Diseño de un Centro de Datos de Alto Rendimiento

UOC - Trabajo Fin de Grado

Autor: Álvaro Díaz Teba
Tutor: Miquel Colobran Huguet

3 de Enero de 2021

Dedicatoria y agradecimientos

Nunca pensé que algún día podría estar escribiendo mi trabajo final de grado, sinceramente no imaginaba que fuera capaz de llegar hasta aquí. Ha sido mucho sacrificio y esfuerzo, pero nada comparado con la compresión, apoyo y cariño que he recibido de mi mujer durante todos estos años de carrera. Por este motivo, quiero dedicar mi último trabajo de carrera a mi mujer Gema, por estar siempre animándome y por levantarme en los momentos más duros, sin ella no habría llegado tan lejos.

También gracias a mi familia por ser comprensiva por perderme tantos momentos con ellos, en especial a mis abuelos por lo valores que me inculcaron, aunque por desgracia no estén entre nosotros. Gracias a mis suegros, por su apoyo incondicional a la salida de cada examen, gracias a mi tío Juan por creer siempre en mí y gracias a mi tía Manuela por cuidar siempre de mí.

Quiero agradecer a mi amigo Kiko y Javier, todos sus consejos y su apoyo a lo largo de la carrera, también a mi amigo y compañero de carrera Fran por compartir tan buenos momentos de estudios juntos.

Una mención especial y agradecer a Miquel Colobran por su ayuda en la elaboración de este trabajo y agradecer a mi profesor Toni por su ayuda incondicional a lo largo de toda la carrera.

Por último, agradecer a mis padres y hermanos toda la ayuda y compresión que han tenido durante estos años. Gracias sobre todo a mi madre por los ánimos que me daban en cada examen.

Resumen

En la actualidad, la información o el dato ha transcendido en su importancia tanto en las organizaciones como en la sociedad. Esta información es digital y accesible desde los Centros de Datos o Data Center, que pueden ser públicos porque ofrecen servicios desde Internet (Cloud públicos) o privados. El objetivo de este trabajo es realizar un análisis de tecnologías y soluciones actuales para realizar un diseño de un Centro de Datos de Alto Rendimiento, teniendo en cuenta las necesidades que demandan las organizaciones y la sociedad de hoy en día.

Para llevar a cabo la investigación, se ha realizado un estudio de las tecnologías y soluciones para un Centro de Datos con un enfoque de proveedor Cloud. A continuación, se ha realizado una revisión de las tecnologías necesarias en un Centro de Datos de Alto Rendimiento, desde el equipamiento hardware a las herramientas software para explotar el Centro de Datos.

En consecuencia, sólo se ha encontrado una única solución con soporte oficial del fabricante que proporciona un Cloud privado capaz de ofrecer servicios IaaS, PaaS y SaaS como cualquier Cloud público en la actualidad. También se han seleccionado elementos hardware y soluciones software de marcas contrastadas, con cierta popularidad, madurez y experiencia en el mercado de las Tecnologías de la Información.

El diseño de un Centro de Datos de Alto Rendimiento, proporciona funcionalidades y soluciones que demandan en la actualidad las organizaciones, la adopción de este Centro de Datos realiza cambios profundos sobre estas aumentando su productividad y capacidad al ofrecer servicios.

Palabras clave: Centro de Datos, Diseño, Disponibilidad, Redundancia, Virtualización, Cloud.

Índice de contenidos

CAPÍTULO 1 INTRODUCCIÓN 8

1.1 JUSTIFICACIÓN 8
1.2 OBJETIVOS 8
1.3 ALCANCE 9
1.4 ENFOQUE Y METODOLOGÍA 10
1.5 PLANIFICACIÓN DEL PROYECTO 10
1.6 PRODUCTOS OBTENIDOS 13
1.7 BREVE DESCRIPCIÓN DE LOS OTROS CAPÍTULOS DE LA MEMORIA. 13

