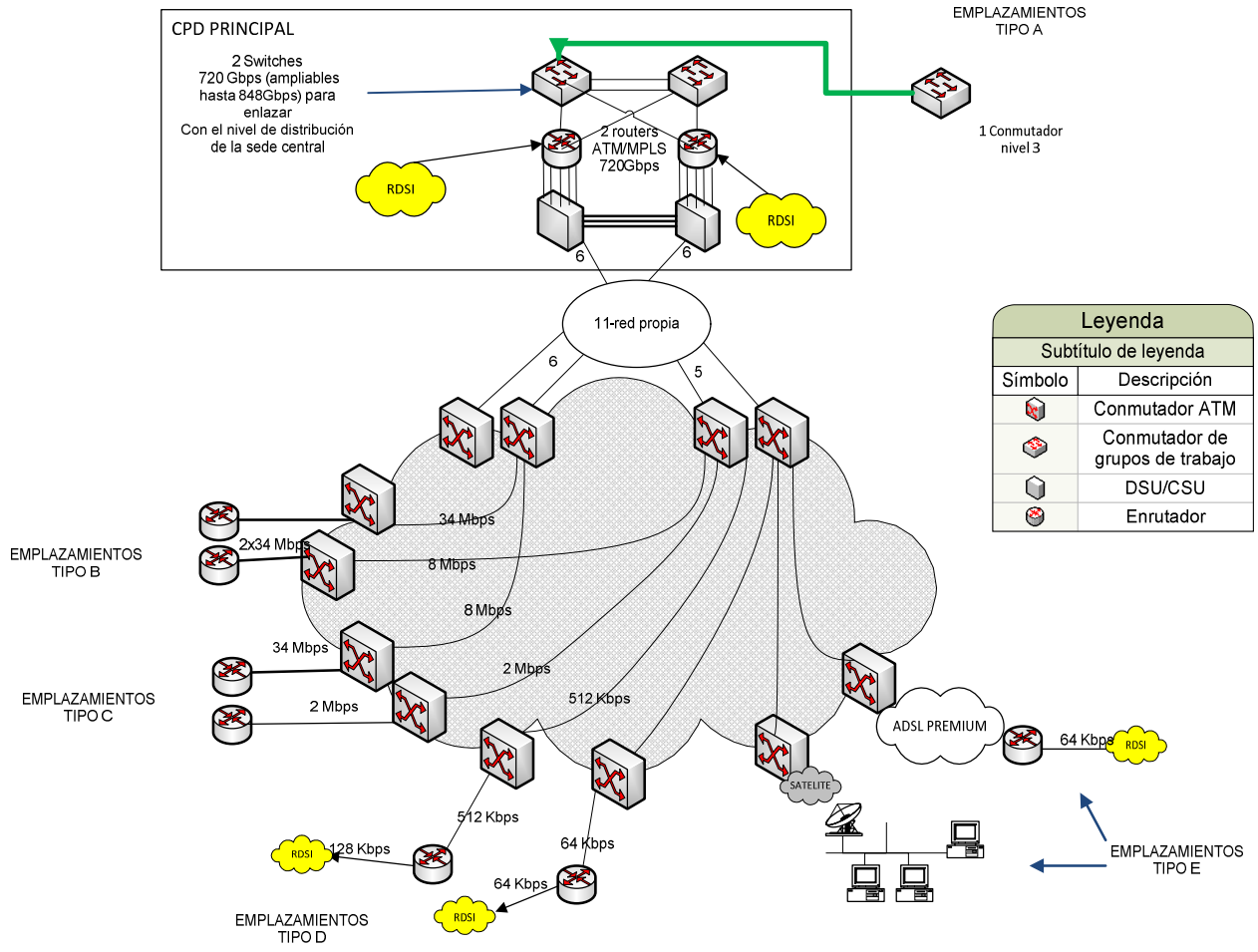


Figura 9 Red WAN de ZEREPSA y conexión del centro principal

La conexiones están clasificada en nodos según el flujo necesario en cada uno de ellos. Los diferentes centros de ZEREPSA y su conectividad con la sede principal se definen en seis tipos diferentes, conforme descrito en la siguiente tabla:

Escenario	Conexión al primer switch	Enlace CPD	Acometidas
A	2 x 1000SX	1 Gbps	2 (una por cada switch)
B	2 x 100 Base T	34 Mbps	2 (una por router)
C	10/100 Base T	8 Mbps	1 + RDSI
D	10/100 Base T	ADSL	1 + RDSI
	10/100 Base T	64 Kbps	1 + RDSI
E	10/100 Base T	64 Kbps	1 xDSL

Tabla 3 Escenarios de conexión con la sede ZEREPSA

2.4 Aplicaciones

Este apartado describe todos los elementos a nivel de aplicación a los que habrá de dar respaldo. Se adjunta en el Anexo B - Censo y priorización de aplicaciones el catálogo de aplicaciones a respaldar. Las características propias de las aplicaciones así como las condiciones de recuperación, operación y restauración del estado inicial (antes del incidente que originase la entrada en funcionamiento de la aplicación de respaldo) se indican en el citado anexo. No obstante, no se

definen las características de las aplicaciones en cada uno de los apartados.

Como aplicaciones de especial atención a la hora de darles respaldo se consideran aquellas que forman la base tecnológica para el funcionamiento de cualquier otro sistema. ZEREPSA ha definido la base tecnológica a partir de una arquitectura de niveles basada en el modelo de infraestructuras adaptativas [*9*].

2.4.1 Tipos de aplicaciones

Como primer paso para el diseño del centro de respaldo se realiza un censo de las aplicaciones actuales de la empresa. En este censo se reúne la siguiente información:

- Nombre de la aplicación
- Descripción
- Entorno: Indica el entorno de ejecución de la aplicación; se indica si es un entorno dedicado o compartido. Si el entorno es dedicado se indicará si este es una máquina completa o es una partición virtual del host. Si el entorno es compartido se dará una referencia para poder localizar el resto de aplicaciones que se ejecutan en el mismo entorno.
- Gestor de BBDD: Indica la tecnología del gestor de bases de datos del que depende (si lo hubiera), indicando si utiliza una instancia independiente o si cohabita con la base de datos de otras aplicaciones en la misma instancia.
- Número de usuarios: Se indicará la población de usuarios que tiene acceso a la aplicación (máximo aproximado) y, si estuviera medido, el número de accesos diarios.
- Entornos replicados: Enumera los entornos replicados de la aplicación (desarrollo, pruebas, etc.) si los hubiera. Los usuarios son tanto personas físicas como otras aplicaciones.
- Dependencias: Indica las dependencias con otros sistemas. En este censo sólo se indican dependencias de manera aproximada; una enumeración completa de las dependencias e integraciones de las aplicaciones debe describirse en la documentación de la aplicación, y es necesaria como parte del plan de recuperación de la aplicación.

Como resultado del censo de las aplicaciones describimos los rasgos principales de las aplicaciones de la empresa:

- Parte de las aplicaciones de negocio de la empresa, así como las de soporte al negocio son aplicaciones históricas (legados) que corren sobre el host IBM Z Series del que dispone la empresa. Pese a que la tendencia ha sido normalizar estas aplicaciones y migrar hacia soluciones de terceros, siguen formando parte del corazón de la operativa de negocio, como son la gestión de nóminas, gestión de personal, la facturación y el sistema integrado de gestión logística (que gestiona la rama principal del negocio).
- Otro grupo de aplicaciones que desarrollan el negocio de la empresa reside en servidores dedicados:
    - La parte de las aplicaciones de negocio que se han unificado reside en un sistema ERP (SAP) que dispone de un entorno dedicado, tanto de ejecución como de base de datos.
    - Por otro lado, la empresa también dispone de un sistema de documentación (DOCUMENTUM), que reside en un servidor dedicado. Este sistema está integrado con el sistema SAP y con algunas aplicaciones web.

  - Otro sistema es un CRM (Siebel) dedicado al centro de atención al cliente y a las campañas de marketing. Este sistema es accesible desde fuera de ZEREPSA para permitir la subcontratación a una empresa de tele operadores. Para ello se dispone de una conexión de VPN con limitación exclusiva a los servidores del sistema CRM.
  - El sistema de control de facturación de telefonía proporcionado por el operador de telefonía, también reside en un entorno separado.
  - Estos sistemas se integran con las aplicaciones legacy y entre sí a través de middleware SOA y un bus de integración TIBCO.
- Se detecta otro grupo diferenciado que son aquellas aplicaciones accesibles desde Internet:
  - Portal corporativo de la empresa (ZEREPSA.COM)
  - Intranet corporativa (INTRANET.ZEREPSA.COM), que permite acceder a los empleados a diversa información (p.ej.: nóminas, carga laboral, directorio, solicitudes de material, gestión del conocimiento, etc.)
  - Portal de clientes, que permite a los clientes acceder a detalles de sus contratos, estado de pedidos, situación de los diferentes contratos, contacto con el personal de la empresa, etc.
- La organización dispone de aplicaciones corporativas que, sin desarrollar la línea principal de negocio, forman parte de la estructura de soporte:
  - Correo electrónico (Exchange)
  - Servidores de directorio (LDAP)
  - Servidores de dominio (DNS)
- Por último se detectan una serie de aplicaciones que dan soporte a la infraestructura de IT
  - Monitorización de sistemas (Tivoli)
  - Virtualización (VMWare virtual Center)
  - Distribución de Antivirus (MCAffee)
  - Distribución de Software (HP RADIA)
  - Control de configuración (COCON)
  - Plataforma de Identidad digital (sistema de PKI), que incluye la emisión y gestión de certificados, así como el control de accesos basado en Tarjeta Electrónica del Empleado, que se integran con sistemas de control biométrico para control de acceso a zonas de seguridad.

Estos sistemas son considerados críticos a efectos de su respaldo. La tabla completa de aplicaciones de ZEREPSA que requieren respaldo se puede encontrar en el Anexo B - Censo y priorización de aplicaciones.

2.4.2 Volumetría

En este punto se estudiaron las necesidades de volumen, tanto de almacenamiento como de ancho de banda de las aplicaciones propuestas; esta volumetría nos dio una base para dimensionar los recursos del centro de respaldo.
Servidores:

- Host: aproximadamente 500.000 transacciones diarias acumuladas para todas las aplicaciones, con un uso de 25% de la capacidad en el momento pico y un 5% en el momento valle.
- Correo-e: 25.000 cuentas; promedio de mensajes enviados/recibidos 10.000
- Controladores de dominio: 20. De estos, cuatro están en el centro principal y el resto distribuidos en diferentes sedes como controladores secundarios.
- Servidores de aplicaciones: 40 servidores, dedicados a las diferentes aplicaciones descritas; algunos agrupados formando clústeres para alta disponibilidad; 10 dan servicio a aplicaciones Web accesibles desde Internet y a la página Web corporativa.

Ancho de banda:

- Interno en el centro principal: 10.000 --> 15.000 usuarios y aplicaciones demandando ocupación de red.
- Entre los distintos centros (WAN) VPN-SSL con 500 conexiones simultaneas.
- Con centros en el extranjero: VPN Internet 15 Mbps – 34 Mbps.
- De Internet: 50Mbps – 155 Mbps.
- De terceros: 30x64Kbps para conexiones RTB + 15Mbps – 34 Mbps.

Almacenamiento:

- Gestor BBDD
  10 máquinas, con una capacidad agregada de 100 TB.
- Ficheros
  SAN: 6 máquinas conectadas a un almacenamiento de 12 TB netos.
  18 máquinas para almacenamiento otros servicios dispares, en proceso de migración a SAN.

2.4.3 Agrupaciones de aplicaciones

Era necesario definir ciertas relaciones entre las distintas aplicaciones, de modo que se puedan detectar dependencias y correspondencias que permitan mejorar el funcionamiento del centro principal como del centro de respaldo. Nos interesan dos tipos de agrupaciones:

- Agrupación lógica: Por agrupación lógica hemos considerado tanto las relaciones que definen un sistema aglutinando varias aplicaciones (relación de integración) como las relaciones que implican una necesidad en un sólo sentido (relación de dependencia).
- Agrupación física: En la agrupación física aportamos la información de cohabitación de las diferentes aplicaciones, de forma que sabemos qué aplicaciones están conviviendo en el mismo entorno lógico o físico (a nivel de servidores de aplicaciones).

2.4.4 Necesidad de respaldo por criticidad

Tras censar todas las aplicaciones, ha sido necesario definir niveles de importancia de estas, de forma que los recursos del centro de respaldo se orienten hacia maximizar el respaldo de las aplicaciones más críticas.

La valoración de la criticidad se realiza conjuntamente entre el departamento de IT, los departamentos que utilizan cada una de las aplicaciones y la Dirección de ZEREPSA. Esta valoración se decidió definitivamente, en reunión conjunta de los responsables de los distintos departamentos, tras disponer la valoración que cada uno de ellos independientemente había efectuado. La dirección aplicó la última palabra en las decisiones contradictorias. Esta valoración indica:

- Tiempo de no disponibilidad deseado: En caso de fallo, el tiempo que se puede admitir que

un sistema o aplicación no esté disponible.
- Tiempo de restauración deseado: En caso de pérdida de datos, la cantidad de datos que se pueden perder debido a no tener copia de respaldo.

Con estos factores definimos los siguientes grupos [***10***]: [***10***]

- **Aplicaciones críticas o de criticidad muy alta:** Son aquellas que forman el núcleo del negocio de la empresa. Sin ellas no se puede llevar a cabo la operativa diaria de la empresa. A este grupo se incorporaron las aplicaciones y sistemas que configuran los sistemas de base o de arquitectura básica de la empresa. De modo que todos aquellos sistemas que son necesarios para soportar el funcionamiento de los demás se consideraron críticos. También se consideraron como críticos aquellos sistemas cuya interrupción supone un impacto importante en la comunicación y bienestar de las personas De este modo se consideran críticos los sistemas tales como el correo electrónico, sistemas de internet y de intranet, sistemas de distribución de software, sistemas de ERP, sistemas de antivirus, LDAP, etc.
- **Aplicaciones semicríticas o de criticidad alta:** Las aplicaciones semicríticas son aquellas que no son aplicaciones críticas pero que cumplen alguno de los dos siguientes supuestos:
  - La aplicación es crítica para el desarrollo del trabajo de la empresa durante un periodo de tiempo específico, mientras que fuera de ese periodo de tiempo su fallo no implica una parada en el funcionamiento de la empresa.
  - Se consideró a tales efectos que los periodos de tiempo que estas aplicaciones deben estar en funcionamiento es como mínimo de dos días, para resolver su funcionamiento y durante esos días no pueden perder ningún dato, convirtiéndose en críticas. Pero fuera de esos días la aplicación no es crítica.
  - La aplicación, sin ser crítica, contiene información importante para el desarrollo del negocio principal, y esta tiene una tasa de variación alta.
- **Aplicaciones subcríticas o de criticidad media:** Aquellas que no son críticas ni semicríticas pero interrelacionan varios departamentos o varios procesos de negocio. Si bien estas aplicaciones no influyen directamente en el proceso general de la empresa, sí le permiten dar valor añadido a los procesos de negocio.
- **Aplicaciones no críticas, o de criticidad baja:** Aquellas aplicaciones que no cumplan los criterios anteriores. Son típicamente aplicaciones departamentales específicas o de gestión internas que no tienen impacto en las líneas de negocio. En este grupo se incluyen también las aplicaciones que no se albergan en el centro de datos principal.

Todas las aplicaciones críticas deben ser respaldadas junto a su equipamiento, redes, comunicaciones en general, almacenamiento ares de ocupación y personal que les da servicio.

Basados en la criticidad de las aplicaciones se marcó la criticidad de los sistemas que las soportan y sobre los que se explotan dando como resultado la tabla del Anexo B - Censo y priorización de aplicaciones, que se resume en la siguiente tabla:

Prioridad	Número de aplicaciones
Muy Alta	96
Alta	64
Baja	29
Media	61
Total general	250

Tabla 4 Resumen de aplicaciones por prioridad

En el anexo expresado se clasifican las aplicaciones CRITICAS como de criticidad MUY ALTA las aplicaciones SEMICRITICAS como de criticidad ALTA, las aplicaciones SUBCRITICAS como de criticidad MEDIA y las aplicaciones NO CRITICAS como de criticidad BAJA y que en su mayoría no serán objeto de respaldo.

2.5 Datos, almacenamiento

A continuación se describe someramente las necesidades de almacenamiento de datos, tanto de réplica como de copias históricas.

Para el almacenamiento de datos se dispone en la sede central de una red SAN con dispositivos de búsqueda y almacenamiento. Se efectúa el almacenamiento sobre RAID de discos, para los datos de uso y cada semana se pasan a un sistema de robots para su disponibilidad como datos históricos. No obstante existen aplicaciones que por su estructura distribuida (correo electrónico interno, sistemas de logísticos de la flota, etc.), efectúan el almacenamiento de forma también distribuida y de la que se mantiene un servidor en el CPD de la sede central con visibilidad completa del estado del almacenamiento y operación de todos y cada uno de los servidores.

En la actualidad, tanto las aplicaciones como los datos se disponen replicados en el CPD de la sede principal. Un elevado número de aplicaciones y sistemas se disponen trabajando en clúster.

Así los sistemas calificados como críticos, semicríticas y subcríticas y no críticas serán respaldados en el almacenamiento de sus datos, de forma que se mantenga la integridad de los mismos con la misma fiabilidad que en el Centro principal. Para ello se prevé un sistema de refresco de los datos diario en formato activo-pasivo. Se efectuará el volcado a partir de las 00 horas de cada día.

El almacenamiento pues de los sistemas será el mismo que en el centro principal, que queda descrito en la Tabla 5 Infraestructura hardware del centro principal del apartado 2.6.

2.6 Servidores, HW necesario

De las aplicaciones distribuidas se dispone de un servidor en cada plataforma (plataformas de tierra, marinas, sedes locales y nacionales) dichos servidores se relacionan con uno en el CPD de la sede central que gestiona el sistema distribuido manteniendo el sincronismo y los datos maestros para las operaciones no síncronas. El estado para tales sistemas es tal que no se admite una pérdida de datos de más de 1 hora.

Tales servidores son para las aplicaciones distribuidas (correo, logística, proveedores, etc.).

El parque de servidores identificado para las aplicaciones principales es de unos 150.

Por decisión corporativa se establece que los sistemas distribuidos, no serán respaldados en su totalidad, limitándose a dar respaldo al servidor que de las aplicaciones que resulten se encuentre en el CPD de la sede central.

Son aplicaciones distribuidas, de entre las que figuran en el Anexo B - Censo y priorización de aplicaciones:

- Correo electrónico
- Sistemas logísticos
- Sistemas de flota, entendiendo por tales aquellas aplicaciones que sirven para la actividad de cada buque, vehículo de ruedas o aeronave de los que dispone bien sea en activo o en estado

de reparación de entre los vehículos que son y sirven a los interesas propios de la compañía.

La infraestructura hardware que da soporte a las aplicaciones mencionadas, se resume en los siguientes elementos:

Entorno	Elementos
Host	2 IBM z900
HP-UX	8 servidores HP ProLiant DL, ocupando 1 rack 10 servidores Integrity, ocupando 2 racks
SUN Solaris	2 racks SunFire 69000 6 racks con 4 servidores SunFire X4200 cada uno
Windows/Linux	18 servidores HP ProLiant DL, ocupando 12 racks
Bases de Datos	25 servidores HP ProLiant DL, ocupando 5 racks
Superdome	1 SX3000 (2 racks) con 128 núcleos, de los cuales están asignados 64, y 8 módulos de I/O.
Servidores Blades	6 racks; cada rack está configurado por 4 bloques c7000, teniendo cada uno 16 blades HP ProLiant BL [***11***] [***11***]
Otros servidores	4 racks albergando diferentes servidores legacy
SAN - Controladores de la red	1 rack para el director SAN Cisco MDS 9700 1 rack para el controlador de volúmenes IBM 1 rack para los controladores de fiber channel con 4 controladores.
SAN - Almacenamiento	4 racks HP EVA 6100 8 racks IBM DS8000
SAN - Librerías de cintas	2 racks IBM Virtualization Engine TS7520, para emular librerías de cintas
DMZ	16 racks de servidores HP ProLiant DL, con 8 servidores por rack, hasta un total de 128 servidores, además de 4 racks para los elementos de red y firewalls

Tabla 5 Infraestructura hardware del centro principal

2.7 Redes, tecnologías específicas, ISP, RTB, VoIP, Telefonía móvil

En este epígrafe se describe otro tipo de redes y tecnologías específicas a las que habrá que dar soporte. En este apartado se incluye tanto los sistemas legacy como sistemas de red no estándares existentes en la empresa.

Describe los proveedores de cada uno de estos servicios, sus conexiones con el centro principal y las necesidades de respaldo para cada uno de ellos, dependiendo de si los diversos servidores

necesarios (por ejemplo, backbone GPRS o HLRs), están ubicados o no en el centro principal. Particularmente, en lo referente a telefonía, el centro de respaldo dará soporte a los sistemas actualmente implantados en el centro principal, así como las previsiones de despliegue de nuevos servicios.

2.7.1 Telefonía fija

El proveedor de telefonía fija da el servicio a ZEREPSA a través de una red privada virtual, en la que las labores de conmutación y todas las funciones de valor añadido propias de las centralitas, se realizan en las centrales de la Red Pública, permitiendo la inclusión de todas las líneas de que disponga como si de extensiones de una centralita común se tratase, y extendiendo las funcionalidades de centralita al entorno WAN.

Para ello, en las instalaciones del Centro Principal y de las distintas delegaciones, se establecen puntos de acceso al operador de telefonía pública. Estos accesos se conectan directamente a las actuales centralitas que posee la compañía en los distintos emplazamientos. En aquellos emplazamientos en que no existe central, se accede través de líneas telefónicas convencionales, RTB o RDSI.

Si bien estos servicios son gestionados por el operador de telefonía, ZEREPSA dispone también de sistemas de gestión de la red privada y de control de la facturación.

La gestión de los servicios que mantiene la empresa exige el empleo de aplicaciones específicas de gestión tanto para la facturación como para las incidencias y cambios que en los equipos o red se originan. Estas aplicaciones se operan desde la sede central de ZEREPSA.

2.7.2 Telefonía móvil

La empresa dispone de una relación con el proveedor del servicio de telefonía que le permite mantener un servicio de convergencia fijo-móvil que se basa en una infraestructura de Red Inteligente para integrar las comunicaciones fijas y móviles.

Básicamente, este servicio permite incluir los teléfonos móviles de la empresa dentro de un único Plan de Numeración Privado que incluya asimismo sus teléfonos fijos, de forma que las comunicaciones entre las extensiones fijas y móviles de ésta sean tratadas como llamadas internas.

Adicionalmente, y adscrito a una extensa gama de funcionalidades, la RPV móvil que establece el servicio permite el establecimiento de grupos de usuarios en el ámbito de la utilización de sus terminales móviles, de cara a categorizar a los mismos desde el punto de vista del uso y del consumo que éstos hagan de sus líneas.

En líneas generales, algunos de los servicios incluidos son: Plan Privado de Numeración, Llamadas Corporativas, Llamadas desde Extensión Fija a Móviles Externos, Llamadas desde Móviles Externos a Operadora, Acceso Directo en Ubicaciones con Centralita Privada, Interfaz de Acceso Primario con señalización Euro-RDSI, Interfaz de Acceso Radio GSM con señalización RDSI, Interfaz de Acceso Radio GSM con señalización analógica, Llamadas Internas cursadas por la red del operador, Llamadas a Móviles Externos establecidas desde la Centralita Privada, Acceso Directo en Ubicaciones sin Centralita Privada, Categorización de los Usuarios, Autorización según Destino, Grupo Especial Restringido, Alarma al Administrador, Alarma a Extensiones Adicionales, Alarma al Usuario, Alarma al 80%, Números de Marcación Abreviada, etc.

2.7.3 Gestión del Servicio

El suministrador del servicio permite a la empresa llevar a cabo su gestión de forma independiente, lo que hace que la empresa disponga de un servicio de gestión del servicio de telefonía en sincronización con el del proveedor del mismo.
Para el seguimiento de la facturación y de la gestión de incidencias internas surgidas o motivadas por el personal de la empresa, se cuenta un punto de contacto (CAU) que recibe las incidencias y las traslada al proveedor del servicio. Los sistemas de gestión tanto de la facturación como de las incidencias serán respaldados.

2.8 Comunicaciones satélite

Asimismo ZEREPSA mantiene contratado un servicio de comunicaciones vía satélite que le permite dar cobertura tanto a sus buques que se desplazan en su labor de recogida y transporte de crudo, como a los vehículos de tierra y de aire así como a los emplazamientos o destacamentos remotos en zonas sin otras coberturas..

Para la gestión de dichas comunicaciones también dispone de aplicaciones que le permiten controlar los acuerdos de nivel de servicio con sus proveedores así como la utilización de los terminales y la gestión de las incidencias que se plantean.

2.9 Seguridad

2.9.1 Sistemas hardware

Los sistemas de mayor riesgo y principales del CPD se hallan actualmente protegidos contra intrusión de tipo electrónico mediante la creación de zonas DMZ, de modo que los accesos se efectúan normalmente a réplicas de los sistemas que se mantienen en esa zona y que están adecuadamente securizados para impedir el acceso a las redes y sistemas principales. Los sistemas en la DMZ se actualizan de cara al exterior en periodo nocturno de igual modo los datos para la actualización de los sistemas en la región de operación normal (LA INTRANET corporativa de la empresa) vuelcan los datos para su actualización a los sistemas principales, en periodo nocturno, tras un filtrado escrupuloso por los sistemas de antivirus. Además todos los sistemas disponen de firewalls en su más próximo acceso. Las zonas desmilitarizadas, contienen a su vez firewalls en ambos sentidos para evitar el paso de sistemas peligrosos.

El esquema general de este sistema se representa en la figura siguiente:

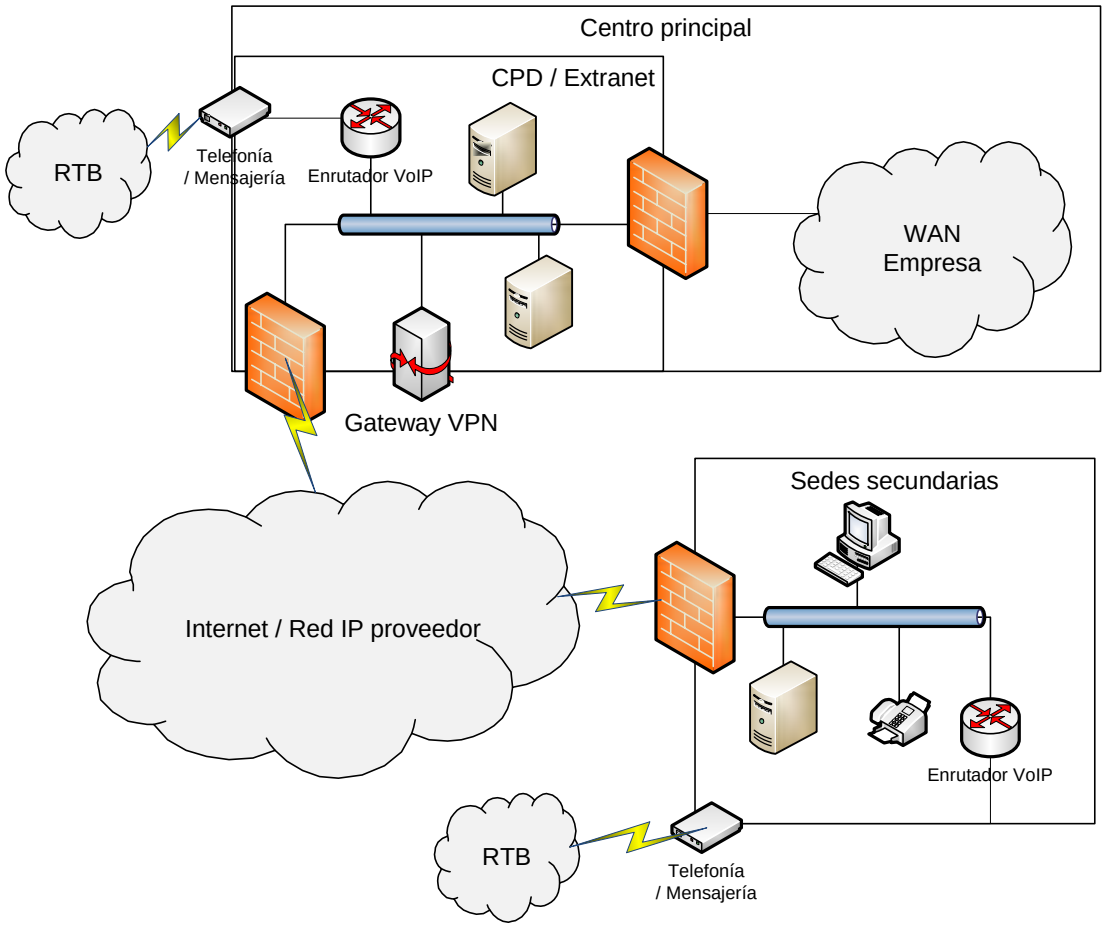


Figura 10 Estructura de Firewall y DMZ

En la siguiente figura se representa el acceso general en el centro principal y los elementos de seguridad que intervienen; destacando que cada componente de seguridad está duplicado y que existe separación entre la red de servicio y la red de gestión.

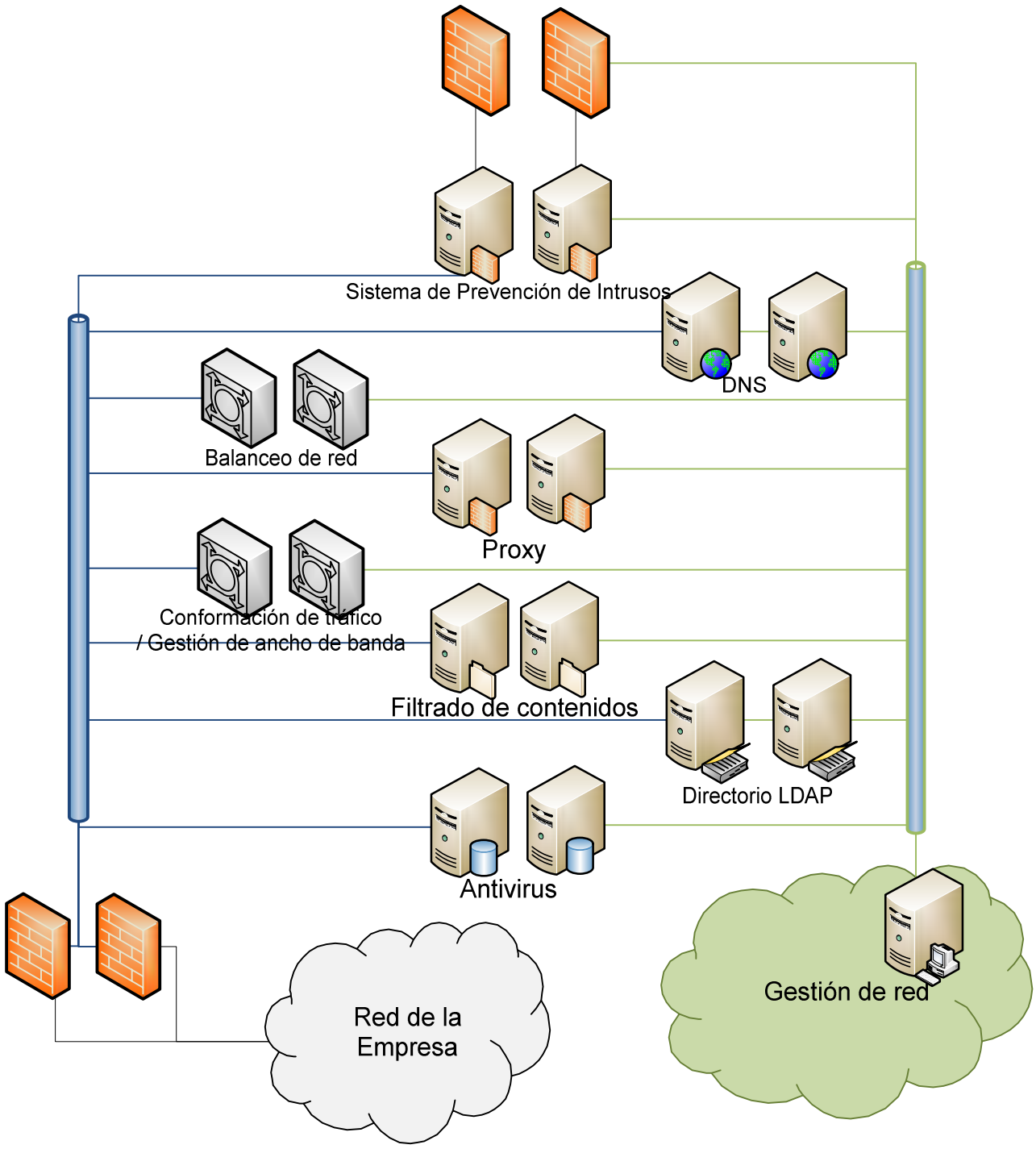


Figura 11 Componentes de seguridad de red; red de servicio y red de gestión

2.9.2 Sistemas software

Los accesos a los diferentes sistemas se realizan mediante los mecanismos de identificación de usuario y la correspondiente habilitación del mismo a través del Directorio Activo en que se tiene registrado a todo el personal de la empresa con sus habilitaciones de acceso a los distintos sistemas y sus capacidades de actuación en los mismos.

La identificación de los usuarios y sus capacidades se realiza de distintas formas:

- **Mediante usuario y contraseña:** Este sistema se centraliza en el Directorio Corporativo y lo administra el personal de informática de la empresa un área particular de la misma.
- **Mediante el uso de clave pública PKI**: Las tarjetas de PKI permiten identificar a los empleados en cualquier sistema, incluidos los sistemas de control de accesos físicos a determinados puntos de las instalaciones de la empresa. Este servicio PKI cubre todos los aspectos de seguridad: confidencialidad (cifrado con certificado), integridad, no repudio, autenticación (firma con certificado) y autorización (basada en los atributos del usuario).

Igualmente este sistema se administra de forma centralizada, si bien las habilitaciones para expedir tarjetas, su creación y su activación y modificaciones se realiza de forma descentralizada en cada zona o área de operación de la empresa.

2.10 Previsiones de crecimiento

Las previsiones de crecimiento son que en un periodo de cinco años:

- Aumento de un 50% del ancho de banda
- Aumento de un 50% del número de usuarios
- Aumento del 100% de capacidad de aplicaciones de extranet
- Aumento del 100% de usuarios móviles
- Aumento del 50% de la capacidad de proceso, distribuida:
    - 10% de la capacidad del mainframe
    - 50% de la capacidad del servidor de blades
    - 50% de la capacidad del servidor de bases de datos

2.11 Requisitos a cumplir

La empresa requiere un grado de disponibilidad de sus aplicaciones del orden del 99,99% para las críticas, del 98% para las semicríticas, del 97 % para las subcríticas y del 95% para el resto de las aplicaciones las no críticas (definidas de acuerdo con lo establecido en el apartado 2.3.4) Para las no clasificadas no se requiere una disponibilidad específica. Pero no obstante la indisponibilidad máxima se establece en una semana.

Es importante considerar que la ubicación del Centro de Respaldo sea tal que una cierta contingencia no pueda afectar a ambos centros simultáneamente.

Ante la presencia de una de tales contingencias, el siguiente objetivo principal es el de dotar de redundancia a los sistemas. Con un modelo de redundancia ACTIVA-ACTIVA para, al menos el 60% de los Sistemas priorizados.

También se pretende disponer de una zona segura para el almacenamiento de los Datos que se manejan en ZEREPSA, que al día de la fecha está muy limitado.

Como hipótesis de funcionamiento para el Centro de Respaldo se seguirá la de redundancia Activo-Activo pudiendo funcionar ambos centros en paralelo, dando servicio en clúster a los sistemas que se explotan en el actual CPD de CME y garantizando un nivel de funcionamiento 4 (máximo nivel) de entre los definidos en la norma TIA-942, considerado de muy alta disponibilidad, consiguiéndose que la disponibilidad de los sistemas y su seguridad ante una contingencia sea elevada (del orden del 99,9%).

El objetivo fundamental a conseguir es que el Centro de Respaldo tome el control de la operación de las aplicaciones y sistemas que se operan en el Centro Principal, cuando se produzca una

contingencia provocada por uno cualquiera de los riesgos que se enuncian anteriormente, de tal modo que se transfiera la responsabilidad de la operación al Centro principal cuando la contingencia haya desaparecido y se haya restablecido la operación del Centro principal.

2.11.1 Capacidad

La capacidad del centro será tal que permita, de manera incremental, alcanzar el total del crecimiento en cinco años. Para ello hay que tener en cuenta:

- Espacios (de centro de cómputo y de zonas de vida)
- Capacidades de red
- Capacidades de aislamiento electromagnético
- Diversificación de proveedores
- Capacidades de disipación de energía (enfriamiento, refrigeración)
- Capacidades eléctricas
- Capacidades de almacenamiento físico

2.11.2 Tiempos de respuesta

Las conexiones, disponibilidad de equipamiento, funcionamiento de las instalaciones, equipos y aplicaciones serán tal que permitan la operación ACTIVO-ACTIVO, al menos para las aplicaciones CRITICAS.

De este modo, caso de producirse una contingencia en el Centro Principal, el Centro de Respaldo tomará el control instantáneamente para las aplicaciones críticas.

Para las aplicaciones semicríticas el tiempo de entrada en producción deberá ser como mucho de 2 horas tras la presencia de la contingencia. Los datos estarán disponibles de inmediato, con una pérdida máxima permitida de 0,5 horas previa a la contingencia.

Las aplicaciones subcríticas serán puestas en operación no después de un día desde la contingencia, no permitiéndose una pérdida de datos superior a 5 horas previas a la contingencia.

La aplicaciones sin clasificar entrarán en explotación sólo si la contingencia se prolonga más de 3 días, sin poderse recuperar el Centro Principal. No obstante la pérdida de datos será inferior a 10 horas previas a la presentación de la contingencia.

La operación del Centro de Respaldo ha de garantizar la recuperación del Centro principal en las mismas condiciones que emplea para tomar el control y con los mismos tiempos de pérdidas de datos.

2.11.3 Supervivencia

En el caso de contingencias de larga duración, consideradas como tales las que se prolongan por más de una semana, se debe garantizar, en Centro de Respaldo la total operación de TODOS los sistemas y aplicaciones que se operan en el Centro principal.

Las capacidades de supervivencia del Centro de respaldo y sobre todo de la continuidad del negocio exigen que se puedan cumplir las siguientes consideraciones:

En cuanto a los equipos y sistemas:

- La necesidad de prever espacio para todos los existentes en el Centro Principal.

En cuanto al aprovisionamiento de servicios y energía:

- Posibilidad de cambio de todos los sistemas de la empresa al centro de respaldo.
- Fiabilidad ante cortes de suministro eléctrico
- Posibilidad de supervivencia ante fallos de los proveedores de comunicaciones.

En cuanto a las contingencias:

- Imposibilidad de que la misma contingencia pueda afectar simultáneamente a los dos Centros (de Respaldo y Principal).

2.11.4 Seguridad

El centro de respaldo debe contemplar las mismas condiciones de seguridad de sistemas hardware y software descritas en los apartados 2.9.1 y 2.9.2.

El centro secundario debe considerar así mismo elementos de seguridad física, incluyendo zonificación de espacios y definición de niveles de acceso.

3 SOLUCIÓN PROPUESTA - INFRAESTRUCTURA DE SOPORTE Y SEGURIDAD FÍSICA

En este capítulo se describen los sistemas del edificio para satisfacer los requisitos de la norma TIA 942 y que serán los que cumplirán para el proyecto que nos ocupa.

Se describirán los criterios de selección de la ubicación apropiada para el CPD de respaldo en el apartado 3.1, y los requisitos generales del diseño del edificio en el apartado 3.2.

Los sistemas de refrigeración y de acondicionamiento de aire y extracción se detallan en el apartado 3.3, y en el apartado 3.5 los sistemas eléctricos, que forman la base del funcionamiento de los sistemas TIC. Asimismo se describen en el apartado 3.4 los sistemas de control del edificio, que formarán parte integrante de los sistemas de tecnologías TIC del mismo, utilizando las redes y el equipamiento que se instale.

Como elemento importante para el diseño del edificio se describen en el apartado 3.6 los puntos de enlace o salas de enlaces, puntos en los cuales se ubicarán los accesos a las redes de los proveedores.

Referentes a los sistemas de seguridad y control, se describen en el apartado 3.7 los elementos constitutivos de las diferentes áreas de control necesarias a instalar en el edificio. En el punto 3.8 se describen las características de sistemas de seguridad del edificio, y seguidamente se define el sistema contra incendios y extractor de humos, que se trata en el punto 3.9. En el apartado 3.10 se atiende a los sistemas de señalización y aviso o de megafonía del edificio.

Finalmente en el apartado 3.11 se definen las características mínimas de iluminación general del edificio.

Todos los sistemas que se mencionan se tratan desde la perspectiva de las exigencias particulares de las salas técnicas, entendiendo por tales las que acogen los equipos tecnológicos de TIC y desde la perspectiva de los requisitos generales para los edificios de oficinas y los particulares para otras salas tecnológicas que acogen a otros sistemas como son el centro de transformación, los centros de grupo electrógeno y de SAIs y los que acogen los sistemas contraincendios y de AA y de salas de bombeo.

No obstante se ahonda con más detalle en los requisitos de los sistemas eléctrico (salas de transformación, GE, SAIs) y por supuesto de los que contienen elementos de TIC (sala técnica, salas de enlaces y elementos TIC de los sistemas de seguridad, CPI y control general del edificio que se apoyan en las redes que se instalen en el edificio.

3.1 Ubicación del centro de respaldo

Para ubicar el centro geográficamente, se consideran los siguientes elementos [***12***]:

- Evitar zonas susceptibles a desastres naturales (p. ej. inundaciones)
- Evitar zonas con posibles interferencias EM/RF (p. ej. instalaciones de comunicaciones)
- Evitar grandes zonas de producción industrial y emisión de contaminantes

- Evitar zonas de vibración (p. ej. líneas de ferrocarril)
- Ubicar el centro en un complejo existente, de forma que se aprovechen las medidas de seguridad y que el edificio no sea un objetivo por sí mismo
- El edificio debe estar aislado de estructuras vecinas
- Deberá haber acceso a servicios de emergencias
- Deberá haber acceso a múltiples fuentes de energía y utilidades
- El acceso al centro debe ser suficiente para que en caso de emergencia, el personal del centro principal pueda ubicarse en él

Con ello en mente, se elige una parcela en un polígono industrial de Madrid, entre las circunvalaciones M-40 y M-50, con facilidad de comunicaciones, y cercano a un hospital, lo que facilita el acceso a las infraestructuras de energía necesarias.

3.2 Diseño del edificio

Con los datos obtenidos en el capítulo 2 sobre los sistemas a respaldar y las áreas que necesitan los mismos así como las unidades de negocio TI que deben estar presentes en el respaldo se han obtenido las superficies a ocupar y así se ha establecido el diseño básico del edificio, en el lugar y las condiciones apropiadas para su establecimiento, que se refleja en el plano D.I Plano general del centro de respaldo del Anexo D - Planos.

3.2.1 Superficies necesarias

Las superficies y áreas necesarias en el centro de respaldo se definen y dimensionan teniendo en consideración:

- Las necesidades de los sistemas a respaldar y el equipamiento asociado a los mismos.
- Los procesos que se han de realizar para el funcionamiento de esos sistemas.
- El personal que debe atenderlo para la toma de control en este Centro de Respaldo ante una emergencia en el Centro principal.
- Los tiempos de recuperación y de la criticidad de los Sistemas
- La necesidad de mantener replicado el almacenamiento del centro principal.
- La implantación de los sistemas de soporte o generales del edificio [***12***] (energía, refrigeración, etc.) y los espacios requeridos para la ubicación de la maquinaria y equipos correspondientes.
- Las necesidades de vigilancia y seguimiento de los Sistemas de Información y de los de soporte.
- Las condiciones de vida del personal que desarrollará los procesos necesarios para el funcionamiento del Centro.

Con todo ello, las áreas que se consideran necesarias en el Centro de Respaldo y sus superficies se describen en la tabla siguiente.

TABLA DE ZONAS Y SUPERFICIES A OCUPAR	**m^2 necesarios**
SALA TECNICA	
COMUNICACIONES	30

REDES	20
SSMM	40
BLADES	15
TELEFONIA (sistemas)	24
inter-intranet	75
HOSTS	40
almacenamiento	30
PUNTO NEUTRO O DE ACCESOS	
Principal	30
secundario	25
TRATAMIENTO DE SOPORTES Y DATOS	
RECUPERACION DATOS	30
RECUPERACION DE SOPORTES	20
DESMAGNETIZACION	15
ALMACEN DE SOPORTES	30
INSTALACION-DESINSTALACION SISTEMAS	
STAGING	30
RECEPCION-ENTREGA	16
OPERACION Y CONTROL SALA	
MONITORIZACION Y CONTROL	40
SERVICIOS GENERALES	
GRUPO ELECTROGENO-CORRECCION	41
Trafo + celdas de entrada y de distribución	38
SAIs + baterías	35
EQUIPOS CI- general y Sala técnica	90
AIRE ACONDICIONADO GRAL	80
MANTENIMIENTO	45
AREAS GENERALES DE OPERACION DE LOS SISTEMAS DEL CENTRO	
OPERACION DE SEGURIDAD	30
CONTROL DE APLICACIONES	50
CONTROL HOST	20
CONTROL REDES	40
CONTROL BBDD	60
CONTROL SISTEMAS	20
DIRECCION	
DIRECTOR	20
SECRETARIA	8
ASEOS EN DOS BLOQUES SEPARADOS	15
DESCANSO-CAFES-COMIDA	20
CONTROL DE ACCESOS – GARITA SEGURIDAD	
RECEPCION AL EDIFICIO Y CONTROLES DE SEGURIDAD	20
PUESTO DE CONTROL	8
PUESTO DE INSPECCION PAQUETERIA	10

PUESTO DE REGISTRO Y ESPERA DE PERSONAS	20

Tabla 6 Superficies mínimas para el Centro

3.2.2 Requisitos de la estructura del edificio

Una estructura correcta del edificio puede derivarse de la interacción entre los conceptos de disponibilidad de los servicios y sistemas a proteger, de las capacidades de backup y de recuperación, de los sistemas y servicios, así como del propio edificio en sí mismo, los cuales combinados con los sistemas de servicios del edificio y la estructura organizativa, se diseñarán para paliar los daños que pudieran producirse en dichos sistemas y servicios, por efecto de acciones naturales, ataques terroristas actos de sabotaje, etc.

Para ello se seguirán las siguientes especificaciones y se preverán las siguientes áreas técnicas como mínimo:

- Separación física del CPD del resto del edificio.
- Localización de las Salas Técnicas del núcleo del CPD (contenedoras de los sistemas y servicios así como de los servicios a las mismas, como son AA, Enfriamiento, Energía, etc.) suficientemente alejadas de la calle como para garantizar un primer grado de protección.
- No deben existir otras áreas bajo estas salas
- Separación física de los CPD de las áreas de aparcamiento
- Asociación directa de los sistemas de servicios del edificio a los sistemas de procesamiento del CPD
- Control del CPD desde un área central desde la que se ejerza un control operacional, organizativo y administrativo
- El público no debe tener acceso directo al CPD
- Disponer de sistemas especiales de supresión de fuego, particularmente para las salas técnicas
- No situar sistemas usuarios bajo los "sprinklers" o sistemas difusores de extinción
- Instalación de sistemas de extinción automático para posibles incendios localizados o provenientes del suelo en salas técnicas con falsos suelos (CPU / DASD, Server)

En lo referente a las áreas en sí mismas:

- Establecer una sala separada y particular para los sistemas de back-ups
- Sala de almacenamiento segura para el equipamiento de TI
- Salas seguras para alojar los sistemas de SAI así como los de baterías
- Salas seguras para alojar la subestación eléctrica y para el Grupo electrógeno
- Salas seguras para alojar los sistemas de Aire Acondicionado tanto de vida como para la refrigeración de los equipos

- Rampas, elevadores para introducir y alojar el equipamiento hasta el suelo dentro del CPD
- Carretillas para desplazamiento horizontal
- Sala de servidores, sala de telecomunicaciones, salas de redes con pasillos de enfriamiento sensibles
- Áreas de pruebas exteriores y separadas del CPD
- Almacenamiento de elementos grandes, combustibles y no utilizables fuera del CPD
- Salas de monitorización, vigilancia y control
- Salas de soporte y operación

3.2.3 Clasificaciones de Zonas de Seguridad

Existen varias clasificaciones de áreas dentro del edificio desde una perspectiva de seguridad [***13***] [***13***]. Se describen a continuación.

Espacio público

Son las áreas del interior del edificio a las que se permite el acceso ilimitado de visitantes. Este acceso deberá limitarse a la recepción y posibles aseos adyacentes a la misma y fuera del área segura. La instalación del propio CPD no deberá tener área pública.

Espacio interior

Se trata de un espacio dentro del edificio en el que el personal que trabaja en él puede moverse libremente sin controles de acceso. Se consideran espacios interiores los distribuidores o salas de estar, áreas de oficinas, áreas de secretarias, etc. Los visitantes y los invitados, deben ser continuamente acompañados, cuando se mueven por áreas interiores. Los espacios interiores deben ser aislados del espacio público mediante construcciones de tipo “desk to desk” (paso al personal de una recepción a otra).

Espacio restringido

Se trata de espacios situados dentro de una instalación, y que pertenecen o son controlados por un grupo específico, de quienes se ha considerado que su trabajo es clasificado como confidencial, crítico o esencial para la empresa. Áreas restringidas, típicas serán:

- Espacios mecánicos o eléctricos (tanto de operación, generación o transformación y distribución, como los de mantenimiento de tales sistemas)
- Almacenamiento de equipos
- Mantenimiento de equipos
- Mantenimiento de registros así como copias, almacenamiento y recuperación de datos
- Zonas de desarrollo y pruebas de productos
- Las Áreas de Explotación, monitorización seguimiento y control de los Sistemas

3.2.4 Salas de control

En el CPD coexisten varios sistemas de control diferentes y debemos diferenciarlos ya que cada uno afecta a áreas de actividad diferentes. Cada sistema de control se vigila y se acciona desde una sala diferente, salvo el caso del control de seguridad y el control técnico que se hace desde la sala de control de Seguridad del edificio.

1. **Sistema de Control técnico** de las instalaciones del edificio. Abarca los controles que se han de efectuar sobre los sistemas de Aire Acondicionado, Contraincendios, de humos, de producción y distribución de energía, equipos de emergencia, de los sistemas contra humedades y agua en salas técnicas, y los mecanismos de actuación de dichos sistemas.

   Este sistema es descrito en el apartado 3.4, y es atendido desde el Centro de Seguridad del Edificio descrito en el apartado 3.7.

2. **Sistema de Control contra intrusión**. En este centro se controla todo el sistema de accesos, de vigilancia de errantes, de videocámaras, de concesión de privilegios para los accesos a las diferentes zonas. Este centro es descrito en el apartado 3.8.

   Este sistema se atiende también desde el Centro de Seguridad del Edificio.

3. Por último y como más importante para la operación del Centro, existen el **Sistema de control de la operación de los sistemas de información**, y el Sistema de control de las Redes desde donde se controlará el funcionamiento de los sistemas de información, las redes de datos, los sistemas de almacenamiento, etc. Estos sistemas, se controlan desde dos zonas diferentes tal como se describe en el apartado 3.7.

3.2.5 Normativa para puertas y pasillos

Las puertas cumplirán las condiciones exigidas en la normativa vigente para cada caso donde se utilicen

La normativa de referencia al efecto es:

- Resistencia al fuego de clase RF 60 según DIN 4102 y estarán certificadas como puertas de protección contra humos.
- Resistencia de al menos nivel 3 descrita en la norma UNE-EN 1627.

Para las puertas de suministro a las áreas técnicas y de proceso de datos, estas serán al menos de un ancho de 1,50 m por 2,5 m de alto. Deberán ser de al menos hoja y media.

Dimensiones de los Pasillos

- Para transportes:> 1.26 - 2.26 m de ancho libre
- Para rutas de rescate: > 1.01 m
- Dotados de detectores de movimiento, detectores de vibraciones o volumétricos para la detección de intentos de intrusión u otros sistemas similares contra intrusión.

3.2.6 Normativa contra incendios para diversos componentes del CPD

de respaldo

Como medida de protección contra los efectos del fuego, los grupos de zonas con una similar relación funcional, se combinarán en compartimentos resistentes al fuego y se diferenciarán además en zonas que se definirán de acuerdo con la resistencia al fuego de sus componentes de contorno (paredes, suelos, puertas, cableados, ductos y huecos o pasamuros de tuberías, etc.).

Para las salas y zonas técnicas se seguirá lo descrito en el Reglamento de seguridad contra incendios en los establecimientos industriales [***14***] [***14***]. Para el resto de zonas de uso se seguirá el Código Técnico de la Edificación (Parte I) [***6***].

En cuanto a las medidas particulares de resistencia al fuego se seguirá, lo establecido en la norma DIN 4102, de clasificación de la resistencia al fuego de los materiales de la construcción, en todo lo que no contravenga los reales decretos mencionados ni su normativa de desarrollo.

Como medida de protección contra los efectos del fuego, las zonas principales (núcleo) del CPD y algunos grupos de áreas técnicas (de tipo mecánicas, eléctricas…) que se definen en los siguientes capítulos estarán separadas entre sí por paredes resistentes al fuego (F90-A según DIN 4102).

Zonas que deberán ser compartimentadas y resistentes al fuego (F90 según DIN 4102)

- Sala técnica
- Puntos neutros y salas de enlace
- Pasillos de enfriamiento o de circulación a la Sala Técnica
- Salas de almacenamiento, staging y desmagnetización

3.2.7 Normas para el suelo elevado

Las áreas con un suelo elevado para facilitar las alteraciones y recuperaciones de servicios sin gran dificultad deberán cumplir con las siguientes funciones:

- Permitirá el movimiento y colocación de equipamiento, maquinaria así como el transporte de material.
- Proporcionará un espacio para suministrar a los equipos los servicios (agua, aire, etc.), entre el suelo elevado y la solera del fondo.
- En las salas técnicas, el volumen entre el falso suelo y la solera actuará como plenum para la distribución de aire frío a las salas. Siendo que el suelo elevado actúa como plenum, se deberá evitar la instalación de cableado estructurado a través de él, conforme descrito en el apartado 4.4.2.

El suelo elevado, cumplirá los siguientes requisitos [***15***]**:**

- Su altura en relación a la solera en que se apoyen los soportes no será inferior a 45 cm ni superior a 85 cm
- Resistencia al fuego F90/F180 según DIN 4102 [***16***] [***16***]
- Deberá preverse el posible drenaje de la solera.
- Las dimensiones modulares serán de 60 x 60 cm

- En la Sala Técnica se aplicarán los siguientes requisitos.

Carga uniforme	3060 Kg/ m^2
Carga puntual por loseta (carga concentrada) (kg sobre probeta de 50mm^2)	580 Kg/50mm^2
Carga rodante	580 Kg/50mm^2
Carga de impacto	60 Kg

Tabla 7 Requisitos de resistencia del suelo técnico

- Existen diversos tipos de losetas para los suelos elevados según DIN 4102 [***16***] [***16***]:
  - **Clase A** (de materiales no combustibles). Tales losetas `pueden ser de hormigón, piedra natural, anhidrita, acero, por ejemplo.
  - **Clase B** (de materiales combustibles). Esta clase se subdivide en Clase B1, retardante de la llama, y Clase B2, de inflamabilidad normal. Son materiales de esta clase, por ejemplo la madera, madera estratificada, madera prensada, cualquier otro derivado de la madera.
- Se instalarán losetas de clase A en la **sala técnica** y en **los puntos de acceso** de los operadores (Puntos neutros). Así mismo se instalarán losetas de este tipo en la sala de staging (preparación de equipos para su traslado a otras departamentos de la empresa) que se consideran salas técnicas.
- Se instalará losetas de clase B2 en las **salas y espacios comunes** así como en las **zonas de trabajo** del personal del Centro.
- Los suelos del centro de transformación, grupo electrógeno, SAIS, sistema contra incendios, sistema de Aire Acondicionado, almacenes y de los pasillos serán de **hormigón pulido**.

3.3 Sistemas de Aire

El Sistema de Aire Acondicionamiento tendrá dos componentes:

- Sistema de Enfriamiento de las Salas Técnicas.
- Sistema de Aire Acondicionado General o de ambientación.

A su vez el sistema de aire de las salas técnicas dispondrá de un sistema extractor de baja velocidad, para los posibles humos que se puedan producir en caso de incendio, de modo que permita una fácil evacuación de las personas que pudieran estar trabajando en el interior, en un tiempo máximo de 2 minutos desde la producción de un posible incendio de cableado o productor de humos tóxicos.

3.3.1 Parámetros de enfriamiento y humedad

Para las diferentes salas del centro, las condiciones son las siguientes [***17***]:

Áreas o Salas/Funcionalidad	Aire acondicionado de la sala		Nivel de Ruido
	Temperatura ºC	Humedad Relativa %	dB(A)
SALA TECNICA Y PUNTOS NEUTROS			
- **HOST/**	16-22,5	30-50	< 50
- **Almacenamiento/SAN**	=	=	< 45
- **Servidores**	=	=	< 45
- **Áreas de Red**	=	=	< 45
- **Archivo**	=	=	<45
Áreas atendidas			
- **Operación**	21-26	35-55	< 35
- **STAGING**	21-26	35-55	< 35
- **Desmagnetización**	21-26	35-55	< 50
- **Mantenimiento**	<30	<60	<50
- **Almacén**	<30	<60	<50
- **Operación de Cintas**	21-26	<60	<50
- **Impresión**	<26	<60	<50
Otras salas			
- **Salas eléctrica y SAIS**	15-35	10-60	< 60
- **Grupo electrógeno**	15-35	45-55	< 60
- **Sala de Baterías**	15-35	45-55	< 60
- **Salas de Aire Acondicionado**	5-35	10-80	< 60
- **Zonas de intercambio al exterior o evaporadores e intercambiadores**	15-3	20-65	<60
Falso Suelo	> 18	< 70	-

Tabla 8 Condiciones de temperatura y humedad para las diferentes áreas del centro

El aire acondicionado de la Sala Técnica debe tener también limitados los límites de partículas en suspensión [***18***] [***19***] [***19***].

	Límites máximos de operación	**Límites mínimos de operación**	**Situación normal**
Temperatura	16ºC	30ºC	16-22,5 ºC

Humedad relativa (HR)	20%	80%	30-50%
Partículas de polvo (en relación peso partículas/ peso de aire)	---	5%	0,5 – 1%

Tabla 9 Condiciones de temperatura, humedad y partículas en las salas técnicas

Estas condiciones se aplicarán a la totalidad de las áreas que contengan equipamiento informático para la explotación de los Sistemas.

3.3.2 Diseño del sistema

Para la Sala Técnica y puesto que se ha de tratar de conseguir que posea un nivel de sala blanca (con un contenido de partículas de polvo en suspensión inferior al 5%, según la tabla anterior y puesto que se prevé una carga térmica de unos 5000 W/m^2, se ha de disponer de una combinación de un sistema de enfriamiento sensitivo que es diferente al de acondicionamiento general que será centralizado, como ya se ha dicho anteriormente

Así para el resto de áreas del Centro, se utilizará un sistema de Aire Acondicionado General. El Sistema Centralizado dispondrá de regulación para la humidificación y deshumidificación y proporcionará el suministro de aire exterior a las salas de uso general (asegurar las renovaciones necesarias del aire de las salas). De igual modo deberán proporcionar las renovaciones de aire necesario para permitir unas condiciones de vida aceptables.

Los enfriadores sensitivos (localizados) se utilizarán según la carga térmica a disipar.

- Por lo general para cargas térmicas entre 200 W/m^2 y los 6000 W/m^2 podrán disponerse en consola o armarios dentro de las propias instalaciones a refrigerar. Este será el caso general de equipos en las zonas de Punto neutro y de Staging
- En el caso de cargas térmicas superiores y hasta los 15000 W/m^2, que es el caso de la Sala Técnica, habrá de estudiarse y disponerse los equipos de modo que se pueda provocar la evacuación siguiendo los procedimientos pasillo caliente-pasillo frío. Este será el caso a aplicar en prácticamente todas las áreas de la Sala técnica excepto en la de Sistemas que reúnen una alta concentración de equipos virtualizados en sistemas Blade[2] y que se tratarán como en se expresa en el caso siguiente:
- Para cargas térmicas superiores a los 15000 W/m^2 (p. ej. área de Blades) se estudió la refrigeración cuidadosamente y se consideró necesario incorporar armarios de refrigeración adyacentes a los propios sistemas a refrigerar.

En estas salas, el aire procedente del sistema centralizado se insuflará directamente al plenum formado por el falso suelo. Las salas sin falso suelo y con una menor carga térmica (< 100 w/m^2) se acondicionarán a través del techo. Estas salas no estarán equipadas con enfriadores sensitivos.

[2] Los dispositivos blade son servidores de alta capacidad y que ocupan un espacio muy reducido pudiendo alcanzar con ellos una densidad de varias decenas en un mismo RACK lo que permite un volumen de procesamiento elevado en un espacio reducido. Se utilizan fundamentalmente para la virtualización de sistemas. Debido a la alta concentración de elementos se desarrolla una elevada concentración de calor que debe ser eliminado (un rack de blades, completo puede llegar a genera hasta 30 KW de energía calorífica).
http://es.wikipedia.org/wiki/Servidor_blade

Cálculo del volumen de aire de circulación en salas con falso suelo: [*15*]

El cálculo del volumen de aire que fluye por cada sala individual, se basa en una diferencia de temperatura de 9 ºC entre el aire de retorno y el aire suministrado. Este volumen de aire será proporcionado por los enfriadores sensitivos. El flujo de aire del sistema central se determinará en base a las relaciones de aire específicas (m^3/h y m^2).

Los volúmenes de aire resultantes fueron a razón de 1,6 renovaciones hora en el caso de áreas generales y de 0,5 en el caso de las salas técnicas.

3.3.3 Sistemas Centralizados

La determinación del flujo de aire del sistema central o insolaciones de los intercambiadores de calor se basa en los correspondientes cálculos. El sistema es controlado para el suministro constante de aire a una temperatura de 16 ºC.

En salas con suelo elevado o con enfriadores sensitivos, el sistema central se utiliza para suministrar el aire exterior necesario y para mantener las necesarias condiciones de humedad de la sala.

Las salas sin suelo elevado que solo necesiten el aire acondicionado del sistema central, serán equipadas con los elementos propios del Aire Acondicionado Central o General reforzándose, caso de ser necesario con consolas individuales para que puedan ser controladas individualmente.

3.3.3.1 Diseño del Sistema de Aire Acondicionado

Sistema Centralizado

- Se dispondrá de doble unidad de climatización de AA, cada una diseñada para el 50% de la capacidad total. De modo que cada una dé servicio a distintas zonas del Centro. Cada unidad dispondrá de un filtrado del aire en dos etapas (primera una EU 5 y posterior EU 7 según UNE-EN 779 [*20*]).
- Los filtros para el Aire que se insufle en salas técnicas (de quipos informáticos) deberán disponer de filtros absolutos con una eficiencia de EU 10 según la norma UNE-EN 779.
- La central de refrigeración se dispondrá en la azotea.
- El agua a la central de intercambio de calor subirá y retornará desde la sala de máquinas a la azotea mediante tubos de diámetro 50 mm.

Sistema para la Sala Técnica. Enfriadores sensitivos o autónomos.

- Los equipos de enfriamiento de la sala técnica serán 5 unidades integradas de una potencia frigorífica de unas 75000 frigorías cada una. Estas unidades estarán alineadas con los pasillos calientes para una mejor extracción.
- El aire de renovación lo aspirarán del pasillo de circunvalación de la Sala Técnica, el cual será suficientemente preparado por el sistema central y suministrado a través de los propios elementos del AA Central.
- Los elementos de enfriamiento serán refrigerados por agua que dispondrá en la azotea del edificio de los sistemas de condensación o enfriadores del agua de refrigeración.

- Cada equipo dispondrá de las conducciones de agua a la azotea mediante tubos de 80 mm de diámetro tanto en subida como en bajada.
- De igual modo se dispondrán los sistemas de enfriamiento para los equipos especiales de alto rendimiento (sistemas Blade) [***21***] [***21***], utilizando dispositivos autónomos para racks que superen los 20000 W/m^2.

3.3.4 Distribución de aire

Sistema General o Central:

- El aire se distribuye mediante conductos adecuados, y se introduce en cada compartimento mediante los difusores adecuados.
- Los difusores se distribuyen por el techo de las instalaciones y son de dos tipos tal como se representan en el plano D.III Aire acondicionado del Anexo D - Planos.
- El aire de los compartimentos se recoge mediante rejillas de extracción que se disponen en los cerramientos exteriores y centralizan en cada uno de los equipos de clima en la sala de máquinas.
- Sobre el techo se disponen de las cajas mezcladoras que proporcionen a cada zona los correspondientes condiciones del aire a insuflar.
- Se situarán trampas contraincendios con conmutadores de límites en los ductos que entren a través de compartimentos contraincendios. Las activaciones de estas trampas se informarán a un sistema centralizado de gestión.

En la Sala Técnica:

El aire siempre se insufla en la Sala Técnica por la parte más baja y así por el propio calor de los equipos se va elevando (menor densidad con la temperatura) y va enfriando el resto de equipamiento hasta alcanzar una cierta altura desde donde se dirige a las máquinas de frío para su tratamiento y de nuevo insuflado. El volumen de insuflado del aire se denomina Plenum y la zona por donde se redirige a las máquinas Extracción.

Por regla general se actúa con el aire como se indica en la tabla a continuación:

Acción	**Salas con suelo elevado**	**Salas sin suelo elevado**
Suministro del aire de entrada	Se insufla dentro del falso suelo como plenum	Se insufla al interior vía insufladores de techo
Extracción del aire de retorno	Se extraerá por encima del nivel del sistema de iluminación	Se extrae vía extractores de techo

Tabla 10 Estrategia para suministro y extracción del aire acondicionado

En nuestro caso:

- El suministro de aire se hará insuflando en el falso suelo de tal modo que se asegure la admisión y un buen mezclado con el aire suministrado por el aire centralizado.

- Todos los sistemas de aire (excepto el centralizado) se dispondrán a lo largo del pasillo, pegados a la sala técnica para así estar más próximo a la zona a enfriar. Se hará mediante 8 máquinas de 75000 frigorías pegadas a la sala técnica con los sistemas de impulsión por el falso suelo (plenum).
- La extracción se hará por encima del sistema de iluminación de la sala.

3.3.5 Diseño del sistema Central de Aire Acondicionado del edificio (aire acondicionado para el bienestar del personal)

El sistema central tendrá una configuración basada en la producción de Aire en una unidad centralizada de tratamiento y distribución por ductos[3] a todo el edificio insuflando el aire en cada zona mediante difusores y extrayéndolo mediante rejillas extractoras situadas en las paredes fundamentalmente exteriores. El sistema de distribución será por zonas con cajas mezcladoras o post calentadores zonales como se refleja en el plano D.III Aire acondicionado del Anexo D - Planos.

La Unidad Central de Tratamiento del Aire se corresponderá con el esquema siguiente, y estará compuesto por dos unidades independientes. Cada una de las unidades estará dimensionada para atender el 50% de la necesidad de AA, aportando redundancia al sistema como un todo.

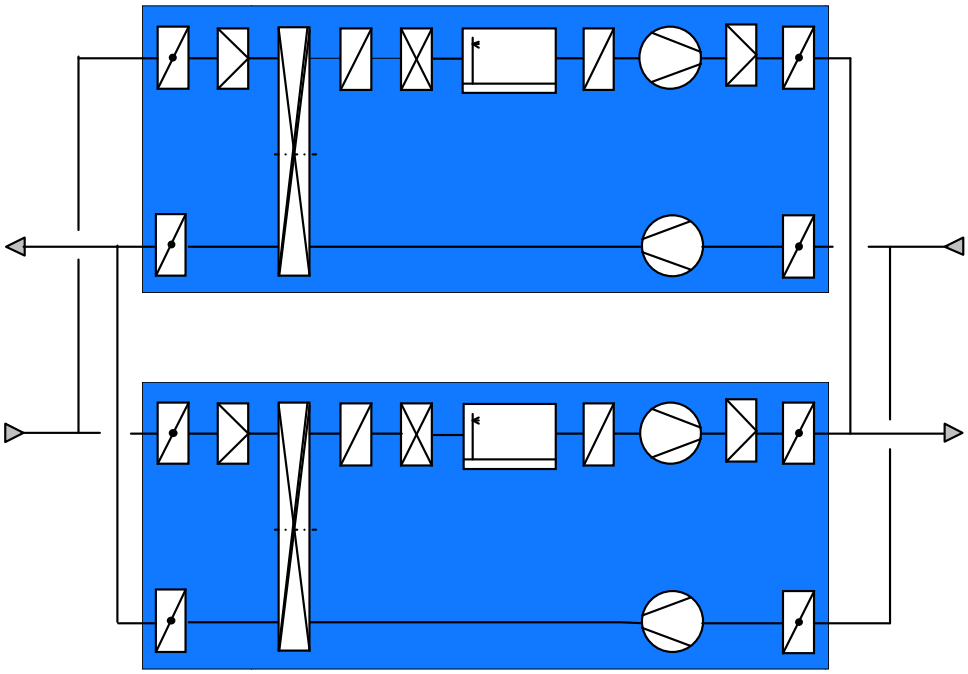


Figura 12 Esquema básico del aire acondicionado

Los componentes básicos del montaje de esquema son los mostrados en la tabla siguiente [***22***]

Componente	Símbolo
Silenciador	

[3] Ducto es un conducto, canal, tubería. Se suelen denominar así a los conductos del aire acondicionado que suelen tener grandes superficies transversales y tener secciones de formas dispares

Compuertas motorizadas contraincendios y reguladoras del caudal	
Mezclador recuperador entálpico de aire	
Filtro del aire	
Precalentador/calentador de aire	
Refrigerador	
Humectador de vapor con generador de vapor calentado por electricidad	
Soplante o impulsor de aire	

Tabla 11 Componentes del sistema de aire acondicionado

Se deberá incorporar un sistema de automatización, permitiendo la monitorización y control remoto desde una central adecuada de modo que pueda regularse los siguientes parámetros:

- Tasa de provisión de aire fresco
- Humidificación
- Deshumidificación
- Función de eliminación de humos.
- Control de la eficiencia del filtrado

3.3.6 Enfriadores sensitivos o Equipos autónomos situados próximos a las zonas de evacuación de calor

Las salas con suelo técnico, deben equiparse con enfriadores sensitivos para disipar la mayor parte de la carga interna de calor producido en los equipos. Los enfriadores sensitivos se dispondrán en los pasillos que circunvalan la sala técnica que constituye el área que va a ser refrigerada. Esto garantizará que el personal de mantenimiento y operación no entrará en las áreas de proceso de Datos o sala técnica.

Los enfriadores sensitivos o locales, se diseñan para una capacidad de 10.000 m^3/h con una capacidad máxima de 15.000 m^3/h, en 2 etapas (velocidades de los motores). Los enfriadores sensitivos se dimensionarán en base de una temperatura media de suministro del aire de 16 ºC y una temperatura del aire de retorno de 25ºC. El número de enfriadores se fija de la temperatura de la sala, suponiendo un promedio de 20ºC con lo que se obtuvo un numero de cinco máquinas dispuestas, en las paredes largas de la sala de forma alternada para que no se produzcan flujos contrapuestos de aire frio en el plenum de la sala (falso suelo). Como se presenta en la figura:

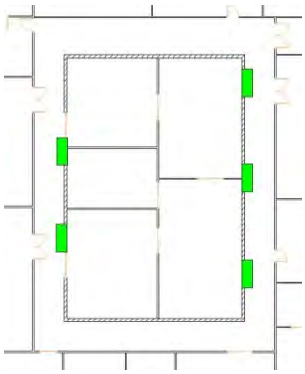


Figura 13 Disposición de máquinas de frio en la Sala técnica

El diseño básico de los enfriadores sensitivos es el siguiente:

- Filtrado EU-7 [***20***]
- Se requiere absorción del sonido de tal modo que no produzcan más de 30 dB(A) de ruido
- El número y capacidad se determinarán de modo que se disponga del 100% de la capacidad en la sala si fallase una unidad, es decir con redundancia (**N**+1).
- Los circuitos del refrigerante (agua o gas) como se establece en el punto anterior, serán visibles en la totalidad de su recorrido, no pasando a la sala técnica y estarán claramente identificadas tanto en las tuberías de ida como en el retorno, de forma distinta.
- Tan sólo penetrarán en la sala por un lado y una longitud no mayor de un metro los tubos de agua de enfriamiento correspondiente a los armarios de Blades.
- Los equipos autónomos o enfriadores sensitivos estarán controlados por un sistema de control directo digital (DDC – Direct Digital Control), que incluya la posibilidad de fijar puntos de temperatura, humedad y alarma conectados al sistema automático de control del edificio. Este control deberá asimismo estar conectado con el sistema contraincendios, de tal modo que, en caso de incendio dejen de funcionar automáticamente.
- Se pondrán rejillas de corte contra fuegos en las salidas de impulsión del Aire frío de modo que se pueda independizar (cerrar) el plenum del falso suelo cuando este se vea inundado por gas de extinción.
- Aun así existirá una instalación de detección de agua en toda la sala técnica.

3.3.6.1 Diagrama de los enfriadores sensitivos

Cada enfriador sensitivo, estará controlado por un Sistema de Control Digital directo (DDC). El sistema Controlador se hallará interconectado con el Sistema Automático de control del Centro.

Los principales elementos pueden identificarse en el diagrama siguiente:

- Pasillos de Enfriadores separados
- Sistema redundante con conmutación automática en cada enfriador y del conjunto con uno de reserva (Redundancia N+1)
- Enfriamiento libre a plenum por falso suelo

- Sistema recuperador de calor para permitir una mayor eficiencia y una menor emisión de calor al exterior

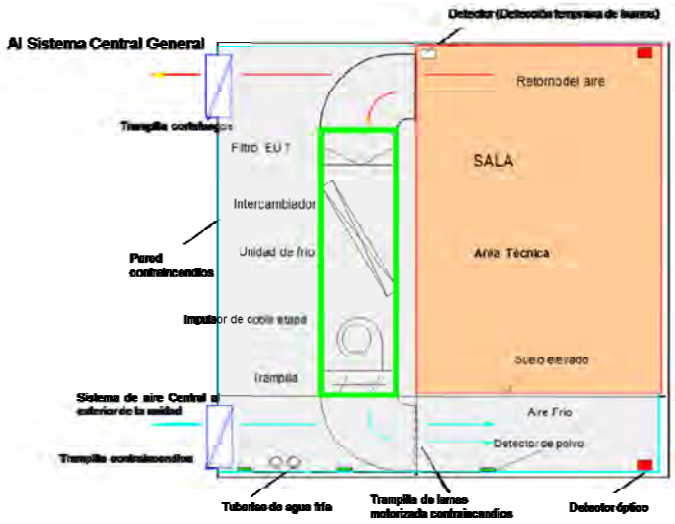


Figura 14 Diagrama de enfriador sensitivo

Las unidades de enfriamiento deben cumplir las siguientes condiciones:

Puntos de temperatura (Temperature Set Points)	65°F a 85°F (18°C a 30°C)
Sensibilidad a la temperatura	+- 1ºC
Punto de Humedad (Humidity Set Point)	40% a 60%
Sensibilidad de la Humedad	1%
Alarmas	Humedad Alta/Baja, Calor elevado, Detección de goteras (humedad), Flujo de aire bajo, Cambio de filtros y alarma general.
Rearranque automático	Una vez restablecida la energía, la unidad de Aire Acondicionado se arrancará automáticamente

Tabla 12 Características deseadas para las unidades de enfriamiento

3.3.6.2 Condiciones de control de la temperatura de las salas técnicas (sala técnica y puntos de acceso o neutros)

Se instalará un sistema de control de la temperatura en las salas técnicas con las siguientes funcionalidades:

- Las temperaturas de la sala se medirán a un nivel de aproximadamente 1,80 m sobre el nivel del falso suelo que es la altura media de un RACK de 42 U[4]s en un número de modo que cada punto de medición abarque una superficie de 16 m^2.
- Las mediciones de todos los puntos se integrarán y la temperatura resultante será la media de la sala.
- Se deberá poder hacer el seguimiento de la evolución de la temperatura en cada uno de los puntos de medición independientemente de los demás.
- Si algún punto sobrepasa un 50% la temperatura media. Se producirá una alarma. De igual modo se producirá una alarma si se supera en algún punto los 30ºC.

3.3.6.3 Condiciones de control de la humedad relativa

Las condiciones de humedad de la sala se medirán de modo similar a las temperaturas, disponiendo de tantos puntos de medición como para los puntos de temperatura. El mecanismo de alarma será como para la temperatura para el caso de que algún punto alcance un 40% del valor medio. En ningún caso se superará el 65% de humedad relativa en la sala. Si esto ocurre se producirá una alarma general.

El sistema de control de temperatura y humedad de las salas técnicas estará incorporado al sistema general de control del edificio del Centro de Respaldo o CPD.

3.3.6.4 Diagramas de enfriamiento de las áreas TI.

Como ya se ha dicho el enfriamiento en la Sala técnica, se hará mediante unidades compactas e independientes que insuflarán aire frio por el falso suelo y absorberán el caliente por el techo de la sala. Las características de los equipos ya se han definido anteriormente en los puntos 3.3.3 y 3.3.6 [***21***] [***21***].

En este diagrama se presenta el modo en que los equipos insuflan el aire y lo recogen. Así como su interacción con el Sistema de Aire Central o General del edificio con el fin de proporcionar las renovaciones de aire necesarias a la sala técnica. Se representan en los puntos 2 y 3 del esquema siguiente.

De igual modo se presenta la disposición de los sistemas de detección y regulación de las máquinas y los cortafuegos.

[4] La U es la unidad de medida vertical del Rack y equivale a 1,75 pulgadas o 4,445 cm

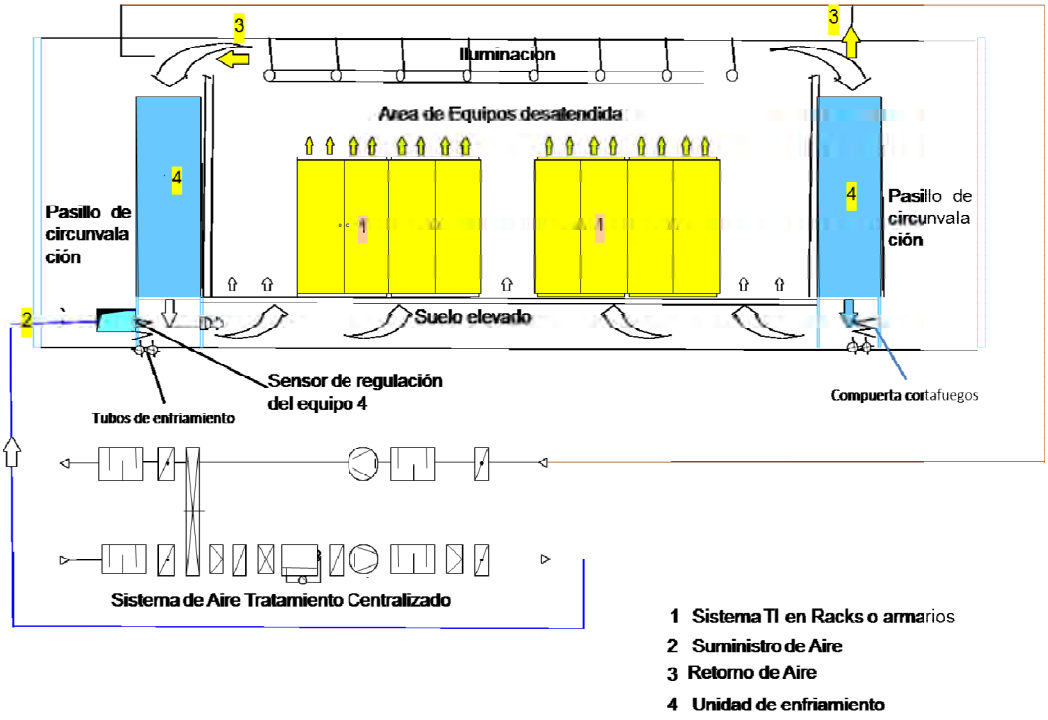


Figura 15 Esquema de enfriamiento de la Sala Técnica mediante equipos autónomos y ventilación procedente del sistema principal o general

3.3.7 Sistemas de Extracción y evacuación de humos

Los sistemas de extracción estarán dotados de las correspondientes rejillas contraincendios para permitir seccionar cada zona del edificio de forma que cumpla los requisitos zonales contraincendios establecidos en el Código Técnico de la Edificación.

Todas las áreas o salas sin ventanas o con ventanas que no puedan ser abiertas deberán estar equipadas con sistemas de extracción de humos dedicados [***23***]. Estos sistemas pueden ser dedicados (por sala) o dar servicio a un grupo de salas (por área).

3.3.7.1 Sistemas de extracción

Estos Sistemas de extracción deberán como mínimo reunir las siguientes características:

Para la función específica de extracción de humos:

- Ventiladores mecánicos de cubierta y/o murales, de distintas capacidades y dimensiones, según las necesidades particulares de la zona de incendio y tipos de productos combustibles y comburentes
- Diseñados para operar, como mínimo a 400 ºC durante 2 horas.

Esto es de aplicación, también a las áreas o salas técnicas mecánicas y eléctricas. Los enlaces con los conductos de extracción de humos se efectuará mediante ensamblajes dotados de compuertas (de lamas no fusibles) que estarán equipadas con motores de recuperación mediante muelle. Estas compuertas trabajarán en las siguientes condiciones:

- Modo normal: Compuertas cerradas
- Modo de extracción de humo: Compuertas abiertas por el motor.

Estas compuertas o ensambles deberán operar en las mismas condiciones, como mínimo a las exigidas para los ventiladores de extracción.

El volumen de aire extraído deberá ser capaz de ser eliminado a través de los conductos de sección suficiente. El aire se enviará al exterior por el tejado. La chimenea del aire extraído, debe situarse de modo tal que no se vea alterada la seguridad del edificio.

Los ventiladores de extracción, los conductos, las aperturas prefabricadas deben ser resistentes al fuego de tipo F90. Según establece la norma DIN 4102 de protección contraincendios [***16***] [***16***].

Todos los sistemas de extracción estarán conectados al sistema de alimentación de emergencia.

El diseño del sistema será conforme con los reglamentos en vigor y coordinado con los criterios de los bomberos locales si fuese necesario.

El diseño del sistema se hará de acuerdo con las disposiciones en vigor.

3.3.7.2 Sectorización de humos

Se diseñarán las zonas y áreas del Edificio que aloje al Centro de Respaldo de modo que se asegure una sectorización antihumos adecuada que permita evacuar los sectores afectados sin riesgos para las personas, en función de los humos que se puedan producir y los volúmenes a controlar.

3.3.7.3 Sistemas de control de temperatura

Asociados a estos sistemas se incorporará un sistema de control de temperatura que permitirá manejar en remoto y en automático los elementos correspondientes para garantizar la eliminación de humos hasta límites apropiados para permitir la evacuación, en caso de incendio.

Este sistema formará parte del sistema contraincendios del Centro y se hallará conectado al sistema general del edificio.

3.4 Sistema de control técnico del edificio

La siguiente ilustración muestra el esquema de los sistemas de gestión y control del edificio, y su conexión con los controladores distribuidos [***24***] [***24***]. Para cada Sistema se seguirá un sistema de este tipo y todos los sistemas se centralizarán en el área de mantenimientos.

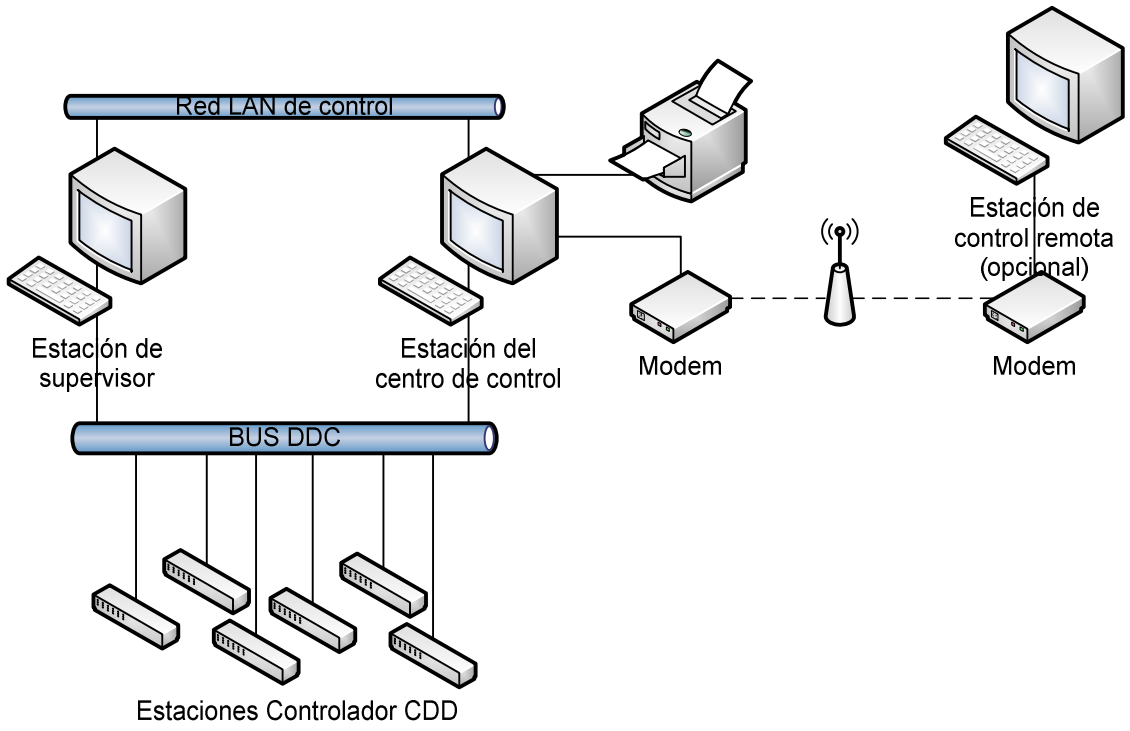


Figura 16 Esquema de red de control técnico del edificio

Los Sistemas de Gestión y Control del edificio se agrupan en un Rack de servidores en la Sala técnica. La presentación de las alarmas se realiza en el área de mantenimiento.

Cada Sistema tendrá sus propios mecanismos de control y supervisión y podrá regularse independientemente. No obstante todos los sistemas estarán integrados en un mismo sistema de alarmas que se presentarán en la oficina de la zona de almacenamiento.

3.4.1 Elementos del sistema de control

Los sistemas de monitorización y control para los sistemas de aire, de refrigeración y de calentamiento habrán de ser diseñados con sistemas de control digital directo (CDD) incluyendo actuadores operados automáticamente, en todos los casos que sea posible, en aquellos casos que sea necesario se usarán sistemas de muelle sencillo para recuperación de movimientos mecánicos. Para cada sistema, se conectarán las unidades de control a una estación de trabajo a través del bus de datos apropiado. Las estaciones de trabajo de todos los sistemas estarán conectadas a través de la Red LAN de Control entre sí y con los servidores de las aplicaciones de los sistemas que se alojarán en la Sala Técnica.

3.4.1.1 Bus de datos de los sistemas de control

El sistema de comunicación de datos de los sistemas de vigilancia monitorización y control, deberá asegurar el funcionamiento correcto del sistema de monitorización y control, en caso de emergencia en el centro durante al menos 2 horas estando sometido a 600 ºC en algunos de sus puntos.

3.4.1.2 Unidades de Control Digital Directo (CDD)

Para cada sistema a controlar y todos entre sí, se debe proporcionar un sistema CDD como unidad de control independiente, para control de bucle abierto y cerrado así como para la monitorización. Este sistema satisfará los siguientes requisitos:

- Conexión con la estación de trabajo (PC o similar, según los sistemas o subsistemas) (con funciones básicas BAS-Broadband Access Server).
- Estación de control aislada:
    - Estación de operación descentralizada. Estación de programación y carga en centro de control
    - Ordenador descentralizado BAS con mensajes de fallos y de estado. y acumulación de logs con alarmas, su estado y su eliminación y corrección
    - Gateway para comunicaciones no propietarias
- Estaciones automáticas DDC
    - Medición, control y regulación de todos los sistemas y servicios
    - Adquisición de valores límites y horas de operación
    - Mantenimiento de logs de alarmas de al menos 1 mes
- Estaciones automáticas DDC (nivel de campo):
    - Servicios y Sistemas del edificio: eléctrico, Aire acondicionado, Calefacción, Refrigeración)

El sistema completo contendrá los dos tipos de estaciones DDC enunciados y una estación de control aislada en que se concentren la totalidad de señales y alarmas así como los sistemas de almacenamiento de las mismas.

3.4.1.3 Monitorización

Los datos de temperaturas y humedad de la sala así como los del falso suelo deben ser suministrados al sistema DDC y monitorizados por el sistema BAS, para vigilar las violaciones y los límites prefijados. Se deben proporcionar información sobre el estado de los siguientes sistemas, por el terminal del operador y presentados en LEDs:

- Sistema Contra incendios.
- Sistema Eléctrico (centro de transformación y SAIs)
- Sistema de Alumbrado.
- Funcionamiento del alumbrado de emergencia y señalización.
- Sistema de emergencia (Centro de grupo electrógeno).
- Sistema de Aire Acondicionado (todas las unidades del sistema general y las de la Sala Técnica):
    - Temperatura (mapa térmico en dos niveles a 1 m y a 1,80m).
    - Humedad.
    - Inundación sala.
    - Nivel y tamaño de partículas.
- Sistema de megafonía.
- Sistema de Accesos.
- Control de la Sala Técnica:
- Sistema de extracción de humos.

3.5 Sistemas Eléctricos

La distribución de energía se hará en estrella distribuyendo las tres fases y el neutro a toda la instalación [***25***] [***26***].

Se dispondrán tres líneas claramente identificadas:

1. Línea comercial
2. Línea de energía estabilizada
3. Línea de energía especial para equipos rotatorios con el fin de impedir las emisiones electromagnéticas conducidas y trasladar a las otras redes los armónicos que se desarrollan en un motor.

Como ya se ha apuntado, la distribución de energía eléctrica, desde las celdas de seccionamiento, mando, maniobra y medida de salida del transformador, se dividirá en dos grupos: uno para energía limpia (o energía estabilizada) y otro para energía normal o comercial.

Se dispondrá de un Grupo electrógeno de emergencia. La conexión de la energía proveniente del grupo a la red de distribución se hará en un cuadro de conmutación que se situará entre el transformador y las celdas de seccionamiento, mando y maniobra.

El ramal de energía estabilizada se encamina a través del sistema de SAIs mientras que el otro se distribuye directamente a todo el edificio.

De forma resumida se reflejan en el esquema simplificado que se presenta en la siguiente figura.

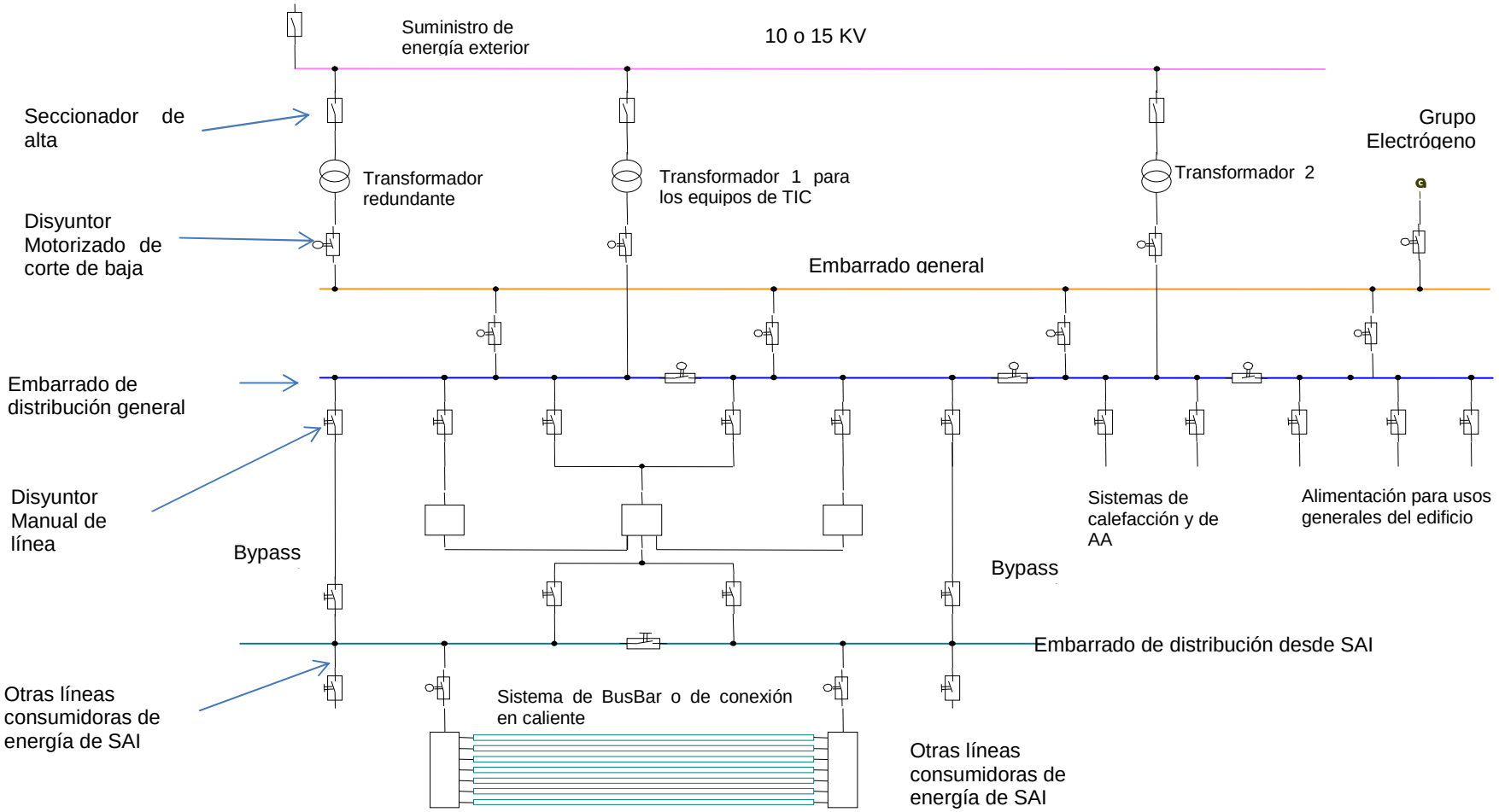


Figura 17 Esquema básico del suministro de energía

En cuanto a la distribución en la Sala técnica se hará por vías aérea soportada en un sistema de rejilla y será de tipo bus-bar para la conexión en caliente de los armarios de distribución a cada línea de Racks. A cada rack se le alimentará con una línea independiente que permita el control de la situación energética de cada uno de ellos.

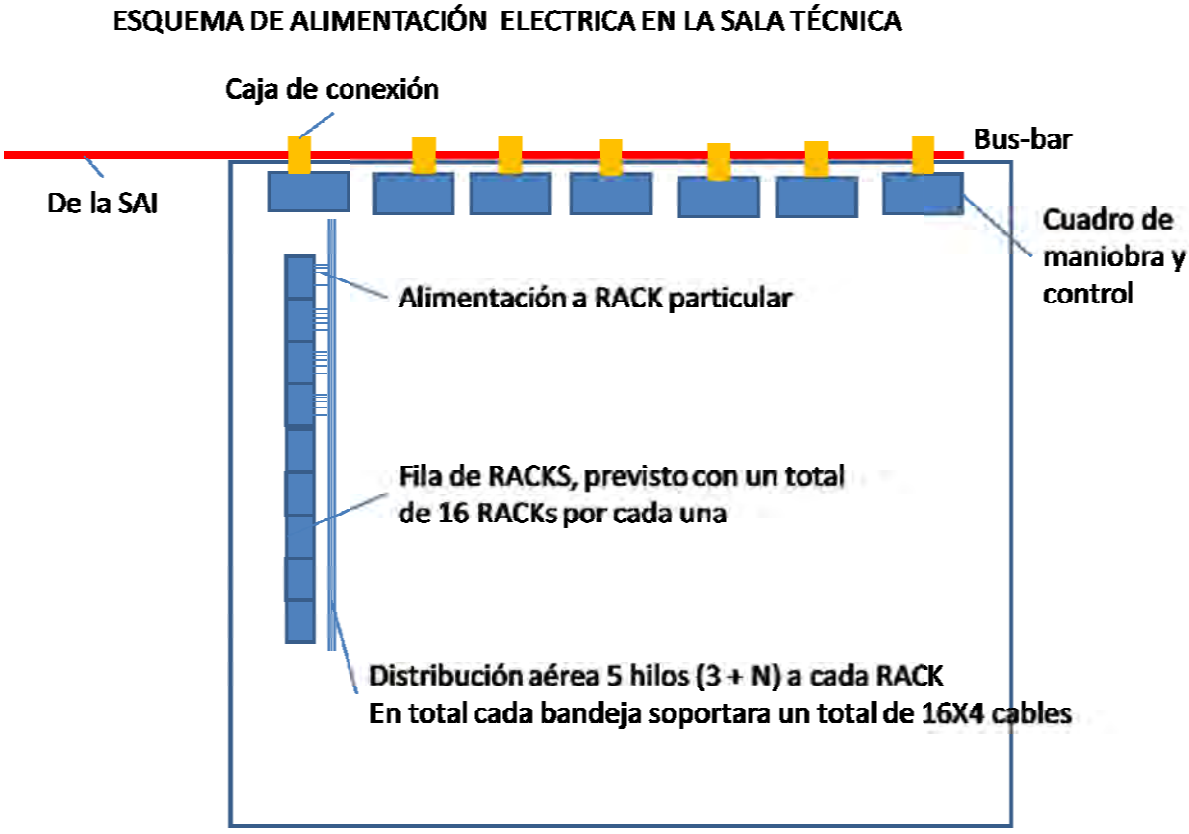


Figura 18 Esquema general de alimentación eléctrica en la sala técnica

3.5.1 Central de transformación

Se ha previsto una carga máxima para el Centro de Respaldo de unos 1000 KVA lo que equivale a aproximadamente una potencia activa de 800 KW (asumiendo un máximo cosf de 0,8, y admitiendo cargas reactivas como máximo de $\sqrt{1000^2 - 800^2}$ = 600 KVAR.