CAPÍTULO 2 CENTRO DE DATOS DE ALTO RENDIMIENTO 14

2.1 DEFINICIÓN 14
2.2 EVOLUCIÓN 15
2.3 ELEMENTOS EN UN CENTRO DE DATOS 17

CAPÍTULO 3 TECNOLOGÍAS SOFTWARE DE UN CENTRO DE DATOS 27

3.1 SOFTWARE 27
3.2 SISTEMA OPERATIVO 27
3.3 VIRTUALIZACIÓN 28
3.4 CONTENEDORES Y KUBERNETES 29
3.5 CLOUD 31

CAPÍTULO 4 NORMATIVAS DE UN CENTRO DE DATOS 34

4.1 IEEE 802.3 34
4.2 ANSI/TIA-942 34

CAPÍTULO 5 MARCOS DE TRABAJO 36

5.1 COBIT 36
5.2 ITIL 37
5.3 COSO 39
5.4 DEVOPS 41

CAPÍTULO 6 DISEÑO DE UN CENTRO DE DATOS DE ALTO RENDIMIENTO 42

CAPÍTULO 7 FASE DE DISEÑO DE UN CENTRO DE DATOS DE ALTO RENDIMIENTO 44

7.1 RECOPILACIÓN DE DOCUMENTACIÓN 44
7.2 REQUISITOS DE LA UBICACIÓN PARA EL CENTRO DE DATOS 44
7.3 CARACTERÍSTICAS FÍSICAS PARA EL CENTRO DE DATOS 46

7.4 EQUIPAMIENTO 48
7.5 DISEÑO DE RED FÍSICA ETHERNET 59
7.6 DISEÑO DE RED SAN 60
7.7 TECNOLOGÍAS SOFTWARE 60
7.8 VMWARE VCLOUD FOUNDATION 62
7.9 CATÁLOGO DE SERVICIOS 77
7.10 ORGANIZACIÓN Y MARCO DE TRABAJO 78
7.11 CAMBIOS Y RIESGOS. 79

CAPÍTULO 8 FASE DE IMPLANTACIÓN DE UN CENTRO DE DATOS DE ALTO RENDIMIENTO 80

8.1 DESCRIPCIÓN DEL CASO FICTICIO. 80
8.2 INSTALACIÓN DE ELEMENTOS FÍSICOS. 82
8.3 IMPLANTACIÓN DE LA SOLUCIÓN DE VMWARE CLOUD FOUNDATION. 88
8.4 SEGURIDAD LÓGICA. 89
8.5 CERTIFICACIÓN 91
8.6 PLANIFICACIÓN DE LA FASE DE IMPLANTACIÓN 94
8.7 ORGANIZACIÓN Y MARCO DE TRABAJO 95
8.8 PLAN DE RIESGOS 96
8.9 BUENAS PRÁCTICAS 97
8.10 OFERTA ECONÓMICA 98

CAPÍTULO 9 CONCLUSIONES 99

CAPÍTULO 10 BIBLIOGRAFÍA DE REFERENCIAS 101

CAPÍTULO 11 ANEXOS 105

11.1 ANEXO I: PLANIFICACIÓN DEL PROYECTO CON DIAGRAMA DE GANTT 105
11.2 ANEXO II: PLANO DE OBRA CIVIL DEL CPD 106
11.3 ANEXO III: ESQUEMA FÍSICO DE RED ETHERNET 107
11.4 ANEXO IV: ESQUEMA DE RED SAN 108
11.5 ANEXO V: PLANO DE LA SALA DEL CENTRO DE DATOS. 109
11.6 ANEXO VI: RACK DE PATCH PANEL. 110
11.7 ANEXO VII: RACK DE EQUIPOS DE COMUNICACIONES. 111
11.8 ANEXO VIII: RACK DE EQUIPOS DE ALMACENAMIENTO. 112
11.9 ANEXO IX: RACK SERVIDORES FÍSICOS. 113
11.10 ANEXO X: DIAGRAMA DE GANTT DE LA FASE DE IMPLANTACIÓN. 114

Índice de figuras

Ilustración 1 - Centro de Datos de Google en Dublín (Irlanda)....14
Ilustración 2 - Dos piezas del ENIAC....15
Ilustración 3 - Piezas de un suelo técnico.....17
Ilustración 4 -Diagrama de un SAI Online....20
Ilustración 5 - Tres grupos electrógenos industriales....20
Ilustración 6 - Circuito de aire en un pasillo frio....21
Ilustración 7 - Elementos de un rack....22
Ilustración 8 - Patch panel de 48 puertos UTP Cat 5....23
Ilustración 9 - Cable con conector C13....24
Ilustración 10 - Conector de chasis C14....24
Ilustración 11 - Conectores Cetac....24
Ilustración 12 - Conector RJ45....24
Ilustración 13 - Conector LC monomodo y multinodo.....25
Ilustración 14 - Virtualización de servidor físico....28
Ilustración 15 - Máquinas virtuales VS Contenedores....30
Ilustración 16 - Arquitectura de Kubernetes....31
Ilustración 17 - Esquema básico de un Cloud....32
Ilustración 18 - Modelo de servicio de un Cloud....33
Ilustración 19 - Imagen del Datacenter de Telefónica en Alcalá de Henares.....45
Ilustración 20 - Esclusa unipersonal de alta seguridad.....48
Ilustración 21 - Imagen de un sistema básico contra incendios.....52
Ilustración 22 – Esquema de soluciones de un CCTV....53
Ilustración 23 - Control de acceso de un CPD....54
Ilustración 24 - Esquema lógico de VCF....62
Ilustración 25 - Ciclo de vida de VCF....63
Ilustración 26 - Arquitectura VMware vSphere....65
Ilustración 27 - Virtualización de servidor VS virtualización de redes....67
Ilustración 28 - Arquitectura y componentes de NSX....68
Ilustración 29 - VMware vRealize Automation....70
Ilustración 30 - VCF con Tanzu....72
Ilustración 31 - Dominios de cargas de trabajo de VCF....73
Ilustración 32 – Componentes de un dominio de gestión....74
Ilustración 33 - Dominio de cómputo....74
Ilustración 34 - Arquitectura estándar VCF....75
Ilustración 35 - Arquitectura consolidada VCF....75
Ilustración 36 - VMware HCX....76
Ilustración 37 - Bimodal IT según Gartner....78
Ilustración 38 - Organización del cableado por encima de un rack....84
Ilustración 39 - Esquema de red lógico con DMZ....89
Ilustración 40 - Planificación de la FASE de Implantación....94
Ilustración 41 - Organigrama para la gestión del Centro de Datos de Alto Rendimiento....95