Derivado del coste del transformador se decide adquirir tres transformadores secos (para un mejor mantenimiento y eliminación riesgos de incendio de los transformadores de aceite [*27*]) de 600 KVA cada uno con lo cual se garantiza una redundancia en transformadores de N+1.

Por otro lado se disponen 3 celdas de entrada para la maniobra de entrada en línea del transformador (Celda de Seccionamiento, celda de protección de línea y celda de medición en alta).

Tras el transformador se dispone un elemento de corrección del factor de potencia de la instalación, que en principio estará puenteado y tan sólo en el caso de que se produzca mucha energía reactiva se activará. El objetivo es que el factor de potencia del centro no sea inferior a un cosf de 0.95 lo que proporcionará una cierta garantía de funcionamiento, adicional toda vez que la producción de armónicos será muy reducida y

así disminuirán los posibles errores por micro cortes derivados de picos de tensión en armónicos indeseados.

Se colocan una serie de celdas de BT de seccionamiento, mando y maniobra para la alimentación de la energía al centro.

Esto se presenta en la siguiente figura del Centro de Transformación que forma parte del plano D.IV.1 Diagrama eléctrico general del Anexo D - Planos.

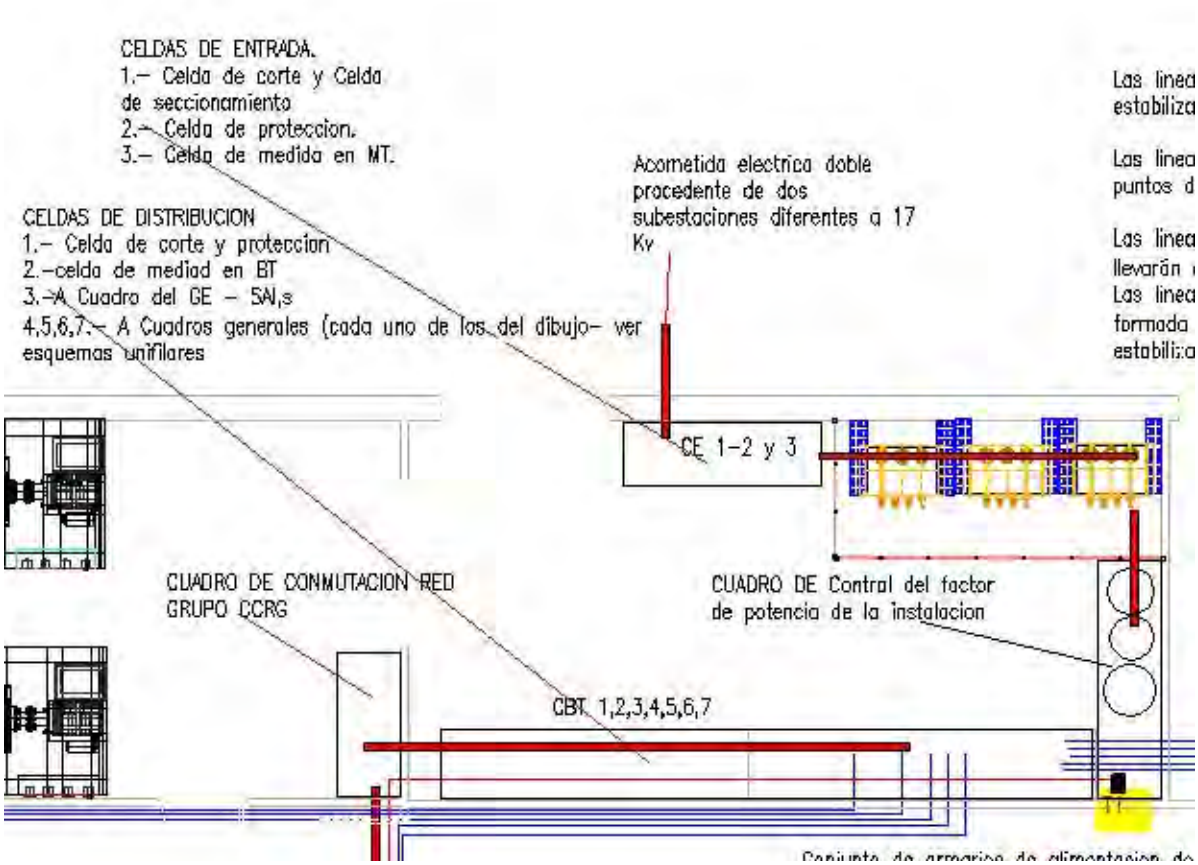


Figura 19 Esquema del centro de transformación del edificio

3.5.2 Suministro de energía de emergencia. Grupo electrógeno

Se debe proporcionar un sistema de emergencia por grupo electrógeno al CPD, para los casos en que los cortes de la red duren más de 20 minutos (tiempo máximo que puede abarcar el sistema de SAIs) [***28***]. Los sistemas que consumirán esta energía de emergencia son:

- Sistemas alimentados a través de SAI.
- Los enfriadores sensitivos y los sistemas de intercambio de calor asociados para el enfriamiento de agua o gas.
- Sistemas de iluminación de emergencia y seguridad.
- Sistemas de iluminación normales de funcionamiento.
- Sistema contraincendios.
- Sistemas de vigilancia, control, señalización y alarmas.

El suministro de energía de emergencia se debe diseñar de forma que en su funcionamiento de régimen se pueda mantener la operación completa del CPD. El grupo Generador debe diseñarse para operación continua para la carga en cuestión. La cantidad de combustible almacenado debe ser suficiente para una operación de 48 horas de operación a plena carga del grupo generador.

Se ha previsto un GE de 800 KVAs y un sistema de combustible para garantizar la operación durante, al menos tres días con una capacidad total de 22500 litros disponiendo de un depósito intermedio de capacidad para operación durante 8 horas de unos 2500 litros.

3.5.3 Sistemas de Alimentación Ininterrumpida (SAI)

El Sistema de Alimentación ininterrumpida debe garantizar el suministro a todas las áreas, ya sean atendidas o no, en el Centro de Datos incluyendo los periféricos durante breves interrupciones del suministro de energía o en el caso de fallos importantes, hasta que el sistema de energía de emergencia se detenga [***12***].

La distribución de Energía procedente de las SAIs deberá recorrer por canalizaciones paralelas a la distribución de energía no limpia y deberá estar constituida por circuitos independientes. En ningún caso deberá usarse las conducciones de energía procedente de las SAIs para alimentar equipamiento como motores, alternadores o sistemas rotatorios de ningún tipo. Por ello en las salas o zonas de equipos informáticos y de telecomunicaciones deberán disponer de circuitos separados de alimentación de energía no estabilizada.

Por el contrario, conviene que se distribuya energía procedente de las SAI, a los puestos de trabajo que hayan de establecerse para el correcto funcionamiento de los Sistemas del Centro.

A los centros de trabajo llegarán circuitos de ambas energías: Estabilizada y comercial, que se identificarán y señalarán adecuadamente (rojos para la energía estabilizada y blanco para la comercial) y se dotará de conexiones de modo que garanticen que no se va a conectar a la energía estabilizada ningún equipo móvil o portátil que pueda funcionar correctamente con energía sin estabilizar.

Se dispondrá de una línea que discurrirá junto a la comercial para la conexión de equipos rotatorios y que no será alimentada por la energía estabilizada.

De igual modo en las zonas o áreas de equipamiento informático o de telecomunicaciones, deberá existir tomas de corriente de energía no estabilizada que permitan la operación de equipos móviles rotatorios o de otro tipo para conectar los equipos de mantenimiento que pudieran ser necesarios. Estos equipos móviles o portátiles de mantenimiento, se dotarán de conectores especiales, que impidan la conexión a los puntos de energía limpia (estabilizada).

Para ellos los equipos móviles estarán dotados de clavija tipo G.

*Figura 20 Clavijas tipo G para conexión de equipos de mantenimiento en zona limpia [**29**]*

El resto de equipamiento tanto informático como no estará dotado de clavijas tifo F

*Figura 21 Clavijas estándar tipo F [**29**]*

Para elevar la disponibilidad, debe instalarse una SAI adicional con el fin de obtener redundancia (n+1). Cada Sistema debe tener sus propias baterías y estas deben ser planificadas de modo que sean de fácil mantenimiento, es decir libres de pérdidas de ácido, y con una esperanza de vida de unos 10 años.

La SAI debe poseer la capacidad suficiente para mantener el servicio de forma autónoma durante un periodo de tiempo de 20 minutos. Esta autonomía es considerada suficiente ya que los principales fallos duran menos que este tiempo y el sistema principal de energía de emergencia no conviene que se arranque durante instantes breves de tiempo de acuerdo con las interrupciones pequeñas, que deben ser manejadas por el Sistema de SAI [***30***] [***30***].

La sala de SAIs estará equipada con un armario de distribución de baja (bus bar de seguridad). Los disyuntores de entrada a las SAIs estarán integrados en las celdas de conmutación de baja tensión.

Se debe disponer de un sincronizador para garantizar la entrada en paralelo de las SAIs. El calor desarrollado en la sala de SAIs deberá eliminarse mediante enfriadores sensitivos conforme descrito en 3.3.6. En nuestro caso el enfriador será de exterior con lo que se podrá utilizar el frío del exterior para refrigerar. El suministro de agua fría a estos enfriadores debe garantizarse, también por 20 minutos de duración, en el caso de fallo de la energía.

El sistema deberá estar equipado con salidas de lectura de la carga residual de las baterías (dependiente de la carga, en minutos). Deben instalarse las lecturas de salida integradas en el área de operación e integradas en el sistema de control del edificio. Los valores de las lecturas de operación, los datos de operación y los mensajes de error se transmitirán al sistema de control automático del edificio.

Pueden usarse bien sistemas dinámicos o estáticos de SAIs. Deberán ser dimensionadas para un factor de utilización no mayor del 85%. Cada sistema debe disponer de sus propias baterías (sin mantenimiento).

En cada zona o área se instalarán cuadros de medida y conexión automáticos que permitan efectuar lecturas de los parámetros de la línea (P, Q, S, I V, COSφ entre fases y fase y neutro. También deberán poder medir el desplazamiento de neutro en las mediciones).

- Los sistemas de SAI deberán dar servicio para la atención de los siguientes sistemas individuales:
    - Iluminación de emergencia en
        - Sala de SAIs
        - Salas de Transformadores
        - Salas desatendidas
        - El 50% de la iluminación en salas desatendidas
    - Alimentación
        - A las bombas de agua de enfriamiento
        - Al menos la mitad de los enfriadores sensitivos
        - Todos los sistemas de seguridad
        - Todas las salas de equipos informáticos
        - etc.

En la siguiente figura se representan las salas de Centro de Transformación, Grupo Electrógeno y de SAIs, recogidas en el plano D.IV.1 Diagrama eléctrico general del Anexo D - Planos.

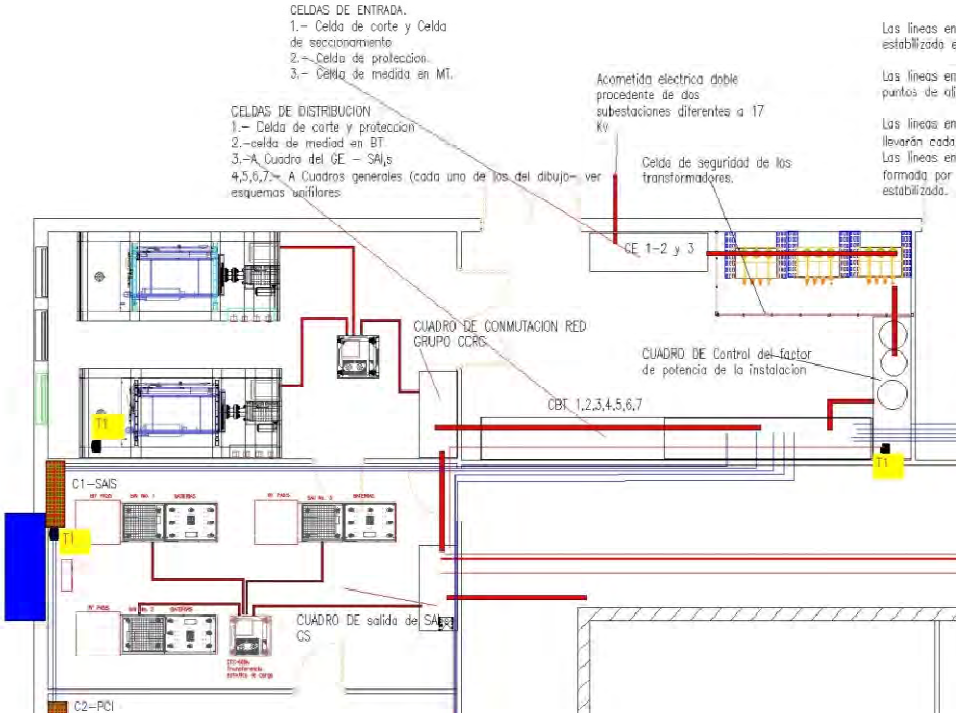


Figura 22 Salas de Transformación, Grupo electrógeno y SAIs

Puede verse como en la sala de SAIs se dispone un enfriador sensitivo conectado directamente al exterior y que insuflará aire frío directamente al ambiente

3.5.4 Redundancias

Con el fin de garantizar la Disponibilidad de las Fuentes y su fácil mantenimiento, se debe proporcionar para, al menos el 30% de los sistemas de suministro eléctrico de los de máximo riesgo disponible, elementos redundantes de aquellos que se considere más críticos de dicho sistema.

Para los sistemas de alimentación eléctrica que se consideren críticos se les dotará de redundancias de tipo N+1 como caso más elemental siendo necesario en casos puntuales que serán objeto de estudio, un sistema de redundancias de 2N. No obstante se preverán sistemas de funcionamiento en paralelo (tipo clúster) para asegurar el correcto funcionamiento del 60% de la instalación en caso de fallo de uno de ellos.

El sistema de suministro de emergencia puede considerarse como una forma redundante, con lo cual se podría obviar la necesidad de una unidad redundante. No

obstante, como se desea una mayor disponibilidad, el sistema de alimentación de emergencia también se dota de una unidad redundante adicional.

No obstante para algunos casos concretos, puede considerarse el caso de funcionamiento en paralelo de doble equipamiento de modo que se pueda asegurar el funcionamiento correcto, en caso de fallo del 60% de la instalación.

Para cada elemento/sistema, la siguiente tabla indica el criterio de redundancia.

Sistema	**Redundancia**
Suministrador	Contrato con dos fuentes diferentes de suministro.
Línea de 15 KV	Anillo redundante de la estación transformadora
Redundancia de Transformadores	Diseño: N transformadores que permitan el retrofit de los transformadores de área.
Sistema de suministro de emergencia	N
Sistema de SAIs	N+1
Celdas de conmutación de baja tensión (tras SAIs)	Bus bar del Suministro de emergencia o sistema de distribución para conexión en caliente
Cuadros de medida y protección	Dispuestos uno por cada área técnica

Tabla 13 Redundancias para cada sistema eléctrico

En nuestro caso se dispondrá tres transformadores de 600 KVA cada uno y uno de ellos en vacío junto con un sistema de conmutación para el caso de emergencia o fallo de uno de ellos cada uno de los otros dos suministrará, como máximo el 60% de la energía eléctrica.

Así estando previsto el Centro para una carga de 1000 KVA, se prevén tres transformadores de 600 KVA cada uno. Con ellos se consigue, en la parte eléctrica de una redundancia (N+1).

De igual modo se dispone de tres SAI de 400 KVA cada una; dos de ellas suministrando el 100% de la energía estabilizada necesaria

En cualquier caso se dispondrá de armarios de medida y protección en cada área y en cada línea de racks en la sala técnica.

3.5.5 Distribución general de la energía eléctrica

A partir de las SAIs la distribución de la energía estabilizada, se efectuará como se ha especificado en el apartado anterior [***12***].

En cada derivación se dispondrá de un cuadro de medición y de protección dotado de sistemas de corte automáticos provocados por extracorrientes de tiempo e intensidad

que para cada caso se determine, en función de la carga de cada circuito y el tipo de respuesta.

En cada cuadro de derivación, se instalarán cuadros de medida y conexión automáticos que permitan efectuar lecturas de los parámetros de la línea (P, Q, S, I V, COSφ entre fases y fase y neutro. También deberán poder medir el desplazamiento de neutro provocado por cargas asimétricas o condiciones de reactiva no centrada).

En cada cuadro se dispondrá de sistemas de protección contra contactos directos de 300mA para la alimentación estabilizada y de 30mA para los circuitos de alimentación no estabilizada. Esto es debido a que la toma de tierra de las salas técnicas está suficientemente cuidada como para no requerir una protección superior. En cambio en las salas generales, si bien también habrá circuito de tierra, es más seguro disponer de una protección mayor.

Se dotará el sistema de dos redes de tierra independientes uno para la energía limpia o estabilizada y el otro para energía comercial. Así las salas técnicas disponen de su propia red de tierras y las salas generales tendrán otra independiente así como ya se ha dicho tendrán tierras propias las salas con grandes equipamientos (CC. AA, SAIs, TRAFO, GE, etc.). Cada uno de ellos tendrá las conexiones a tierra que sean necesarias debiendo quedar, al menos una arqueta registrable para la medición. Siendo todas las arquetas accesibles para su mantenimiento (mediante placas en arquetas registrables y preparadas para su mantenimiento).

De igual modo se empleará un sistema de equipotencialidad que asegure la conexión de todos los elementos metálicos de los equipos. También estos sistemas serán separados. La red de equipotencialidad se conectará a tierra, ya que es la condición general en los equipos que se suministran. En aquellos casos que se conecten a neutro se estudiará caso a caso.

En definitiva la distribución de energía se efectuará mediante los 3 hilos de fase, el neutro, un cable de tierra y un conductor de equipotencialidad.

En cuanto a los puntos de toma de energía, estarán formados por cajas con cuatro tomas de corriente estabilizada y dos tomas de energía comercial, tal como se muestra en la figura.

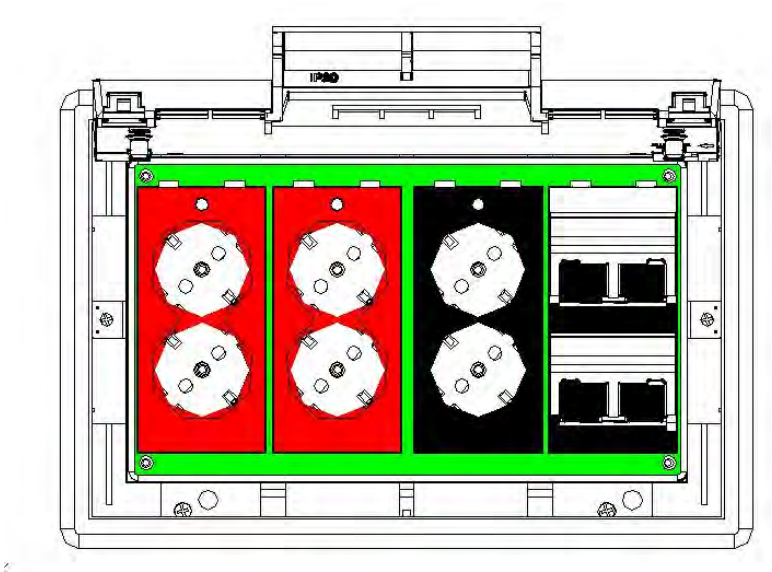


Figura 23 Cajas de conexión a la energía eléctrica y a las redes de un puesto de trabajo. Caja tipo SIMON de 4 niveles

Los puestos de trabajo que no sean de desarrollo sólo llevarán tomas de energía comercial.

La distribución general de la energía eléctrica se puede ver en el plano D.IV.1 Diagrama eléctrico general del Anexo D - Planos.

3.5.6 Instalación de Bus-Bar

Se ha demostrado eficiente el uso de bus-bar u otros mecanismos que permitan el conexionado en caliente de equipos, en la mayoría de los casos para el suministro eléctrico.

El empleo de Bus-Bar ofrece la ventaja de que los cables de energía para nuevos equipos y para recableados pueden disponerse rápida y cómodamente, permitiendo seleccionar la menor distancia al próximo punto operativo. De este modo se facilita el conexionado y el recableado de máquinas individuales. El bus-bar permite también la conexión de los equipos al sistema de distribución con conexión en caliente.

Los bus-bar o el sistema equivalente empleado, que en nuestro caso será aéreo y tan sólo para el suministro hasta los armarios de derivación y control de línea de Racks, se planificarán con los siguientes parámetros [***31***] [***31***]:

- Envolvente tipo IP 54
- Los bus bar serán de alimentación por ambos extremos para asegurar una alimentación fiable y de fácil mantenimiento de los cuadros de conmutación.
- Solo se activará un extremo de la alimentación. El segundo alimentador será redundante.
- Deben ser de corte todas las fases e incluso el neutro.
- Número de conductores L1, L2, L3, N, PE.

Como se ha dejado dicho anteriormente, todos los cuadros de derivación llevarán incorporados elementos de medida y de control e irán equipados con medidores de corriente, tensión, potencia, etc., junto con monitores de seguridad.

Los mensajes que se generen de alarma, de operación y de error se transmitirán al sistema de control automático de mayor nivel del edificio.

3.5.7 Cortafuegos

El recorrido de los cables de suministro del sistema de suministro de emergencia, de la iluminación, del alumbrado de emergencia, sistema de alarma contra incendios y megafonía se planificarán para que sean separados de los recorridos de otros cableados de acuerdo con la normativa de protección aplicable.

Si fuese necesario, los cables de alimentación sobre estos recorridos habrán de ser recubiertos con compuestos que formen una capa aislante de acuerdo con la normativa de protección contra incendios aplicable. Todos los huecos en paredes y techos deben ser cerrados.

Todos los pasamuros deben quedar sellados mediante cualquier sistema de sellado en vigor, preferentemente con sellantes de auto hinchado.

Se deben cerrar todas las penetraciones de cable a través de compartimentos contra incendios de acuerdo con la normativa de protección contra incendios.

3.5.8 Tierras y Equipotencialidad

3.5.8.1 Red de tierras

Para la red de tierras se aplicará lo establecido en el Reglamento electrotécnico de Baja Tensión.

Se establecerán dos redes de tierras independientes una para los equipamientos de datos que se alimenten con energía estabilizada, y otra para los equipos que sirven a elementos de uso general o que no requieran energía estabilizada.

La red de tierra estará constituida por un embarrado de cobre no menos de 20 mm^2 de sección y con al menos una pica de tierra cada 20 metros de longitud. Será una red sin ningún tipo de corte (es decir continua en su totalidad).

Los posibles embornados de los sistemas procedentes de armarios, conectores, etc. garantizarán una conexión de resistencia inferior a la que supondrían diez metros de longitud de la red (nunca superior a 0,05 ohmios).

La sala Técnica tendrá una red de tierras como se presenta en la figura.

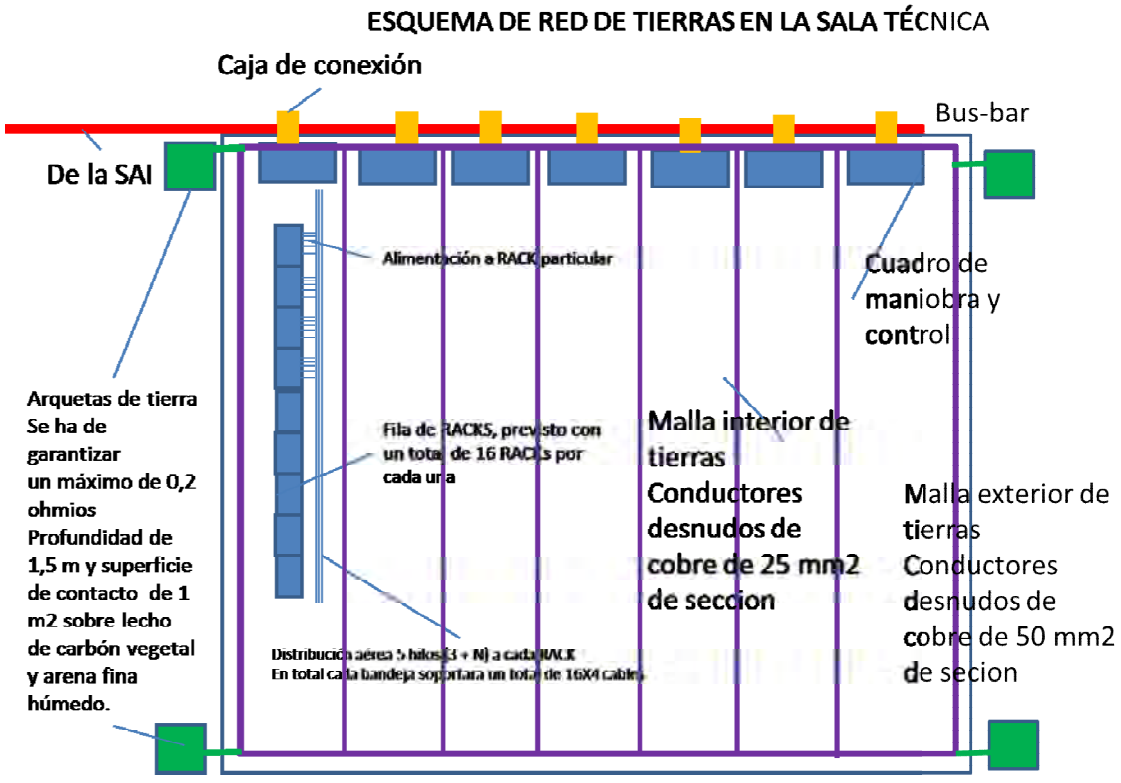


Figura 24 Esquema de tierras en sala técnica

Los recintos que colindan el pasillo de circunvalación se conectarán a las arquetas de tierra de las esquinas de la misma a excepción de las ya mencionadas anteriormente que lo harán a su propio sistema de tierra.

Como ha quedado dicho el resto de zonas dispondrá de una red diferente a las anteriores.

3.5.8.2 Sistema de equipotencialidad

De igual modo que para la red de tierras, se dispondrá de una red de equipotencialidad en todas las salas técnicas que garantice que los elementos metálicos y envolventes de equipamiento electrónico o de otro tipo se hallan a un mismo potencial, que impida la derivación de corriente por contactos indirectos o directos sobre ellos.

Esta red equipotencial se conectará a un embarrado general que a su vez se conectará al embarrado de tierra.

Se estará a lo dispuesto en la ITC-BT-38 del Reglamento electrotécnico de baja tensión.

3.5.8.3 Mediciones de tierras y equipotencialidad

Las mediciones de las tierras se efectuarán en una única zona de medición, preparada para tal hecho y se llevará a cabo mediante el siguiente sistema.

En cada armario de distribución a la sala técnica, se dispondrá de un sistema de evaluación de la derivación a tierra de las líneas de racks a él conectado, de modo que se pueda conocer la derivación a tierra a nivel de Rack.

Se establecerá una zona en que se dispongan de tres arquetas de referencia a tierra (en un arco de circunferencia de radio de 5 m, separadas entre sí al menos 3 m) En dicha zona deberán coexistir, a una distancia no menor a 3 m, una arqueta de la red de tierras para la energía estabilizada y otra para la energía comercial.

3.5.9 Protección contra interferencias electromagnéticas.

Se deberá construir el edificio de modo que cumpla los requisitos de compatibilidad electromagnética establecidos en la normativa TEMPEST, con la intención de reducir tanto la generación de interferencia como el impacto de interferencias externas en la sala de proceso. Algunas técnicas para alcanzar esta protección son [***32***] [***32***]:

- Recubrimientos de hoja de aluminio
- Apantallado por junturas de sándwich (Sandwich Seam Shielding)
- Separación de líneas de alimentación
- Disminución de radiaciones conducidas e inducidas para evitar malfuncionamiento de los equipos. Sobre todo aislando los conductos de energía contra radiaciones y evitando la conexión de cargas que generen mucho ruido a las líneas de alimentación que suministran a equipos informáticos. Para ello se dispone de las formas de alimentación particular para motores que ya se ha indicado en el apartado 3.5.3.

3.6 Sala de enlaces

Es de especial interés disponer de una zona en que concurran todos los enlaces con el exterior, identificados por proveedores de servicios de enlace y que, asimismo sea origen de la completa gama de enlaces de conexionado interior del edificio.

Según establece la norma TIA 942, esta área de enlaces constituirá lo que la norma denomina “primary entry room” [***1***].

A efectos de identificarlo correctamente se incorpora un esquema de la estructura que propone la norma para un Centro de Proceso de Datos.

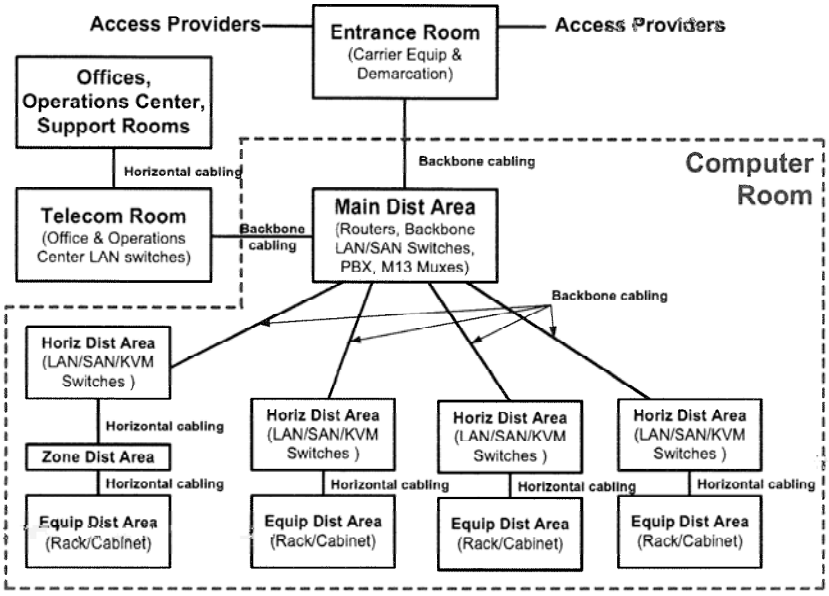


*Figura 25 Ejemplo de topología de centro de datos [**1**]*

3.6.1 Conformación y estructura

De acuerdo con lo reflejado en la figura anterior, proveniente de la propia norma TIA 942, se dispondrá de un centro en que se concentrarán la totalidad de los proveedores de servicios de la empresa.

Por necesidades de redundancia, se dispondrá de dos locales idénticos para esta sala de accesos tal como se recoge en la figura:

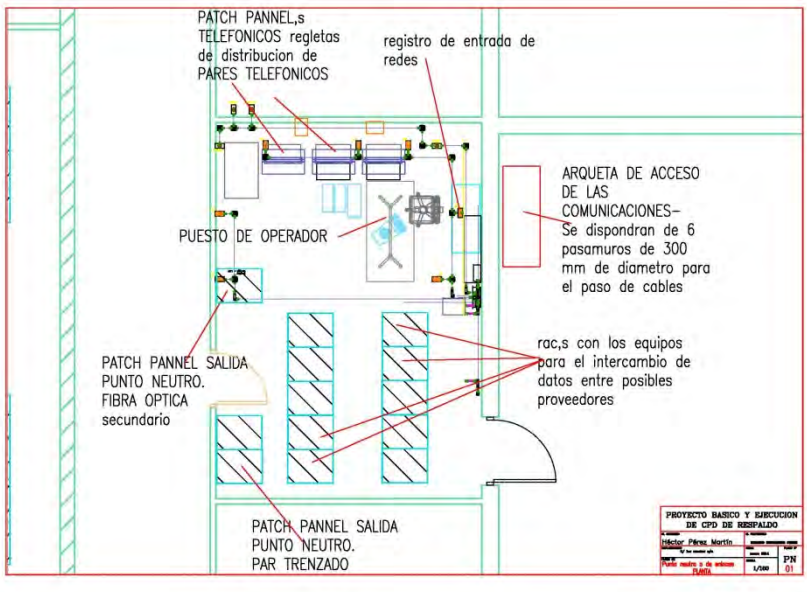


Figura 26.- estructura y distribución de cada una de las salas de accesos

Dicha sala será considerada como sala técnica de telecomunicaciones a todos los efectos y estará físicamente ubicada al lado de la sala en que se disponga la central de conmutación telefónica del edificio. En el caso que nos ocupa ambas salas se funden en una sola. Para cada una de las dos en redundancia.

Para adecuar el acceso a la sala se dispondrán de canalizaciones desde un conjunto de arquetas al exterior del edificio; acogidas por la protección perimetral del mismo y con un nivel máximo de seguridad.

A estas arquetas acometerán los proveedores de servicios desde el exterior y también llegarán los servicios de comunicaciones de radio.

Desde estas arquetas (no menos de dos con unas dimensiones mínimas de 150x150x100 cm^3 irán en baterías de tres grupos de tubos para separar las acometidas de cobre, de las de fibra y de las guía ondas o coaxiales procedentes de las antenas o servicios radio.

Cada conducto que canalice cables del tipo que sea no tendrá un diámetro inferior a 150 mm. De modo que se distribuirán en baterías o grupos de 3 tubos de 150 mm de diámetro.

Así cada arqueta dispondrá de una capacidad de 30 baterías de tubos, distribuidos en las paredes de la arqueta.

3.6.2 Acceso de comunicaciones a la sala

La sala presentará un panel del tamaño apropiado para la terminación de los cables que provengan de las arquetas exteriores. Dicho panel estará subdividido en tres grandes áreas clasificadas por la tecnología del enlace o tipo de cable en cobre-datos, fibra óptica y sistemas de radio (provenientes de antenas), debiendo preverse otras dos áreas de expansión y una para otros tipos de enlaces.

Esto puede materializarse mediante un panelado de la forma de la figura, extendiendo las zonas verticalmente a la totalidad del muro de acceso a la zona de enlaces.

El formato tendrá la forma de la figura.

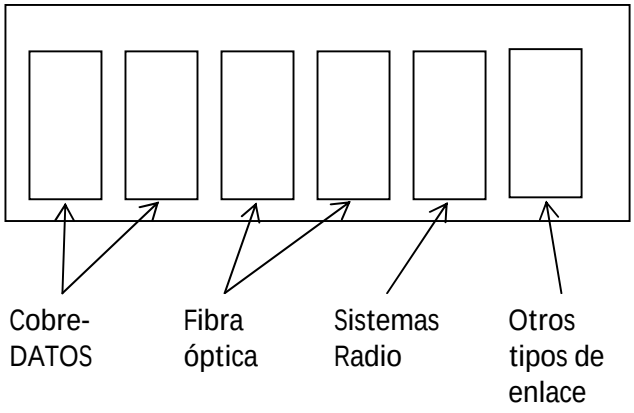


Figura 27 Sugerencia de panelado para el acceso de comunicaciones a la sala

El orden definitivo de los paneles será definido, dependiendo de la obra definitiva.

3.6.3 Salida de datos de la sala

En cuanto a las salidas de datos de la sala de enlaces se efectuará mediante paneles en las paredes mejor orientadas en relación con las salas técnicas de informática y comunicaciones.

El panelado estará formado por paneles correspondientes a los proveedores de servicios de la EMPRESA y estos paneles estarán subdivididos en función de la tecnología de los enlaces (cobre o fibra óptica), pudiendo estar el panelado de cobre, subdividido a su vez

en paneles correspondientes a los tipos de conexión (RJ 11, RJ 45, Coaxial, tipo BNC, etc.).

De esta forma, en función del proveedor, se dispondrá de tomas que permitan llevar la señal, cualquiera que esta sea a los puntos en que sea necesario, facilitando el intercambio de las posiciones de los equipos, sin necesidad de alterar el cableado definitivo de las redes tendidas en el Centro.

3.6.4 Equipamiento y tratamiento de señal y modificaciones y ampliaciones

En el interior de la sala se dispondrá del equipamiento necesario para la regeneración y distribución de la señal en ambas direcciones (desde el exterior y al exterior).

El panelado de acceso a la sala tendrá un equivalente interior en el que se dispondrá de conexiones hasta los equipos de los proveedores, o que den servicio a los elementos de los proveedores, que se dispondrán en bastidores (racks normalizados según norma IEC 60297 de 19").

Para la dotación de este equipamiento se prevé un espacio equivalente al ocupado por ocho racks de equipos de 80x60 cm^2 en planta, con sus correspondientes pasillos de mantenimiento y de operación.

Asimismo se deberá prever otros dos rack para cableado

Estará dotada de suelo técnico y dispondrá de los medios necesarios para refrigerar los equipos a razón de 100 W/m^2 (salvo que requisitos posteriores de los proveedores, exigieran condiciones particulares). Se dispondrá de una dotación de energía de similar a la establecida para las salas técnicas con un mínimo de unos 100Kw.

Esta energía estará estabilizada a través de SAI.

De igual modo dispondrá de alimentación de emergencia (como todas las salas técnicas) y estará adecuadamente protegida por las redes de tierras y equipotencial.

Un posible esquema general de la sala sería del tipo siguiente.

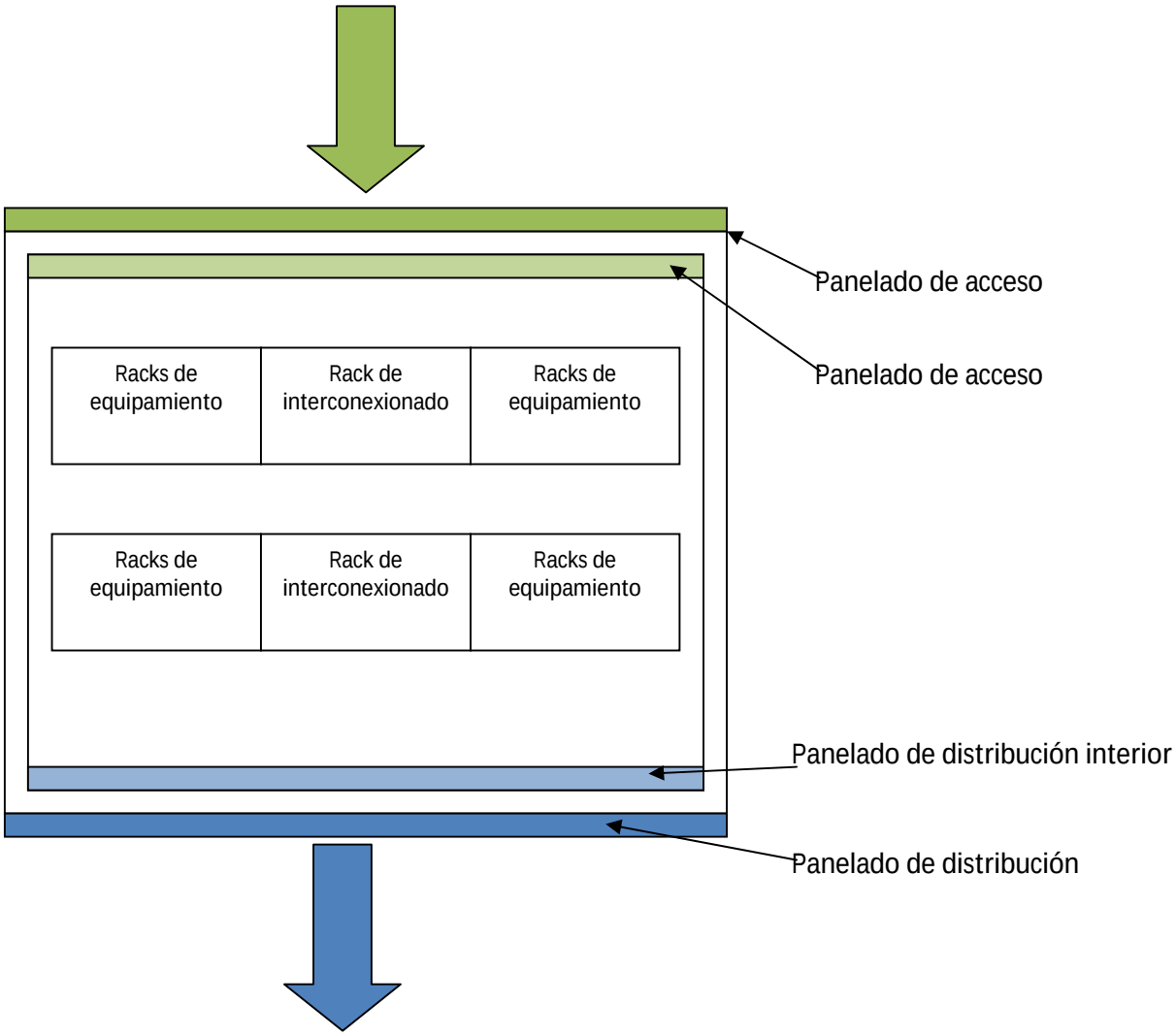


Figura 28 Esquema de interconexionado para el acceso a la sala

En la actualidad se dispone de los siguientes proveedores de telecomunicaciones que deberán estar presentes en el Centro de Respaldo:

- Telefónica/Movistar
- BT
- Colt
- France telecom/Orange

No obstante, como se ha establecido deberá preverse la posibilidad de otros proveedores que puedan interconectarse en el área de enlaces, de modo que puedan alcanzar cualquier punto de las salas sin tener que alterar los cableados del Centro de respaldo.

3.7 Salas o zonas de control

A continuación se describen las salas de control que llevará el centro de respaldo con una breve descripción de su función.

Los sistemas a supervisar son los descritos 3.4.1.3 y para cada uno de ellos se debe disponer de una zona particular para la supervisión y control. Para lo que se dispone de los espacios y el equipamiento adecuados.

Constituyen Salas de Operación y de control:

- La sala de Operación, para los Sistemas informáticos.
- La sala de Control de Red
- La sala de Control General para la monitorización y control de los sistemas "Domóticos del edificio"
- y la Sala de Seguridad para las actividades propias del control de la seguridad contra intrusión.

Las dos últimas se centralizan en una única sala en el Área de seguridad

Todas las Salas se presentan en el plano D.I Plano general del centro de respaldo del Anexo D - Planos del que se incluye una imagen a continuación, siendo las zonas de Seguridad y de Operación las zonas en que se incorporan los monitores y dispositivos de control. Cabe resaltar que todo el equipamiento de proceso y gestión informático, se hallará instalado en la Sala Técnica.

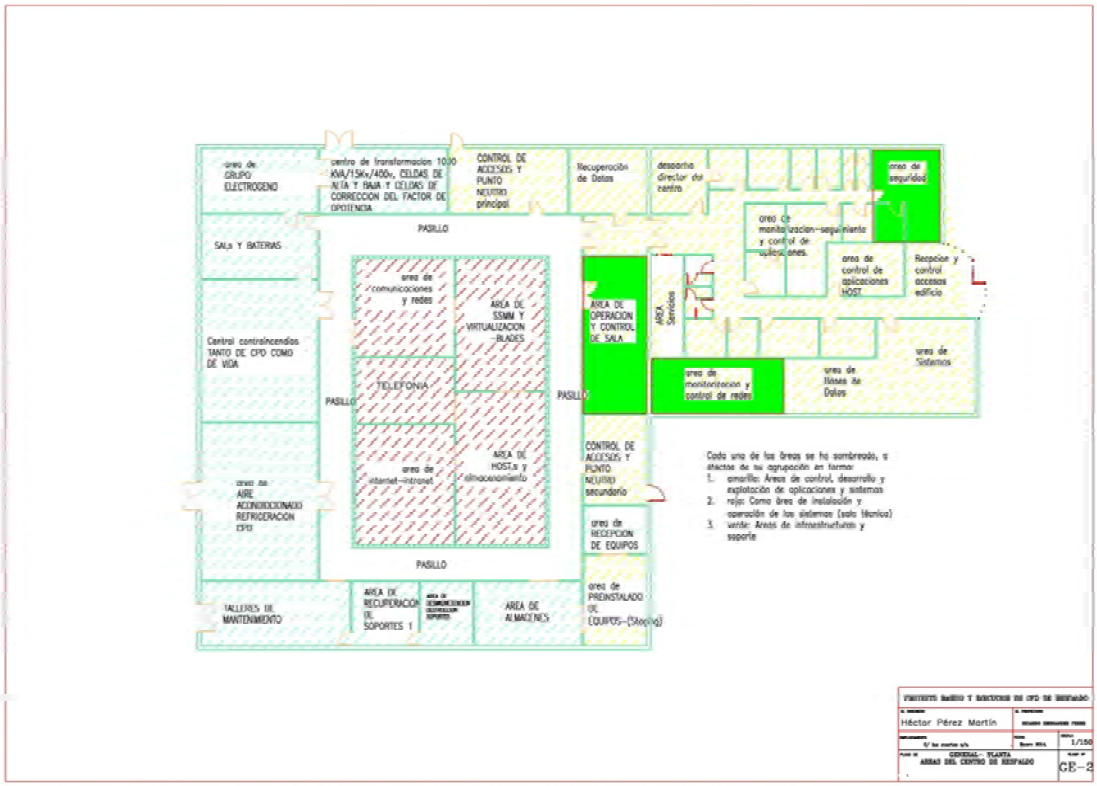


Figura 29 Salas de monitorización y control

3.8 Sistemas de Seguridad

3.8.1 Sistemas de Detección de Intrusión

Se deberá proporcionar un sistema de detección de intrusión para dotar de las condiciones de seguridad necesarias en el Centro. El sistema de detección de intrusión formará parte del sistema de gestión de seguridad al cual se integrará a través de un concentrador inteligente [***33***]. El sistema de detección de intrusión deberá monitorizar todo el Centro. Especialmente las áreas técnicas y en particular las que contengan equipos de informática y de telecomunicaciones, con los medios indicados o similares.

- Contactos y cierres magnéticos
- Contactos y cerrojos magnéticos así como detectores de rotura de ventanas.
- Detectores de movimiento en salas sensibles

Se proveerán los necesarios huecos, cortes, tubos transiciones de cables, etc. que sean necesarios en las puertas y ventanas. Las señales de alarma serán enviadas, directamente a la sala de control de seguridad del edificio.

3.8.2 *Sistemas de alarmas*

Las áreas sometidas al peligro de asaltos, tales como sala de control de seguridad, área de recepción, punto de control de accesos, sala de operaciones, etc. deberá equiparse con sistemas de alarma contra asaltos. La estación de control estará localizada en el área de seguridad. Estos sistemas dispondrán de sensores de tipo velocímetros y volumétricos así como de rotura de plano o línea en huecos

Se dispondrá de un botón de alarma para solicitar apoyo directamente de las fuerzas de seguridad en la sala de control de seguridad

En el resto de las salas se dispondrá de una alarma conectada a la sala de control de seguridad.

3.8.3 *Sistemas de Cámara (CCTV)*

Se instalará un sistema de vigilancia por videocámaras al exterior del edificio así como para vigilancia adicional del interior del mismo. Las cámaras se instalarán de tal forma que cada dos de ellas cubran la totalidad del espacio vigilado con visibilidad de la una a la otra.

Dependiendo del tipo de uso, el control de alarmas de las cámaras se realizará mediante sensores de vídeo, detectores de movimiento o contactos del sistema de acceso controlado.

Se grabarán en vídeo las sesiones de vídeo vigilancia. Se emplearán cámaras en blanco y negro. El sistema debe ser completamente digital y conectado en red con direccionamientos IP.