Índice de tablas

TABLA 1 - MARCO DE TRABAJO COBIT 36
TABLA 2 - MARCO DE TRABAJO ITIL 38
TABLA 3 - MARCO DE TRABAJO COSO 40
TABLA 4 - CARACTERISTICAS DEL SAI 50
TABLA 5 - ESPECIFICACIONES TÉCNICAS DEL CABLE DE FIBRA 57
TABLA 6 - CARACTERÍSTICAS VMWARE NSX 67
TABLA 7 - PRUEBAS Y RESULTADOS DE LA CERTIFICACIÓN 92
TABLA 8 - PLAN DE RIESGOS EN LA FASE DE IMPLANTACIÓN 96
TABLA 9 - PRESUPUESTO ECONÓMICO 98

Capítulo 1 Introducción

1.1 Justificación

En la actualidad, hay un amplio consenso que considera que el "dato" es el "nuevo oro" de nuestra época. El concepto del "dato" ha conseguido tal transcendencia que las organizaciones más ricas del mundo son aquellas que tienen la capacidad de gestionar grandes volúmenes de datos de forma más óptima. Además, la transformación digital después de la aparición del Covid19 ha venido para quedarse, después de que la Unión Europea haya anunciado una estrategia económica basada en la transformación digital. Así pues, parece que después de muchos años hablando de la transformación digital ha llegado su momento.

En este escenario el dato está en el centro de todas las decisiones de cualquier organización que impulsa la transformación digital. Es muy posible, que se fomente un gran avance en la tecnología y en la cantidad de información que se genera cada día en cada organización. Estos nuevos sistemas de información resultantes demandarán nuevas herramientas y métodos de trabajo, y hacen casi inviable gestionarlos con los actuales.

Por este motivo, es imprescindible contar con un Centro de Datos que cuente con equipamiento y herramientas, que agilicen la gestión y el mantenimiento de los sistemas de información. Este sistema *resiliente* estará preparado ante cualquier cambio que pueda comprometer a dicho sistema y lo suficientemente escalable para suministrar recursos ante cualquier demanda ya sea imprevista o circunstancial.

1.2 Objetivos

Los principales objetivos de este proyecto son:

- ❖ Análisis y estudio actual de las tecnologías y soluciones para un Centro de Datos.
- ❖ Revisión de las tecnologías actuales para la creación de un Centro de Datos.
- ❖ Análisis y desarrollo para la creación de un Centro de Datos.

Los objetivos parciales para lograrlo son los siguientes:

- ❒ Definir los requisitos y alcance del proyecto.
- ❒ Identificar todos los elementos necesarios según el alcance, para implementar un Análisis y estudio actual de las tecnologías y soluciones para un Centro de Datos.
- ❒ Definir y documentar la FASE de Diseño orientado a la solución de Vmware vCloud Foundation.
- ❒ Definir y documentar la FASE de Implantación.
- ❒ Definir marco de trabajo.
- ❒ Ejecución de un presupuesto económico.
- ❒ Conclusiones, bibliografía y ANEXOS.
- ❒ Resumir el proyecto destacando los puntos importantes.

1.3 Alcance

En base a los objetivos se definen tres fases para el desarrollo del proyecto, estas son:

1. **FASE de Diseño de un Centro de Datos de Alto Rendimiento**

   En esta fase se recopila documentación para luego definir los requisitos y características que debe tener el Centro de Datos. También se documentan los diferentes elementos y soluciones necesarias para satisfacer dichos requisitos y objetivos del proyecto. Por último, se describirán recomendaciones para elaborar un catálogo de servicios y un marco de trabajo para el Centro de Datos.

2. **FASE de Implantación de un Centro de Datos de Alto Rendimiento**

   Una vez concluida la fase de diseño, hay que aplicar o hacer realidad todas las soluciones aportadas en la fase de diseño que satisfagan el nivel de disponibilidad, seguridad y *resiliencia*, que son exigidos por los objetivos y requisitos.

3. **Oferta económica, marco de trabajo y conclusiones**

   En esta fase final se presentarán, lo más claro posible, todos los importes desglosados de los diferentes elementos necesarios involucrados en las diferentes fases, por supuesto se presentará un resumen e importe total. También incluirá un modelo de trabajo necesario para gestionar y proveer servicios. Por último, se contarán las conclusiones del proyecto que se han podido extraer durante todo el desarrollo del mismo.

A continuación, se detallan cuestiones que quedan fuera del alcance de este proyecto, pero que es necesario identificar para poder desarrollar con éxito todas las fases:

- Proyectos y diseños de obra civil, relacionados con la construcción de la sala del Centro de Datos, quedan fuera del alcance de este proyecto, la empresa o empresas que desarrollen estos trabajos tendrán la obligación de cumplir las normativas vigentes y los estándares que se definen en las normativas vigentes.

- En este diseño se da por supuesto, que se han realizado y aprobado todos los estudios necesarios para determinar la idoneidad de la ubicación física del Centro de Datos, teniendo en cuenta las probabilidades que hay de fenómenos atmosféricos y catástrofes naturales en un lugar concreto. En consecuencia, se debe seleccionar un lugar con menos probabilidad a sufrir estos eventos. Los estudios tienen que tener en cuenta, que el edificio desde fuera no de apariencias de ser un Centro de Datos y esté aislado sin edificios contiguos para favorecer la seguridad del mismo.

- El diseño y proyectos de las salas que tienen que albergar equipos eléctricos, SAI, baterías y grupos electrógenos. Este último elemento como será común para todo el edificio está fuera del alcance del proyecto.

- El diseño e instalación de techos, falsos suelos y paredes según normativa también quedan fuera del alcance, aunque se definirán los requisitos que deben que tener.

- Las puertas y esclusa con control de accesos según normativa y requisitos de la fase de diseño serán instaladas por la constructora y deberán estar instaladas cuando se entregue la obra.

- También quedan fuera del alcance del proyecto, el detalle o instalación de los cuadros generales de red eléctrica que deben cumplir la normativa, en el plano ANEXO V se recomienda su ubicación en la sala.

- Tampoco entrará en el diseño todos los soportes necesarios para el cableado.

- El diseño del alumbrado se entiende que se realiza por parte de la constructora.

- Manuales de instalación del Hardware o Software necesarios para la implementación del Centro de Datos, estos no se pueden entregar en este documento porque se suelen proporcionar cuando se realiza el pedido o compra de dicho Hardware o Software.

- Por último, queda fuera del alcance el desarrollo del Plan de Riesgos Laborales y el desarrollo del Plan de negocio.

1.4 Enfoque y metodología

Una vez definido el tema que hay que desarrollar y los objetivos, lo primero que se ha realizado es un estudio de las tecnologías y soluciones para un Centro de Datos con un enfoque de proveedores Cloud. Actualmente, son bastantes los proveedores de Cloud que tienen Centros de Datos por todo el mundo y algunos con herramientas propietarias que no se pueden adquirir o comprar.

En consecuencia, se ha realizado una revisión de las tecnologías actuales que son necesarias en un Centro de Datos de Alto Rendimiento, desde el equipamiento hardware a las herramientas software necesarias para explotar el Centro de Datos. Se ha optado por marcas y soluciones contrastadas, con cierta popularidad y madurez en el mercado.

La ejecución del proyecto se basa en la realización de tres fases desglosadas en siete tareas, este proyecto es de una magnitud considerable como para realizarlo en una única tarea. En consecuencia, se ha desglosado en siete tareas para facilitar la ejecución y seguimiento del mismo, de otra forma sería muy complicado realizar no solo este proyecto, si no cualquier otro con la misma magnitud.

1.5 Planificación del proyecto

A continuación, se detallan las siete tareas desglosadas que componen todo el proyecto.

Tarea 1: Análisis y estudio de tecnologías, soluciones y equipamiento para un Centro de Datos.

- **Descripción de la tarea**
  Análisis y estudio de las tecnologías, soluciones y equipamiento que hay actualmente en el mercado, es necesario identificar cada una de las tecnologías y soluciones que son necesarias dado que estas nos recomendarán o identificarán el equipamiento que está certificado para cada solución.