Los sistemas de cámaras vigilarán las siguientes áreas:

- Unidades de proceso situadas en las salas de control correspondientes.
- Activación de las cámaras mediante sensores de vídeo o detectores de movimiento.
- Sistemas cara a cara de acceso al edificio (control de entradas).
- Áreas fuera del alcance de las cámaras vigiladas por iluminación de apoyo por infrarrojos.
- Cámaras exteriores:
    - Vigilancia de las fachadas y de las verjas.
    - Vigilancia de las áreas de entrada y de entrega de productos.
- Cámaras interiores

- Todas las cerraduras o bloqueos de la zona de dirección y de almacenes de materiales.
- Salas y pasillos sensibles.

3.8.4 Sistemas de acceso controlado (Controlled Access Systems, CAS)

El sistema de seguridad del edificio y o de las instalaciones generales tendrá un sistema de control de accesos por ordenador con capacidad de vigilancia continua.

Todo el personal dispondrá de tarjetas individualizadas que permitirán el acceso a áreas específicas basadas en áreas de nivel de seguridad.

El sistema controlará, monitorizará y generará señales de alarma para todas las transiciones de acceso.

El sistema proporcionará alarma de las entradas forzadas así como de las puertas no cerradas según el nivel de contención requerido.

El sistema de acceso controlado puede combinarse con el sistema de registro de tiempos y de atención (presencia-ausencia). Por su parte las tarjetas de acceso pueden combinar elementos de control de acceso como elementos de identidad digital (PKI).

Se identificarán las tarjetas de los empleados mediante un código de color un código grabado en memoria la memoria de un chip legible. Esto permitirá identificar el tipo de acceso permitido al empleado según su categoría laboral, su dedicación y su pertenencia al servicio. Este código de colores coincidirá con las marcas de color para las diferentes categorías de las áreas del edificio.

De igual modo permitirá dotar a los visitantes de un código de acceso a determinadas zonas. TODAS las personas se registrarán y dispondrán de una tarjeta, ya sea temporal o permanente.

Todos los subsistemas del sistema de seguridad: Accesos, Megafonía y CCTV quedan reflejados en el plano D.V Instalaciones de seguridad del Anexo D - Planos, que se reproduce en la Figura 30.

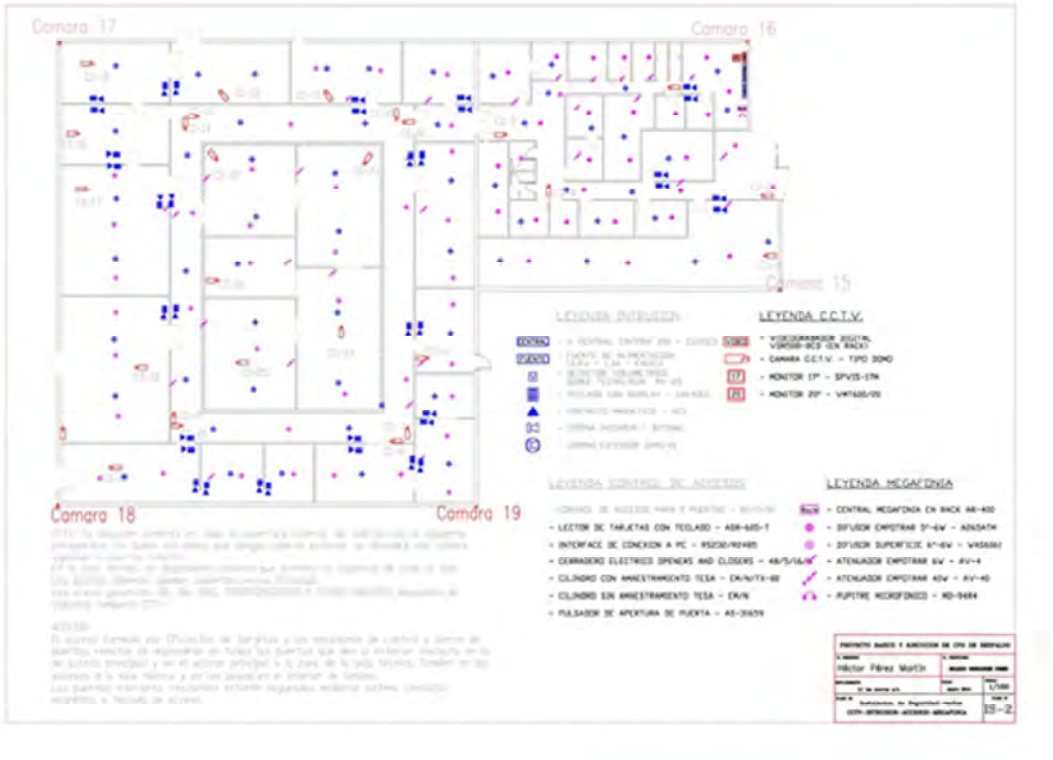


Figura 30.- Instalación de los diversos sistemas de seguridad

En dicho plano se recogen los principios de la ubicación de las cámaras CCTV y de los mecanismos de control de accesos en puertas.

3.9 Protección contraincendios

Al igual que con todos los sistemas del edificio, para el sistema de Protección contra Incendios se hace la distinción entre el sistema de protección contra incendios General y el Sistema protección contra incendios para la Sala Técnica.

Así para el caso de protección general el sistema de detección estará conformado por elementos medidores de partículas de humo en suspensión y por sensores térmicos adjuntos al propio sistema de extinción (difusores de agua).

El sistema de extinción para el caso de general estará formado por una red de rociadores automáticos de agua. Los sistemas de rociadores automáticos de agua, sus características y especificaciones, así como las condiciones de instalación se ajustarán a las normas: UNE 23.590, UNE 23.591, UNE 23.592, UNE 23.594, UNE 23.596 y UNE 23.597 [***34***] [***34***].

Esta red estará soportada en los puntos de riesgo de incendio con extintores apropiados y BIES tal como se expresa a continuación.

Así en el pasillo de circunvalación de la sala técnica se dispondrá de un rociador por cada metro lineal de pasillo en el centro del mismo y a la altura del techo. Así mismo se dispondrá un equipo con dos extintores uno Los extintores de polvo ABC, que sirven para apagar todo tipo de fuegos y otro de CO2, que se usan en lugares en los que haya riesgos eléctricos porque no dejan residuos, no conducen la electricidad y no estropean los cuadros eléctricos.

En las zonas de equipos de AA, de Contraincendios, de SAIs, de GE y de TRAFO, se dispondrá de igual modo de rociadores (1 por cada 4 m^2 de planta, dispuestos en el techo y de carros con dos extintores de CO2).

En las salas generales se dispondrá de un rociador por cada 9 m^2 y como apoyo de un extintor de tipo ABC por cada 250mml de desarrollo de pasillo o paredes.

A continuación se describen con mayor detalle y cuidado los sistemas de protección contra incendios que se aplicarán en el centro de respaldo desde la detección hasta la extinción y la extracción de humos.

3.9.1 Sistemas de detección

Se diseña de modo que al menos dos detectores que se hallen en la condición de alarma, antes de iniciar la secuencia de supresión. Esto se consigue disponiendo de dos diferentes bucles de detección (bucle A y bucle B). Este tipo de sistema se conoce como "sistemas de zonas cruzada" (cross-zoned system) [***35***]. A su vez puede ser de enclavamiento simple o doble.

El sistema cumplirá las condiciones del Código Técnico de la Edificación y la normativa que aplique y tendrá en cuenta las condiciones establecidas por los bomberos locales, si las hubiese.

El sistema de detección de la Sala Técnica operará en la sala técnica; pero tendrá una réplica que estará instalada en la sala de seguridad. El sistema utilizará sistemas de bus (para la identificación de cada elemento que pueda producir señal de alarma).

Los elementos sensores serán:

- Sistema de detección y alerta temprana de humos (VESDA), en las salas técnicas.
- Sensores fotoeléctricos distribuidos en cada sala.
- Para las zonas con falso techo y/o suelo técnico (más de 30 cm de vano), habrá detectores tanto en los falsos techos como bajo el suelo técnico.

El sistema de alarma contraincendios permitirá la identificación individual del generador de la alarma, incluso en el caso de los pulsadores de alarma manual descritos en el apartado 3.9.1.2.

Todas las alarmas serán visibles desde el centro de control contra incendios. El tiempo de respuesta del equipo de personas contraincendios no será mayor de 3 minutos; en el caso de un incendio, debe asegurarse una llamada directa a los bomberos.

*3.9.1.1 Sistemas de detección y alerta temprana de humos (VESDA) [*35*]*

Un sistema de este tipo muestrea el aire continuamente para desarrollar una referencia de las partículas en el ambiente. El sistema detecta micro partículas producidas por pirolisis. El sistema de control monitoriza desviaciones de la línea de base y dispara una alarma que se dirige a la estación de control central si los niveles aumentan por encima de un valor predeterminado.

En salas que son particularmente sensibles, será obligatoria la instalación de un sistema de alerta temprana de humos. En particular, estará instalado en las siguientes salas:

- Almacén, Desmagnetización, Staging
- Salas Técnicas (HOST, SERVIDORES, RED), toda la Sala Técnica

- Salas Técnicas de telefonía o Puntos de acceso
- Salas técnicas de electricidad en SAIs y TRAFO

Este sistema proporcionará detección de la sala en su totalidad y particularmente de los enfriadores sensitivos.

En la siguiente tabla se resumen los tipos de salas y el mecanismo de detección asociado:

Área	**Sistema de alarma contraincendios**	**Sistema de detección temprana de incendio (VESDA)**
HOST/SAN	√	√
Servidores	√	√
Áreas de Red (electrónica)	√	√
Archivo	√	
Operación	√	
Operación de cintas	√	
Área de impresión	√	
Áreas técnicas	√	√
Resto edificio	√	

Tabla 14 Sistemas de detección para cada tipo de sala

3.9.1.2 Pulsadores de alarma manuales

Habrá de disponerse de un sistema de alarma de incendio con identificación de puntos individuales de llamada.

Se ubicarán estos pulsadores en las salidas de emergencia, en la sala de control de seguridad así como en salas técnicas de todo tipo y de almacenamiento. También se dispondrán, más distanciados, en las zonas de uso común del edifico y próximos a las bocas equipadas y extintores.

Los pulsadores deberán estar conectados al sistema informático de control de alarmas.

3.9.2 Sistemas de extinción

Se utilizará el sistema de extinción por agua nebulizada en las salas técnicas ya que, en general es el sistema reconocido como menos perjudicial para los equipos y sistemas [***36***]. Existen otras alternativas basadas en la utilización de gases inertes, que sólo consideraremos en caso la extinción por agua nebulizada no sea viable.

Las siguientes salas serán equipadas con sistemas de extinción por nebulización, rociado o descarga automático: Sala Técnica, SAIs y GE.

En cuanto a las zonas generales y no técnicas en general se utilizará, como ya se ha dicho sistemas más sencillos de rociado de agua de sprinklers o similares. Todo ello soportado por sistemas de extinción mediante extintores para el tipo de fuego adecuado.

El sistema de extinción se armará cuando dos líneas o dos detectores del sistema de alarma contraincendios se activen.

Al mismo tiempo, el sistema de aire acondicionado/ventilación asociado, debe apagarse y las puertas rendijas y compuertas cortafuegos deben cerrarse. El mismo procedimiento se aplicará a las salas con protección en suelo elevado.

Además de estos sistemas, se dispondrá de los sistemas exigidos por la normativa contraincendios reflejada en el Código Técnico de la Edificación, disponiendo las bocas equipadas y los extintores que sean apropiados a cada zona y conforme a las distancias reglamentarias.

3.9.2.1 Sistemas de nebulización, rociado o descarga automático

La necesidad de descargadores automáticos constituye la base de los sistemas contraincendios en las salas técnicas, particularmente las desatendidas. Su disposición y número se decide por el riesgo potencial de incendio en las áreas a controlar.

Se empleará este sistema ya que el Centro de Respaldo, además de requerir la protección máxima posible a los equipos informáticos y de apoyo a los mismos, siempre cumplirá una o varias de las condiciones reglamentariamente exigidas:

- Edificios con múltiples plantas, garajes bajo tierra
- Acceso difícil al edificio en caso de incendio, debido a un nivel de alta seguridad o construcción subterránea.

A continuación se presentan en forma esquemática algunos sistemas de los empleados en el centro de respaldo para la extinción de incendios.

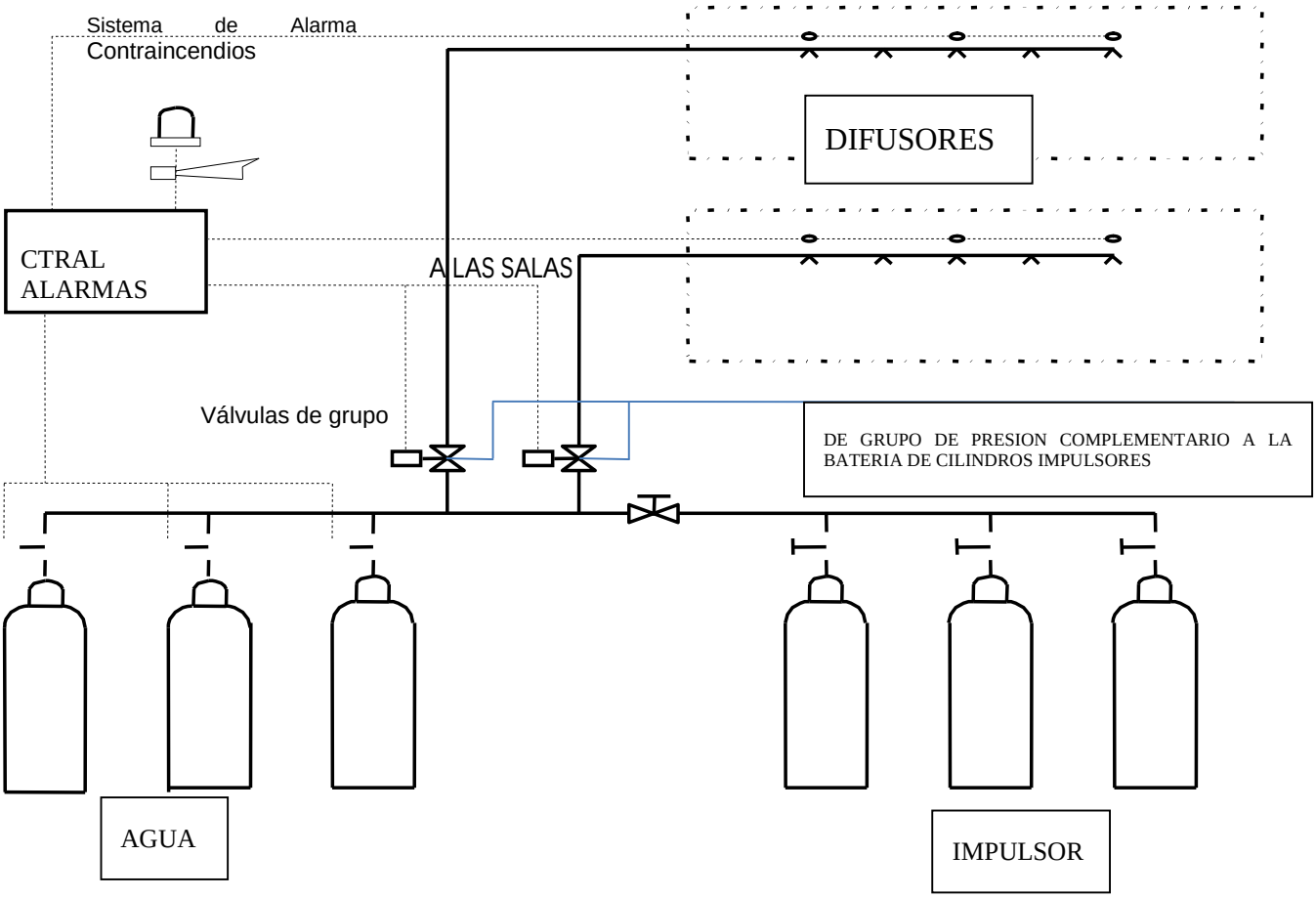


Figura 31 Diagrama de los sistemas de extinción automática mediante agua nebulizada o gas

3.9.2.2 Sistemas de pre-acción

La mayoría de los Centros de Datos que necesitan una segunda línea de defensa contra el fuego utilizan un sistema de descarga de acción preliminar o de pre-acción. Este proporciona un elevado nivel de confianza de que el agua no se descargará salvo que el fuego exista [***38***] [***38***].

Se implantará este sistema de pre-acción para minimizar la operación accidental del sistema de descarga con resultado de una inundación y sobre todo de posibles daños indeseados.

El sistema de pre-acción trabajará como sigue:

1. Las tuberías de los descargadores en el techo estarán presurizadas con aire comprimido, continuamente. Un conmutador de presión monitoriza la presión del sistema de tuberías.
2. La válvula de llenado se controla por el sistema de detección de humos. Una vez disparada la válvula se abre, para liberar el agua dentro del sistema de tuberías.
3. El agua no se descargará de ninguna cabeza nebulizadora o rociadora (sprinkler) hasta que el mismo no se abra por el calor provocada por el fuego. La cabeza rociadora se abre cuando la temperatura alcanza el punto prefijado (típicamente unos 70 º C) o cuando se quita el elemento de disparo.

4. El sistema de descarga se diseñará de acuerdo con la normativa aplicable para los mismos (Código Técnico de la Edificación y normas UNE referenciadas en el párrafo inicial de esta sección).

Se utilizará el Sistema de preacción en:

- Todas las salas técnicas, ya sean desatendidas o no
- En los pasillos
- Todas las áreas técnicas y de servicio del edificio.

3.9.3 Sistemas extractores de humo

Se dispondrá de un sistema extractor de humos que ha de estar separado de los sistemas centrales. El volumen de aire extraído de las salas debe ser igual a la mínima tasa de aire que posibilite el mantener un índice de humo inferior al 40% del humo producido durante el tiempo necesario para evacuar la zona prevista y para un fuego tipo dependiendo de la tipología de los productos que pueden arder en esa zona).

Además de cumplir lo establecido en el apartado 3.3.7, se cumplirá lo siguiente:

- Serán necesarios ventiladores que expelan el agente extintor en caso de descarga.
- El panel de control de ventiladores de extracción debe hallarse fuera del Centro de Datos.
- Instalación de sistemas de eliminación de humos para extraer el humo y el calor del Centro de Datos.

3.9.4 Equipamiento de lucha contra el fuego

Aparte de los sistemas de extinción automáticos descritos en el apartado anterior, el centro deberá disponer de equipamiento de lucha contra el fuego, como hidrantes y extintores portátiles [***38***] [***38***].

3.9.4.1 Hidrantes

Se dispondrá de hidrantes y bocas de incendio equipadas:

- Fuera del edificio cada 80 a 100 m.
- En el interior del mismo en todas las salas con cargas de fuego elevadas (que superen los 100 MJ/m^2 según el R.D.2267/2004 “Reglamento de seguridad contra incendios en establecimientos industriales. Y colocado sobre los pasillos y rutas de evacuación. Se dispondrán hidrantes en el pasillo de circunvalación uno en cada esquina BIE de 45 mm según Reglamento de Instalaciones de Protección Contra Incendios.

Todo ello atendiendo a la normativa en vigor al respecto

- Reglamento de instalaciones de protección contra incendios (Real Decreto 1942/1993)
- Reglamento de seguridad contra incendios en los establecimientos industriales (Real Decreto 2267/2004)
- Código Técnico de la Edificación

- Norma UNE-EN 671

3.9.4.2 Extintores de fuego portátiles

Debe disponerse de extintores de fuego con agentes de extinción apropiados (para sistemas TIC será CO2).

Dichos extintores se situarán de conformidad con la normativa en vigor, en función del tipo de equipamientos de la sala:

- De CO2 móviles (30 Kg) en salas técnicas de grandes dimensiones y desatendidas
- De CO2 portátiles en otras áreas de Proceso de Datos y en salas eléctricas
- Extintores de espuma para el resto de salas y espacios de oficinas
- Extintores de polvo para aparcamientos, garajes y almacenes

Los extintores se colocarán con su base a 40 o 50 cm del suelo para que puedan ser fácilmente extraíbles y manipulables en caso de incendio.

3.9.5 Sistemas de alarma de incendios

Se instalará un sistema de megafonía con un amplificador en standby y una línea de monitorización en el área de control contraincendios.

Se establecerá una estación de comunicaciones de voz en la sala de control contraincendios y conectada directamente al sistema de megafonía general del edificio descrito en el apartado 3.10.

- Alarma de evacuación, alarma de incendio, amenazas y alarmas técnicas (fugas de gas y de agua)
- Altavoces en cada sala
- Micrófono en la sala de control contraincendios y registros de mensajes de evacuación

3.9.6 Iluminación de seguridad

Signos iluminados con soporte electrónico se instalarán en la parte superior de las salidas y a lo largo de todas las rutas de evacuación. Su suministro de energía se garantizará mediante una central de baterías separada con un tiempo de energía almacenada al menos 1 hora, con intercambio al sistema de suministro de energía de emergencia.

- Signos iluminados en las rutas de evacuación y sobre las salidas.
- Iluminación mínima de 1 lux.

3.9.7 Señalización contraincendios

Los hidrantes, los extintores y las áreas o corredores de evacuación, estarán debidamente señalizados. En cada punto en que haya un elemento de lucha contraincendios, así como en todos los espacios amplios habrá un plano en que se refleje la parte del plan de evacuación que corresponde a esa área del edificio, quedando las rutas de evacuación adecuadamente señalizadas sobre el plano con expresa

identificación del punto en que se halla situado (mediante una leyenda del tipo “Ud. está aquí” o similar).

El sistema contra incendios se presenta en la figura siguiente.

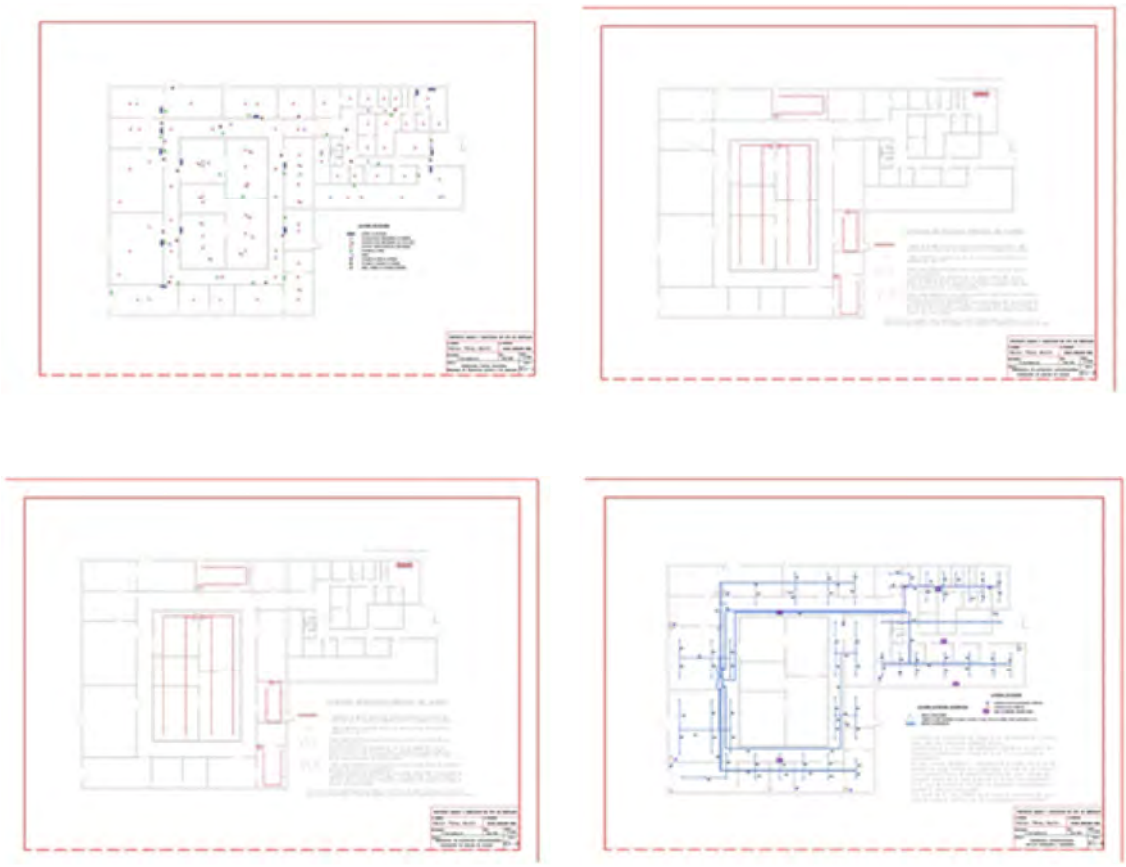


Figura 32 Dimensionamiento y medición del sistema contraincendios

3.10 Sistema de megafonía

El edificio contará con un sistema de megafonía con hilo musical ambiental en las áreas de trabajo. Este sistema de megafonía deberá estar asociado con el sistema de avisos acústicos contraincendios.

En salas técnicas y de apoyo podrá disponerse este sistema a discreción.

El sistema estará dotado del número de altavoces necesarios para que el lóbulo acústico en el plano de trabajo suponga un nivel musical que enmascare los posibles ruidos provocados por las instalaciones permitiendo un ambiente de trabajo agradable.

Se garantizará un nivel medio de sonoridad no inferior a 25 decibelios musicales con una desviación máxima de +-5 decibelios a la altura del plano de trabajo.

El equipo de sonido estará formado por:

- Fuente de alimentación
- amplificador mezclador
- un sintonizador y
- un rack de reproductores de CD/DVD

- dos micrófonos
- cascos para la audición previa

De igual modo un ordenador y una aplicación informática podrán controlar el equipo de sonido, su intensidad, etc. y registrar las indicaciones de funcionamiento o averías que trasladarán al sistema general de señalización y control del edificio.

El equipo se dispondrá físicamente en la sala de Control general que se define en el apartado 3.7 y ubicada en la misma sala que la zona seguridad del edificio.

El sistema de megafonía se presenta en el plano D.V Instalaciones de seguridad del Anexo D - Planos.

Sobre dicho plano se efectúan las mediciones y el dimensionamiento de los sistemas mencionados.

3.11 Iluminación general del edificio

En todo el recinto sea dispondrán los sistemas de iluminación de tal modo que se impida el deslumbramiento.

Se seguirá lo dispuesto en el Código Técnico de la Edificación [***6***], estableciendo los siguientes niveles según las exigencias visuales de cada área de trabajo:

- Bajas exigencias visuales / 100 lux
- Exigencias visuales moderadas / 200 lux
- Exigencias visuales altas / 500 lux
- Exigencias visuales muy altas / 1.000 lux
- Áreas o locales de uso ocasional / 50 lux
- Áreas o locales de uso habitual / 100 lux
- Vías de circulación de uso ocasional / 25 lux
- Vías de circulación de uso habitual / 50 lux

La iluminación de los lugares de trabajo deberá cumplir, además, en cuanto a su distribución y otras características, las siguientes condiciones:

a) La distribución de los niveles de iluminación será lo más uniforme posible.

b) Se procurará mantener unos niveles y contrastes de luminancia adecuados a las exigencias visuales de la tarea, evitando variaciones bruscas de luminancia dentro de la zona de operación y entre ésta y sus alrededores.

c) Se evitarán los deslumbramientos directos producidos por la luz solar o por fuentes de luz artificial de alta luminancia. En ningún caso éstas se colocarán sin protección en el campo visual del trabajador.

d) Se evitarán, asimismo, los deslumbramientos indirectos producidos por superficies reflectantes situadas en la zona de operación o sus proximidades.

e) No se utilizarán sistemas o fuentes de luz que perjudiquen la percepción de los contrastes, de la profundidad o de la distancia entre objetos en la zona de trabajo, que produzcan una impresión visual de intermitencia o que puedan dar lugar a efectos estroboscópico.

Además se deberá garantizar que las fluctuaciones de luminosidad provocada por equipos de tipo fluorescente o similares, no sean inferiores a los 50 Hz ni tampoco superen los 100Hz.

Conforme estas especificaciones y el tipo de tareas de cada zona definida para el centro, se establecen los siguientes tipos de iluminación.

Área	Tipo de iluminación
Sala Técnica	La iluminación será fría, entendiendo que el espectro se halle desplazado hacia el verde . Las luminarias serán de fácil evacuación del calor a fin de garantizar que la refrigeración de las salas extrae el calor que pueda generarse. Las intensidades serán: • 700 lux plano 1 m sobre el suelo • 200 lux paredes en el pasillo entre Racks.
Otras Salas técnicas (trafo, SAIs,..)	En salas técnicas se deberá disponer iluminación incandescente en aquellas salas que dispongan de equipos rotatorios móviles (motores o similar). Se garantizará un mínimo de 500 lux en el plano de trabajo y de 200 lux en planos verticales.
Pasillos	En pasillos se garantizará un mínimo de 200 lux en un plano a 85 cm del suelo
Salas de recepción, visitas, etc.	Se garantizará un mínimo de 300 lux en un plano a 85 cm del suelo y en paredes verticales un mínimo de 150 lux.
Oficinas, salas de reuniones, etc.	En zonas de oficinas y donde se realicen tareas de monitorización, vigilancia y control de sistemas de información y telecomunicaciones se garantizará un mínimo de 800 lux sobre el plano de trabajo. Se garantizará un cambio de luminosidad bajo de modo que la iluminación ambiental supere, en todo momento a nivel de al menos los 400 lux.
Almacenes	En almacenes de datos se dispondrá una iluminación de igual características que las establecidas para oficinas. En estos no se dispondrán halógenos sino que serán incandescentes.
Recepción de materiales	En las áreas de recepción de materiales se dispondrá una iluminación superior a los 1000 lux en el plano de trabajo no generándose un contraste de más de 300 lux.

Tabla 15 Tipos de iluminación por tipo de sala del centro

3.11.1 Iluminación de emergencia

De acuerdo con el Código Técnico de la Edificación[***6***], contarán con alumbrado de emergencia las zonas y los elementos siguientes:

a) Todo recinto cuya ocupación sea mayor que 100 personas

b) Todo recorrido de evacuación

c) Los aparcamientos cerrados o cubiertos cuya superficie construida exceda de 100 m^2, incluidos los pasillos y las escaleras que conduzcan hasta el exterior o hasta las zonas generales del edificio.

d) Los locales que alberguen equipos generales de las instalaciones de protección contra incendios y los de riesgos especiales indicados en DB-SI 1 [***6***].

e) Los aseos generales de planta en edificios de uso público

f) Los lugares en los que se ubican cuadros de distribución o de accionamiento de la instalación de alumbrado de las zonas antes citadas.

g) Las señales de seguridad

Además se instalarán en todas las salas técnicas, y de apoyo en las mismas condiciones que las requeridas para las zonas anteriormente indicadas.

Con el fin de proporcionar una iluminación adecuada las luminarias cumplirán las siguientes condiciones:

1) se situarán al menos a 2 m por encima del nivel del suelo

2) se dispondrá una en cada puerta de salida y en posiciones en las que sea necesario destacar un peligro potencial o el emplazamiento de un equipo de seguridad. Como mínimo se dispondrán en los siguientes puntos:

    a. en las puertas existentes en los recorridos de evacuación

    b. en las escaleras, de modo que cada tramo de escaleras reciba iluminación directa

    c. en cualquier otro cambio de nivel

    d. en los cambios de dirección y en las intersecciones de pasillos

Se iluminará con al menos 5 lux el eje de los pasillos de evacuación y se dispondrá de al menos 10 lux en todas las áreas técnicas y que contengan elementos de seguridad contraincendios.

La iluminación normal y de emergencia del edificio se presenta en la imagen siguiente.

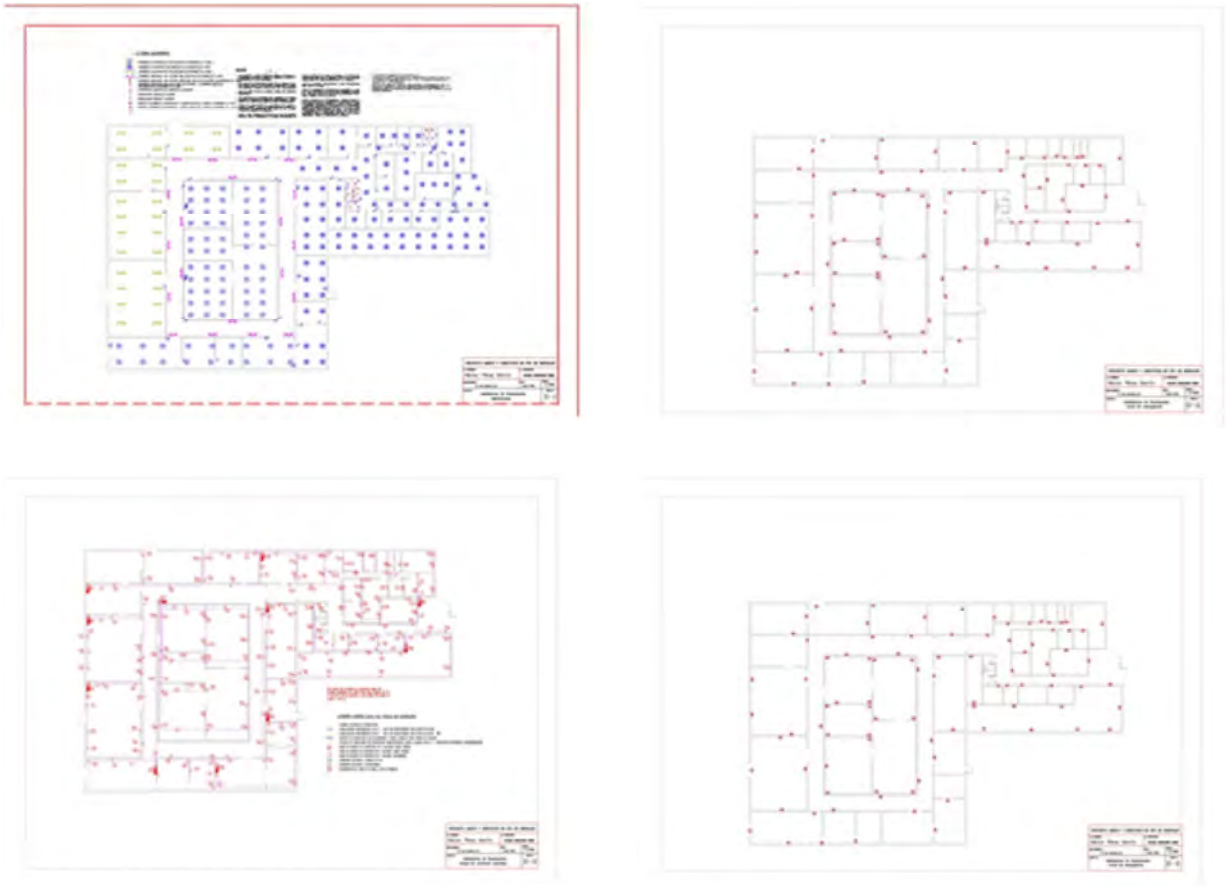


Figura 33.- Cálculos y mediciones de las instalaciones e iluminación

4 SOLUCIÓN PROPUESTA - INFRAESTRUCTURA INFORMÁTICA Y DE COMUNICACIONES

En este capítulo se describen los sistemas TIC propiamente dichos que satisfacen la norma TIA 942, así como el dimensionado de los elementos de hardware y servidores.

En primer lugar en el apartado 4.1 se revisan las aplicaciones a respaldar, y conjuntamente con la priorización vista anteriormente, se proponen mecanismos de consolidación para optimizar la utilización de los recursos del centro.

Seguidamente en el apartado 4.2 se revisan las necesidades de hardware para dar servicio a las aplicaciones, así como las estrategias para simplificar el almacenamiento.

Una vez determinadas las demandas de capacidad, se procede en el apartado 4.3 a diseñar el centro de respaldo a nivel de redes, tanto desde el punto de vista de las redes internas como de la conectividad con el backbone, con el centro principal y proveedores.

En el apartado 4.4 se detallan las redes y sus a nivel físico, detallando las guías generales para la implantación de la red, así como los elementos principales que la norma TIA 942 exige en el diseño físico de la red.

4.1 Nivel de aplicación

A este nivel se describen los mecanismos de copia de seguridad y respaldo a nivel de aplicación, en función de la criticidad de estas. Así se ha definido la estrategia de respaldo a seguir (Activo-Activo, Activo-Pasivo). La solución contiene una mezcla de estrategias, en función de la criticidad y nivel de transacciones de las distintas aplicaciones. Estas estrategias permiten dimensionar el enlace entre el centro principal y el centro de respaldo.

En cuanto a las necesidades de funcionamiento del CPD de respaldo se han considerado que hace falta que sean de dos tipos:

- Activo / Pasivo (Réplica de datos offline). El Respaldo entra en funcionamiento cuando cae el principal. Normalmente existirá una pérdida de datos que dependerá del tiempo objetivo de recuperación (RTO), establecido para el Sistema en concreto.
- Activo / Activo (Réplica de datos en tiempo real). El Centro de respaldo (o CPD alternativo) está continuamente en funcionamiento y actuando con los mismos datos que el Sistema en operación. De modo que el fallo de uno de ellos no es determinante toda vez que el alternativo sigue trabajando y cuando se produce la recuperación del que ha fallado basta con una sincronización de los datos para mantener los dos sistemas actualizados.

Para la selección del tipo de respaldo a cada sistema se han priorizado los sistemas según el documento del Anexo B - Censo y priorización de aplicaciones, considerando las siguientes prioridades para el respaldo, dependiendo del nivel de criticidad de dichos sistemas:

Cada nivel de criticidad va asociado unívocamente con el correspondiente nivel de prioridad, así sólo se han descrito las prioridades, ya que constituyen el resultado del análisis de los sistemas y son la base para su respaldo.
De acuerdo con lo descrito en el apartado 2.4.4 Necesidad de respaldo por criticidad, las aplicaciones se clasificaron por prioridad. Para cada priorización, se definen los objetivos de recuperación, que influyen en la definición y dimensionamiento del centro.

Para cada nivel de criticidad se fija un tiempo máximo correspondiente al RPO (Recovery Point Objective): antigüedad de los datos con los que se quiere ser capaz de recuperar un sistema en el caso de un desastre. Por ejemplo, si el RPO es de 4 horas, se pretende ser capaz de restaurar el sistema hasta un estado nunca anterior a 4 horas.

De acuerdo con estos criterios, los niveles o perfiles fijados son los mostrados en la tabla:

Criticidad	**RPO**	**RTO**
Muy Alta	30 segundos a 10 minutos (Copia remota por un periodo nunca superior a 10 minutos)	Menor de 1 hora (Recuperación del servicio con un tiempo máximo de 1 hora)
Alta	4 horas (Copia remota por un periodo nunca superior a cuatro 4 horas)	24 horas (Recuperación del servicio con un tiempo máximo de 24 horas)
Media	12 horas (Copia remota por un periodo nunca superior a doce horas)	48 horas (Recuperación del servicio con un tiempo máximo de 48 horas)
Baja	24 horas (Copia remota por un periodo nunca superior a veinticuatro horas)	7 días (Recuperación del servicio con un tiempo máximo de cuarenta y ocho horas)

Tabla 16 Objetivos de recuperación por prioridad de la aplicación

En el Anexo B - Censo y priorización de aplicaciones se contienen los sistemas y aplicaciones a respaldar de la empresa y que deberán ser soportados por el Centro de Respaldo.

En lo respectivo a la red corporativa, se mantendrá un nivel de conectividad equivalente al descrito en el apartado 2.3 Estructura geográfica de la empresa, servicios y conexión de centros para el centro principal (ver Figura 9 Red WAN de ZEREPSA y conexión del centro principal). Igualmente se dispondrá de un enlace directo entre los dos centros.

4.1.1 Consolidación

Tras el análisis de aplicaciones y la priorización de estas, nos encontramos con la posibilidad de consolidar aplicaciones. La consolidación consiste en agrupar múltiples aplicaciones en unas pocas plataformas, mucho más potentes, utilizando típicamente particionamiento (lógico, físico, y software) y gestión de cargas [***39***] [***39***].
Si bien este proceso se ha llevado a cabo en el centro principal y es la tendencia a la hora de introducir nuevas aplicaciones, el centro de respaldo añade un nuevo nivel de consolidación de aplicaciones. A este fin, se consolidarán aquellas aplicaciones de

criticidad baja que no estén consolidadas en el centro principal.

Los mecanismos de particionamiento que dan lugar a la consolidación son los siguientes [***40***] [***40***]:

1. **Particionamiento Hardware**: En particionamiento hardware, cada partición tiene uno o más procesadores, bloques de memoria y entrada/salida aisladas eléctricamente entre cada una de ellas, para que un fallo en una de ellas no afecte a ninguna de las otras. Se asignan los recursos a las particiones o dominios con la granularidad de los componentes físicos.
2. **Particionamiento Lógico**: El particionamiento lógico típicamente utiliza una capa de micro código hardware o firmware (algunas veces software) para controlar las particiones y permitir granularidad de los recursos (procesador, memoria y entrada/salida) que pueden ser asignados en porciones más pequeñas que los bloques físicos.
3. **Particionamiento Software**: El particionamiento software se implementa utilizando una capa de software que controla el hardware y asigna los recursos a particiones. Permite que la granularidad sea también más pequeña que los propios componentes físicos. Este tipo de software, el sistema operativo host se ejecuta en el servidor físico y permite ejecutar múltiples sistemas operativos "invitados" ejecutándose como máquinas virtuales.

En el centro principal se aplican mecanismos de particionamiento software mediante virtualización usando el producto VMWare. Para mejorar la utilización de los recursos en el centro de respaldo, se aplicará también virtualización en los mainframes, mediante el producto IBM PowerVM para el entorno Host y HP Virtual Server Environment OE (VSE-OE) [***41***] [***41***] para e entorno Superdome. De este modo, se aumentará la carga de trabajo sobre el mainframe en el centro de respaldo, optimizando el uso de este recurso.

De este modo, se determina la estrategia de consolidación de las aplicaciones, con los siguientes niveles:

- Las aplicaciones de prioridad muy alta no se consolidarán, **manteniendo** su entorno exacto del centro principal.
- Se **virtualizarán en los entornos Superdome y Host** exclusivamente las aplicaciones ya virtualizadas en el centro principal y que no sean de alta prioridad.
- Las aplicaciones ya virtualizadas y que sean de prioridad media o baja, **compartirán recursos**, de forma que no se exigirá una réplica exacta del entorno. El factor de reducción se identifica basado en las mediciones del centro principal, estimado entre un 10% y un 30%.
- Se identifican algunas aplicaciones viables para **virtualización** completa. En estos casos el dimensionado será basado en los recursos consumidos en el centro principal en régimen normal, aplicando reducciones entre un 30% y un 60%.
- Finalmente las aplicaciones que no entran en ninguno de los casos arriba mencionados **mantendrán** su entorno exacto.

En el Anexo C - Estrategia de consolidación de aplicaciones se listan las aplicaciones a ser respaldadas junto con su estrategia de consolidación asignada y el porcentaje de reducción identificado. En la siguiente tabla se presenta un resumen de la consolidación, y el factor de reducción alcanzado:

Prioridad	Acción	Aplicaciones	Factor de reducción
Muy Alta	Mantener	96	0%
Alta		64	2%
	Compartir recursos	1	40%
	Mantener	61	0%
	Virtualizar	2	53%
Media		61	29%
	Compartir recursos	8	25%
	Mantener	30	0%
	Virtualizar	13	43%
	Virtualizar en Host	4	100%
	Virtualizar en Superdome	6	100%
Baja		29	31%
	Compartir recursos	7	28%
	Mantener	14	0%
	Virtualizar	2	53%
	Virtualizar en Host	5	100%
	Virtualizar en Superdome	1	100%
Total general		**250**	**11%**

Tabla 17 Resumen de las acciones de consolidación

4.2 Servidores

Los equipos serán, en su práctica mayoría, una réplica de los servidores existentes en el centro principal. Sin embargo, y consecuencia directa de la estrategias de consolidación, el centro secundario no será una réplica exacta del centro principal, ya que se reduce la cantidad de servidores físicos necesarios.

Con la clasificación del Anexo C - Estrategia de consolidación de aplicaciones, y comparando con la infraestructura de hardware necesario con el del centro principal, los elementos necesarios para el centro de respaldo se resumen en la siguiente tabla.

Entorno	Elementos centro de respaldo	Elementos centro principal
Host	2 IBM z900	2 IBM z900
HP-UX	5 servidores HP ProLiant DL, ocupando 1 rack 9 servidores Integrity, ocupando 2 racks	8 servidores HP ProLiant DL, ocupando 1 rack 10 servidores Integrity, ocupando 2 racks
SUN Solaris	2 racks SunFire 69000 5 racks con 4 servidores SunFire X42000 cada uno	2 racks SunFire 69000 6 racks con 4 servidores SunFire X4200 cada uno
Windows/Linux	16 servidores HP ProLiant	18 servidores HP ProLiant DL,

	DL, ocupando 10 racks	ocupando 12 racks
Bases de Datos	25 servidores HP ProLiant DL, ocupando 5 racks	25 servidores HP ProLiant DL, ocupando 5 racks
Superdome	1 SX3000 (2 racks) con 128 núcleos, de los cuales están asignados 98, y 8 módulos de I/O.	1 SX3000 (2 racks) con 128 núcleos, de los cuales están asignados 64, y 8 módulos de I/O.
Servidores Blades	5 racks; cada rack está configurado por 4 bloques c7000, teniendo cada uno 16 blades HP ProLiant BL	6 racks; cada rack está configurado por 4 bloques c7000, teniendo cada uno 16 blades HP ProLiant BL
Otros servidores	4 racks albergando diferentes servidores legacy	4 racks albergando diferentes servidores legacy
DMZ	14 racks de servidores HP ProLiant DL, con 8 servidores por rack, hasta un total de 128 servidores, además de 4 racks para los elementos de red y firewalls	16 racks de servidores HP ProLiant DL, con 8 servidores por rack, hasta un total de 128 servidores, además de 4 racks para los elementos de red y firewalls

Tabla 18 Equipos de hardware para los servidores tras la consolidación

Además de estos elementos, se respaldará el equipamiento de:

- Sistemas
- Redes
- Comunicaciones-telefonía
- Nodo int-net
- Supervisión y control
- Almacenamiento

4.2.1 Servidores de datos (BBDD y almacenamiento)

La solución propuesta consiste en un pool de servidores de datos (almacenamiento SAN), en vez de agrupar el almacenamiento por aplicaciones. A excepción, claro está de aquellos sistemas distribuidos cuyo sistema de almacenamiento también lo sea. De este modo se simplifica el almacenamiento y la copia de seguridad.

En el centro de respaldo el almacenamiento de datos se centraliza en un pool de servidores de datos, en lugar de utilizar múltiples mecanismos de almacenamiento. Esta es una tendencia del centro principal, pero no está desarrollada completamente. La utilización de esta distribución simplifica la copia de seguridad y aumenta la escalabilidad del almacenamiento.
En lo tocante a los sistemas de almacenamiento, existen dos tecnologías coexistiendo en el centro principal.

4.2.1.1 NAS (Network-Attached Storage)

En una arquitectura NAS se utilizan dispositivos de almacenamiento conectados directamente a una red LAN TCP/IP, de manera que los datos son accesibles desde cualquier equipo conectado a la red.

Por lo general, los dispositivos de almacenamiento son armarios de discos externos con procesadores dedicados o librerías de cintas. Al utilizar procesadores especializados para el acceso al almacenamiento, tienen un alto rendimiento frente al almacenamiento por bloques.

NAS contempla la necesidad de acceso y compartición de los mismos ficheros por aplicaciones con clientes heterogéneos. Algunas de las soluciones NAS tienen la capacidad de mantener los permisos entre diferentes plataformas, consiguiendo por ejemplo, que clientes Windows puedan acceder a ficheros basados en Solaris y viceversa.

Las tecnologías de soporte a la transmisión y almacenamiento de datos la arquitectura NAS son:

- Ultra SCSI. Es una variedad de SCSI (Small Computer System Interface), estándar de interfaz paralelo para la conexión de periféricos. Ultra SCSI usa un bus de 8 bits y consigue hasta 20Mbps.
- Fibre Channel (FC). Es una arquitectura de transferencia en serie de datos. El estándar más destacado de FC es Fibre Channel Arbitrated Loop (FC-AL), FC-AL usa fibra óptica para conectar dispositivos y alcanza tasa de transferencia full-dúplex de 100Mbps.
- ESCON (Enterprise Systems Connection Architecture) para mainframe.

En el centro principal existen sistemas utilizando esta tecnología, si bien la tendencia es a utilizar almacenamiento SAN. Para el centro de respaldo, todo el almacenamiento será basado en tecnología SAN.