- **Objetivos de la tarea**
  Estudio de la situación actual de tecnologías y soluciones para un Centro de Datos dado que este sector está bajo cambios continuos en todo el mundo, una vez realizado el estudio, identificar las soluciones que son necesarias realizando un análisis más profundo para evaluar sus beneficios y sus costes.

□ Tarea 2: Definir y documentar la FASE de Diseño.

- **Descripción de la tarea**
  Teniendo en cuenta el estándar internacional TIA 942 (Diseño y Construcción de CPDs) y con la premisa de un nivel de disponibilidad TIER III, es necesario definir unos requisitos y un alcance del proyecto que nos proporcionarán una visión de las necesidades que debe cumplir el Centro de Datos y en base a todo esto se realizará un diseño del Centro de Datos.

- **Objetivos de la tarea**
  Recopilar y seleccionar información de los estándares relacionados que deben y pueden aplicarse a un Centro de Datos y estén relacionados con las infraestructuras de un CPD, además de todas las buenas prácticas que aplican.
  Definir los requisitos y alcance del proyecto, y en base a estos, identificar todos los elementos y sus características que son necesarios para implementar un Centro de Datos de Alto Rendimiento.
  Análisis de riesgos y cambios que puedan producirse a lo largo del proyecto.
  Obtener un documento que contenga la FASE de Diseño de un Centro de Datos de Alto Rendimiento, basándonos en la solución de VMware vCloud Foundation que proporciona la solución de un Cloud privado.

□ Tarea 3: Definir y documentar la FASE de Implantación.

- **Descripción de la tarea**
  Es necesario hacer realidad todo aquello que se ha identificado y definido en la FASE de Diseño, por este motivo es imprescindible definir y documentar lo más detallado y conciso posible como se realiza una implantación de un Centro de Datos teniendo en cuenta que esta FASE es la más crítica de un proyecto, cualquier error en esta FASE puede incluso fracasar todo el proyecto.

- **Objetivos de la tarea**
  Desarrollar una FASE de Implantación sobre un caso ficticio que cumpla todos los requisitos y normativas que se han definido en la FASE de Diseño, teniendo en cuenta que hay elementos o soluciones que salen fuera del alcance y en esta fase se pasarán por alto.
  Obtener un documento que contenga la FASE de Implantación de un Centro de Datos de Alto Rendimiento.

□ Tarea 4: Definir marco de trabajo.

- **Descripción de la tarea**
  Análisis y estudio de los diferentes marcos de trabajo que hay actualmente en el mercado, para definir los procesos y procedimientos que son necesarios a lo largo del proyecto y una vez que finalice.

- **Objetivos de la tarea**
  Definir con qué marco de trabajo se va a desarrollar todo el proyecto y una vez que finalice este marco también será utilizado para la gestión y administración del Centro de Datos una vez preste servicio.

□ Tarea 5: Ejecución de un presupuesto económico.

- **Descripción de la tarea**
  Realizar un presupuesto económico lo más real posible para poder realizar con éxito todo el proyecto.

- **Objetivos de la tarea**
  Identificar todo el equipamiento necesario en la FASE de Implantación y horas de trabajo de los diferentes consultores o técnicos que son necesarias para desarrollar con éxito todo el proyecto.
  Buscar o contactar con los diferentes proveedores para obtener un presupuesto de cada uno de los elementos necesarios.
  Realizar y documentar un presupuesto económico para el desarrollo de todo el proyecto.

□ Tarea 6: Conclusiones, bibliografía y ANEXOS

- **Descripción de la tarea**
  Antes de finalizar el proyecto, es importante que se realicen las conclusiones que se han sacado del mismo y documentar escrupulosamente las fuentes que se han obtenido para desarrollar el proyecto.

- **Objetivos de la tarea**
  Obtener las ideas y/o puntos importantes que se han obtenido a lo largo del proyecto y que se quieren destacar reflexionando sobre ellas en un documento.
  Obtener un documento bien referenciado siguiendo los estándares de todas las fuentes que se han usado a lo largo del proyecto.

□ Tarea 7: Presentación del proyecto.

- **Descripción de la tarea**
  Realizar una presentación digital resumiendo y haciendo énfasis en los puntos importantes del proyecto, esta presentación está orientada a vender el proyecto y que las personas que la ven se hagan una idea a alto nivel del proyecto.

- **Objetivos de la tarea**
  Obtener una presentación atractiva que contenga una información resumida de todo el proyecto destacando los puntos más importantes del mismo, esta información será a muy alto nivel.

En el ANEXO I, se detallan un diagrama de Gantt, donde aparecen todas las tareas con fechas y tiempo estimado de finalización para cada tarea.

1.6 Productos obtenidos

El desarrollo final de este proyecto proporcionará un documento de un Diseño de un Centro de Datos de Alto Rendimiento. Este documento incluirá todas fases del proyecto necesarias para el desarrollo del diseño de un Centro de Datos actual y con una visión de futuro.

Este diseño de un Centro de Datos de Alto Rendimiento está orientado a organizaciones públicas o privadas lo suficientemente grandes. Estas tienen que tener la necesidad de ofrecer servicios Cloud (IaaS, PaaS y SaaS) de forma eficiente y ágil, ya sea así misma u otra organización externa. Evidentemente la inversión es grande y no está al alcance de todas las organizaciones, por este motivo antes es aconsejable realizar un estudio o plan de negocio para evaluar si es rentable y realmente necesario para la organización.

Este proyecto afecta a toda la organización, tanto a sus recursos como a toda su plantilla, dado que la implantación del proyecto implica cambios en toda la organización: nuevos procesos, nuevas herramientas, nuevos servicios, nuevos equipamientos, nuevas tecnologías, nuevas comunicaciones, etc. Es importante, que desde un principio la dirección de la organización esté implicada en el proyecto para tener el apoyo en las resistencias al cambio y problemas que puedan ir sucediendo en la implantación del mismo.

1.7 Breve descripción de los otros capítulos de la memoria.

En los últimos años, los datos son imprescindibles para cualquiera de nosotros, por ejemplo, todos usamos *Gmail*. Estos datos se encuentran en Centros de Datos o Data Center, estos pueden ser públicos porque ofrecen servicios desde Internet (Cloud públicos) o pueden ser privados porque están al servicio de la organización que lo gestiona. Estas infraestructuras cada día son más complejas e imprescindibles dado que el negocio de cualquier organización depende del buen funcionamiento del mismo, pero también cada vez es más necesario que puedan interoperar entre ellos.

Este proyecto ambiciona ser capaz de definir los diferentes elementos y aspectos que son necesarios para el diseño de un de un Centro de Datos de Alto Rendimiento con Alta Seguridad y Alta Disponibilidad. Este tiene que garantizar a una organización o institución, la capacidad y disponibilidad de los servicios que preste en forma de IaaS, PaaS o SaaS. Con posibilidad de ofrecer estos servicios como públicos o privados, además de integración con cualquier servicio de Cloud público.

Los primeros capítulos explican qué ha sido y es un Centro de Datos en la actualidad. También se explican todos los elementos que aparecen en un Centro de Datos, las normativas que aplican a este y los marcos de trabajo para su gestión. Estos capítulos sirven al lector de punto de partida como base de conocimientos para entender el lenguaje y todos los elementos que se usan a lo largo del proyecto.

En la fase de diseño nos centraremos, en saber cómo se auto provisionarán los servicios, en el diseño a alto nivel de la solución de *VMware vCloud Foundation* que proporciona un Cloud privado en un Data Center. En este proyecto se detallan todas las soluciones y características que proporcionan *VMware vCloud Foundation* en un Centro de Datos que aspira ofrecer servicios en Cloud.

En la fase de implantación se propone un caso ficticio con una serie de requisitos, en esta fase se documentarán todos los elementos instalados, teniendo en cuenta el estándar internacional TIA 942 (Diseño y Construcción de CPDs) y con un nivel de disponibilidad TIER III. También se detallará un presupuesto económico de todos los elementos implantados, así como una planificación de la fase de implantación. El último capítulo reflejará las conclusiones que se han ido extrayendo a largo del proyecto.

Capítulo 2 Centro de Datos de Alto Rendimiento

A continuación, en este capítulo veremos explicaciones y definiciones de Centro de Datos de Alto Rendimiento, sus elementos más importantes y necesarios en cualquier Centro de Datos en la actualidad.

2.1 Definición

La Wikipedia define Centro de Datos como: "*Un edificio o espacio dentro de un edificio, incluso pueden ser un grupo de edificios, que se usan para albergar sistemas informáticos y componentes asociados, como los sistemas de almacenamiento y telecomunicaciones*" [2.1].

También la normativa TIA 942 define Centro de Datos como "*Un edificio o parte de un edificio cuya función principal es la de albergar una sala de computación y sus áreas de apoyo.*"

El fabricante líder en virtualización define Centro de Datos como: "*Son instalaciones físicas centralizadas donde se alojan ordenadores, redes, almacenamiento y otros equipos de TI que permiten el funcionamiento de una empresa. Los ordenadores de un centro de datos contienen o facilitan aplicaciones, servicios y datos esenciales para la empresa.*"

En definitiva, un Centro de Datos de Alto Rendimiento es un edificio, parte del mismo o un grupo de edificios donde se custodian sistemas de información de una o varias organizaciones y donde se ofrecen servicios informáticos a una organización o varias organizaciones. Se le denomina de Alto Rendimiento porque es capaz de ofrecer servicios que requieren la mayor capacidad, robustez y flexibilidad posible con la actual tecnología del mercado.