4.2.1.2 SAN (Storage Area Network)

Una SAN es una red de alta velocidad compuesta por dispositivos de almacenamiento compartidos, que son accesibles por todos los servidores conectados a la misma LAN que la SAN.

Este tipo de solución se basa en una serie de principios, que se basan en la centralización del almacenamiento en una infraestructura específica y la descarga del tráfico de la red a una red específica de almacenamiento. Estos sistemas también presentan como ventaja la posibilidad de realizar terceras copias y backup instantáneo.

El objetivo de esta arquitectura es mejorar la gestión del almacenamiento a través del uso de hardware y software que minimice el impacto operacional del aumento de las capacidades de almacenamiento. Esta solución, al proponer que los datos no residan en los servidores sino en una red específica, provoca que la potencia de éstos se aproveche al máximo para las aplicaciones de negocio, descargando las tareas de acceso a datos en la SAN. Algunos fabricantes de SAN implementan un sistema NAS añadiendo un módulo gestor adicional conectado directamente a la red.

También se ha hecho necesario definir un respaldo para los sistemas distribuidos cuya forma de almacenamiento, a su vez sea distribuida entre los distintos centros, áreas o zonas de la empresa.

Como se ha descrito en el capítulo anterior, la empresa dispone de aplicaciones que

almacenan datos distribuidos entre las distintas sedes y Áreas o Zonas de Actuación, y que se sincronizan de forma intermitente con el centro principal y entre sí. A fin de dotar de redundancia a estas aplicaciones el centro de respaldo se diseña para:

- Respaldar los datos del centro principal
- Replicar al centro principal en caso de caída, de forma que las bases de datos distribuidas se sincronicen contra el centro de respaldo de forma transparente en caso de caída del centro principal.

En cuanto al mecanismo de respaldo de las Bases de Datos locales se desarrolla un procedimiento que se distribuye a todas las sedes y zonas de modo que las aplicaciones de carácter distribuido tengan previsto un mecanismo de respaldo local, y que sean tolerantes a errores de sincronización con el centro principal o entre los distintos elementos.

El hardware necesario para SAN y para bases de datos se resume en la siguiente tabla.

Entorno	**Elementos centro de respaldo**
SAN - Controladores de la red	1 rack para el director SAN Cisco MDS 9700 1 rack para el controlador de volúmenes IBM 1 rack para los controladores de fiber channel con 4 controladores.
SAN - Almacenamiento	4 racks HP EVA 6100 8 racks IBM DS8000
SAN - Librerías de cintas	2 racks IBM Virtualization Engine TS7520, para emular librerías de cintas
Bases de Datos	25 servidores HP ProLiant DL, ocupando 5 racks

Tabla 19 Equipos de hardware para BBDD y SAN del centro de respaldo

4.2.1.3 Requisitos de conectividad y de ancho de banda

Para los equipos residentes en la DMZ, se utiliza un firewall a nivel de SAN, de forma que se acceda a la misma red de almacenamiento pero de forma segura. Para aquellos casos en que esto no ha sido posible, se ha implementado otra red SAN separada de la principal para los datos de la DMZ, de forma que esos datos queden aislados de los datos internos.

En cuanto a los routers y firewalls que tienen acceso a datos se efectúan backups de sus datos que, a su vez se almacenan utilizando los sistemas SAN de tipo general o de la DMZ, según sea el caso y tal como se muestra en el diagrama de la estructura de almacenamiento del centro de respaldo.

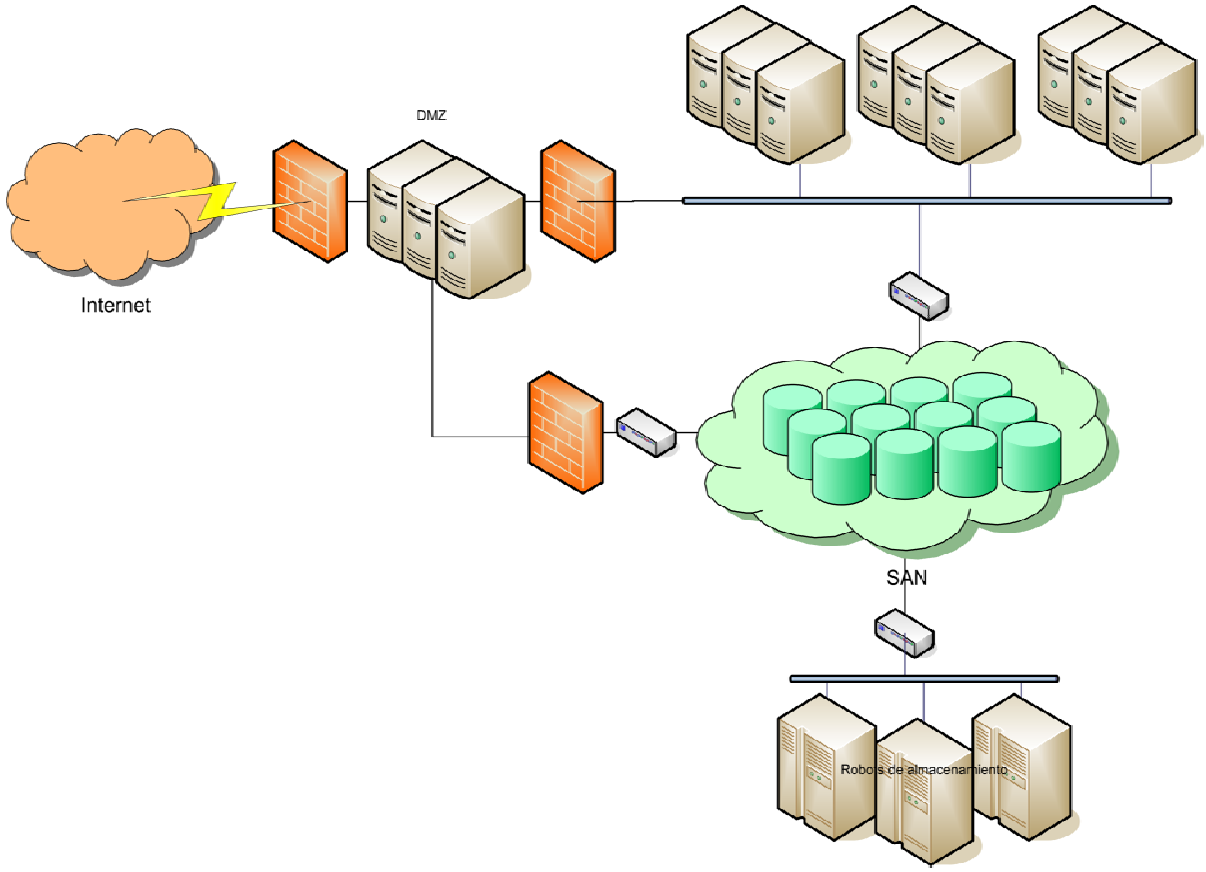


Figura 34 Diagrama de situación de la red SAN en el centro

4.2.2 Servidores de back-ups

Estos servidores, que sirven como histórico de datos, son exclusivos del centro de respaldo (el centro principal tendrá sólo un 30% de los históricos). Consisten principalmente de robots de cintas y equipos similares de almacenamiento masivo. Además de los servidores en sí, se plantea una solución para albergar las cintas históricas durante un cierto tiempo una vez se han retirado de los robots.

El centro de respaldo dispone de un grupo de robots de cintas que permiten almacenar históricos de datos, tanto de back-ups como aquellos registros requeridos legalmente. Hay que notar que esta será una característica del centro de respaldo de la que carece el centro principal, que almacenará un número limitado de histórico de datos.

Dado que se ha elegido utilizar una arquitectura SAN para el almacenamiento, los robots de cintas estarán conectados a esta red y realizarán copias en caliente.

En cuanto al almacenamiento físico de las cintas (almacén de datos) la condición que se ha exigido es que debe tratarse de un lugar seguro, limpio (no tanto como la sala limpia), con volumen suficiente para albergar las cintas.

Por otro lado se ha dispuesto de una zona para la destrucción de datos y reutilización de cintas.

También se ha dispuesto de una zona para la recuperación de datos que se hallen en soportes obsoletos o tratados con sistemas ya obsoletos. En dicho lugar se mantienen los sistemas obsoletos con la finalidad de recuperar dichos datos.

4.3 Nivel de red

En el nivel de red se mantendrá el esquema de conectividad general de la empresa replicado para este centro, tanto en canales como de servicios. Para la red interna del Centro de Respaldo que es lo que más afectará al proyecto, se seguirá lo establecido en la norma TIA 942 que se resume en el esquema siguiente [***1***].

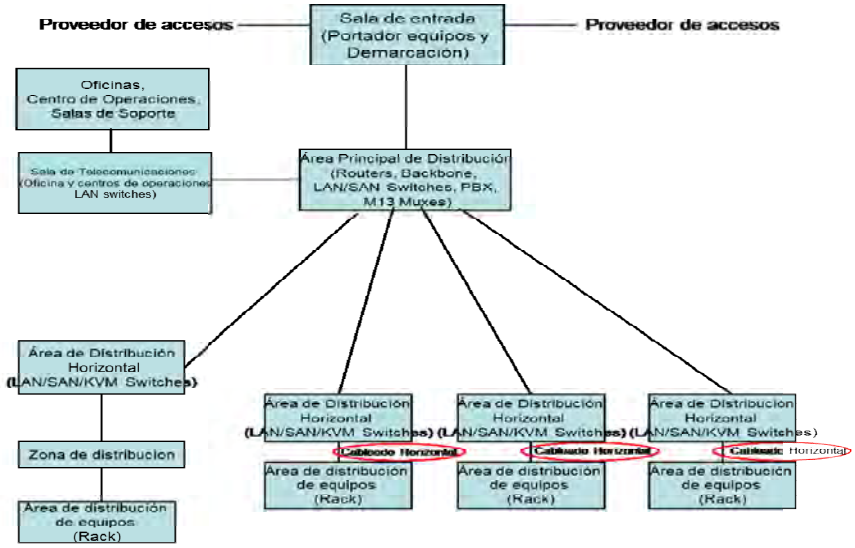


Figura 35 Elementos de red definidos en la norma TIA942

4.3.1 Red interna

Las redes que componen el Centro de respaldo seguirán las siguientes especificaciones generales:

- Existirá una única Red de Área Local de propósito general. Si bien podrá subdividirse en varios segmentos, en función de las características físicas del emplazamiento.
- Esta LAN de Propósito General dispondrá de un único punto de acceso externo.
- Por otro lado en la sala técnica y dentro de la subred de almacenamiento y back-up se consideran dos subredes distintas:
    - Por un lado la subred de almacenamiento del sistema MAIN-FRAME, que controla el almacenamiento y recuperación de los Sistemas informáticos que se ejecutan en dicho sistema.
    - Por otro lado la subred de almacenamiento (SAN) de los distintos sistemas informáticos, distintos de los que funcionan en el Mainframe.

La arquitectura adoptada en el CPD es una arquitectura en niveles, donde cada nivel cumple una función determinada.

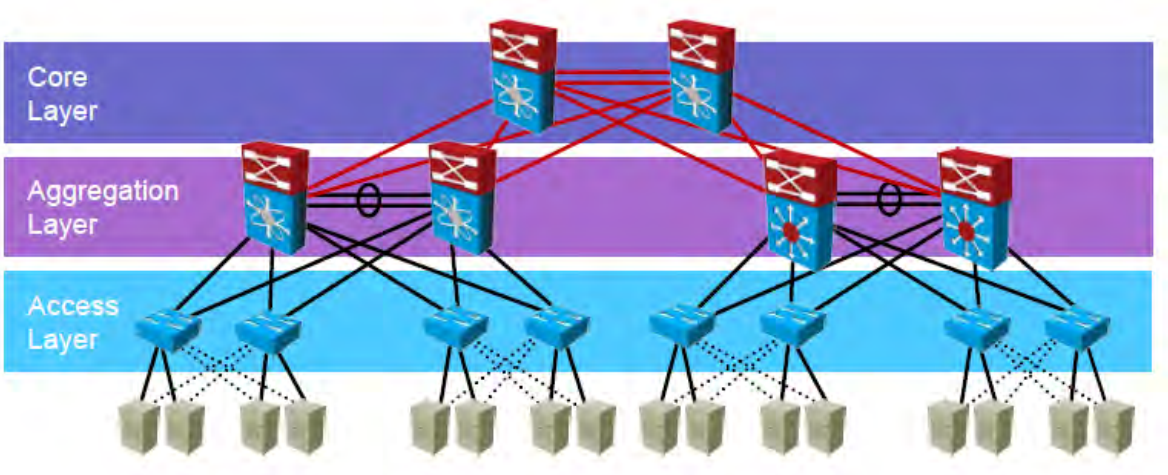


Figura 36 Estructura de red en capas *[**40**]*

- Nivel core del CPD e interconexión con la red corporativa
- Nivel de agregación
- Nivel de acceso

Para el diseño de la topología red se tendrán en cuenta consideraciones de consolidación y virtualización de infraestructura, obteniendo una mayor densidad de servicio, que conlleva [***40***]:

- Menor consumo de energía
- Menor espacio ocupado
- Reducción en puertos y cableado
- Simplificación de la operación
- Menores costes de mantenimiento

4.3.1.1 Zonificación lógica de redes

La zonificación lógica de las redes que compondrán el Centro de Respaldo responde a la estructura de redes del centro principal, y está compuesta por:

1. Red de Sistemas medios que contendrá los servidores, equipamiento y todo el personal, equipos de trabajo y medios auxiliares (impresoras, dispositivos móviles, etc.) que sirven a este concepto y el almacenamiento asociado Esta red contemplará los sistemas de correo y de recuperación lógica de datos así como los elementos de desmagnetización. De igual modo corresponden a esta red los equipos y elementos que se disponen en la zona de preinstalación o staging.
2. Red de HOST. Igualmente contendrá el Servidor HOST IBM con sus sistemas y servicios y a todo el personal que presta servicio al HOST con sus puestos de trabajo respectivos (PCs, impresoras, dispositivos móviles).
3. Red de almacenamiento. Se trata de una red que dará servicios a TODOS los sistemas del centro y por lo tanto contendrá bridges que la conectarán con TODAS las redes del centro. A través de esos puentes se efectuará la transmisión de los datos para el almacenamiento, bien sea directamente para los servicios de almacenaje de información directos de operación y trabajo de los sistemas como para los servicios de Back-up y recuperación de información.
4. Red de Internet-Intranet. Contendrá todos los servidores y equipamiento que da

el servicio de internet y de intranet y a todos los puestos de trabajo del personal que se dedican a su funcionamiento al igual que las otras redes mantendrá una conexión con la red de almacenamiento.

5. Red de Telefonía y de Comunicaciones. Contendrá los servidores que se utilizan para las aplicaciones de telefonía y las centrales de interconexión así como los elementos de los puntos neutros y de accesos de operadores. De igual modo contendrá todo el equipamiento de red (switches y servidores de acceso y control de red, como son DNS, etc.). Al igual que el resto contendrá los puestos de trabajo del personal de telefonía y el puente de conexión con la red de almacenamiento.
6. Red de monitorización, control y operación del centro. Esta red contendrá todos los equipos de monitorización y control que se consideran.
    a. Contendrá los sistemas de monitorización y control de los parámetros técnicos de funcionamiento de la sala técnica principal (humedad, temperatura de equipos particulares, distribución de temperatura de la sala, flujos de refrigeración, partículas en suspensión, suministro de energía a los equipos, estabilidad de tierras y equilibrio de cargas). Estos sistemas contemplan tanto a los sistemas propios de servidores de aplicaciones, de ficheros y su puente al almacenamiento así como los puestos de trabajo del personal que los atiende.
    b. Contendrá los sistemas de monitorización y control de funcionamiento de aplicaciones.
    c. Contendrá los sistemas de monitorización y control de los servicios de RED que se presten desde el centro contemplando.
7. Red de recepción de equipos, sistemas-PRUEBAS. Similarmente a la red de almacenamiento, esta red dispondrá de bridges para su conexión con otras redes del centro como son (SSMM, Host, Monitorización y control, Almacenamiento, Mantenimiento, etc.).
8. Red de infraestructuras y mantenimiento. Esta red estará conformada por los sistemas de energía, contraincendios, mantenimiento, almacenamiento refrigeración y Aire acondicionado. Por consiguiente estarán conectados a esta red los equipos servidores tanto de aplicaciones como de ficheros y los equipos de medición y control de los citados sistemas así como los puestos de trabajo del personal que da servicio a los mismos.
9. Red de propósito general y de gestión. A esta red pertenecerá todo el personal (sus puestos de trabajo y equipamiento asociado – impresoras, video conferencia, etc.) que trabaja en el centro y su actividad es fundamentalmente de soporte al resto de actividades que se consideran principales. Al igual que el resto de redes dispondrá de su bridge para interconectarse con la red de almacenamiento.

4.3.1.2 Direccionamiento

La red interna utilizará direccionamiento IPv4, pero los equipos deben poseer capacidades para evolución a IPv6. En el diseño del direccionamiento se considerarán las siguientes guías generales, comunes para los dos protocolos [***40***]:

- Se considerarán los rangos de IP públicas correspondientes a los servicios de intranet y extranet.
- Se utilizará una subred para separación completa de la red de gestión, que puede a su vez separarse en subredes específicas, por ejemplo, por las características de los elementos a ser gestionados.
- El plan de direccionamiento debe aproximarse a la estructura de nivel físico; se debe utilizar conceptos de "Network summarization" para facilitar el encaminamiento simplificando la complexidad de tablas de encaminamiento.
- Se definirán rangos separados para subredes de servidores, e igualmente rangos separados para subredes de enlace y para VLANs.
- Los rangos IPv4 deben corresponder con los rangos IPv6 para simplificar el diseño de red.

4.3.1.3 Encaminamiento

El protocolo de encaminamiento interior será único y homogéneo para todo el centro. Para mantener la correspondencia con el centro principal será utilizado EIGRP (Enhanced Interior Gateway Routing Protocol). Para la configuración del protocolo se seguirán las siguientes guías generales [***40***]:

- Utilizar un protocolo que ofrezca convergencia rápida.
- Aprovechar segmentación de redes y sumarización (para unificar segmentos adyacentes).
- Se debe permitir intervalos configurables de descubrimiento para ajustar el algoritmo Shortest Path First para protocolos de estado del enlace.
- Soporte de autenticación para identificar los extremos de los enlaces.
- Usar protocolo que permita aplicar IPv6 para mantener compatibilidad futura.
- Los firewalls deben soportar la configuración del protocolo escogido.

Adicionalmente, se utilizarán protocolos de alta disponibilidad a nivel IP, conocidos como First Hop Redundancy Protocols (FHRPs); en particular se utilizará Virtual Router Redundancy Protocol (VRRP), definido en la RFC 5798 del IETF [***41***], si bien existen otros protocolos propietarios similares (HRSP, Hot Standby Router Protocol y GLBP, Gateway Load Balancing Protocol).

Conforme dicho anteriormente, se utilizarán además protocolos de estado de enlace del tipo Spanning Tree. Estos protocolos aumentan la escalabilidad y permiten mejorar el rendimiento manteniendo activos los enlaces que, en caso de utilizar el protocolo spanning tree estarían inactivos. Son:

- Rapid Per VLAN Spanning Tree Plus (Rapid PVST+)
- Multiple Spanning Tree (MST)

Escogeremos MST ya que es un algoritmo con mayor capacidad de escalado.

Estos protocolos se apoyan en las tecnologías de encaminamiento múltiple (multipathing) [***40***]. Estas tecnologías virtualizan los enlaces, de modo que se pueden agrupar múltiplos enlaces físicos en un único enlace lógico. Ejemplos de estas

tecnologías son el estándar IEEE 802.3ad, EtherChannel (Cisco), Multi-Link Trunking (Avaya) o Ethernet Virtual Interconnect (HP) [***42***].

4.3.1.4 Virtualización de redes

El centro utilizará virtualización de redes, específicamente estableciendo VLANs [***40***]. Una VLAN es una virtualización de un segmento de nivel 2 de red, independiente de la capa física. Esta virtualización permite la conexión de dos servidores en un mismo switch físico, aunque participen de diferentes dominios de broadcast (diferentes VLANs). Además, la virtualización de redes mejora la fiabilidad del sistema, permitiendo la reconfiguración dinámica de la red. La implementación de VLANs a nivel de enlace será conforme a lo definido en el estándar IEEE 802.1Q [***43***].

En adición a los elementos de virtualización, se utilizarán protocolos adicionales:

- Se utilizará Data Center Bridging para conseguir interconexión a los elementos SAN que utilizan Fibre Channel, siguiendo los protocolos:
  - Priority-based Flow Control, PFC - IEEE 802.11Qbb
  - Enhanced Transmission Selection, ETS - IEEE 802.1Qaz
  - Congestion Notification - IEEE 802.1Qau
  - Data Center Bridging Capabilities Exchange Protocol, DCBX - IEEE 802.1AB
- Para los servidores blades y servidores de virtualización, ya que poseen un switch o softswitch intermedio, se utilizará Edge Virtual Bridging, conforme definido en el estándar 802.1Qbg. Este mecanismo permite a un switch principal crear una asociación con el switch intermedio, convirtiéndose este en la ruta para los datos de las máquinas virtuales subyacentes. Este protocolo también es conocido como NIV (Network Interface Virtualization) [***40***].
- Para la configuración de VLANs y su distribución y mantenimiento en todos los elementos de encaminamiento de la red, se utilizará el protocolo Multiple VLAN Registration Protocol, MVRP, también definido en el estándar 802.1Q.

4.3.1.5 Red de almacenamiento

Para el centro de respaldo por tanto se opta por una solución SAN, con posibilidad de incorporar un módulo NAS si es estrictamente necesario.
La red de almacenamiento SAN será un segmento gestionado separadamente del resto de elementos de la red. Conforme dicho anteriormente, se utilizará FCoE para encapsular las tramas de FiberChannel sobre Ethernet.

Esta solución permite también la definición de segmentos SAN virtuales (VSAN), similares al concepto de VLAN. Estos segmentos serán utilizados para facilitar la gestión de la red, y para consolidar y simplificar la infraestructura necesaria, apoyando así los esfuerzos de consolidación y virtualización a nivel de respaldo de aplicaciones descritos en el apartado 4.1.1 Consolidación. Tras la consolidación de los sistemas en el CPD de respaldo, aún cuando se mantienen replicados la diversidad de servidores que existen en el CPD principal, la red de almacenamiento se ve simplificada.

4.3.2 Conexión con centro principal

Existen varias alternativas para la interconexión de los dos centros de datos a nivel de red [***40***]:

- Interconexión a nivel IP:
  - Una única ruta, utilizando encaminamiento tradicional.
  - Conexión a nivel IP con separación de rutas, utilizando segmentos separados que conectan en paralelo (p.ej. aplicaciones, base de datos, gestión almacenamiento).
- Interconexión a nivel 2, utilizando VLANs

En nuestro caso, usaremos interconexión a nivel IP, con una única ruta, ya que al disponer de un ancho de banda de alta velocidad, no se hace necesario la encapsulación de datos o la utilización de protocolos complejos para la transmisión de datos. De esta manera, la simplificación y la utilización de una electrónica de última generación permiten la transmisión de los datos en su formato original a lo que se denomina "velocidad de cable".

La conexión del centro de respaldo con el principal se efectúa mediante dos elementos:

- Conexión directa de fibra óptica de 10Gb, utilizando dos conexiones dedicadas con separación física de caminos para redundancia. Cada una de las conexiones se constituye mediante dos fibras ópticas monomodo con terminación en interface 10GBASE según la norma IEEE 802.3ae con conector SC/PC.
- En caso de que la conexión directa no esté disponible, se encaminará el tráfico a través de la red MAN (caudal estimado 8Gbps), utilizando mecanismos de routing dinámico, obteniendo así una capa mayor de redundancia.

El esquema de conexiones se puede reducir al de la figura, que corresponde con la Figura 9 del apartado 2.3, con la conexión directa al centro principal entrando en la capa de agregación (línea verde sólida) y la ruta alternativa a través de la MAN (línea verde a trazos).

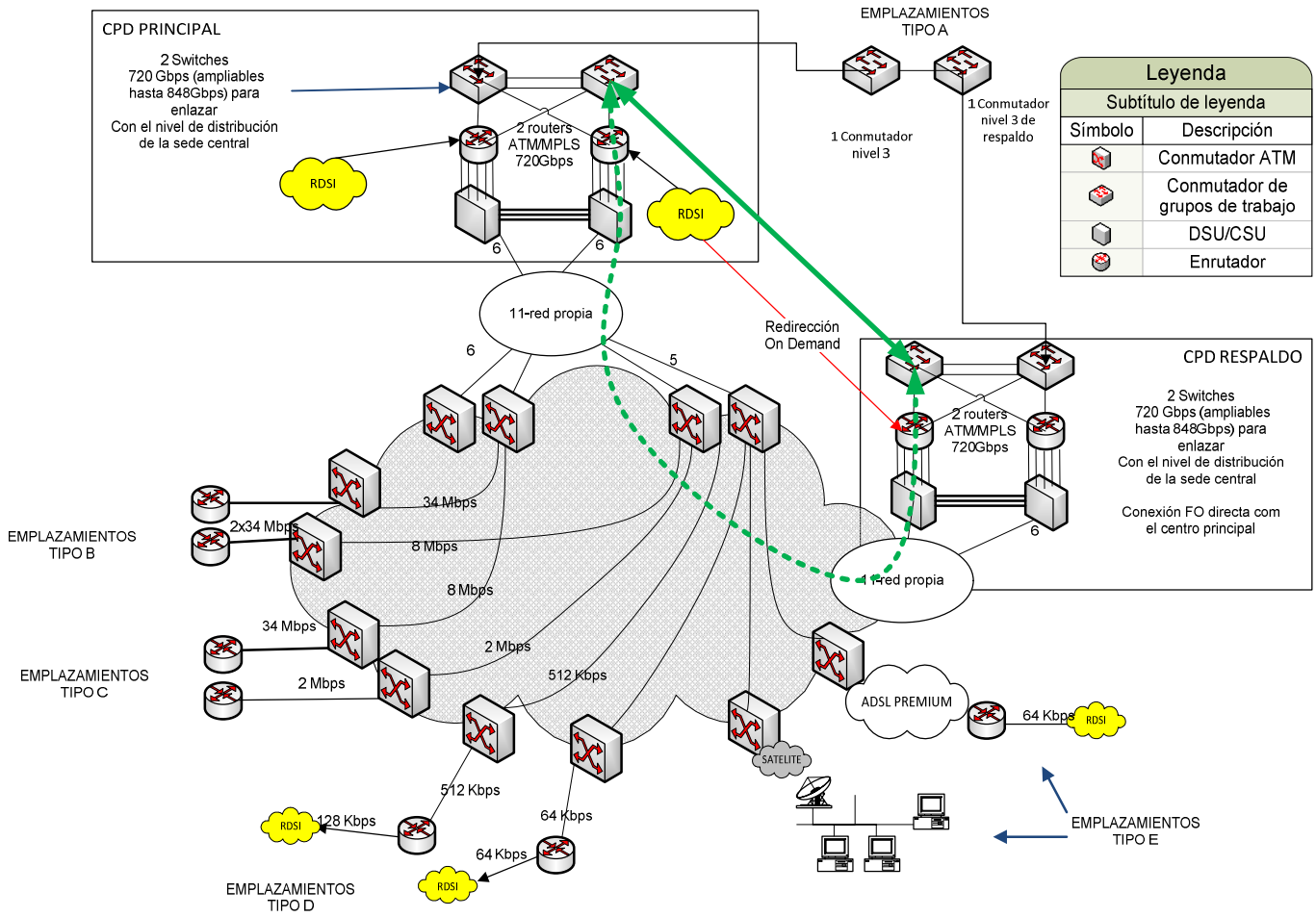


Figura 37 Red WAN de ZEREPSA incluyendo al centro de respaldo

Existirá una red virtual única que será réplica de la existente en el centro principal tanto para el acceso a los datos del CPD desde el CPD principal y otra red de interconexión con las sedes de la empresa y las zonas de operación así como el acceso de los medios y vehículos de la empresa. todo ello será replica de la red que ya está conformada y que se controla desde el centro principal, de acuerdo con la arquitectura ya expresada en la Figura 9 del capítulo 2.3 Estructura geográfica de la empresa, servicios y conexión de centros.

4.3.3 Conexión con el backbone y otros centros

Conforme representado en la mencionada Figura 9, el backbone MAN de ZEREPSA es formado por una red IP basada en MPLS, permitiendo la conectividad "Todos con todos", y utilizando VPNs basadas en MPLS.

La conectividad es IP sobre Ethernet, con los siguientes elementos de configuración:

- Circuito de Acceso con velocidad 10Gbps. Este circuito une el Equipo en Domicilio de Cliente (EDC) con el nodo de acceso más cercano de la MAN. En el caso del centro de respaldo, así como para el principal, habrá dos circuitos y dos EDCs para redundancia en cada uno.
- Caudal, previsto 8Gbps (80% del centro principal).

- VLANs configuradas para acceder a los diferentes centros, con configuración idéntica al del centro principal.

Durante el modelo normal, todos los nodos estarán activos, y el tráfico se cursará siempre por el centro principal, marcando con una métrica peor los nodos del centro de respaldo. En caso de caída del centro principal, los protocolos de encaminamiento dinámico automáticamente identificaran la caída del centro principal, marcando ese nodo como con peor métrica que los del centro de respaldo, y el tráfico entonces se dirigirá al centro de respaldo.

Este mecanismo es suficiente para dar respaldo a todos los accesos desde las delegaciones descritos en el apartado 2.3 Estructura geográfica de la empresa, servicios y conexión de centros.

4.3.4 Conexión con proveedores. Salas de enlace

Habida cuenta que el sistema de comunicaciones de la empresa dispone de un variado conjunto de puntos con diferentes formatos de conexión y con distintos tipos de las mismas, se ha dispuesto que la conexión lógica al exterior se realiza a través de un único punto de salida y que se describirá en el apartado siguiente.

Según las recomendaciones de la ANSI-TIA 942, para un centro de comunicaciones de nivel 3 o superior, el centro tiene que estar servido por al menos dos proveedores de comunicaciones, y debe provenir de al menos dos oficinas o puntos de presencia diferentes del proveedor. El cableado del proveedor de acceso debe estar separado al menos 20 metros en todo el camino [***1***].

Para ello el acceso será a través de más de un proveedor (inicialmente dos, aunque debe preverse para aumentar este número). Se dispondrán dos salas o centros de enlaces, siendo que cada sala tendrá al menos un acceso a dos proveedores (idealmente accesos a cada proveedor), y al menos dos proveedores deberán dar acceso a ambas salas y estas conexiones deben ser de dos instalaciones del proveedor diferentes. La red física del proveedor de servicio de red terminará en esta sala, albergando los equipos de los proveedores.

Para facilitar el aislamiento de las redes de los proveedores y hacer transparente el acceso a la red externa, se configurará un esquema conforme la figura siguiente.

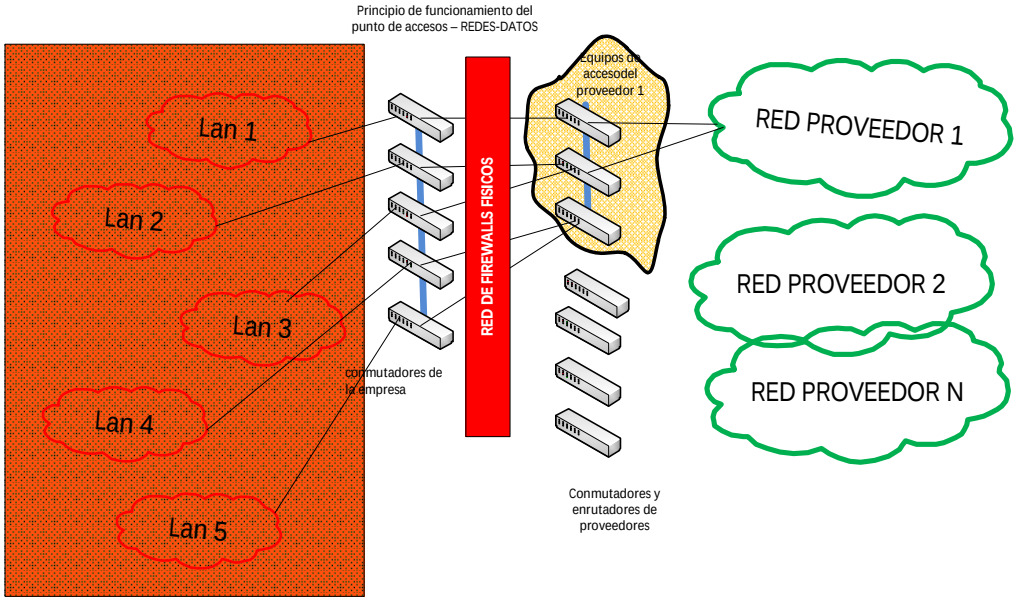


Figura 38 Accesos de los proveedores de red al centro de datos

Se pretende disponer de un lugar donde establecer las conexiones con diferentes proveedores de forma que se disponga de la flexibilidad de cambio de proveedor de servicios sin necesidad de efectuar diferentes conexionados y, si fuera el caso que haya redundancia de conexión del centro de respaldo con el exterior.

En este punto de accesos pretende que puedan llegar los distintos proveedores de conectividad y con los equipos de cada uno de ellos poder establecer las conexiones rápidas que sean necesarias para poder transferir los servicios desde uno cualquiera a cualquier otro.

Una vez en el centro los elementos de los diferentes proveedores de acceso deben estar etiquetados y distribuidos físicamente de forma que se puedan mantener por los terceros sin influir, impactar o necesitar la intervención de otros operadores (seguridad a nivel de rack, distribución de los racks, etc.).

Una vez solventado la llegada física al centro habrá que definir con los proveedores el uso que haremos de sus conexiones. Hay varias opciones:

- Considerar un operador como principal y los demás sólo se utilizarán como back-up.
- Considerar todas las conexiones de los diferentes proveedores como activos y distribuir el flujo de datos entre los diferentes proveedores.

Será utilizado el segundo escenario, con configuración de multihoming BGP, de forma que las diferentes conexiones de los diferentes proveedores poseen el mismo rango de direcciones de IP. Esta configuración permite que, en el caso de fallos a nivel de ISP, se pueda intercambiar rápidamente el acceso a través de las reglas de encaminamiento. Como punto de atención, esto requiere que el centro participe del enrutado entre dominios definido en BGP [***44***].

En cuanto a la distribución física del punto de accesos se refleja en la siguiente figura.

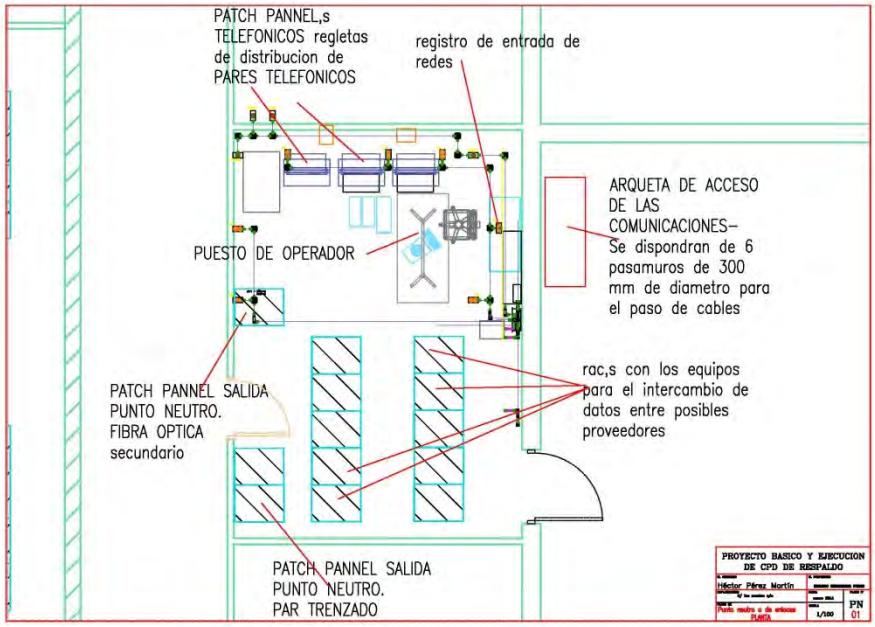


Figura 39 Detalle del plano correspondiente a la conexión con proveedores

4.4 Nivel físico

En este capítulo se describen los elementos de red a nivel físico; partiendo de los elementos descritos en el nivel de red. Se determinarán los protocolos intervinientes (10Gb Ethernet, infiniband, etc.).

En los planos D.II.1 Red de Datos General y D.II.2 Redes y distribución del punto de acceso del Anexo D - Planos., se describen las redes principales del centro, desde la acometida al mismo, contemplado en el plano segundo hasta la distribución en la Sala Técnica y a los puestos de trabajo. Como ya se ha dicho existen otras redes que se han ido describiendo en cada caso. Pero nos centramos en estas ya que el cableado de las mismas supondrá el cableado físico de todas las redes del centro. En los planos mencionados se hallan las mediciones, la distribución de Patch pannels y equipos de zonificación física.

La siguiente figura representa esquemáticamente la forma en que se subdivide el cableado horizontal, de acuerdo con la norma TIA 498

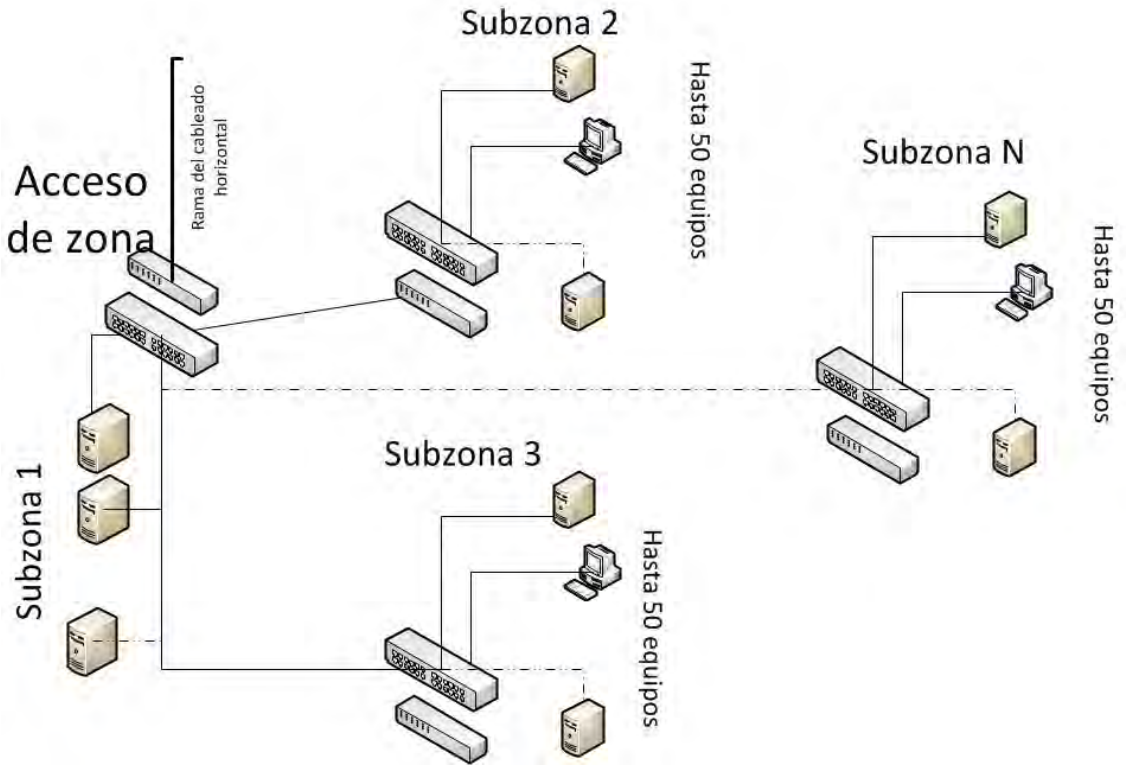


Figura 40 Esquema de zonificación física

4.4.1 Zonificación física de redes

Para el diseño del nivel físico, se han tenido en consideración los aspectos de la norma TIA-942 referentes a las telecomunicaciones, a fin de que el centro de respaldo cumpla los requisitos de "Tier 4" en este aspecto. Estos criterios son [***1***]:

- El cableado del backbone debe ser redundante. El cableado entre dos espacios debe recorrer dos rutas físicas, con caminos comunes únicamente en los dos espacios finales. El cableado debe estar protegido en base a enrutar a través de conductos o por el uso de cables con armadura "interlocking".
- Debe haber backup automático (no en standby) para todo el equipamiento crítico de telecomunicaciones, equipos del proveedor de acceso, routers del núcleo de producción y switches centrales LAN/SAN. Las sesiones/conexiones deben cambiar automáticamente al equipamiento de backup.
- El centro debe tener una MDA y una SDA preferentemente en lados opuestos, o al menos separados 20 metros. No se deben compartir zonas de protección de incendios, energía, aire acondicionado. La SDA es opcional si la sala es un espacio único continuo.
- Los routers y switches de distribución redundantes deben estar distribuidos entre la MDA y la SDA de forma que las redes del centro de datos pueden continuar operando si hay un fallo total en la MDA, SDA o en una de las salas de entrada.
- Cada zona de distribución horizontal debe tener conectividad hacia la MDA y la SDA.
- Los sistemas críticos deben tener cableado horizontal a dos zonas de distribución horizontal. El cableado horizontal redundante es opcional incluso para el Tier 4.

- Todo el cableado, conexiones y cables de parcheado debe estar documentado usando hojas de cálculo, bases de datos o aplicaciones diseñadas para administrar el cableado. Este es un requisito imprescindible.
- El cableado interno del centro de datos de LAN y SAN desde los switches de las áreas de distribución horizontal a los switches de distribución horizontal de la MDA deben tener pares redundantes de fibra o cable. Las conexiones redundantes han de estar en distintos mazos de cable.
- Todos los jumpers y patch cords deben estar etiquetados en los dos lados del cable, con el nombre de la conexión en ambos lados del cable.
- Los armarios y racks están etiquetados en la parte frontal y la parte trasera.
- Los patch pannels están etiquetados según la ANSI/TIA/EIA-606-A.

SALA TECNICA PRINCIPAL: Las conexiones troncales a esta sala se pueden ver en el esquema de la figura.

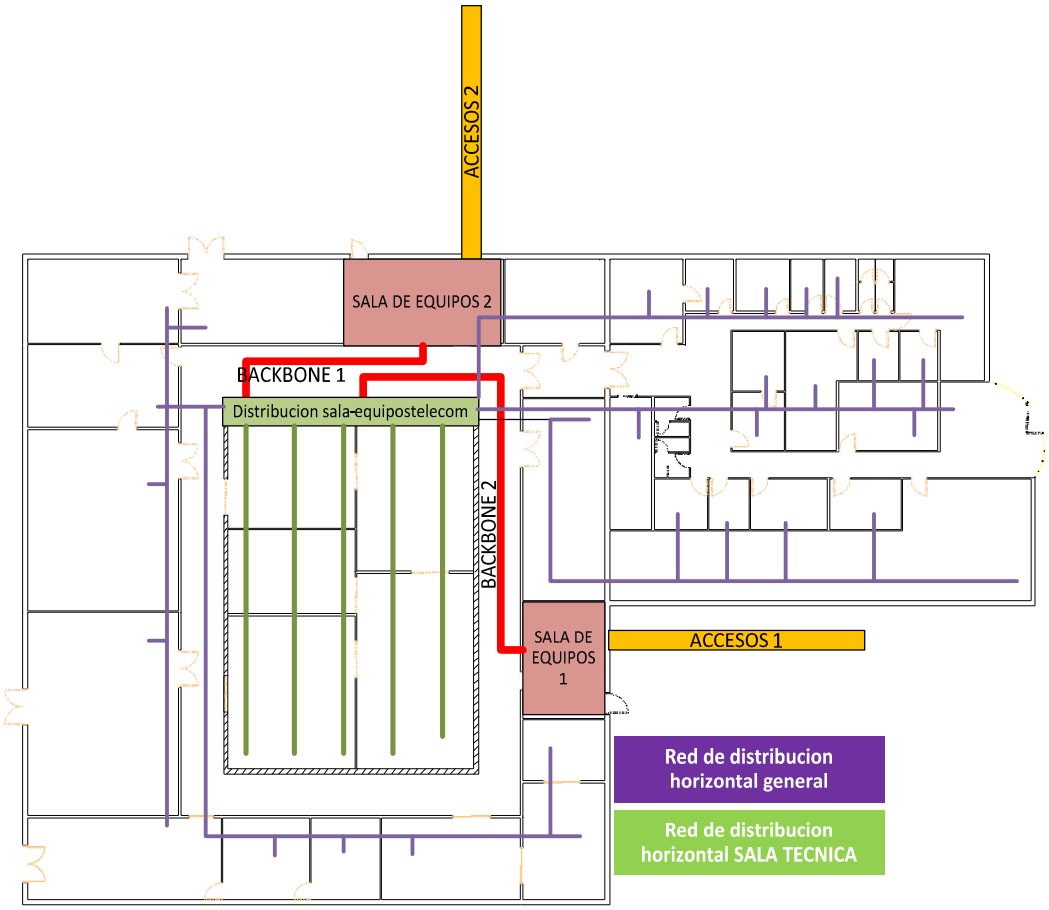


Figura 41 Plano de conexiones físicas a la sala técnica

ZONAS DE TRABAJO OFIMATICO Y DE GESTION (Áreas de oficinas y salas de trabajo)

En la siguiente figura se presentan la distribución horizontal de la red general del CPD siguiendo la estructura del plano D.II.1 Red de Datos General del Anexo D - Planos en el que se hallan las mediciones de los troncales y los puntos de red totales y su ubicación en cada área.

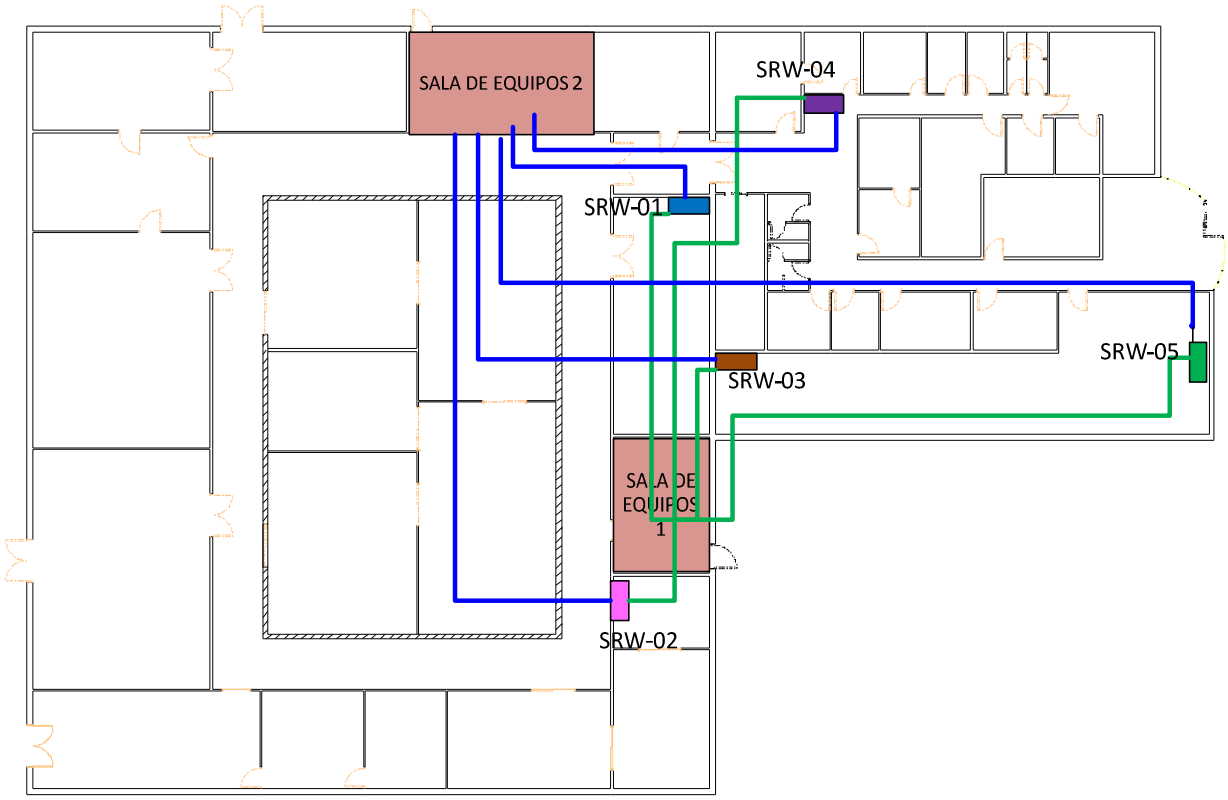


Figura 42 Plano de conexiones físicas a las zonas de gestión

OTRAS SALAS TECNICAS: Estas áreas se reflejan en al plano D.II.1 Red de Datos General y D.II.2 Redes y distribución del punto de acceso del Anexo D - Planos y las longitudes de red en cada punto.