Ilustración 1 - Centro de Datos de Google en Dublín (Irlanda)

2.2 Evolución

En 1936 comenzó la era de la informática gracias a la máquina de *Turing,* pero no fue hasta el año 1946 que apareció el primer superordenador que se llamó ENIAC y con éste, el primer centro de datos, esta supercomputadora era de tubos de vacío que ocupaba un espacio de más de 150 m2 y era muy compleja de operar y mantener. Unos años después en 1954 llegó TRADIC dando un salto en la computación porque fue la primera en usar transistores y diodos, dejando de lado los tubos de vacío.

En estos primeros años se idearon métodos para acomodar y organizar un centro de datos, como bastidores o rack que son un estándar para montar equipos, falsos suelos sobre todo para la refrigeración y bandejas de cables que se instalan por el techo o debajo del falso suelo. También se diseñaron pautas básicas de diseño para controlar el acceso a la sala que contenía las supercomputadoras.

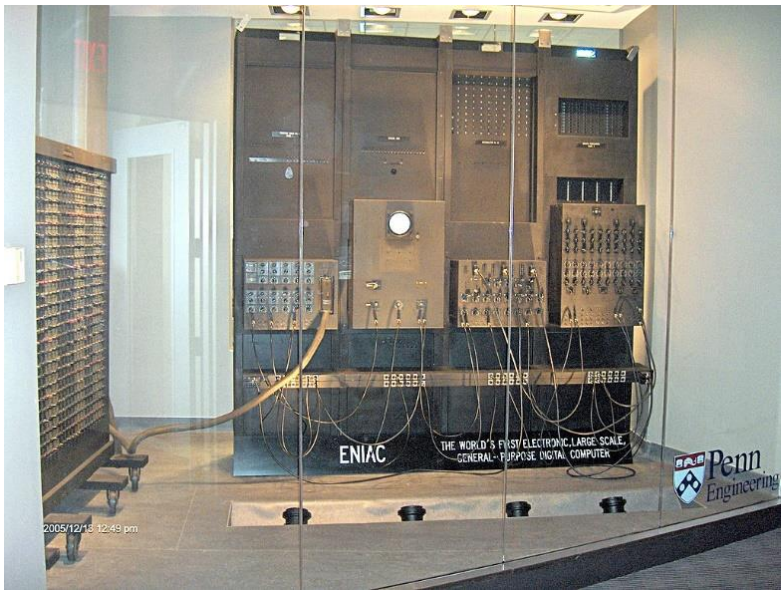


Ilustración 2 - Dos piezas del ENIAC

En estos primeros años y hasta principios de los años 70, los centros de datos se usaban para albergar estas supercomputadoras, a partir de los años 60 con el CDC 6600 de IBM comenzaron a llamarse *mainframes*. Estos tenían capacidad de ejecutar varias tareas y sistemas operativos simultáneamente, además de una gran potencia y velocidad de cómputo. Este sistema centralizado de información se encontró con varios problemas, los costes de mantenimiento debido al gran consumo de energía y un gran desembolso inicial para la implantación propiciaron que estos sistemas fueran usados solo por organizaciones con suficientes recursos.

En el año 1971 Intel presentó el primer procesador programable de propósito general, esto propició que los minicomputadores se convirtieron en una alternativa a los mainframes durante la década de los 70 y 80. Esto procesadores eran más pequeños y eso era una gran ventaja porque reducía los costes. En estos años también aparecieron los primeros PC personales con tarjeta gráfica como *Xerox Alto* y las primeras redes informáticas para conectar hasta 255 computadoras simultáneamente como *ARCnet*. Esto supuso en los años 80 un cambio muy significativo en las tecnologías de un centro de datos junto con la inclusión de las comunicaciones.

En la década de los años 90, los centros de datos comenzaron a contar con tecnologías diferentes dependiendo del uso y su modelo cliente-servidor. Los servidores eran más pequeños pero la información crecía exponencialmente y se necesitaron grandes equipos para almacenar la información. En consecuencia, aparecieron las cabinas de almacenamiento y mecanismos de backup o respaldo. Estos necesitaban librerías de cintas magnéticas para salvaguardar el respaldo de la información de las cabinas de almacenamiento, siendo un hándicap porque eran muy voluminosos y ocupaban mucho espacio en la sala del centro de datos.