4.4.2 Cableado estructurado

Es evidente que en un centro de datos, como es el CPD de respaldo, la complejidad y extensión de los sistemas que se instalan, generan la necesidad de planificar convenientemente todo el sistema de cableado de datos. Un sistema estructurado del cableado bien diseñado es un componente esencial que puede ayudar a manejar la complejidad del centro y facilitar el crecimiento futuro y las posibles modificaciones del sistema.

Tal como se muestra en la imagen, además del cableado estructurado, es necesario aplicar ciertas normas o recomendaciones que permitan un adecuado mantenimiento de los sistemas, que por su complejidad podrían llegar a una situación como la que se muestra en la imagen.

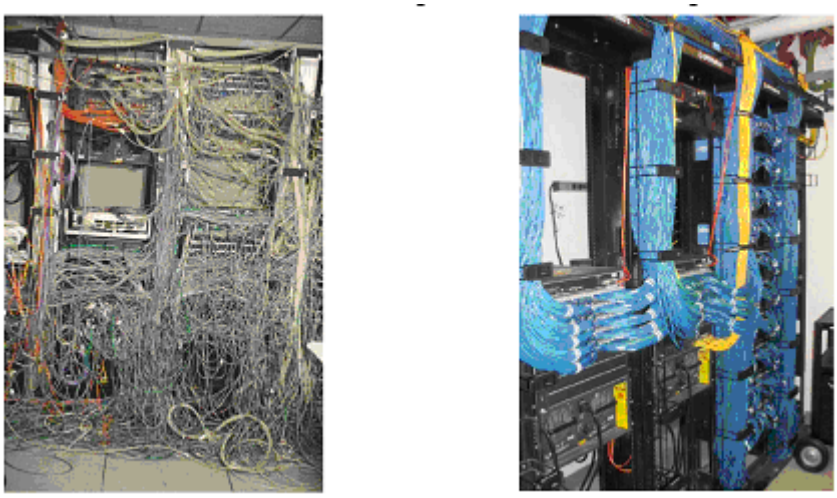


Figura 43 Cableado no estructurado vs cableado estructurado *[**45**]*

Por ello se definen un conjunto de normas que permitan mantener en orden y convenientemente identificado, todo el cableado de las instalaciones del Centro de Respaldo.

Como primera medida se establecerá un sistema de cableado estructurado, para las salas técnicas, particularmente las salas de equipamiento informático y de telecomunicaciones, que se hará siguiendo las directrices contenidas en la norma TIA 942 [***1***], y en la norma TIA 568 donde aplique [***46***].

Esta normativa comprende un conjunto de recomendaciones para los diseñadores de Centros de Datos, que se dividen en dos partes principales, una dedicada a los espacios que debe tener el Centro de Datos, y otra parte dedicada a los subsistemas de cableado.

En este sentido el sistema de cableado del centro de datos se puede dividir en dos partes principales:

- Subsistema de Cableado Troncal
- Subsistema de Cableado Horizontal

Como norma general el cableado se efectuará de forma estructurada y se dispondrán, a la entrada de cada sala técnica un cuadro (armario o rack) para acoger la totalidad de los cableados de datos, de modo que de este armario se distribuirá un troncal que distribuya a armarios zonales distribuidos por la sala, como se muestra en el plano D.II.1 Red de Datos General del Anexo D - Planos.

El cableado troncal principal repartirá la señal de datos a armarios de distribución zonales, donde se concentrarán las comunicaciones necesarias para cubrir una superficie de 30 m^2 de equipamiento informático y de telecomunicaciones, para cada armario zonal. O bien la correspondiente a una zona identificada en la zonificación o sectorización de las redes..

Se garantizará que las comunicaciones necesarias para cada equipo, se hallan disponibles en todos los racks, para todos los equipos, estén instalados o no. Para ello, desde cada armario zonal, se llevará una derivación a cada rack de todos los servicios y comunicaciones posibles.

De esta forma, podemos tener una instalación con todo el cableado preparado, de modo que todos los servidores estarán conectados, sin necesidad de tender cableado cada vez que se realice una ampliación o modificación del sistema.

El cableado de las salas técnicas. Particularmente las salas de equipamiento informático y de telecomunicaciones, se hará siguiendo las directrices contenidas en la norma TIA 942 [***1***].

En general se efectuará en forma estructurada y se dispondrán, a la entrada de cada sala técnica un cuadro (armario rack o los necesarios) para acoger la totalidad de los cableados de datos, de modo que de este armario se distribuirá un troncal que distribuya a armarios zonales distribuidos por la sala.

Las salas se distribuirán zonalmente con la filosofía "X"/"Y" en áreas de 30 m^2.

El troncal principal distribuirá a armarios de distribución zonales en que se concentrarán las comunicaciones para dar servicio al menos a unos 30 m^2 de ocupación de equipamiento. En toda la superficie de las salas técnicas de equipamiento informático y de telecomunicaciones se dispondrán los armarios zonales necesarios para cubrir cada uno una superficie de 30 m^2.

Se garantizará que las comunicaciones necesarias a cada equipo, se hallan disponibles en el rack que va a ocupar el equipo. Para ello, de cada armario zonal, se llevará una derivación a cada rack de todos los servicios de comunicaciones posibles, disponibilizando las comunicaciones en cada rack.

Los rack se numerarán por el nombre de la cuadrícula que ocupen seguido de un número de orden. Dentro de cada rack, se numerarán los huecos de alojamiento de equipamiento en módulos de altura la del más estrecho de los equipos susceptibles de ser ubicados en el mismo (el tipo blade) (de abajo arriba). Dentro de cada módulo se enunciarán los conectores con las siglas del tipo de cable (FO, RJ45, RJ11, Coax, etc.) seguidos del orden que el conector ocupa en el equipo (de izda. a dcha.) efectivamente identificando cada conexión por (zona-nº orden rack-ubicación del modulo-tipo conector orden).

De esta forma, podremos tender los cableados de modo que no hayan de ser alterados al cambiar o poner nuevos equipos ya que todos están servidos sin necesidad de tender cableado cada vez. Del mismo modo, con esta nomenclatura, tendremos identificado el servicio en los armarios de zona y en ellos podremos efectuar las conexiones que sean procedentes para garantizar que el servicio llega al equipo concreto.

En la sala técnica, la distribución de los cables de datos ser hará en bandejas metálicas elevadas. Así evitaremos que el falso suelo que se utilizará para la circulación aire acondicionado de refrigeración de los equipos. Se minimiza también que el mantenimiento del cableado requiera la retirada y remontaje de las baldosas para nuevas instalaciones con el consiguiente acumulación de partículas de polvo que podrían generar impulsados por el aire malfuncionamiento de equipos y aplicaciones [***12***].

También la energía eléctrica será de forma elevada a través de bandejas de distribución y un sistema de bus-bar elevado que permita la conexión y desconexión en caliente de los equipos.

Como consecuencia de esto y para evitar que las bandejas se sobrecarguen de cables se efectuará un cableado en estrella jerarquizado, manteniendo las zonas que se expresan más abajo y, para cada zona generando subzonas que permitan el aligeramiento de cables perseguido, de forma que no se atenderá, en cada subzona a más de 50 equipos, ya sean físicos o lógicos (en el caso de los sistemas virtualizados).

Así la distribución en la Sala técnica se hará mediante un patch panel de entrada a la misma todo el de fibra óptica, con 4 entradas y 24 salidas que permitan efectuar la distribución zonal y queden puertos para futuro crecimiento.

Desde este se distribuirá mediante fibras al resto de las zonas en que se dispondrá de otro patch panel con su switch correspondiente desde el que se atenderán al menos a 50 equipos (tres switches de 24 puertos de cable UTP y otro switch, de al menos 12 puertos de fibra óptica). Desde este patch panel se atenderá a cada subzona que dará servicio a otros 50 equipos y por cada grupo de 50 equipos se dispondrá de un switch y su patch panel correspondiente.

Este sistema es algo más complejo de mantener; pero resulta beneficioso en cuanto a longitudes de cables y en cuanto a la cantidad de los mismos que discurren por las bandejas de distribución, haciendo más ligera la instalación y más estética.

En el resto de zonas la instalación se efectuará por falso suelo o sobre pared, por zócalos y suelos.

En cada zona se dispondrá del correspondiente switch y, de nuevo, si se supera el número de 50 equipos los atendidos se efectuará la división en subzonas de 50.

El haber elegido el número de 50 equipos para ser atendidos por cada subzona es debido a que pueden ser atendidos con dos switches de 24 bocas cada uno o uno de 48, permitiendo mantener otro switch, para futuros crecimientos o mejoras.

4.4.2.1 Especificaciones técnicas del cableado

- El cableado a instalar debe cumplir o exceder los requisitos de Cat.5 E (Categoría 5 Enhanced) para los puestos de usuario.
- Las tomas de usuario deberán permitir, en función de su configuración, ser usadas tanto para servicios de transmisión de datos como para servicios de voz y/o fax.
- Existirán armarios de conexiones con paneles de distribución que permitan la asignación de servicios (datos y/o voz) de manera sencilla mediante latiguillos. Estos armarios deberán contar con elementos de seguridad que impidan el acceso a personal no autorizado.
- En los servicios troncales se hará uso de fibra óptica multimodo y, en caso de que sea necesario una mayor tasa de transmisión de información, monomodo, garantizando una futura capacidad de transmisión de 10Gbps.
- Se cumplirán las normas establecidas en ANSI/EIA TIA-568-B [***46***] (Referencia H) e ISO/IEC 11801 (Referencia I).
- El esquema de cableado de los conectores RJ45 de los puntos de acceso se realizará siguiendo el esquema T568B incluido en la referencia H.
- La instalación debe ser "certificada"; por tanto, su ejecución y supervisión deberán ser realizadas por personal cualificado para la citada certificación.
- La garantía del cableado instalado deberá abarcar un plazo mínimo de 10 años.

4.4.2.2 Especificaciones técnicas de los equipos

Los equipos que conforman la red de área local deberán cumplir las siguientes características:

- No se utilizarán equipos concentradores (hub).

- No se usarán equipos enrutadores internamente en la LAN, aunque los conmutadores podrán tener ciertas capacidades de gestión de capa 3 o superior.
- Toda la electrónica ha de poseer capacidades para gestión remota.
- Se procurará que en el núcleo central de la electrónica de red estén incluidos el/los equipos enrutador/es, recomendándose que este núcleo esté dotado de un Sistema de Alimentación Ininterrumpida (SAI).
- Las piezas fundamentales serán los equipos conmutadores (switches), cuyas características técnicas mínimas recomendadas figuran en la siguiente tabla.

Característica	**Característica deseada**
Velocidad puertos	Puestos de trabajo: mínimo 10/100 BaseTx, autosense. Servidores: con capacidad para establecer enlaces a 1000BaseTx o Sx (cobre o fibra).
Número de puertos (por conmutador)	Se recomienda un mínimo de 24 puertos.
Configuración	• Con capacidad de ser apilables, y puerto uplink mínimo de 1Gbps. • En grandes instalaciones, se recomienda que se utilicen configuraciones en chasis (racks) con fuente de alimentación redundante.
Calidad de Servicio	La Calidad de Servicio (QoS), deberá manejar un número adecuado de colas por puerto (8 es la recomendación), para controlar el flujo de tráfico y aumentar el rendimiento de la red. Se recomienda que soporte el estándar de calidad de servicio IEEE 802.1p.
Disponibilidad	Se recomienda que soporten los siguientes estándares en los segmentos troncales de la instalación: • IEEE 802.1D Spanning Tree Protocol (STP) para enlaces redundantes. • IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) para recuperación de enlaces caídos. • IEEE802.3ad (LACP) para agregación de enlaces.
Redes virtuales (VLAN)	Se recomienda que soporte el estándar de redes virtuales IEEE 802.1Q.
Administración	• Se recomienda con administración basada en web. • Administración por línea de comandos permitida por consola y vía telnet. • Gestionable vía SNMP. • Debe de cumplir los siguientes estándares: o SNMP v1 (IETF Std 5/RFC 1157). o SNMP v2c (IETF RFC 1901). o RMON v1 (RFC 1757) o superior.

	o MIB II (IETF Std 17/RFC 1213). Nota: Recomendable el soporte de SNMP v3 (RFC 2271-2275).
Servicios de valor añadido	• 3 años de Garantía, debidamente avalada. • Se recomiendan 2 años adicionales de mantenimiento y soporte. • Documentación técnica asociada al equipo, a ser posible, en castellano.

Tabla 20 Características técnicas para los conmutadores

4.4.2.3 Fibra Óptica

- Reduce considerablemente el número y las longitudes acumuladas de cables en el suelo elevado o en la distribución (troncales y distribuciones con sistemas de patch-cords para el interconexionado).
- Reduce la complejidad de conexiones físicas
- Reduce el tiempo y el esfuerzo en las instalaciones, movimientos, adiciones y cambios de equipamiento.
- Apropiado para todos los tipos de fibra usados en la comunicación de datos:
    - multimodo de 62,5/125 µm
    - multimodo de 50/125 µm
    - monomodo de 9/129 µm

El tipo de fibra dependerá del tipo de componentes instalados y de los protocolos utilizados por ellos. Debe planificarse cuidadosamente.

Como elementos de conexión, se utilizarán conectores multifibra (12 fibras) en los troncales de fibra para facilitar la conexión. Para reducir el espacio físico necesario para las interconexiones, se usarán conectores de pequeño factor de forma SFF (Small form factor) en el CPL. Utilizando conectores SFF se reduce el espacio requerido para los paneles de conexionado.

Dentro del CPL, las interconexiones se realizan mediante cables de conexión cortos con 3 mm de diámetro disponibles en longitudes variables.

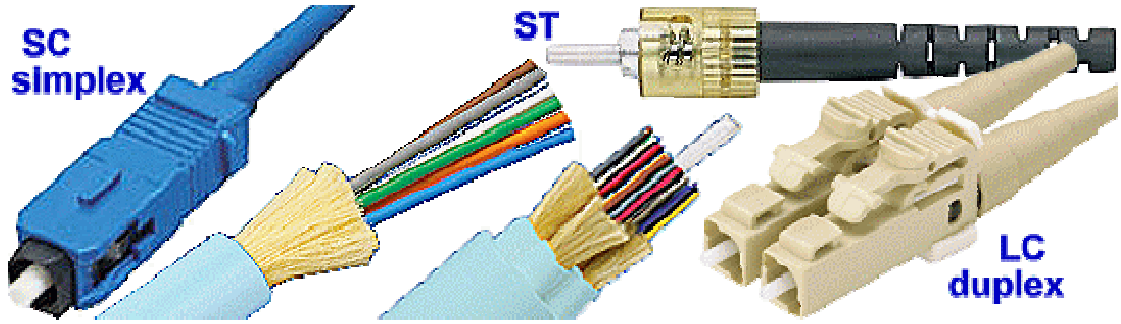


Figura 44 Diferentes tipos de conectores de FO *[**45**]*

4.4.2.4 Sistemas de cableado de Rack

La distribución hasta los armarios de comunicaciones se efectuará mediante montantes (verticales) y sistemas de cableado de racks (horizontales) que deben planificarse para

los diferentes sistemas de suministro de los cableados de comunicaciones y de redes. Los montantes y cableados de Rack se deben efectuar con el código definido anteriormente (opcionalmente se puede hacer corresponder con un código de colores) a intervalos regulares para la identificación del sistema.

Se debe asegurar la accesibilidad tanto en los falsos techos como en los suelos técnicos.

En las áreas desatendidas, se debe instalar un rack de cableado y un sistema de barras bajo el falso suelo que deberán ser válidos para los diferentes tipos de sistemas de suministro e instalación.

Los sistemas de apoyo de los rack se instalarán sobre la solera.

4.4.3 Conexión Centralizada (Central Patching Location)

Para diseñar el cableado de datos estructurado de un centro de datos, es importante plantear la utilización de un sistema de conexiones centralizadas (Central Patching Location – CPL). Este método se basa en la utilización de paneles de conexión, conocidos como “Patch Pannels” para establecer rutas predeterminadas para el cableado y mantener separadas las áreas de interconexión.

Tal como se muestra en la imagen, todos los equipos se conectan en estrella al CPL, y después el CPL se conectará a uno a varios switches que repartirán los datos a los servidores de almacenamiento. Además de la obvia mejora en ordenación, al añadir un nuevo elemento las nuevas conexiones (líneas negras) son más fáciles de gestionar.

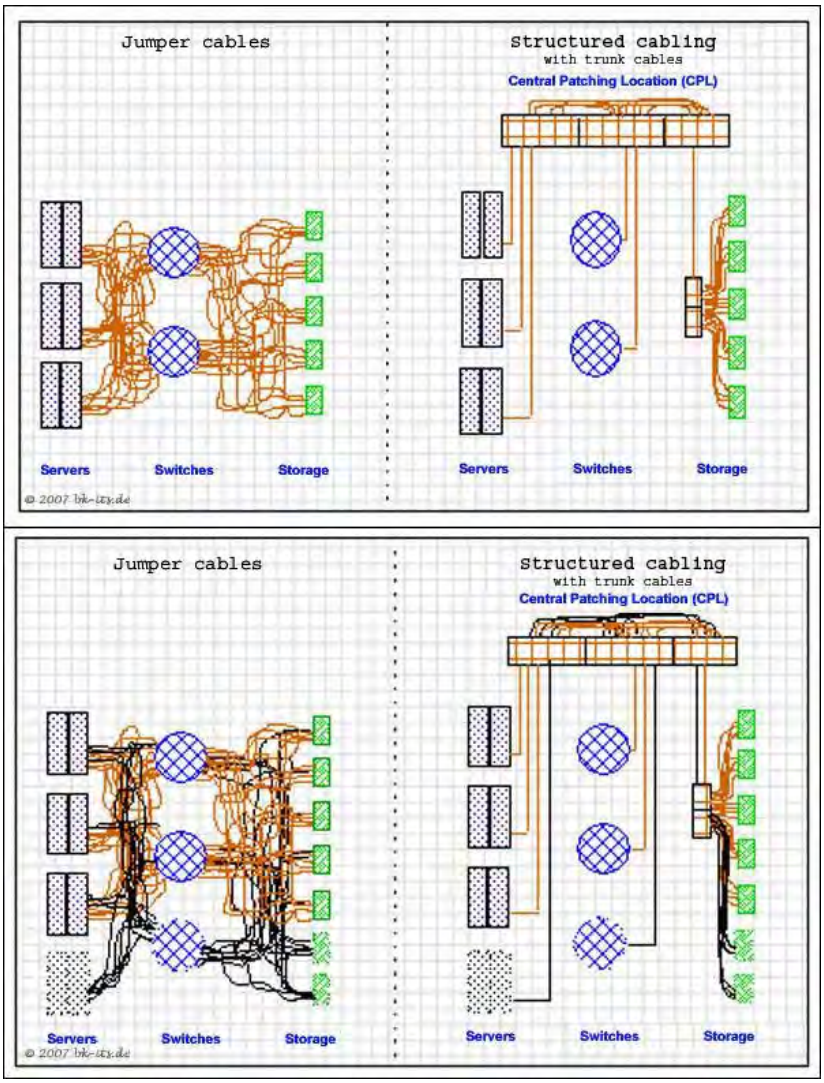


Figura 45 Función del Central Patching Location en el cableado [**47**]

De esta forma el punto de conexión se aleja del dispositivo y se concentra en una sola zona de conexión de cableado. El CPL sirve como punto único de conexión entre los componentes hardware de una sala y como troncal para la interconexión entre salas, pisos o edificios de la instalación.

Así las conexiones entre los equipos se hacen por medio de cables más cortos que no están situados en el suelo técnico, y las posibles modificaciones debidas a cambios de hardware, se pueden realizar de forma independiente de la infraestructura general del centro de datos. Esto simplifica en gran medida las posibles modificaciones del cableado, centrando las actividades de estos cambios en los lugares definidos para ello, en lugar de tener que desconectar y volver a conectar los cables de conexión situados bajo el suelo elevado.

Para estas conexiones se recomienda utilizar conectores multifibra (12 fibras) en los troncales, y del tipo pequeño factor de forma SFF (Small form factor – Pequeño factor de forma) en el CPL, que pueden ser del tipo MT-RJ o el conector SC-DC. Los conectores SFF contienen ambas fibras en una misma cabeza por lo que reducen las dimensiones de alojamiento a la mitad e incluso menos en relación con los conectores dúplex tradicionales.

Todos los componentes hardware, como servidores, mainframes, switches, controladores, dispositivos de almacenaje, sistemas de robot, equipos de red se conectarán en estrella a su CPL.

Cualquier cambio de configuración solo requerirá la reconexión de los cables de conexión dentro del CPL. No requiriéndose aperturas del falso suelo para volver a instalar largos cables, y tampoco se requiere la manipulación de los equipos para obtener el acceso a los puntos de conexión. En el caso de instalación de nuevas máquinas se requerirá la instalación de nuevos cables troncales al CPL y de cables de conexión adicionales en el patch panel.

Correspondiente con los principios descritos en los apartados anteriores, el CPD dispondrá de varias ubicaciones centralizadas de conexión, o CPL. Esta Instalación de Conexión Centralizada consistente en uno o más racks con paneles de distribución para conectores de fibra.

4.4.3.1 Localización del CPL en la sala

Se recomienda la colación de los armarios de distribución (CPL) en el centro de la zona a servir (30 m2) para compensar las longitudes medias de cable desde el CPL hasta los otros componentes se recomienda el acceso a las partes frontal y trasera de los armarios CPL, acceso frontal para las interconexiones y trasera para la instalación de cables troncales adicionales

Los armarios serán de 80 cm de ancho para la fácil instalación de los cables troncales y para cumplir con el mínimo radio de curvatura de los cables troncales.

Será condición deseable el uso de armarios con posibilidades de entrada de cables por la parte superior e inferior para mantener la posibilidad de entrar cables desde bandejas instaladas en los techos y en el falso suelo.

4.4.3.2 Patch-pannels

Los sistemas de patch panel se dispondrán de la forma expresada en el apartado anterior y dispondrán de las tomas suficientes para poder interconectar los equipos que correspondan teniendo en cuenta la totalidad de alojamiento que se calcula para el centro de respaldo.

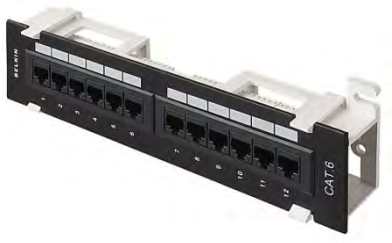


Figura 46 Ejemplo de patch-pannel [**48**]

Se dispondrá de dos armarios de patch pannels para la distribución interna.

Uno troncal sencillo y dos dobles situados en la mitad de la sala para la distribución horizontal.

Cada armario contendrá espacio para ubicar las fuentes de alimentación individuales, y al menos 10 Us con patch panel de 24 puertos cada una de par trenzado y otros 10 para fibra.

4.4.4 Armarios de distribución

Se recomienda la colocación de los armarios de distribución (CPL) en el centro de la zona a servir (un armario para cada 30 m^2) para compensar las longitudes medias de cable desde el CPL hasta los otros componentes. Dentro de un mismo armario, pueden efectuarse hasta más de 800 conexiones, que se realizarán mediante cables de conexión cortos con solo 3 mm de diámetro, disponibles en longitudes variables.

Además se recomienda el acceso a las partes frontal y trasera de los armarios CPL, acceso frontal para las interconexiones, y trasera para la instalación de cables troncales adicionales. Se debe asegurar la accesibilidad tanto en los falsos techos como en los suelos técnicos a todos los armarios, colocando los racks adecuadamente sobre el suelo técnico.

Los armarios serán de 80 cm de ancho para la fácil instalación de los cables troncales y para cumplir con el mínimo radio de curvatura de los cables troncales. Será condición deseable el uso de armarios con posibilidades de entrada de cables por la parte superior e inferior para mantener la posibilidad de entrar cables desde bandejas instaladas en los techos y en el falso suelo.

La distribución a los armarios se efectuará mediante montantes (verticales) y sistemas de cableado de racks (horizontales) que deben planificarse para los diferentes sistemas de suministro de los cableados de comunicaciones y de redes.

Los montantes y cableados de Rack se deben identificar según un código que se define posteriormente en el apartado 4.4.6 de este mismo capítulo, aunque opcionalmente se puede hacer corresponder con un código de colores a intervalos regulares para la identificación del sistema.

Debido a la dificultad de identificar los cables de alimentación y de datos, para evitar un enmarañamiento extremo, es importante separar los cables, primero en dos grandes grupos, los de alimentación por una lado y los de datos por otro. Generalmente y como norma se establecerá el cableado de alimentación de los equipos en la parte trasera derecha del bastidor o armario, de forma que se pueda llevar de forma adecuada alimentación a todos los equipos instalados.

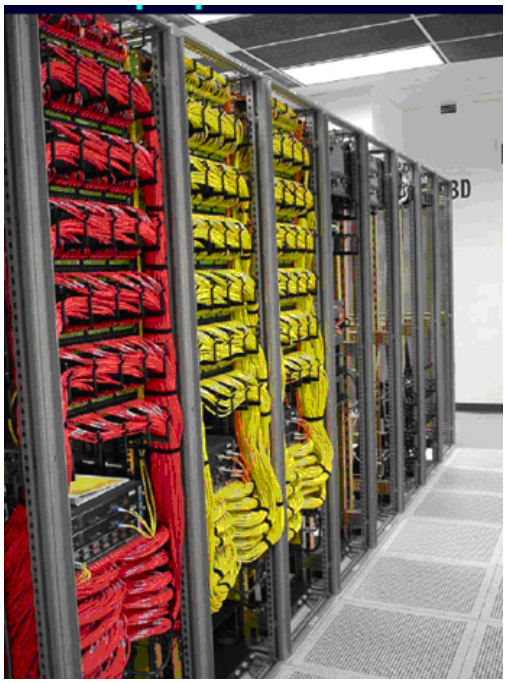


Figura 47 Visión del cableado en un rack [**49**]

El cableado de datos debe encontrarse separado de los cables de alimentación, para evitar posibles interferencias sobre la señal, por lo que se recomienda hacerlo en la parte posterior izquierda del bastidor.

Además en aquellos sistemas que contengan diferente tipo de cableado, este se distribuirá en el armario por diferentes zonas, por ejemplo el cableado de fibra podrá ir por la parte trasera izquierda del rack, mientras que el par de cobre o de cable coaxial irá por la zona delantera.

En todo caso, es importante evitar que tanto los cables de alimentación y los cables de datos puedan obstaculizar la circulación de aire, dañando los equipos que no estén bien refrigerados. Además se recomienda que los bastidores se diseñen con canales integrados que faciliten el manejo, el tendido y la acumulación de extensas longitudes de cable.

4.4.5 Sistemas para agrupar y ordenar el Cableado

Dentro de los bastidores es posible ordenar y agrupar el cableado utilizando diversos sistemas. De forma habitual estos armarios vienen equipados con sistemas de abrazaderas en los laterales o en la parte posterior, o en otras ocasiones vienen con carretes para la recogida del cable.

Si el armario no viene equipado con estos sistemas, o existe la necesidad de ampliar el cableado, se pueden acoplar Paneles de Administración de cables para bastidores, que tal como se muestra en la figura pueden ser horizontales o verticales, según la necesidad que tengamos para estructurar el cableado:

Figura 48 Modelos de paneles de administración de cables en rack [**48**]

Además en el mercado existe una gran variedad de sistemas de abrazaderas que permiten reconducir los cables de forma ordenada dentro de los bastidores:

Figura 49 Ejemplos de abrazaderas y su montaje [***50***]

Es muy importante evitar que los cables dentro del bastidor, se encuentren sometidos a demasiada tensión, ya que esta presión podría causar daños en la parte más sensible del cable, que son los conectores, haciendo que la transmisión de la señal no se haga correctamente. Por eso es importante utilizar cables con la longitud adecuada, evitando los cables con longitudes demasiado cortas.

Tampoco es conveniente utilizar cables demasiado largos, pero en caso de hacerlo, es importante recoger el sobrante del cable de forma adecuada y siempre dentro del suelo técnico, y evitar realizar bucles que puedan afectar a la señal o al estado físico del cable. En la siguiente figura vemos algunas recomendaciones de cómo debe colocarse el cableado en los patch pannels habilitados con carretes para la recogida del cable.

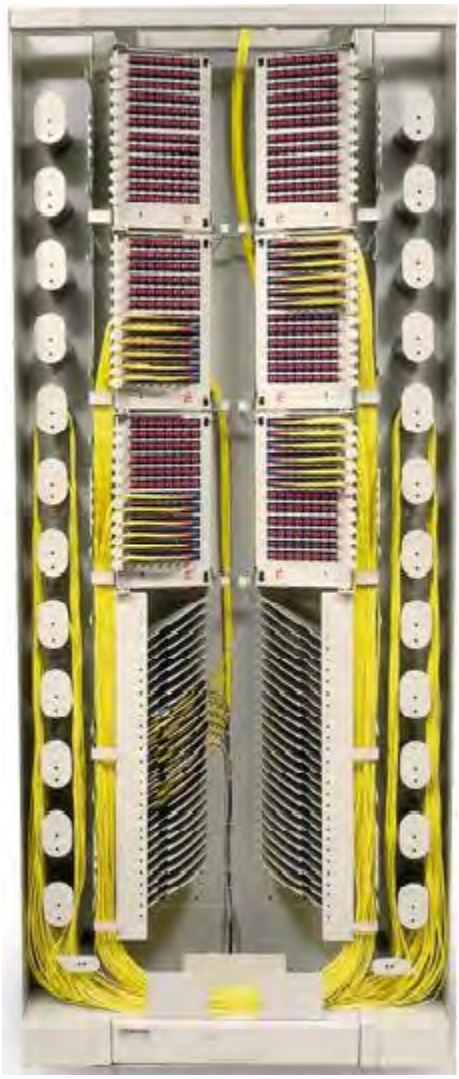


Figura 50 Distribución de cableado en carrete [**51**]

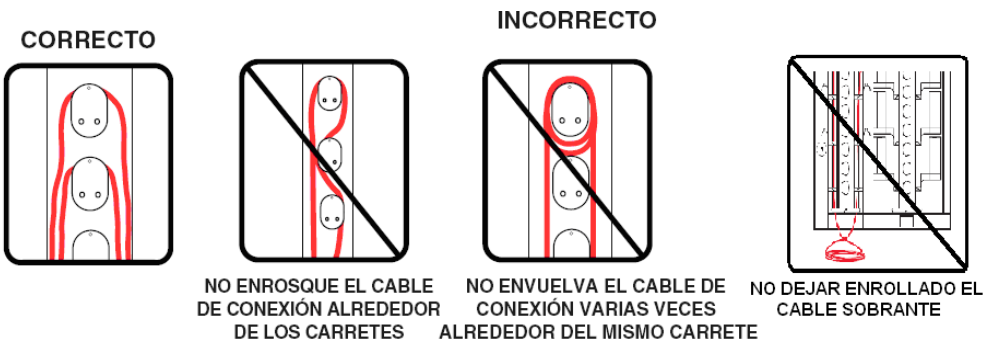


Figura 51 Instrucciones para la distribución de cables en bastidor [***52***]

En el caso de que los cables sean demasiado cortos, no se recomienda el uso de alargadores de cable, ya que estos pueden producir atenuación en la señal y es posible que los puntos de conexión del alargador coincidan en lugares donde cualquier tensión o movimiento puede desconectarlos, o provocar alteraciones en la calidad de la señal. En estos casos se recomienda la sustitución del cable por uno de la longitud adecuada, o utilizar patch pannels para conectar el cable con otro de más longitud.

Otro sistema para mantener el cableado estructurado, es el uso de bridas para agrupar el cableado. Estos dispositivos, además de realizar la función de ordenar los cables, también son muy útiles, porque permiten eliminar las posibles tensiones a las que se puede someter el cable, que pueden provocar el deterioro del mismo, sobre todo en la parte de los conectores. Sobre las bridas para agrupar cables, pueden variar según su forma, material, tamaño o características especiales. Además la variedad de los colores de dichas bridas nos permiten poder clasificar el cableado según un código de color y así saber en todo momento el uso que se le da a cada cable.

Figura 52 Ejemplos de bridas [**50**]

En determinadas ocasiones las bridas puede que no sean adecuadas para agrupar el cableado, ya que si se aprietan demasiado, pueden causar daños a los cables. Para estos casos existen otras opciones para ordenar los cables, como son los tubos estriados. Estos tubos de poliuretano corrugado, son flexibles y además permiten añadir nuevos cables, pasándolos a través del tubo, una vez que está finalizada la instalación. Tal como se muestra en las imágenes, también existe una gran variedad de tubos, en lo que respecta a colores, materiales y tamaños:

Figura 53 Ejemplos de tubos estriados [**50**]

Finalmente también es posible encontrar diversos sistemas de fundas y cubiertas para la protección y agrupamiento de cables. Cabe destacar en este sentido los sistemas termo contráctiles, que bajo la aplicación de calor, se ajustan al mazo de cables, proporcionando una protección perfecta y consiguiendo que el cableado ocupe el mínimo espacio dentro del rack.

4.4.6 Identificación y etiquetado del cableado

Tan importante como mantener el cableado ordenado, es la necesidad de esté perfectamente etiquetado e identificado, de forma que en cualquier momento sepamos de qué cable se trata y qué sistemas está conectando.

Para llevar este control y poder administrar el cableado en los bastidores, es necesario tener la documentación con el esquema de etiquetado de todos los componentes del sistema. Para esto se deben seguir las recomendaciones de la normativa TIA-606-A, que

es considerado como el esquema de etiquetado más extendido en los centros de datos. Todos los bastidores, racks, patch pannels, cables y conectores para parcheos, deben ser etiquetados.

La normativa indica que los bastidores y racks se etiquetan según su localización, utilizando como referencia la red de baldosas del suelo y después indicando la fila dentro del bastidor y finalmente la posición dentro del estante del rack. En la siguiente figura se muestra un ejemplo de este sistema de etiquetado.

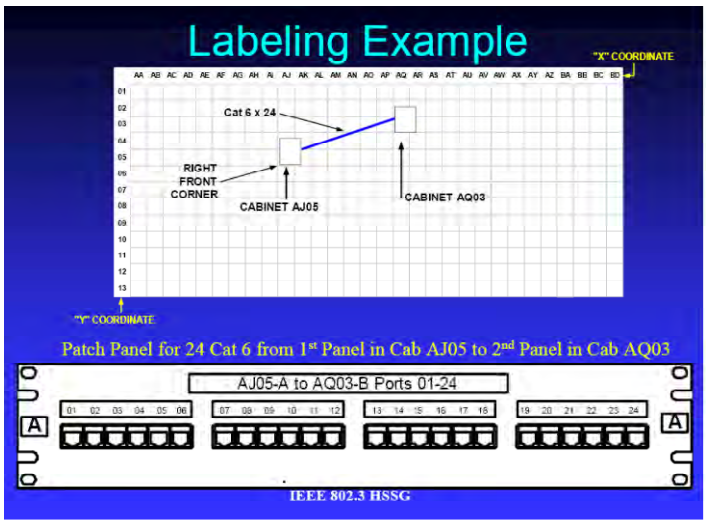


Figura 54 Ejemplo de etiquetado de un patch pannel [**49**]

Los rack se numerarán por el nombre de la cuadrícula que forman las baldosas del suelo donde están instalados, seguido de un número de orden.

Dentro de cada rack, se numerarán, de abajo a arriba, los huecos de alojamiento de equipamiento, en módulos de altura, la del más estrecho de los equipos susceptibles de ser ubicados en el mismo, por ejemplo el tipo blade.

Dentro de cada módulo se enunciarán los conectores con las siglas del tipo de cable (FO, RJ45, RJ11, Coax, etc.) seguidos del orden que el conector ocupa en el equipo de izquierda a derecha, con lo que cada conexión quedará identificada por: número de zona, orden de rack, ubicación del módulo, tipo conector y orden.

Con esta nomenclatura, tendremos identificado el servicio en los armarios de zona y en ellos podremos efectuar las conexiones que sean procedentes para garantizar que el servicio llega al equipo concreto. Todos los cables deben estar identificados, de forma clara y visible en ambos extremos, ya sea utilizando etiquetas o impreso sobre el mismo cable.

4.4.7 Distribución del cableado

Para la distribución del cableado de forma estructurada entre los diferentes armarios de la sala técnica, es necesario utilizar una infraestructura adecuada. Esta instalación de cables de datos debe hacerse o bien en bandejas en el falso suelo técnico, o bien, por el techo, según sea la distribución que se defina, a lo largo de las filas de bastidores con un ancho mínimo de 25 cm.

4.4.7.1 Suelo técnico

La altura del suelo técnico será de entre 60 y 80 cm para asegurar una fácil instalación de todo tipo de cableados. Las dimensiones de las baldosas debe ser de 60x60 cm^2. Las aperturas en las baldosas bajo, enfrente o detrás de los armarios o racks se deben cortar en dimensiones de aproximadamente 15 x 15 cm^2.

El suelo técnico debe estar hecho de un material adecuado, que combine la resistencia con propiedades anti-estáticas, y además debe estar completamente conectado a tierra. La normativa TIA-942 recomienda suelos que aguanten una carga distribuida de 250 lbf/ft^2 (12kPA) (el mínimo de carga distribuida permitida es de 150 lbf/ft^2 (7.2kPA)). Con respecto a la resistencia contra incendios, el suelo técnico debe cumplir como mínimo los requerimientos de la normativa NFPA 75.

La utilización del falso suelo técnico para el cableado, aporta las siguientes ventajas:

- La apariencia de este cableado es más discreta que el cableado aéreo.
- El cableado en falso suelo permite mayores densidades de potencia, mejor control de los sistemas de enfriamiento y mayor flexibilidad en la colocación de los equipos de aire acondicionado.
- La mayor parte de los sistemas están diseñados para ser cableados desde abajo.
- Permite un fácil acceso para posibles cambios en el cableado.

Se recomienda el uso de bandejas de alambre para en el cableado en los pasillos calientes para el cableado de telecomunicaciones en el suelo técnico. Para permitir el crecimiento del cableado, se debe dejar un espacio del 40% de la capacidad de la bandeja, disponible para posibles ampliaciones.

En la siguiente figura se muestra un ejemplo de cableado en falso suelo elevado con uso de bandejas de alambre para cableado:

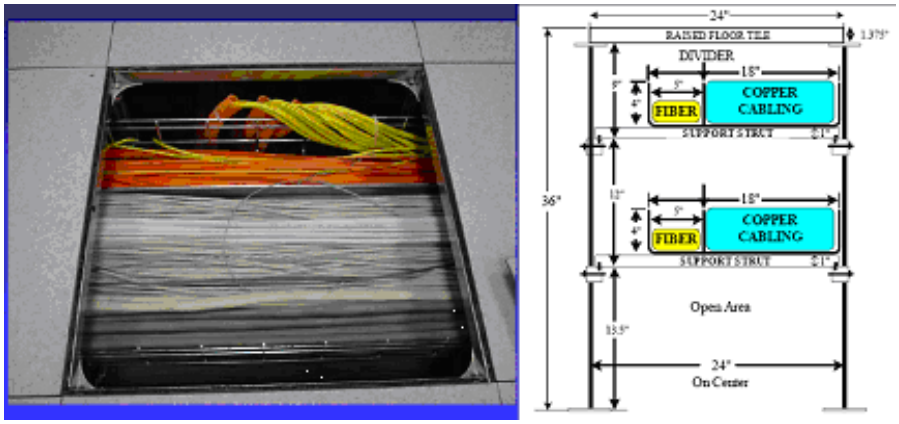


Figura 55 Ejemplo de cableado en falso suelo elevado [**49**]

4.4.7.2 Bandejas de Cables Elevadas

El sistema de cableado mediante bandejas elevadas, consiste en un conjunto bandejas de cables suspendidas del techo. De esta forma este sistema, además de ser más económico que los sistemas de falso suelo elevado, proporcionan más flexibilidad para el uso de bastidores o racks de varias alturas. Es necesario coordinar su colocación con las otras instalaciones de iluminación, tuberías, conductos de aire, sistema de alimentación eléctrica, etc., que también están instalados en el techo.

Este sistema permite además utilizar diversas alturas para organizar el cableado de datos y alimentación en diferentes capas, tal como se muestra en la imagen:

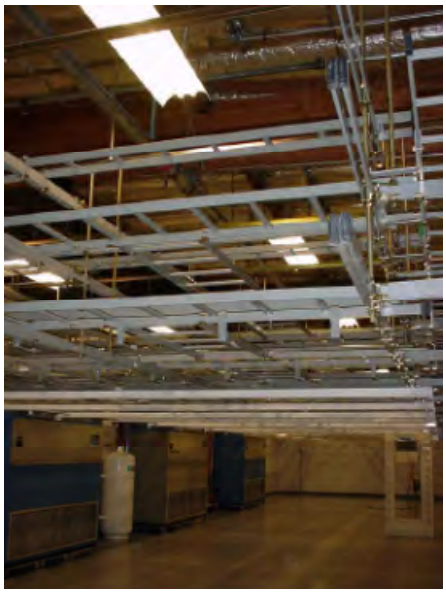


Figura 56 Canaletas de distribución aérea [**49**]

4.4.7.3 Recomendaciones de cableado

Hay disponibles una gran cantidad de tipos de cables para cubrir las necesidades y tamaños de las diferentes conexiones dentro de un CPD. Principalmente se pueden agrupar en tres grupos:

- Cable coaxial.
- Cable de par trenzado (apantallado y no apantallado).
- Cable de fibra óptica.

Cable Coaxial

Presenta propiedades mucho más favorables frente a interferencias y a la longitud de la línea de datos, de modo que el ancho de banda puede ser mayor. Esto permite una mayor concentración de las transmisiones analógicas o más capacidad de las transmisiones digitales.

Su estructura es la de un cable formado por un conductor central macizo o compuesto por múltiples fibras al que rodea un aislante dieléctrico de mayor diámetro. Una malla exterior aísla de interferencias al conductor central. Por último, utiliza un material aislante para recubrir y proteger todo el conjunto. Presenta condiciones eléctricas más favorables.

En redes de área local se utilizan dos tipos de cable coaxial: fino y grueso. Tiene una capacidad de llegar a anchos de banda comprendidos entre los 80Mhz y los 400Mhz (dependiendo de si es fino o grueso). Esto quiere decir que en transmisión de señal analógica se puede tener del orden de 10.000 circuitos de voz.

Hay dos tipos de cable coaxial:

- Cable fino (Thinnet): es un cable coaxial flexible de unos 0,64 centímetros de grueso (0,25 pulgadas). Este tipo de cable se puede utilizar para la

mayoría de los tipos de instalaciones de redes, ya que es un cable flexible y fácil de manejar.

- Cable grueso (Thicknet): es un cable coaxial relativamente rígido de aproximadamente 1,27 centímetros de diámetro. Al cable Thicknet a veces se le denomina Ethernet estándar debido a que fue el primer tipo de cable utilizado con la conocida arquitectura de red Ethernet. El núcleo de cobre del cable Thicknet es más grueso que el del cable Thinnet. Cuanto mayor sea el grosor del núcleo de cobre, más lejos puede transportar las señales.

En lo que respecta a las recomendaciones sobre el tipo de cable que hay que utilizar en los Centros de Datos, según la normativa TIA-942, se requiere que el tipo de cable sea cable coaxial de 75Ω Tipo 734 ó 735 con conector coaxial tipo T1.404.

Cable Par Trenzado

El cable par trenzado está compuesto de conductores de cobre aislados por papel o plástico y trenzados en pares. Esos pares son después trenzados en grupos llamados unidades, y estas unidades son a su vez trenzadas hasta tener el cable terminado que se cubre por lo general por plástico. El trenzado de los pares de cable y de las unidades disminuyen el ruido de interferencia, mejor conocido como diafonía. Los cables de par trenzado tienen la ventaja de no ser caros, ser flexibles y fáciles de conectar, entre otras.

Como medio de comunicación tiene la desventaja de tener que usarse a distancias limitadas ya que la señal se va atenuando y puede llegar a ser imperceptible; es por eso que a determinadas distancias se deben emplear repetidores que regeneren la señal.

Los cables de par trenzado se llaman así porque están trenzados en pares. Este trenzado ayuda a disminuir la diafonía, el ruido y la interferencia. El trenzado es en promedio de tres trenzas por pulgada. Para mejores resultados, el trenzado debe ser variado entre los diferentes pares.

Existen dos tipos de cable par trenzado:

1.- UTP (Unshielded Twisted Pair Cabling), o cable par trenzado sin blindaje

2.- STP (Shielded Twisted Pair Cabling), o cable par trenzado blindado

En lo que respecta a las recomendaciones sobre el tipo de cable que hay que utilizar en los Centros de Datos, según la normativa TIA-942, se requiere que el tipo de cable sea un cable de cobre par trenzado de 100Ω, como mínimo de Categoría 3 o 5e, aunque se recomienda de Categoría 6.

Cable de Fibra Óptica

Es un filamento de vidrio sumamente delgado diseñado para la transmisión de la luz. Las fibras ópticas poseen enormes capacidades de transmisión, del orden de miles de millones de bits por segundo. Además de que los impulsos luminosos no son afectados por interferencias causadas por la radiación aleatoria del ambiente. Actualmente la fibra óptica está remplazando en grandes cantidades a los cables comunes de cobre.

Actualmente se utilizan tres tipos de fibras ópticas para la transmisión de datos:

- Monomodo:. Permite la transmisión de señales con ancho de banda hasta 2GHz.
- Multimodo de índice gradual: Permite transmisiones hasta 500MHz.

- Multimodo de índice escalonado: Permite transmisiones hasta 35MHz.

Se han llegado a efectuar transmisiones de decenas de miles de llamadas telefónicas a través de una sola fibra, debido a su gran ancho de banda. Otra ventaja es la gran fiabilidad, su tasa de error es mínima. Su peso y diámetro la hacen ideal frente a cables de pares o coaxiales. Normalmente se encuentra instalada en grupos, en forma de mangueras, con un núcleo metálico que les sirve de protección y soporte frente a las tensiones producidas. Su principal inconveniente es la dificultad de realizar una buena conexión de distintas fibras con el fin de evitar reflexiones de la señal, así como su fragilidad.

En lo que respecta a las recomendaciones sobre el tipo de cable que hay que utilizar en los Centros de Datos, según la normativa TIA-942, se requiere que el tipo de cable sea:

- Fibra Óptica Multimodo: 62.5/125 μm ó 50/125 μm, aunque se recomienda fibra multimodo 50/125 μm optimizada para láser de 850nm.
- Fibra Óptica Monomodo 9/129 μm.

Para minimizar el volumen de cables y su caótica distribución en el falso suelo, o sobre la distribución aérea, si fuese el caso, se utilizarán cables troncales de 8 a 144 fibras para la conexión entre CPLs y los componentes hardware, dependiendo del número de puertos/adaptadores disponibles (por ejemplo, en lugar de 36 cables con dos fibras, usar un solo cable con 72 fibras. Un terminal con conectores MTP de 12 fibras el otro Terminal con conectores dúplex SFF. Los soportes de los transceptores utilizados en la máquina, se adaptarán a los conectores MTP.

También la norma TIA- 942 incluye recomendaciones sobre las distancias horizontales máximas de los cables:

- La máxima distancia del cableado en horizontal debe ser de 90 metros independientemente del tipo de medio.
- La distancia máxima entre canales, incluyendo los conectores, es de 100 metros.
- La máxima distancia de los cables en el centro de datos, sin contar con la distribución horizontal, es de 300 metros para los canales de fibra óptica, incluyendo los conectores, y de 100 metros para el cableado de pares de cobre, incluyendo los conectores.

Historia del proyecto

Elaboración del proyecto

La elaboración de este proyecto se divide en tres fases específicas:

1. **Concepción y estructuración inicial**, en la que se hizo un análisis de la norma TIA-942 y se definieron los objetivos y la estructura del documento, y se diseñó el escenario de partida, esto es, la estructura y situación inicial de la compañía ZEREPSA.
2. **Diseño de la solución**, en la que se dividieron las diferentes frentes de trabajo, divididas en:
    a. Solución - Infraestructura de soporte
        i. Diseño del edificio
        ii. Sistemas de Aire
        iii. Sistemas Eléctricos
        iv. Arquitectura salas de enlaces
        v. Protección contraincendios
        vi. Otros sistemas
    b. Solución - Infraestructura de comunicaciones
        i. Aplicación
        ii. Red
        iii. Físico

    Se paralelizaron todas las frentes, dividiendo el trabajo en tres momentos: **estudio, solución alto nivel y solución detallada** que entrelazaban todas las frentes, de modo que primero se hizo el estudio para todas las frentes, para seguir con la solución alto nivel para todas las frentes y finalmente detallar la solución.
3. **Revisión y correcciones** al material elaborado.

El cronograma se detalla en el Anexo E - Cronograma detallado de la elaboración del proyecto, del que se muestra un resumen en la siguiente figura.

ID	Task Name	Duration	Start	Finish
1	Concepción y estructuración	110 days	14/08/10 11:00	14/01/11
2	Diseño de la solución	790,25 days	16/01/11 14:00	24/01/14
3	Estudio	170 days	16/01/11 14:00	09/09/11 14
4	Solución alto nivel	265 days	10/09/11 11:00	14/09/12
5	Solución detallada	355 days	16/09/12 16:00	24/01/14
6	Revisión y correcciones	35 days	01/02/14 09:00	21/03/14
7	Revisión y correcciones	35 days	01/02/14 09:00	21/03/14

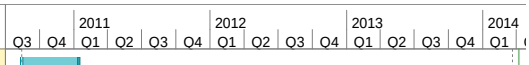


Figura 57 Cronograma de la elaboración del proyecto

Los esfuerzos y costes de la elaboración se muestran en la tabla a continuación.

Recursos	Esfuerzo total	U.m.	Tasa	**TOTAL**
Alumno	3.336	horas	9 €/hora	**€ 30.024,00**

Profesor	112	horas	16 €/hora	**€ 1.792,00**
Total Recursos				**€ 31.816,00**
Material	Cantidad	u.m.	Valor	**TOTAL**
Subscripción normas UNE	2	años	€ 99,00	**€ 198,00**
Adquisición TIA-942	1	unidad	€ 450,00	**€ 450,00**
Equipos	1	unidad	€ 600,00	**€ 600,00**
Total Material				**€ 1.248,00**
Total				**€ 33.064,00**

Tabla 21 Costes de elaboración del proyecto

Ejecución del proyecto

Debido al volumen de tareas a ejecutar para ejecutar el proyecto del centro de respaldo sólo se elabora un presupuesto alto nivel, considerando los capítulos descritos en el documento, y basado en los valores de mercado publicados en diversas fuentes de sector en España [***55***] [***55***] [***56***] Este presupuesto debe servir como guía a la hora de solicitar las ofertas para los proveedores, como queda descrito en el apartado Conclusiones y trabajos futuros.

Concepto			**Total**
01 Obra civil			**600.000 €**
02 Climatización y AA			**375.000 €**
	02.01 Climatización salas técnicas		200.000 €
	02.02 AA general		175.000 €
03 Electricidad			**1.375.000 €**
	03.01 Transformadores		325.000 €
	03.02 SAIs y grupo electrógeno		300.000 €
	03.03 Instalación eléctrica general		750.000 €
04 Seguridad y control de accesos			**350.000 €**
05 Protección contra incendios			**525.000** €
	05.01 Extinción sala técnica		200.000 €
	05.02 Extinción general		325.000 €
06 Redes de datos			**1.250.000 €**
	06.01 Acometidas y puntos de conexión		300.000 €
	06.02 Redes sala técnica		750.000 €
		06.02.01 Cableado	150.000 €
		06.02.02 Electrónica de red	600.000 €
	06.03 Redes generales		200.000 €
07 Equipos			**7.050.000 €**
	07.01 Equipos sala técnica		**6.750.000** €
		07.01.01 Servidores de alta capacidad	5.000.000 €
		07.01.02 Servidores medios	1.750.000 €

	07.02 Equipos de uso general	300.000 €
08 Red de almacenamiento		**4.000.000 €**
09 DMZ y nodo int-net		**3.250.000 €**
	09.01 Electrónica de red	2.000.000 €
	09.02 Proxy, firewall y accesos remotos	700.000 €
	09.03 Servidores	550.000 €
Total General		**18.775.000 €**

Tabla 22 Presupuesto de alto nivel de ejecución del centro de respaldo

Conclusiones y trabajos futuros

Las TIC dan soporte a toda la organización; si bien su funcionamiento correcto no es visible en las operaciones diarias, una disfunción (temporal o permanente) produce un gran impacto en todos los niveles organizativos. Para diseñar una solución que minimice este impacto es necesario tener un conocimiento del uso de las TIC que hace la organización para priorizar objetivos y enfocar los esfuerzos. En este sentido es necesaria una buena comunicación entre las áreas clientes y las áreas de TI de la compañía que permita tomar decisiones de diseño para la solución de respaldo.

Alcanzar un CPD de alta fiabilidad requiere considerar todos los aspectos de la solución, considerando no sólo las soluciones TIC sino también los elementos que las soportan. Esto convierte la solución al problema en un proyecto multidisciplinar, en el que se combinan soluciones arquitectónicas e industriales con soluciones de telecomunicaciones e informática.

La norma TIA-942 es un marco para el diseño de alto nivel, definiendo requisitos específicos a cumplir en cada campo multidisciplinar, desde la arquitectura de red hasta el control ambiental, pasando por la gestión energética o el control de accesos. La norma sin embargo deja amplio margen para las decisiones de más bajo nivel, que tienen que basarse en otros criterios, ya sea la normativa local específica (diseminada entre los diferentes campos de conocimiento y órganos normativos), las mejores prácticas de la industria (no siempre públicas o bien documentadas), los recursos disponibles o las políticas específicas de la compañía. Esto convierte la tarea del diseño de un centro de datos un trabajo único, basado en una receta general pero que toma forma basado en innúmeras soluciones de compromiso tomadas para cada situación específica.

Si bien este proyecto cubre todos los elementos de la solución del centro de respaldo, este sólo un punto de inicio para la organización, que deberá dar continuidad a las tareas, hasta el momento de entrada en funcionamiento del centro. Entre los trabajos futuros decurrentes de este proyecto están los siguientes:

- **Análisis del ROI y factores económicos** de la implementación del centro de respaldo para la empresa, considerando los costes de pérdidas de servicio frente a la inversión inicial y los costes de operación de este centro.
- **Segmentar los componentes de la solución**, de forma que se puedan abordar por equipos diferentes que gestionen las siguientes fases del centro, siempre respondiendo a un órgano de coordinación. La primera tarea de este órgano será definir un plan de proyecto y un cronograma de alto nivel, considerando las dependencias entre cada componente y las necesidades de la organización.
- Una vez identificado el cronograma y apoyado en los presupuestos de alto nivel, se deberán **detallar las diferentes solicitudes de ofertas** para los procesos de contratación de cada componente. Dentro de estas solicitudes de ofertas será especialmente importante la relacionada con los servicios de conectividad entre centros y la conexión con la red WAN de la compañía, así como las acometidas de red de los diferentes proveedores.

- Será también necesario **definir los procesos de trabajo del centro de respaldo**, y englobarlos en los procesos de gestión TIC de la compañía, ya que para cada acción en los sistemas de la compañía deben considerarse los impactos en el centro de respaldo. Por ejemplo, un proyecto de implantación de un nuevo sistema debe considerar en el presupuesto también las necesidades de réplica en el centro de respaldo.
- De igual modo, se deberá **dimensionar el equipo profesional** del centro de respaldo, definiendo cargos, especialidades y carreras profesionales y considerar este personal adicional en los presupuestos de RH del área de TI.
- Dentro de los trabajos de detalle necesarios cabe resaltar las tareas de **diseño detallado de las redes**, incluyendo la evaluación de los diferentes proveedores de equipos de red y las posibles soluciones específicas de cada proveedor dentro de la estrategia de red ya definida, la implantación de un proyecto piloto que sirva como **prueba de concepto** de las soluciones adoptadas, y finalmente los detalles de configuración de los diferentes elementos de red del centro, así como la numeración y segmentación detallada de las redes.

Además de los trabajos específicos a la construcción y puesta en marcha del centro de respaldo, se proponen algunos planos de trabajo paralelos, orientados todos a aprovechar al máximo la inversión en el centro. Todos estos trabajos precisan primero de una fase de análisis de viabilidad y fundamentos teóricos y prácticos, que a su vez pueden convertirse en proyectos de entidad propia.

- Utilización del centro de datos de respaldo en combinación con el centro principal para **monitorizar el parque de aplicaciones**, identificando aplicaciones y servidores no identificados o no utilizados (por ejemplo, basado en el tráfico de réplica de datos hacia el centro de respaldo), y proporcionando una estrategia de baja de los servicios (por ejemplo, manteniendo la copia del centro de respaldo durante un tiempo tras la baja en el centro principal).
- Ya que el centro de respaldo posee conexiones con diferentes proveedores que no son utilizadas normalmente, surge la posibilidad de **utilizar los puntos de acceso como puntos de interconexión entre proveedores** (puntos neutros), encaminando paquetes entre los diferentes proveedores cuando estos recursos no sean utilizados por el centro de respaldo, lo que puede reducir los costes de conexión.
- Dado el uso de virtualización y granjas de servidores, se puede contemplar la disponibilización de recursos del centro de respaldo para empresas del grupo o socios comerciales, **ofreciendo servicios de colocalización**, permitiendo a terceros el acceso al centro, u **ofreciendo servicios de computación en la nube** que, en caso de caída del centro principal, puedan desactivarse o encaminarse a otros centros de la nube sin interrumpir los servicios.
- Investigar métodos para mantener bajos los costes del centro de datos; en particular los costes energéticos. Entre estos métodos se encuentra la utilización de soluciones de **gestión de energía basada en aplicaciones** (Application Aware Power Management [***55***] [***58***] [***58***]), ya sea basadas en soluciones comerciales como las de TSO Logic [***57***] o en nuevas soluciones, por ejemplo basadas en monitorización y virtualización. Este tipo de soluciones buscan reducir el consumo de energía de los servidores cuando

las aplicaciones basado en la demanda de cada aplicación, llegando a detener los servidores si estas no son utilizadas.

- Basado en las tendencias actuales, ZEREPSA está analizando la implantación de soluciones de análisis masivo de datos (Big Data Analytics), que se basan en la recolección de grandes volúmenes de informaciones. Si bien este es un proyecto a medio-largo plazo, el **respaldo de Big Data** requiere que el sistema pueda respaldar grandes volúmenes de datos en tiempo real [***58***], introduciendo nuevos retos de diseño en la red y en las estrategias de almacenamiento.

Referencias y Bibliografía

[1] Telecommunications Industry Association, *TIA-942 Telecommunications Infrastructure Standard for Data Centers*.: TELECOMMUNICATIONS INDUSTRY ASSOCIATION, 2005.

[2] Kevin Roebuck, *Business Impact Analysis (BIA): High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors*.: Emereo Pty Limited, 2011.

[3] Contingency Planning Research, Inc., *Contingency Planning Research, Inc.*, 1995.

[4] Varios, *MAGERIT versión 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*.: Ministerio de Hacienda y Administraciones Públicas, 2012, http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

[5] Centro Criptológico Nacional. (2014) EAR / PILAR 5.3.1 - Entorno de Análisis de Riesgos. [Online]. https://www.ccn-cert.cni.es/index.php?option=com_wrapper&view=wrapper&Itemid=213&lang=es

[6] Ministerio de Fomento - Gobierno de España, *Código Técnico de la Edificación - Parte I.*, 2013, http://www.codigotecnico.org/cte/export/sites/default/web/galerias/archivos/Parte_I_28jun2013.pdf.

[7] AEN/CTN 108, *EN 1047-1:2005 Unidades de almacenamiento de seguridad. Clasificación y métodos de ensayo de resistencia al fuego. Parte 1: Muebles ignífugos y contenedores para soportes sensibles.*: AENOR, 2006.

[8] AEN/CTN 108, *EN 1047-2:2009+A1:2013 Unidades de almacenamiento de seguridad. Clasificación y métodos de ensayo de resistencia al fuego. Parte 2: Cámaras y contenedores ignífugos.*: AENOR, 2013.

[9] Bruce Robertson and Valentin Sribar, *The Adaptive Enterprise: IT Infrastructure Strategies to Manage Change and Enable Growth*.: Intel Press, 2002.

[10] Victor Avelar, *Guidelines for Specifying Data Center Criticality / Tier Levels*.: American Power Conversion, 2007.

[11] Hewlett-Packard Development Company, L.P, *HP Power Advisor utility: a tool for estimating power requirements for HP ProLiant server systems*., 2009.

[12] Sun Microsystems, Inc., *Sun Microsystems Data Center Site - Data Centers' Best Practices*., 2003.

[13] W. Timothy Coombs, *Security Self-Assesment Guide for Information Technology Systems*., 2008.

[14] Cristina Vega Giménez, *Reglamento de seguridad contra incendios enestablecimientos industriales (RD 2267/2004)*.: Centro Nacional De Condiciones de Trabajo - Instituto Nacional de Seguridad e Higiene en el Trabajo, 2004.

[15] OLARETTA Serivicios Generales SAC.. Guía para la selección del piso técnico. [Online]. http://www.olaretta.com/index.php?option=com_content&view=article&id=62&Itemid=94&showall=1

[16] Peter Neufert Ernst Neufert, *Architects' Data*.: Wiley-Blackwell, 2012.

[17] Carrier, *Manual de aire acondicionado*.: Marcombo, 1972.

[18] P. Nuno, J. L. Rivas, and J. E. Ares. (2006, May) Climatización en los Centros de Proceso de Datos. [Online]. https://www.rediris.es/difusion/publicaciones/boletin/76/enfoque2.pdf

[19] Prime Energy IT, *Infraestructura y hardware informático energéticamente eficiente - Ejemplos de las mejores prácticas*.: Austrian Energy Agency, 2012, http://www.efficient-datacenter.eu/fileadmin/docs/dam/best_practice/es/Best_practice_ES.pdf.

[20] AEN/CTN 100 - CLIMATIZACIÓN, *Filtros de aire utilizados en ventilación general para eliminación de partículas. Determinación de las prestaciones de los filtros.*: AENOR, 2013.

[21] Peter Hannaford, *Diez pasos para resolver los problemas de enfriamiento ocasionados por la implementación de servidores de alta densidad*.: American Power Conversion (APC), 2005.

[22] Gunt Hamburg. Montaje de un sistema de aire acondicionado. [Online]. http://www.gunt.de/download/setup%20of%20air%20con%20systems_spanish.pdf

[23] Mapfre. (2007, Jan.) Seguridad en centros de procesamiento de datos. [Online]. http://www.mapfre.com/documentacion/publico/i18n/catalogo_imagenes/grupo.cmd?path=1030491

[24] Cristina Miralles Cid, *Control y Gestión integrada de un Edificio Inteligente para Oficinas (Proyecto Final de Carrera)*.: Escola Técnica Superior Enginyeria - Universitat Rovira I Virgili, Septiembre 2006. [Online].

http://deeea.urv.cat/public/PROPOSTES/pub/pdf/520pub.pdf

[25] CommScope, *CommScope® Enterprise Data Center Design Guide*.: CommScope, 2011.

[26] SERVICIO MADRILEÑO DE SALUD. (2010, Septiembre) PROYECTO DE CENTRO DE PROCESO DE DATOS HOSPITAL 12 DE OCTUBRE. [Online]. http://www.madrid.org/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadervalue1=filename%3DProyecto+CPD-203592.pdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1271827309716&ssbinary=true

[27] Alex Bustos. (2011, Junio) Schneider Electric - TBB Brasil - Tecnologias de Transformadores Secos Encapsulados. [Online]. http://www.schneider-electric.com.co/documents/eventos/memorias-jornadas-conecta/Seguridad/tecnologias-transf-secos-encapsulados.pdf

[28] Amper Online. Definición de aspectos eléctricos (UPS y Grupo Generador) a ser tomados en cuenta al momento de diseñar un Centro de Datos (CPD). [Online]. http://www.amperonline.com/biblioteca/art-principal-boletin4.pdf

[29] Otae. (2005) Enchufes & electricidad en los países del mundo. [Online]. http://www.otae.com/enchufes/enchufes.htm

[30] Ronald B. Standler, *Mittigation of Disturbances on Mains*.: Courier Dover Publications, 2002.

[31] UCA - Área de Informática, *Anteproyecto del expediente de contratación de Proyecto y obra de adecuación de espacios del Centro de Proceso de Datos de la UNIVERSIDAD DE CÁDIZ*.: Vicerrectorado de Tecnologías de la Información e Innovación Docente, 2009.

[32] Leland H. Hemming, *Architectural Electromagnetic Shielding Handbook: A Design and Specification Guide*.: John Wiley & Sons, 2000.

[33] Douglas Alger, *Build the Best Data Center Facility for Your Business*.: Cisco Press, 2005.

[34] España, *Apéndice I - Características e instalaciones de los aparatos, equipos y sistemas de protección contra incendios*.: La Ley, 2005.

[35] Robert F. Halper, *Computer Data Center Design: A Guide to Planning, Designing, Constructing, and Operating Computer Data Centers*.: Wiley-Interscience, 1985.

[36] Douglas Landoll, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*.: CRC Press, 2011.

[37] Jesús Manuel Quintela Cortés, *Instalaciones contra incendios*.: UOC, 2008.

[38] José Antonio Neira Rodríguez, *Instalaciones de acción previa o preacción*.: FC Editorial.

[39] VMware inc., *Consolidating Web Applications Using VMware Infrastructure*., 2008.

[40] VMware, inc., *Virtualization Overview*., 2006.

[41] Hewlett-Packard Development Company, L.P., *Accelerate deployment of mission-critical virtualization on Integrity Superdome 2 servers*., 2012, http://h20195.www2.hp.com/V2/GetPDF.aspx/4AA3-7324ENW.pdf.

[42] Cisco Systems Learning, *Designing Cisco Data Center Unified Fabric - Student Guide*.: Cisco, 2012.

[43] IETF, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*., 2010.

[44] Wikipedia contributors. (2014, Feb.) Link aggregation. [Online]. http://en.wikipedia.org/w/index.php?title=Link_aggregation&oldid=596874881

[45] WG802.1 - Higher Layer LAN Protocols Working Group, *802.1Q-2011 - IEEE Standard for Local and metropolitan area networks--Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks*.: IEEE Computer Society, 2011.

[46] Iljitsch van Beijnum. (2002, Dec.) A Look at Multihoming and BGP. [Online]. http://www.oreillynet.com/pub/a/network/2002/08/12/multihoming.html

[47] Rago Dragic. IT - Informatics Alphabet. [Online]. http://www.informatics.buzdo.com/p928-intranet-structured-cabling.htm

[48] Telecommunications Industry Association, *TIA-568 - Commercial Building Telecommunications Cabling Standard*.: Telecommunications Industry Assn. (TIA), 2012.

[49] B&K Internet Service. Systemerweiterungen im vergleich. [Online]. http://bk-is.de/index.php?article_id=313

[50] Belkin Business. (2013) Catalog - Patch Panels & Rack Accessories. [Online]. http://www.belkinbusiness.com/search_products/patch-panels-rack-accessories?cat_id=277

[51] Chris DiMinico. SlideShare - Telecommunications Infrastructure Standard for Data Centers. [Online]. http://pt.slideshare.net/datacenters/microsoft-powerpoint-tia942-datacenter-infrastructure-standard

[52] CableOrganizer.com. (2014) Cable Organizer - Ties, Clips & Wraps for Cabinets, Racks, Enclosures. [Online]. http://www.cableorganizer.com/computer-cabinets/clips-wraps-ties.html

[53] Fiber Optics Online. ADC Telecommunications Optical Distribution Frame. [Online]. http://www.fiberopticsonline.com/doc/optical-distribution-frame-0001

[54] ADC Telecommunications, Inc., *Bastidor Principal para Distribución de Fibras (FMDF) Guía de Enrutamiento de Cables para FOTSB.*, 2004.

[55] Ministerio de Hacienda y Administraciones Públicas de España - Secretaría General Técnica, *Informe REINA 2013 - Las Tecnologías de la Información y las Comunicaciones en la Administración del Estado*. Madrid, 2013.

[56] Adjudicaciones TIC. (2014, Mar.) Adjudicaciones TIC. [Online]. http://www.adjudicacionestic.com/inicio

[57] Heather Hanson, Juan Rubio, Soraya Ghiasi and Freeman Rawson Karthick Rajamani, "Application-Aware Power Management," IBM Austin Research Lab and The University of Texas at Austin, 2006.

[58] A.A. Bhattacharya, D. Culler, A. Kansal, S. Govindan, and S. Sankar, *The need for speed and stability in data center power capping.*, 2012.

[59] TSO Logic. (2014, Feb.) Energy efficiency software for data centers. [Online]. http://tsologic.com/data-center-power-management/

[60] George Crump. (2011, Oct.) Big Data A Big Backup Challenge - Information Wiik. [Online]. http://www.informationweek.com/data-protection/big-data-a-big-backup-challenge/d/d-id/1098260

[61] José Francisco Quesada Moreno. Consejería Justicia y Administración Pública. Junta de Andalucía. [Online]. http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Tecnimap/pae_TECNIMAP_2004/pae_COM_2004-Perspectivas_de_futuro/6_017.pdf

[62] Euro Segur. UNE EN 1627 - Resistencia a la Efracción de las puertas. [Online]. http://www.eurosegur.com/w/87/une-en-1627

[63] AEN/CTN 85, *UNE-EN 1627:2011 - Puertas peatonales, ventanas, fachadas ligeras, rejas y persianas. Resistencia a la efracción. Requisitos y clasificación.*, 2011.

[64] ADO S.A. Catálogo Puertas Cortafuegos. [Online]. http://issuu.com/adocerramientosmetalicos/docs/puertas_corfafuegos_rf__cortafuegos_de_madera/1?e=0

[65] Novoferm - Alsal. Catálogo Bemo® Puertas cortafuegos EI230, EI260, EI290 y fijos EI230, EI260, EI290 y Antihumos. [Online]. http://www.novofermalsal.com/web/media_get.php?mediaid=5929&fileid=10271

Anexos

Anexo A - ÁREAS Y PROCESOS

A.I Áreas y procesos de ZEREPSA

La compañía se encuentra dividida en los siguientes departamentos:

- **Planificación, control y dirección estratégica**, cuyos procesos principales son la dirección estratégica, la planificación de recursos, I+D e infraestructuras, relaciones externas e institucionales y gestión y seguimiento de crisis.
- **Operaciones**, cuyos procesos principales son la planificación operativa, la ejecución y gestión operacional (explotación marítima y terrestre), la coordinación y logística de operaciones, gestión cartográfica, meteorológica y oceanográfica, evaluación y gestión del personal, y apoyo TIC a las operaciones.
- **Personal**, cuyos principales componentes son los procesos de recursos humanos, sanidad, seguros de personal, alojamiento del personal (incluyendo la gestión de instalaciones propias de alojamiento).
- **Económica**, que realiza los procesos económicos tales como gestión de contabilidad, gestión de activos, facturación tesorería y presupuestos. También realiza procesos de financiación y compras.
- **Recursos**, encargada de la gestión logística (ya sea a nivel global o a nivel local), la programación de recursos, control de activos, gestión de infraestructuras (incluyendo infraestructuras de extracción), inspección de infraestructuras, ingeniería e I+D.
- **Cultura y promoción**, encargada de los procesos de marketing, gestión de publicaciones, actos culturales y actos promocionales.
- **Apoyo a la organización**, encargada de procesos horizontales a toda la organización, como gestión de la documentación y mensajería (incluyendo documentación internacional o de acceso restringido), seguridad, normalización y calidad y servicios jurídicos. Dentro de este departamento se incluye el área de TI, cuyos procesos principales son la gestión de proyectos y la sustentación de la operación. En el apartado A.II se detallan los procesos relacionados con la sustentación de la operación.

A.II Procesos y servicios TIC de ZEREPSA

Dentro del departamento de TI de ZEREPSA, se definen dos áreas principales, gestión de proyectos y sustentación de la operación.

El área de gestión de proyectos se encarga de la coordinación y seguimiento de proyectos, desde la identificación de la necesidad inicial hasta la implantación y estabilización de los mismos.

El área de sustentación de la operación es responsable de los servicios TIC una vez implantados, y de las plataformas sobre las que se apoyan. Siendo así, este área define los procesos en los siguientes bloques, cada uno encuadrado en una gerencia:

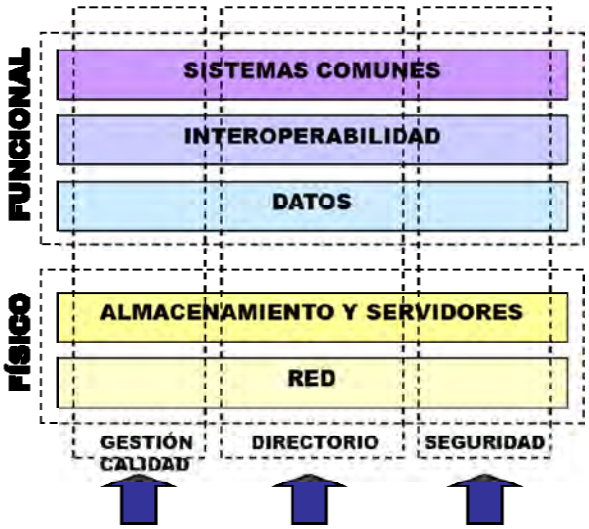


Figura 58 Matriz de procesos TIC de sustentación

- **Sistemas comunes** agrupa la plataforma principal, definiendo el nivel de sistemas operativos, servicios web, suites ofimática y colaboración y servicios de terminal.
- **Interoperabilidad** agrupa los servicios de integración, middleware, soluciones de arquitectura orientada a servicios (SOA), mensajería asíncrona y estructura canónica de servicios.
- **Datos** se encarga de los servicios de bases de datos, inteligencia de negocio (BI), almacén de datos (Data Warehouse) y modelo de datos corporativo.
- **Almacenamiento y servidores** gestiona el hardware físico de servidores y servidores de almacenamiento (SAN, cintas, etc.).
- **Red** consiste en la supervisión y control de redes y la infraestructura relacionada.

Anexo B - CENSO Y PRIORIZACIÓN DE APLICACIONES

Las aplicaciones censadas en el centro principal, y su distribución entre las áreas se detallan en la siguiente tabla, ordenadas por prioridad:

Aplicación	Prioridad	Entorno	Tecnología
Almacén del departamento y gerencias	Muy Alta	Host	Host
Análisis y niveles de disponibilidad	Muy Alta	Superdome	Superdome
Antivirus corporativo	Muy Alta	SUN Solaris	SunFire X4200
Apertura y cierre de pozos	Muy Alta	SUN Solaris	SunFire 69000
Aplicaciones informáticas para los grupos de gestión económica	Muy Alta	Windows/Linux	HP ProLiant DL
Apoyo a la investigación y la ingeniería	Muy Alta	Blades	HP ProLiant BL
Apoyo al empleo	Muy Alta	Host	Host
Atención de llamadas	Muy Alta	Superdome	Superdome
Base de reconocimiento de subsuelo	Muy Alta	Blades	HP ProLiant BL
Centro de investigación	Muy Alta	Blades	HP ProLiant BL
Centro de producción 1	Muy Alta	Host	Host
Centro de producción 10	Muy Alta	SUN Solaris	SunFire X4200
Centro de producción 11	Muy Alta	Blades	HP ProLiant BL
Centro de producción 12	Muy Alta	SUN Solaris	SunFire 69000
Centro de producción 2	Muy Alta	Superdome	Superdome
Centro de producción 3	Muy Alta	Blades	HP ProLiant BL
Centro de producción 4	Muy Alta	SUN Solaris	SunFire 69000
Centro de producción 5	Muy Alta	Blades	HP ProLiant BL
Centro de producción 6	Muy Alta	Windows/Linux	HP ProLiant DL
Centro de producción 7	Muy Alta	Blades	HP ProLiant BL
Centro de producción 8	Muy Alta	Blades	HP ProLiant BL
Centro de producción 9	Muy Alta	Host	Host
Combustibles	Muy Alta	Blades	HP ProLiant BL
Contratación en el extranjero	Muy Alta	DMZ	HP ProLiant DL
Control de cálculos y diseño	Muy Alta	Superdome	Superdome
Control de combustibles	Muy Alta	HP-UX	HP ProLiant DL
Control de vehículos	Muy Alta	Superdome	Superdome
Ctrlcolas	Muy Alta	Windows/Linux	HP ProLiant DL
Datos de recambios y logísticos	Muy Alta	SUN Solaris	SunFire 69000

Depósitos	Muy Alta	Superdome	Superdome
Directorio corporativo	Muy Alta	SUN Solaris	SunFire X4200
Dominio corporativo	Muy Alta	HP-UX	HP ProLiant DL
Dote (documentación técnica)	Muy Alta	Superdome	Superdome
Empresa-101	Muy Alta	Blades	HP ProLiant BL
Estado de los activos infraestructura	Muy Alta	Blades	HP ProLiant BL
Estudios	Muy Alta	SUN Solaris	SunFire 69000
Evolución de plantilla	Muy Alta	Superdome	Superdome
Fasempleo	Muy Alta	DMZ	HP ProLiant DL
Gestión de activos y distribución para el departamento	Muy Alta	Windows/Linux	HP ProLiant DL
Gestión de calidad del software	Muy Alta	SUN Solaris	SunFire 69000
Gestión de integración	Muy Alta	Blades	HP ProLiant BL
Gestión de oleoductos	Muy Alta	Blades	HP ProLiant BL
Gestión presupuestaria	Muy Alta	SUN Solaris	SunFire 69000
Grupos de análisis de suelos y búsqueda de bolsas	Muy Alta	Superdome	Superdome
Grupos de prospección	Muy Alta	SUN Solaris	SunFire 69000
Helpdesk departamento	Muy Alta	Superdome	Superdome
Información empleo	Muy Alta	DMZ	HP ProLiant DL
Informes de dirección	Muy Alta	DMZ	HP ProLiant DL
Infraestructuras	Muy Alta	SUN Solaris	SunFire 69000
Infraestructuras de plataforma	Muy Alta	Blades	HP ProLiant BL
Ingeniería y desarrollo	Muy Alta	SUN Solaris	SunFire X4200
Intranet	Muy Alta	DMZ	HP ProLiant DL
Jubilaciones	Muy Alta	SUN Solaris	SunFire 69000
Lanzadera	Muy Alta	SUN Solaris	SunFire X4200
Legal y judicial	Muy Alta	Blades	HP ProLiant BL
Material e infraestructuras de la empresa	Muy Alta	SUN Solaris	SunFire 69000
Medioambiente	Muy Alta	Host	Host
Modulo de personal directivo	Muy Alta	Superdome	Superdome
Monitorización	Muy Alta	Superdome	Superdome
Monitorización del sistema logístico	Muy Alta	Blades	HP ProLiant BL
Operativa anual	Muy Alta	Blades	HP ProLiant BL
Pensiones - 1090	Muy Alta	Blades	HP ProLiant BL
Personal	Muy Alta	Blades	HP ProLiant BL
Personal y plan de carrera	Muy Alta	SUN Solaris	SunFire 69000
Planificación de la obtención del	Muy Alta	SUN Solaris	SunFire X4200

material y las infraestructuras			
Potencial de operación	Muy Alta	Blades	HP ProLiant BL
Programación y seguimiento de la producción	Muy Alta	Windows/Linux	HP ProLiant DL
Programas y proyectos	Muy Alta	Windows/Linux	HP ProLiant DL
Ras	Muy Alta	Windows/Linux	HP ProLiant DL
Registro	Muy Alta	HP-UX	HP ProLiant DL
Registro general	Muy Alta	Host	Host
SAN del centro principal y datos	Muy Alta	HP-UX	HP ProLiant DL
Seguridad del departamento	Muy Alta	SUN Solaris	SunFire 69000
Seguridad a los desplazados	Muy Alta	Superdome	Superdome
Seguridad personal desplazado	Muy Alta	Superdome	Superdome
Seguridad social	Muy Alta	Blades	HP ProLiant BL
Servicios de fax y comunicaciones	Muy Alta	Host	Host
Sistema de prevención de recursos humanos	Muy Alta	HP-UX	HP ProLiant DL
Sistema de formación	Muy Alta	Blades	HP ProLiant BL
Sistema de integración de vehículos	Muy Alta	Blades	HP ProLiant BL
Sistema de mensajería	Muy Alta	DMZ	HP ProLiant DL
Sistema de seguros	Muy Alta	SUN Solaris	SunFire 69000
Sistema de selección	Muy Alta	Superdome	Superdome
Sistema general de gestión del personal	Muy Alta	Host	Host
Sistema logístico de vehículos	Muy Alta	SUN Solaris	SunFire X4200
Sistema logístico integral	Muy Alta	Otros	Otros
Sistema logístico prospección	Muy Alta	Blades	HP ProLiant BL
Sistemas de control de incidencias y acuerdos	Muy Alta	Blades	HP ProLiant BL
Sistemas de satélites	Muy Alta	Host	Host
Sistemas gis	Muy Alta	Blades	HP ProLiant BL
Tarifas y cobros	Muy Alta	Blades	HP ProLiant BL
Telefonía	Muy Alta	Superdome	Superdome
Traslados médicos	Muy Alta	Superdome	Superdome
Usabilidad	Muy Alta	SUN Solaris	SunFire 69000
Volumen colas	Muy Alta	SUN Solaris	SunFire 69000
Web del departamento	Muy Alta	DMZ	HP ProLiant DL
Catalogo productos	Alta	HP-UX	Integrity
pedidos de material	Alta	Host	Host
registro del departamento	Alta	DMZ	HP ProLiant DL
Análisis de mercado	Alta	SUN Solaris	SunFire X4200

Aplicación de repuestos del servicio de aprovisionamiento	Alta	SUN Solaris	SunFire X4200
Apoyo a la dirección	Alta	SUN Solaris	SunFire X4200
Biblioteca actuaciones técnicas de mantenimiento	Alta	Blades	HP ProLiant BL
Catalogación de productos	Alta	SUN Solaris	SunFire 69000
Competencia	Alta	Host	Host
Control de accesos a internet	Alta	Superdome	Superdome
Control de acciones telefónicas y mantenimiento	Alta	SUN Solaris	SunFire 69000
Control de aprovisionamiento y almacenes	Alta	Superdome	Superdome
Control de vehículos	Alta	Windows/Linux	HP ProLiant DL
Control incidencia de redes	Alta	Blades	HP ProLiant BL
Control vehículos	Alta	SUN Solaris	SunFire 69000
Correo electrónico	Alta	SUN Solaris	SunFire 69000
Desplazamientos	Alta	HP-UX	Integrity
Directorio corporativo	Alta	Host	Host
Distribución de software	Alta	HP-UX	Integrity
Expedientes personal	Alta	Blades	HP ProLiant BL
Geoespacial	Alta	Superdome	Superdome
Geostat	Alta	SUN Solaris	SunFire 69000
Gestión pagos	Alta	Host	Host
Gestión almacenes	Alta	Blades	HP ProLiant BL
Gestión de automóviles	Alta	SUN Solaris	SunFire 69000
Gestión de bancos	Alta	Host	Host
Gestión de los laboratorios de calibración	Alta	SUN Solaris	SunFire 69000
Gestión de pedidos	Alta	Superdome	Superdome
Gestión de provisiones y enseres	Alta	Superdome	Superdome
Gestión de variabilidad	Alta	Superdome	Superdome
Helpdesk departamento - gerencia 1	Alta	Superdome	Superdome
Helpdesk departamento - gerencia 2	Alta	Blades	HP ProLiant BL
Helpdesk departamento - gerencia 3	Alta	SUN Solaris	SunFire X4200
Helpdesk departamento - gerencia 4	Alta	SUN Solaris	SunFire X4200
Helpdesk departamento - gerencia 5	Alta	Blades	HP ProLiant BL
Inventarios	Alta	DMZ	HP ProLiant DL
Inventarios	Alta	SUN Solaris	SunFire 69000
Manuales técnicos de vehículos	Alta	SUN Solaris	SunFire 69000

Moneda extranjera	Alta	Superdome	Superdome
Motorización vehículos	Alta	Blades	HP ProLiant BL
Nominas	Alta	Blades	HP ProLiant BL
Ordenes de trabajo mantenimientos	Alta	SUN Solaris	SunFire 69000
Personal desplazado	Alta	Blades	HP ProLiant BL
Proveedores	Alta	DMZ	HP ProLiant DL
Proveedores	Alta	Host	Host
Recursos humanos del departamento	Alta	Windows/Linux	HP ProLiant DL
Registro documentación	Alta	Blades	HP ProLiant BL
Registro general	Alta	Windows/Linux	HP ProLiant DL
Repostaje de vehículos-combustibles	Alta	Blades	HP ProLiant BL
Seguridad de accesos físicos	Alta	Windows/Linux	HP ProLiant DL
Servicios gestión y aprobación peticiones GIS	Alta	Host	Host
Sistema de alimentación del personal desplazado	Alta	DMZ	HP ProLiant DL
Sistema de contratación de personal	Alta	Blades	HP ProLiant BL
Sistema de gestión inventario	Alta	Blades	HP ProLiant BL
Sistema de peticiones	Alta	Blades	HP ProLiant BL
Sistema logístico	Alta	HP-UX	Integrity
Sistemas de gestión y control de redes	Alta	HP-UX	Integrity
Solicitudes de material	Alta	Superdome	Superdome
Spectrum	Alta	DMZ	HP ProLiant DL
Telefonía fija	Alta	Windows/Linux	HP ProLiant DL
Tramitación de peticiones de accesos	Alta	Blades	HP ProLiant BL
Ubicaciones	Alta	SUN Solaris	SunFire 69000
Vestuarios	Alta	SUN Solaris	SunFire 69000
Vigilancia y control	Alta	Host	Host
Anuncios y concursos para la contratación	Media	DMZ	HP ProLiant DL
Archivo general e histórico	Media	SUN Solaris	SunFire 69000
Base de datos de pozos	Media	SUN Solaris	SunFire 69000
Biblioteca	Media	DMZ	HP ProLiant DL
Biblioteca	Media	Superdome	Superdome
Biblioteca	Media	SUN Solaris	SunFire 69000
Capacidades de distribución y transporte	Media	Blades	HP ProLiant BL
Centro de control de producción	Media	HP-UX	Integrity
Centro documentación de productos	Media	SUN Solaris	SunFire 69000

Combustibles y lubricantes vehículos	Media	Host	Host
Control amortización vehículos	Media	HP-UX	Integrity
Control de movimientos y situaciones de flota	Media	Blades	HP ProLiant BL
Control de visitas	Media	DMZ	HP ProLiant DL
Control médico personal	Media	Blades	HP ProLiant BL
Convenios nacionales	Media	Host	Host
Cuadro de mando	Media	Blades	HP ProLiant BL
Formación	Media	DMZ	HP ProLiant DL
Formación personal	Media	DMZ	HP ProLiant DL
Fórum de intercambio	Media	DMZ	HP ProLiant DL
Gastos en comunicaciones personales	Media	DMZ	HP ProLiant DL
Gestión almacén de apoyo	Media	Superdome	Superdome
Gestión calidad	Media	Blades	HP ProLiant BL
Gestión de caja	Media	Host	Host
Gestión de la calidad en los laboratorios	Media	SUN Solaris	SunFire X4200
Gestión de recursos de instalaciones de extracción y prospección	Media	SUN Solaris	SunFire X4200
Gestión de repuestos del departamento	Media	DMZ	HP ProLiant DL
Gestión de suministros del personal	Media	Superdome	Superdome
Grupos de trabajo	Media	Blades	HP ProLiant BL
Guía telefónica	Media	DMZ	HP ProLiant DL
Guías técnicas informáticas	Media	DMZ	HP ProLiant DL
Incidencias	Media	HP-UX	Integrity
Información recursos	Media	DMZ	HP ProLiant DL
Instrucciones generales	Media	DMZ	HP ProLiant DL
Instrucciones particulares	Media	SUN Solaris	SunFire X4200
Jornadas formativas	Media	SUN Solaris	SunFire 69000
Mantenimiento de las infraestructuras	Media	SUN Solaris	SunFire 69000
Material de oficina no inventariable	Media	Superdome	Superdome
Museo	Media	Blades	HP ProLiant BL
Normas y normalización	Media	Blades	HP ProLiant BL
Pagina web para el departamento	Media	DMZ	HP ProLiant DL
Parque de vehículos	Media	SUN Solaris	SunFire 69000
Pasaportes	Media	Host	Host
Personal desplazado en el exterior	Media	DMZ	HP ProLiant DL
Política empresarial	Media	DMZ	HP ProLiant DL
Política internacional	Media	DMZ	HP ProLiant DL

Presupuestos generales	Media	Host	Host
Prevención	Media	Blades	HP ProLiant BL
Procedimientos operativos (p.o.s.)	Media	Windows/Linux	HP ProLiant DL
Pruebas de estado vehículos	Media	Superdome	Superdome
Reconocimientos médicos enfermería	Media	DMZ	HP ProLiant DL
Recursos humanos	Media	Blades	HP ProLiant BL
Reporte discrepancias	Media	Blades	HP ProLiant BL
Resúmenes de prensa	Media	SUN Solaris	SunFire 69000
Revistas y difusión	Media	Host	Host
Seguridad operativa	Media	HP-UX	Integrity
Sistema de mantenimiento	Media	SUN Solaris	SunFire 69000
Sitio web del departamento	Media	DMZ	HP ProLiant DL
Tablones de las gerencias	Media	DMZ	HP ProLiant DL
Transporte	Media	Blades	HP ProLiant BL
Tratados, convenios y acuerdos	Media	DMZ	HP ProLiant DL
Unidad de normalización	Media	DMZ	HP ProLiant DL
Análisis de riesgos	Baja	Windows/Linux	HP ProLiant DL
Archivos y dotaciones vehiculares	Baja	SUN Solaris	SunFire 69000
Backup	Baja	SUN Solaris	SunFire 69000
Contratación explotación producción	Baja	Blades	HP ProLiant BL
Contratación material	Baja	Host	Host
Contratación personal	Baja	Blades	HP ProLiant BL
Control de vehículos del departamento	Baja	Blades	HP ProLiant BL
Correo	Baja	DMZ	HP ProLiant DL
Destinos y ocupaciones	Baja	DMZ	HP ProLiant DL
Dirección corporativa	Baja	SUN Solaris	SunFire X4200
Elementos productivos	Baja	Blades	HP ProLiant BL
Equipamiento y vehículos	Baja	Superdome	Superdome
Expedientes personal	Baja	Superdome	Superdome
Gestión de activos	Baja	Host	Host
Gestión de personal	Baja	Host	Host
Gestión de proveedores del grupo	Baja	DMZ	HP ProLiant DL
Gestión electrónica y hardware	Baja	Blades	HP ProLiant BL
Impresión	Baja	Host	Host
Indemnizaciones	Baja	Blades	HP ProLiant BL
Laboratorios	Baja	Superdome	Superdome
Material de análisis y prospección	Baja	SUN Solaris	SunFire 69000

Material diverso	Baja	SUN Solaris	SunFire 69000
Recursos materiales	Baja	Blades	HP ProLiant BL
Red	Baja	Blades	HP ProLiant BL
Red área local	Baja	Windows/Linux	HP ProLiant DL
Registro	Baja	Blades	HP ProLiant BL
Sistemas PKI	Baja	Blades	HP ProLiant BL
Vacaciones y permisos	Baja	Blades	HP ProLiant BL
Vacaciones	Baja	DMZ	HP ProLiant DL

Tabla 23 Censo y priorización de aplicaciones ZEREPSA

Anexo C - ESTRATEGIA DE CONSOLIDACIÓN DE APLICACIONES

Aplicación	Prioridad	Estrategia Consolidación	Factor de reducción
Almacén del departamento y gerencias	Muy Alta	Mantener	n/a
Análisis y niveles de disponibilidad	Muy Alta	Mantener	n/a
Antivirus corporativo	Muy Alta	Mantener	n/a
Apertura y cierre de pozos	Muy Alta	Mantener	n/a
Aplicaciones informáticas para los grupos de gestión económica	Muy Alta	Mantener	n/a
Apoyo a la investigación y la ingeniería	Muy Alta	Mantener	n/a
Apoyo al empleo	Muy Alta	Mantener	n/a
Atención de llamadas	Muy Alta	Mantener	n/a
Base de reconocimiento de subsuelo	Muy Alta	Mantener	n/a
Centro de investigación	Muy Alta	Mantener	n/a
Centro de producción 1	Muy Alta	Mantener	n/a
Centro de producción 10	Muy Alta	Mantener	n/a
Centro de producción 11	Muy Alta	Mantener	n/a
Centro de producción 12	Muy Alta	Mantener	n/a
Centro de producción 2	Muy Alta	Mantener	n/a
Centro de producción 3	Muy Alta	Mantener	n/a
Centro de producción 4	Muy Alta	Mantener	n/a
Centro de producción 5	Muy Alta	Mantener	n/a
Centro de producción 6	Muy Alta	Mantener	n/a
Centro de producción 7	Muy Alta	Mantener	n/a
Centro de producción 8	Muy Alta	Mantener	n/a
Centro de producción 9	Muy Alta	Mantener	n/a

Combustibles	Muy Alta	Mantener	n/a
Contratación en el extranjero	Muy Alta	Mantener	n/a
Control de cálculos y diseño	Muy Alta	Mantener	n/a
Control de combustibles	Muy Alta	Mantener	n/a
Control de vehículos	Muy Alta	Mantener	n/a
Ctrlcolas	Muy Alta	Mantener	n/a
Datos de recambios y logísticos	Muy Alta	Mantener	n/a
Depósitos	Muy Alta	Mantener	n/a
Directorio corporativo	Muy Alta	Mantener	n/a
Dominio corporativo	Muy Alta	Mantener	n/a
Dote (documentación técnica)	Muy Alta	Mantener	n/a
Empresa-101	Muy Alta	Mantener	n/a
Estado de los activos infraestructura	Muy Alta	Mantener	n/a
Estudios	Muy Alta	Mantener	n/a
Evolución de plantilla	Muy Alta	Mantener	n/a
Fasempleo	Muy Alta	Mantener	n/a
Gestión de activos y distribución para el departamento	Muy Alta	Mantener	n/a
Gestión de calidad del software	Muy Alta	Mantener	n/a
Gestión de integración	Muy Alta	Mantener	n/a
Gestión de oleoductos	Muy Alta	Mantener	n/a
Gestión presupuestaria	Muy Alta	Mantener	n/a
Grupos de análisis de suelos y búsqueda de bolsas	Muy Alta	Mantener	n/a
Grupos de prospección	Muy Alta	Mantener	n/a
Helpdesk departamento	Muy Alta	Mantener	n/a
Información empleo	Muy Alta	Mantener	n/a
Informes de dirección	Muy Alta	Mantener	n/a

Infraestructuras	Muy Alta	Mantener	n/a
Infraestructuras de plataforma	Muy Alta	Mantener	n/a
Ingeniería y desarrollo	Muy Alta	Mantener	n/a
Intranet	Muy Alta	Mantener	n/a
Jubilaciones	Muy Alta	Mantener	n/a
Lanzadera	Muy Alta	Mantener	n/a
Legal y judicial	Muy Alta	Mantener	n/a
Material e infraestructuras de la empresa	Muy Alta	Mantener	n/a
Medioambiente	Muy Alta	Mantener	n/a
Modulo de personal directivo	Muy Alta	Mantener	n/a
Monitorización	Muy Alta	Mantener	n/a
Monitorización del sistema logístico	Muy Alta	Mantener	n/a
Operativa anual	Muy Alta	Mantener	n/a
Pensiones - 1090	Muy Alta	Mantener	n/a
Personal	Muy Alta	Mantener	n/a
Personal y plan de carrera	Muy Alta	Mantener	n/a
Planificación de la obtención del material y las infraestructuras	Muy Alta	Mantener	n/a
Potencial de operación	Muy Alta	Mantener	n/a
Programación y seguimiento de la producción	Muy Alta	Mantener	n/a
Programas y proyectos	Muy Alta	Mantener	n/a
Ras	Muy Alta	Mantener	n/a
Registro	Muy Alta	Mantener	n/a
Registro general	Muy Alta	Mantener	n/a
SAN del centro principal y datos	Muy Alta	Mantener	n/a
Seguridad del departamento	Muy Alta	Mantener	n/a

Seguridad a los desplazados	Muy Alta	Mantener	n/a
Seguridad personal desplazado	Muy Alta	Mantener	n/a
Seguridad social	Muy Alta	Mantener	n/a
Servicios de fax y comunicaciones	Muy Alta	Mantener	n/a
Sistema de prevención de recursos humanos	Muy Alta	Mantener	n/a
Sistema de formación	Muy Alta	Mantener	n/a
Sistema de integración de vehículos	Muy Alta	Mantener	n/a
Sistema de mensajería	Muy Alta	Mantener	n/a
Sistema de seguros	Muy Alta	Mantener	n/a
Sistema de selección	Muy Alta	Mantener	n/a
Sistema general de gestión del personal	Muy Alta	Mantener	n/a
Sistema logístico de vehículos	Muy Alta	Mantener	n/a
Sistema logístico integral	Muy Alta	Mantener	n/a
Sistema logístico prospección	Muy Alta	Mantener	n/a
Sistemas de control de incidencias y acuerdos	Muy Alta	Mantener	n/a
Sistemas de satélites	Muy Alta	Mantener	n/a
Sistemas gis	Muy Alta	Mantener	n/a
Tarifas y cobros	Muy Alta	Mantener	n/a
Telefonía	Muy Alta	Mantener	n/a
Traslados médicos	Muy Alta	Mantener	n/a
Usabilidad	Muy Alta	Mantener	n/a
Volumen colas	Muy Alta	Mantener	n/a
Web del departamento	Muy Alta	Mantener	n/a
Catalogo productos	Alta	Mantener	n/a
pedidos de material	Alta	Mantener	n/a
registro del departamento	Alta	Mantener	n/a

Análisis de mercado	Alta	Mantener	n/a
Aplicación de repuestos del servicio de aprovisionamiento	Alta	Mantener	n/a
Apoyo a la dirección	Alta	Mantener	n/a
Biblioteca actuaciones técnicas de mantenimiento	Alta	Mantener	n/a
Catalogación de productos	Alta	Mantener	n/a
Competencia	Alta	Mantener	n/a
Control de accesos a internet	Alta	Mantener	n/a
Control de acciones telefónicas y mantenimiento	Alta	Mantener	n/a
Control de aprovisionamiento y almacenes	Alta	Mantener	n/a
Control de vehículos	Alta	Mantener	n/a
Control incidencia de redes	Alta	Mantener	n/a
Control vehículos	Alta	Mantener	n/a
Correo electrónico	Alta	Mantener	n/a
Desplazamientos	Alta	Mantener	n/a
Directorio corporativo	Alta	Mantener	n/a
Distribución de software	Alta	Mantener	n/a
Expedientes personal	Alta	Mantener	n/a
Geoespacial	Alta	Mantener	n/a
Geostat	Alta	Mantener	n/a
Gestión pagos	Alta	Mantener	n/a
Gestión almacenes	Alta	Mantener	n/a
Gestión de automóviles	Alta	Mantener	n/a
Gestión de bancos	Alta	Mantener	n/a
Gestión de los laboratorios de calibración	Alta	Mantener	n/a
Gestión de pedidos	Alta	Mantener	n/a

Gestión de provisiones y enseres	Alta	Mantener	n/a
Gestión de variabilidad	Alta	Mantener	n/a
Helpdesk departamento - gerencia 1	Alta	Mantener	n/a
Helpdesk departamento - gerencia 2	Alta	Mantener	n/a
Helpdesk departamento - gerencia 3	Alta	Mantener	n/a
Helpdesk departamento - gerencia 4	Alta	Mantener	n/a
Helpdesk departamento - gerencia 5	Alta	Mantener	n/a
Inventarios	Alta	Mantener	n/a
Inventarios	Alta	Mantener	n/a
Manuales técnicos de vehículos	Alta	Mantener	n/a
Moneda extranjera	Alta	Mantener	n/a
Motorización vehículos	Alta	Mantener	n/a
Nominas	Alta	Mantener	n/a
Ordenes de trabajo mantenimientos	Alta	Mantener	n/a
Personal desplazado	Alta	Mantener	n/a
Proveedores	Alta	Mantener	n/a
Proveedores	Alta	Mantener	n/a
Recursos humanos del departamento	Alta	Virtualizar	70%
Registro documentación	Alta	Mantener	n/a
Registro general	Alta	Virtualizar	35%
Repostaje de vehículos-combustibles	Alta	Mantener	n/a
Seguridad de accesos físicos	Alta	Compartir recursos	70%
Servicios gestión y aprobación peticiones GIS	Alta	Mantener	n/a
Sistema de alimentación del personal desplazado	Alta	Mantener	n/a
Sistema de contratación de personal	Alta	Mantener	n/a

Sistema de gestión inventario	Alta	Mantener	n/a
Sistema de peticiones	Alta	Mantener	n/a
Sistema logístico	Alta	Mantener	n/a
Sistemas de gestión y control de redes	Alta	Mantener	n/a
Solicitudes de material	Alta	Mantener	n/a
Spectrum	Alta	Mantener	n/a
Telefonía fija	Alta	Mantener	n/a
Tramitación de peticiones de accesos	Alta	Mantener	n/a
Ubicaciones	Alta	Mantener	n/a
Vestuarios	Alta	Mantener	n/a
Vigilancia y control	Alta	Mantener	n/a
Anuncios y concursos para la contratación	Media	Mantener	n/a
Archivo general e histórico	Media	Virtualizar en Superdome	0%
Base de datos de pozos	Media	Mantener	n/a
Biblioteca	Media	Mantener	n/a
Biblioteca	Media	Mantener	n/a
Biblioteca	Media	Virtualizar en Superdome	0%
Capacidades de distribución y transporte	Media	Mantener	n/a
Centro de control de producción	Media	Mantener	n/a
Centro documentación de productos	Media	Virtualizar en Host	0%
Combustibles y lubricantes vehículos	Media	Mantener	n/a
Control amortización vehículos	Media	Mantener	n/a
Control de movimientos y situaciones de flota	Media	Mantener	n/a
Control de visitas	Media	Mantener	n/a

Control médico personal	Media	Virtualizar en Superdome	0%
Convenios nacionales	Media	Mantener	n/a
Cuadro de mando	Media	Virtualizar en Superdome	0%
Formación	Media	Mantener	n/a
Formación personal	Media	Mantener	n/a
Fórum de intercambio	Media	Virtualizar	60%
Gastos en comunicaciones personales	Media	Virtualizar	45%
Gestión almacén de apoyo	Media	Mantener	n/a
Gestión calidad	Media	Compartir recursos	80%
Gestión de caja	Media	Mantener	n/a
Gestión de la calidad en los laboratorios	Media	Virtualizar en Host	0%
Gestión de recursos de instalaciones de extracción y prospección	Media	Virtualizar en Host	0%
Gestión de repuestos del departamento	Media	Virtualizar	60%
Gestión de suministros del personal	Media	Mantener	n/a
Grupos de trabajo	Media	Virtualizar	65%
Guía telefónica	Media	Mantener	n/a
Guías técnicas informáticas	Media	Mantener	n/a
Incidencias	Media	Virtualizar	45%
Información recursos	Media	Mantener	n/a
Instrucciones generales	Media	Virtualizar	45%
Instrucciones particulares	Media	Compartir recursos	90%
Jornadas formativas	Media	Virtualizar	60%
Mantenimiento de las infraestructuras	Media	Mantener	n/a
Material de oficina no inventariable	Media	Mantener	n/a

Museo	Media	Virtualizar	60%
Normas y normalización	Media	Virtualizar en Superdome	0%
Pagina web para el departamento	Media	Compartir recursos	65%
Parque de vehículos	Media	Mantener	n/a
Pasaportes	Media	Mantener	n/a
Personal desplazado en el exterior	Media	Compartir recursos	90%
Política empresarial	Media	Virtualizar	40%
Política internacional	Media	Virtualizar	70%
Presupuestos generales	Media	Mantener	n/a
Prevención	Media	Compartir recursos	65%
Procedimientos operativos (p.o.s.)	Media	Mantener	n/a
Pruebas de estado vehículos	Media	Mantener	n/a
Reconocimientos médicos enfermería	Media	Mantener	n/a
Recursos humanos	Media	Virtualizar	35%
Reporte discrepancias	Media	Mantener	n/a
Resúmenes de prensa	Media	Virtualizar	30%
Revistas y difusión	Media	Mantener	n/a
Seguridad operativa	Media	Virtualizar en Host	-
Sistema de mantenimiento	Media	Mantener	n/a
Sitio web del departamento	Media	Compartir recursos	65%
Tablones de las gerencias	Media	Compartir recursos	75%
Transporte	Media	Virtualizar en Superdome	-
Tratados, convenios y acuerdos	Media	Virtualizar	40%

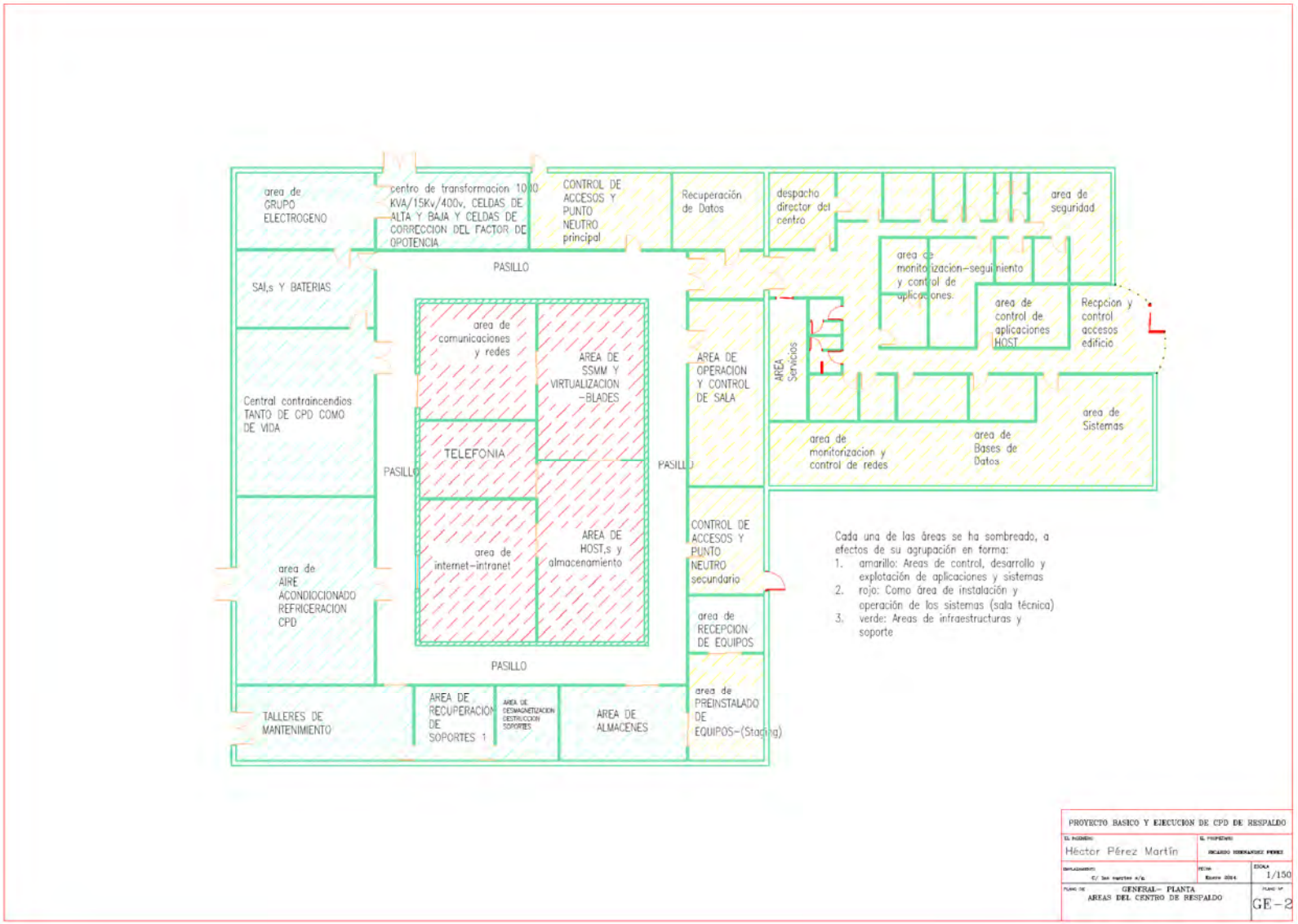
Unidad de normalización	Media	Compartir recursos	65%
Análisis de riesgos	Baja	Compartir recursos	80%
Archivos y dotaciones vehiculares	Baja	Compartir recursos	65%
Backup	Baja	Mantener	n/a
Contratación explotación producción	Baja	Mantener	n/a
Contratación material	Baja	Mantener	n/a
Contratación personal	Baja	Compartir recursos	70%
Control de vehículos del departamento	Baja	Compartir recursos	65%
Correo	Baja	Mantener	n/a
Destinos y ocupaciones	Baja	Mantener	n/a
Dirección corporativa	Baja	Virtualizar en Host	0%
Elementos productivos	Baja	Virtualizar en Host	0%
Equipamiento y vehículos	Baja	Mantener	n/a
Expedientes personal	Baja	Mantener	n/a
Gestión de activos	Baja	Mantener	n/a
Gestión de personal	Baja	Mantener	n/a
Gestión de proveedores del grupo	Baja	Virtualizar	35%
Gestión electrónica y hardware	Baja	Virtualizar en Host	0%
Impresión	Baja	Mantener	n/a
Indemnizaciones	Baja	Virtualizar en Host	0%
Laboratorios	Baja	Mantener	n/a
Material de análisis y prospección	Baja	Virtualizar en Host	0%

Material diverso	Baja	Compartir recursos	70%
Recursos materiales	Baja	Virtualizar en Superdome	0%
Red	Baja	Mantener	n/a
Red área local	Baja	Mantener	n/a
Registro	Baja	Compartir recursos	85%
Sistemas PKI	Baja	Mantener	n/a
Vacaciones y permisos	Baja	Compartir recursos	65%
Vacaciones	Baja	Virtualizar	60%

Tabla 24 Estrategia de consolidación de aplicaciones

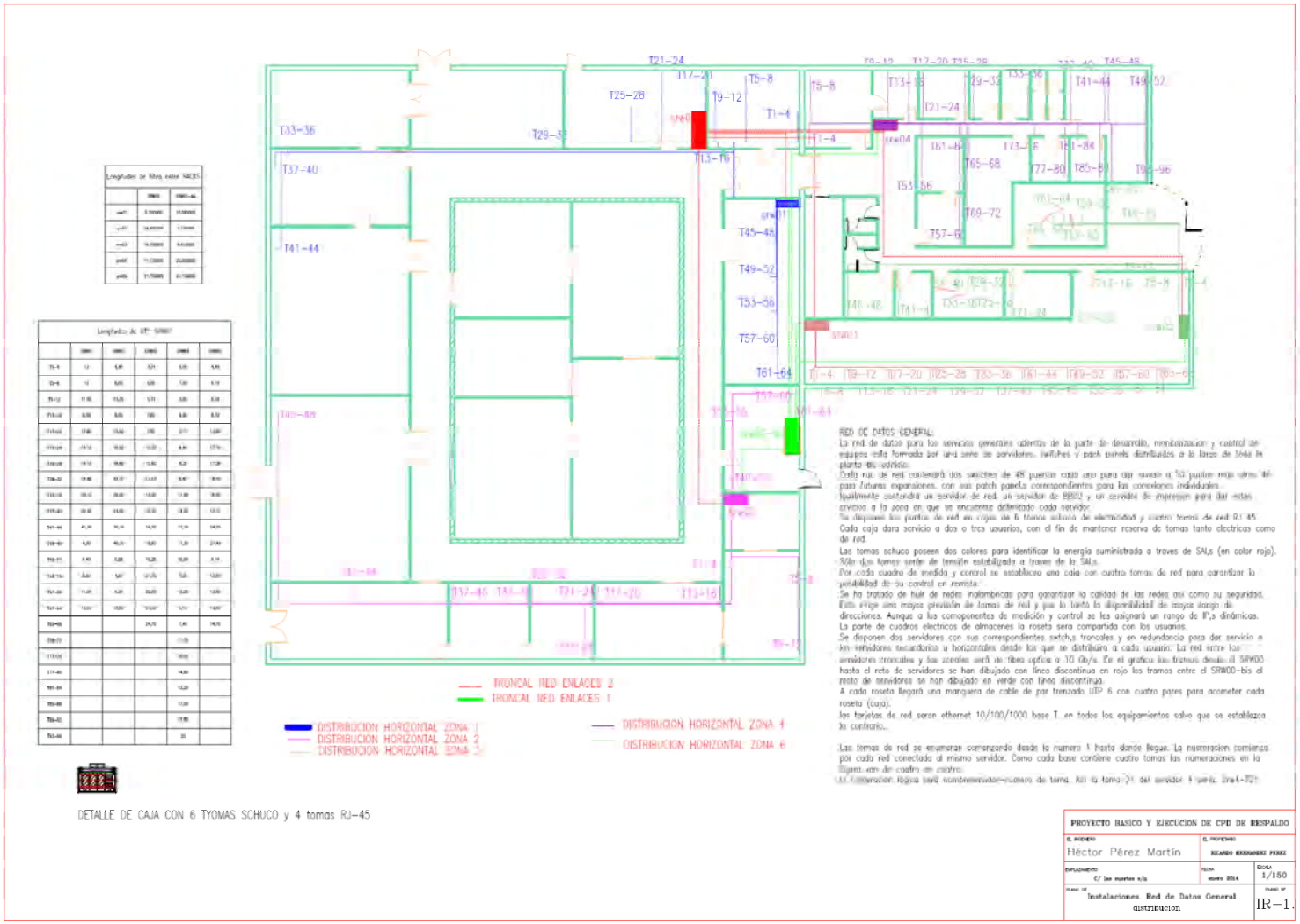
Anexo D - PLANOS

D.I Plano general del centro de respaldo

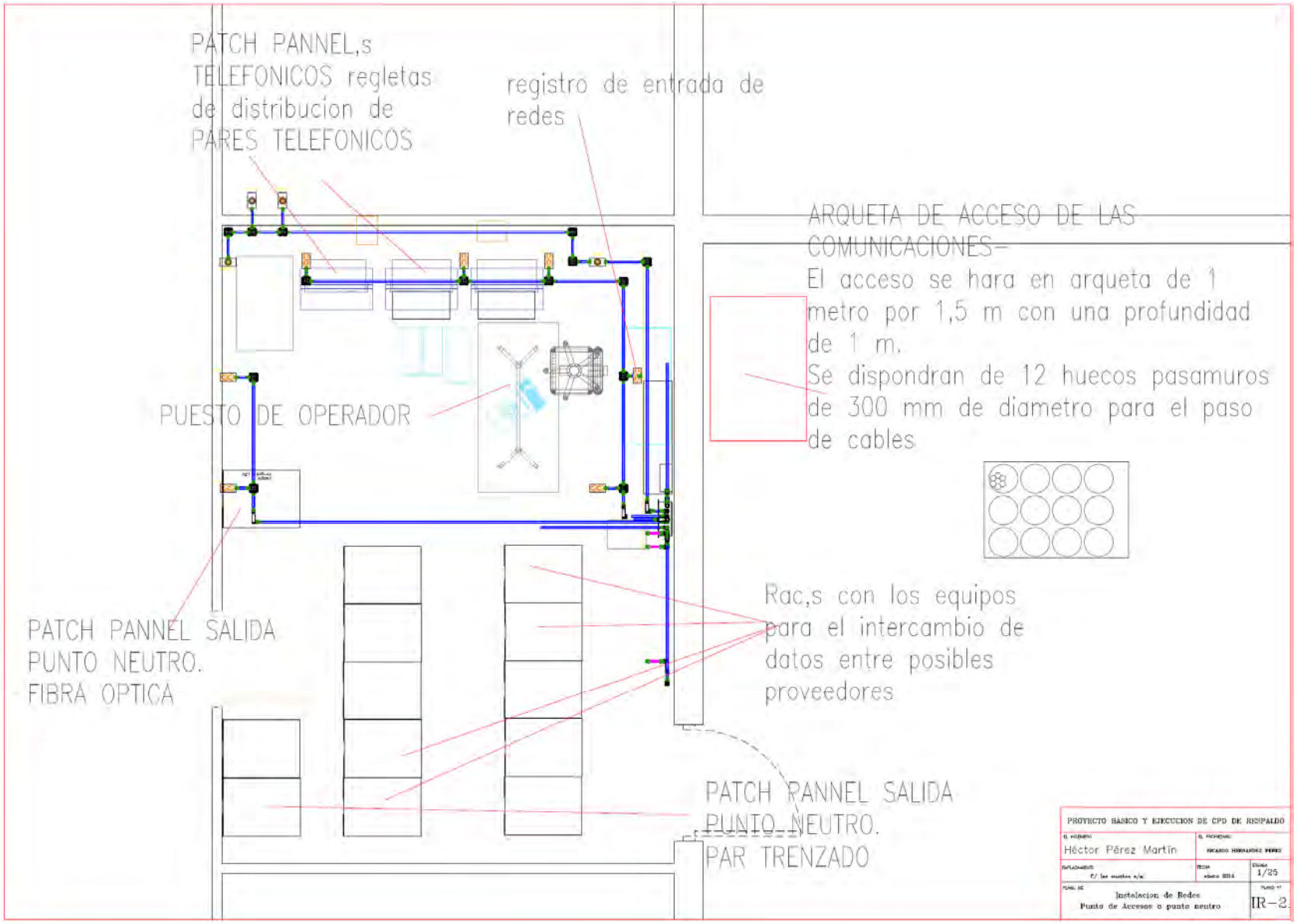


D.II Instalaciones de red

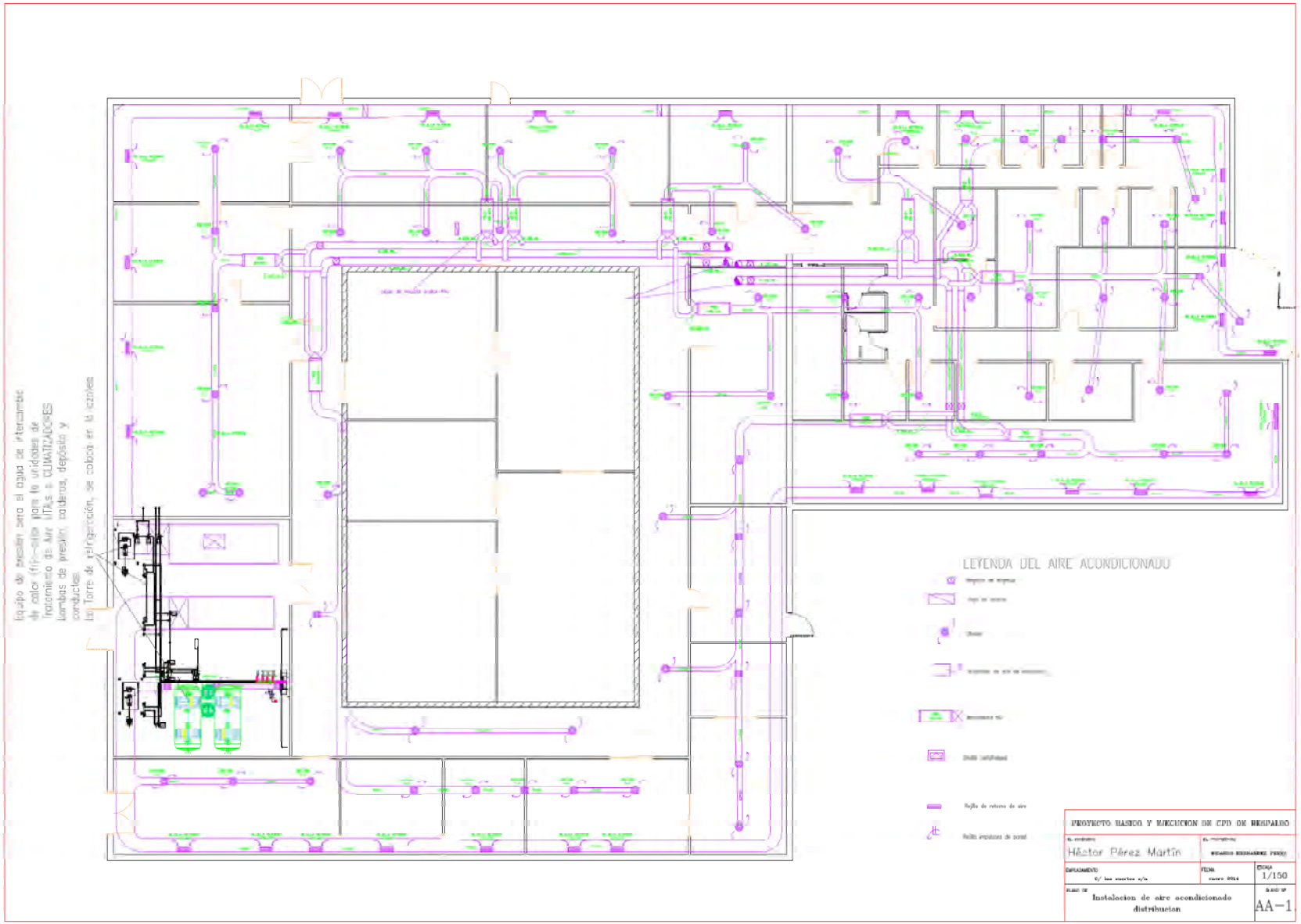
D.II.1 Red de Datos General



D.II.2 Redes y distribución del punto de acceso

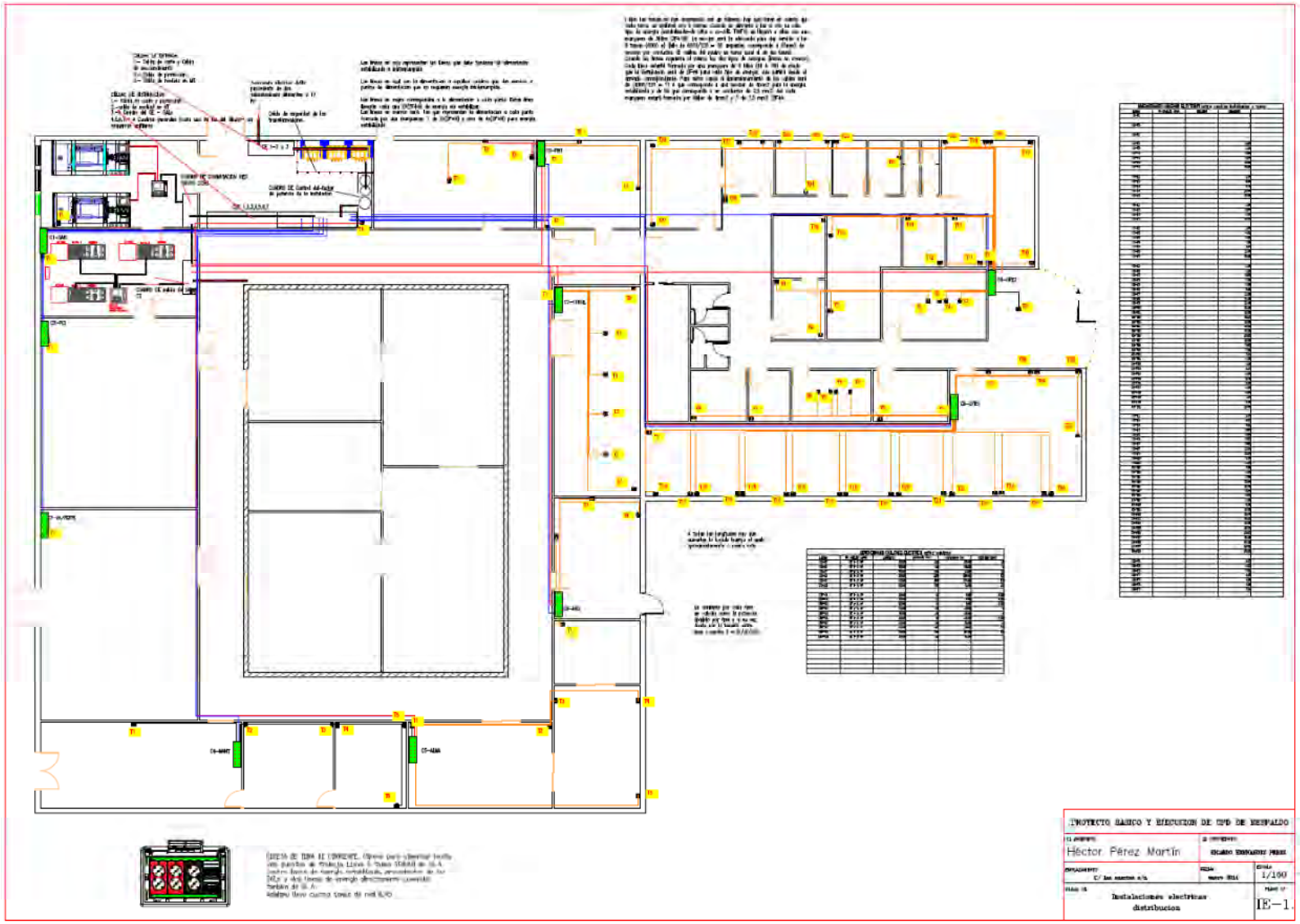


D.III Aire acondicionado

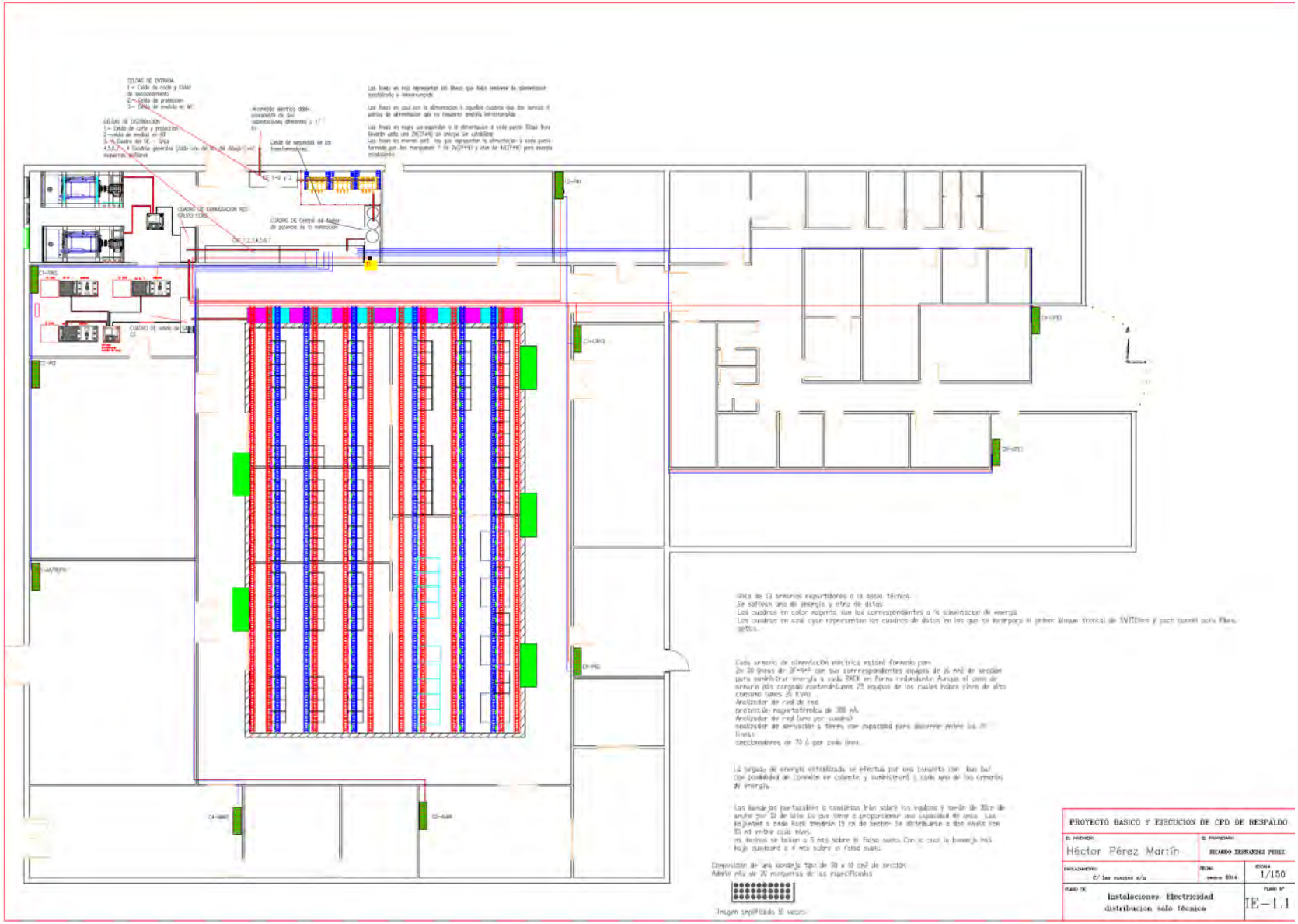


D.IV Instalaciones eléctricas

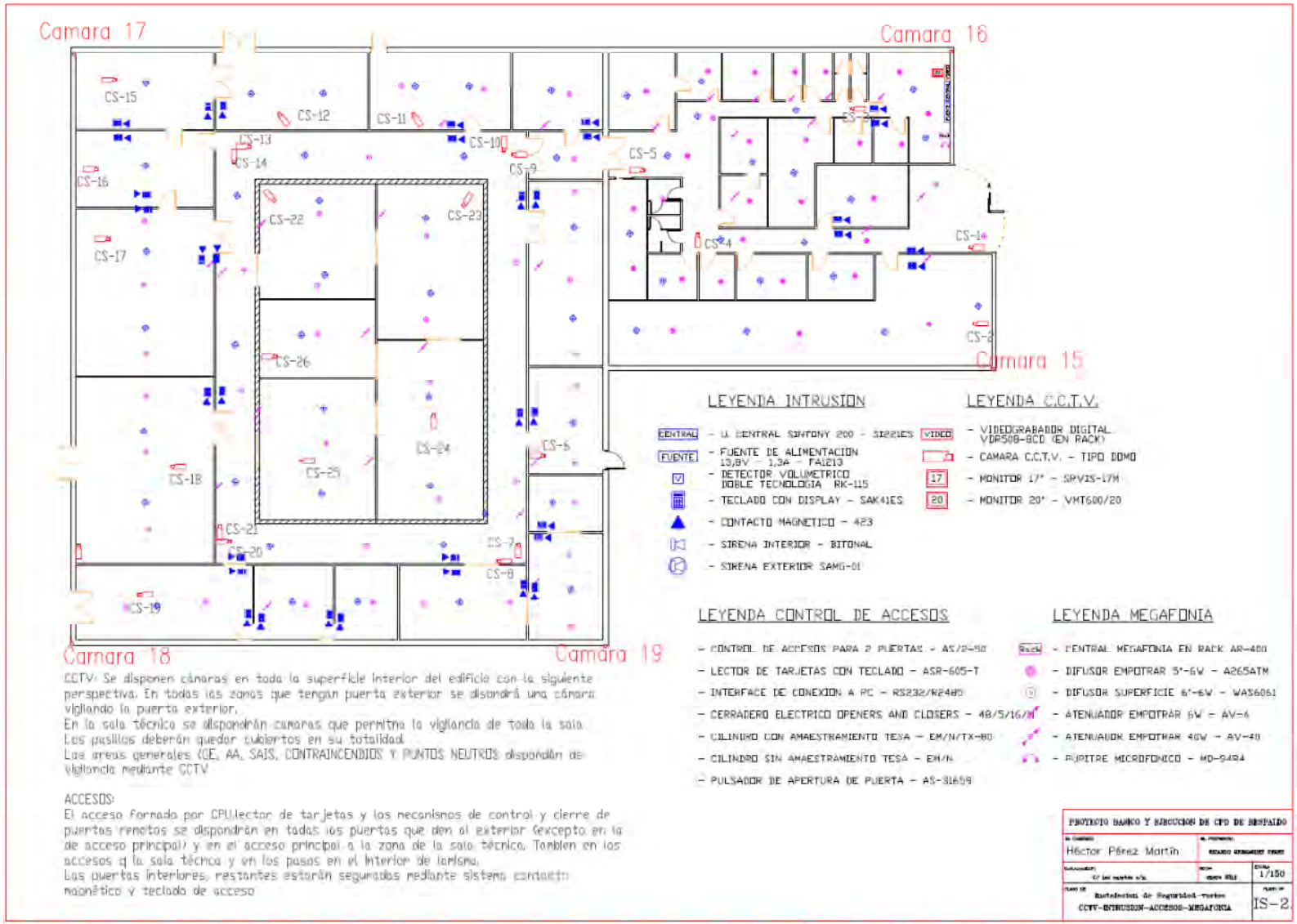
D.IV.1 Diagrama eléctrico general



D.IV.2 Diagrama eléctrico Sala técnica

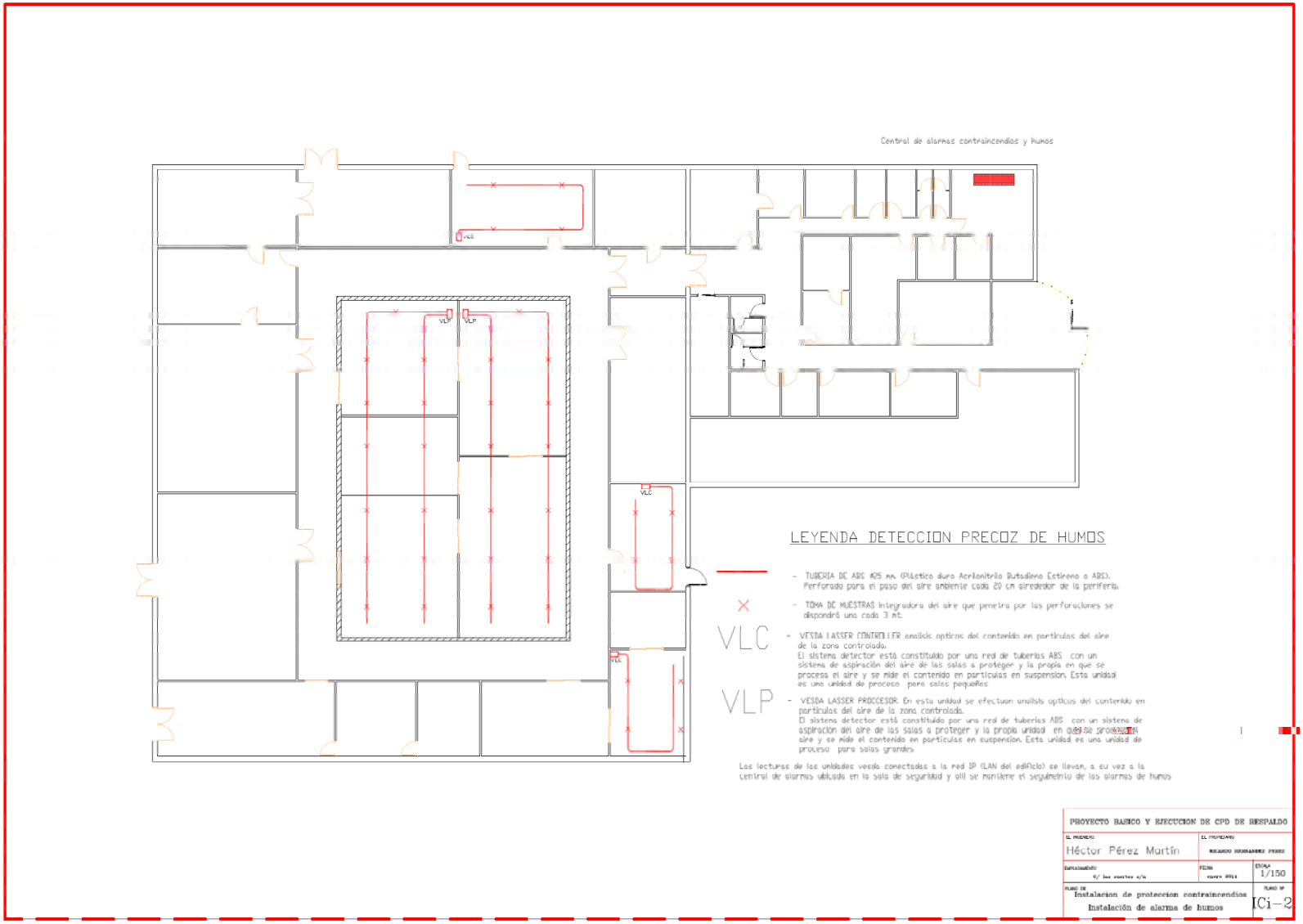


D.V Instalaciones de seguridad

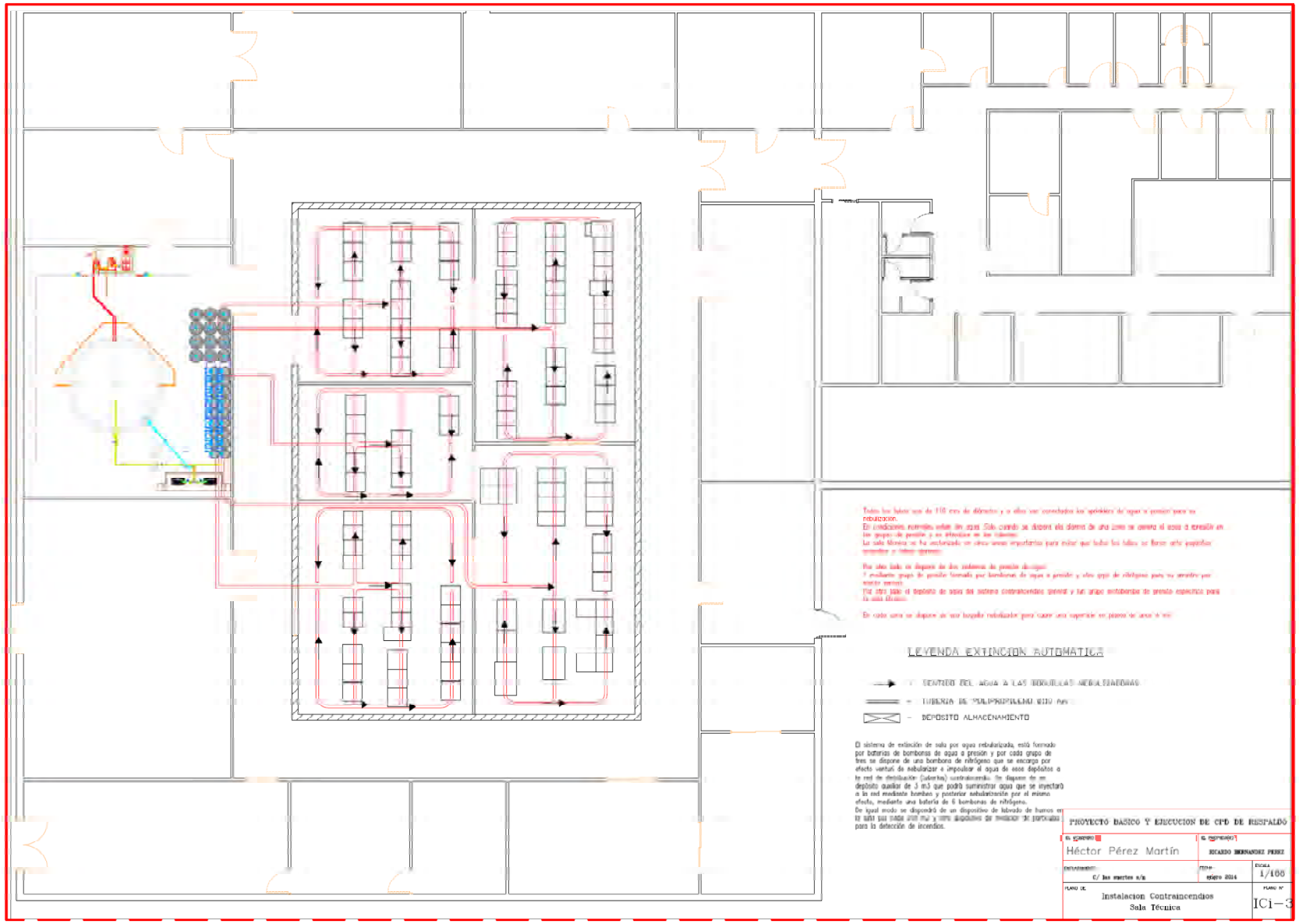


D.VI Instalaciones contraincendios

D.VI.1 Detección precoz de humos - sala técnica



D.VI.2 Extinción sala técnica



Anexo E - CRONOGRAMA DETALLADO DE LA ELABORACIÓN DEL PROYECTO

ID	Task Mode	Task Name	Duration	Start	Finish
1		**Concepción y estructuración**	**110 days**	**14/08/10 11:0**	**16/01/11 14:0**
2		Análisis inicial norma TIA-942	10 days	14/08/10 11:0	12/09/10 10:0
3		Definir conceptos principales y esqueleto	5 days	12/09/10 10:0	26/09/10 14:0
4		Presentación idea inicial	1 day	26/09/10 14:0	02/10/10 13:0
5		Validación y estructura del documento	6 days	26/09/10 14:0	16/10/10 17:0
6		Definición de escenario de partida y requi	35 days	02/10/10 13:0	16/01/11 14:0
7		**Diseño de la solución**	**790 days**	**16/01/11 14:0**	**26/01/14 18:0**
8		**Solución - Infraestructura de soporte**	**790 days**	**16/01/11 14:0**	**26/01/14 18:0**
9		Diseño del edificio	5 days	16/01/11 14:0	30/01/11 18:0
10		**Sistemas de Aire**	**615 days**	**03/04/11 16:0**	**11/08/13 10:0**
11		Estudio de normativa y tendencias	10 days	03/04/11 16:0	07/05/11 15:0
12		Solución alto nivel	15 days	11/02/12 15:0	25/03/12 18:0
13		Revisión, detalle y planos	25 days	25/05/13 17:0	11/08/13 10:0
14		**Sistemas Eléctricos**	**655 days**	**07/05/11 15:0**	**10/11/13 16:0**
15		Estudio de normativa y tendencias	10 days	07/05/11 15:0	05/06/11 14:0
16		Solución alto nivel	18 days	28/04/12 17:0	23/06/12 17:0
17		Revisión, detalle y planos	20 days	14/09/13 09:0	10/11/13 16:0
18		**Arquitectura salas de enlaces**	**320 days**	**30/07/11 15:0**	**20/10/12 15:0**
19		Estudio de normativa y tendencias	8 days	30/07/11 15:0	21/08/11 16:0
20		Solución alto nivel	10 days	31/03/12 09:0	28/04/12 17:0
21		Revisión, detalle y planos	10 days	16/09/12 16:0	20/10/12 15:0
22		**Protección contraincendios**	**775 days**	**05/02/11 09:0**	**26/01/14 18:0**
23		Estudio de normativa y tendencias	15 days	05/02/11 09:0	20/03/11 12:0
24		Solución alto nivel	20 days	21/07/12 09:0	16/09/12 16:0
25		Revisión, detalle y planos	25 days	10/11/13 16:0	26/01/14 18:0
26		**Otros sistemas**	**590 days**	**05/06/11 14:0**	**08/09/13 18:0**
27		Estudio de normativa y soluciones	5 days	05/06/11 14:0	19/06/11 18:0
28		Solución alto nivel	20 days	10/12/11 17:0	11/02/12 15:0
29		Revisión, detalle y planos	10 days	11/08/13 10:0	08/09/13 18:0
30		**Solución - Infraestructura de comunicaci**	**570 days**	**20/03/11 12:0**	**25/05/13 17:0**
31		**Aplicación**	**505 days**	**20/03/11 12:0**	**23/02/13 11:0**
32		Estudios tecnológicos	5 days	20/03/11 12:0	03/04/11 16:0
33		Propuesta solución alto nivel	15 days	23/10/11 14:0	10/12/11 17:0
34		Detalles e inventario	25 days	08/12/12 09:0	23/02/13 11:0
35		**Red**	**460 days**	**21/08/11 16:0**	**25/05/13 17:0**
36		Estudios tecnológicos	5 days	21/08/11 16:0	10/09/11 11:0
37		Propuesta solución alto nivel	15 days	10/09/11 11:0	23/10/11 14:0
38		Detalles y planos	30 days	23/02/13 11:0	25/05/13 17:0
39		**Físico**	**375 days**	**25/06/11 09:0**	**02/12/12 18:0**
40		Estudio de normativa y soluciones	12 days	25/06/11 09:0	30/07/11 15:0
41		Solución alto nivel	8 days	23/06/12 17:0	15/07/12 18:0
42		Revisión, detalle y planos	15 days	20/10/12 15:0	02/12/12 18:0
43		Fin etapa de estudio	0 days	17/07/12 13:0	17/07/12 13:0
44		Fin de etapa de solución de alto nivel	0 days	12/11/13 15:0	12/11/13 15:0
45		Fin de etapa de solución detallada	0 days	26/01/14 18:0	26/01/14 18:0
46		Entrega Borrador v0	0 days	23/03/14 18:0	23/03/14 18:0
47		**Revisión y correcciones**	**35 days**	**01/02/14 09:0**	**23/03/14 18:0**
48		Entrega Borrador v1	0 days	01/02/14 09:0	01/02/14 09:0
49		Revisión borrador v1	8 days	01/02/14 09:0	23/02/14 10:0
50		Correcciones al borrador	10 days	23/02/14 10:0	23/03/14 18:0
51		Entrega final	0 days	23/03/14 18:0	23/03/14 18:0