También aparecen los primeros *clusters,* que es un conjunto de servidores que se comunican mediante una red de alta velocidad, para proporcionar recursos informáticos como un único servidor, proporcionando un mejor rendimiento, eficiencia y disponibilidad de los mismos.

En los años 90 cada persona en una organización tenía una PC personal y para compartir su trabajo necesitaba conectarse en red, esto propició un aumento de equipos de comunicaciones en los centros de datos, sobre todo al auge que supuso las *puntocom* de Internet. En este momento aparecen nuevos estándares de cableado estructurado que hizo posible un diseño jerárquico colocando los servidores en lugares específicos de la organización.

Las empresas necesitaban una conexión a Internet rápida y sin cortes para establecer una presencia mundial en un sitio web en Internet. Se comenzaron a construir instalaciones muy grandes, llamadas centros de datos de Internet (IDC), para proporcionar mejores capacidades como el respaldo cruzado que evita quedarse sin conexión.

A finales de los años 90 y los primeros años del 2000, los Centros de Datos empiezan a tomar importancia en las organizaciones, custodian equipos de cómputo, de comunicaciones y almacenamiento, cada vez son más grandes y más costosos. A finales de los años 90 nace la tecnología de la virtualización que proporciona que un servidor físico pueda ofrecer recursos a un servidor o varios servidores virtuales simultáneamente, esto hizo posible un ahorro considerable de espacio al necesitar un menor número de servidores físicos por centro de datos.

En estos años comienza la externalización de los centros de datos con el Housing y Hosting, compañías que no podían asumir el coste de todo un centro de datos instalan sus servidores en un espacio alquilado en otro centro de datos que explota otra organización. El Housing proporciona dicho espacio refrigerado y acceso a la alimentación eléctrica como a las comunicaciones del centro de datos. En cambio, el Hosting proporciona todo lo anterior pero el servidor no lo tiene que aportar el cliente si no que es instalado y mantenido por el proveedor de Hosting.

A finales de los años 2000, la mayoría de las organizaciones tenían un centro de datos propio que cada día necesitaba más espacio y más presupuesto para el equipamiento nuevo y el mantenimiento. Aunque la virtualización y los equipos de almacenamiento de información habían reducido las necesidades de espacio, las aplicaciones y servicios no paraban de crecer. Ante esta necesidad y la evolución del Hosting nace el Cloud.

En la actualidad, la mayoría de los centros de datos ofrecen servicios a la propia organización u otras porque están conectados a Internet, es muy fácil que dos centros de datos de diferentes organizaciones se puedan comunicar, pero también se pueden comunicar con centro de datos en la nube. Las organizaciones grandes apuestan por un centro de datos propio con integraciones e interoperabilidad con Cloud públicas y otros centros de datos que garanticen la disponibilidad de los servicios con la mejor optimización y seguridad de los mismos [2.1] [2.2].

2.3 Elementos en un Centro de Datos

En la actualidad, un Centro de Datos está compuesto de muchos elementos físicos, algunos son imprescindibles y de ninguna de las maneras se podría poner en marcha un Centro de Datos sin la presencia de estos. A continuación, se describen los elementos más importantes y necesarios en un Centro de Datos, cada elemento pertenece a una categoría y ofrece una solución al propio Centro de Datos u otro elemento [2.3].

2.3.1 Obra civil

Un Centro de Datos forma parte de un edificio o una sala, por este motivo, tiene la necesidad de contar con los elementos de una obra civil como son:

- Paredes y muros
- Techos
- Suelos
- Paneles
- Puertas

Estos elementos tienen que cumplir normativas nacionales e internacionales sobre el comportamiento frente al fuego, agua, polvo e intrusiones.

El suelo de la sala de un Centro de Datos que alberga los equipos informáticos, es un falso suelo o suelo técnico. Este suelo se compone de paneles con una medida estándar de 60x60 cm, estos paneles se apoyan sobre una estructura de acero que se sujeta con cuatro patas. Esto permite ajustar la altura y proporcionar firmeza al suelo, creando un *plenum* bajo el suelo elevado por donde se canaliza la climatización [2.3] [2.4].

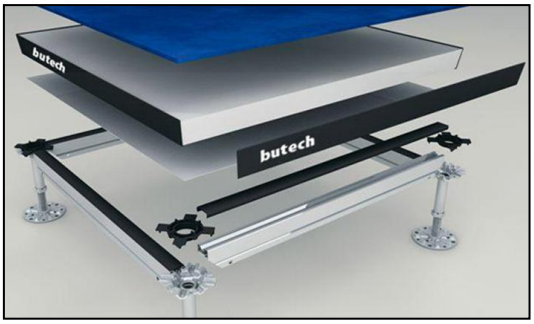


Ilustración 3 - Piezas de un suelo técnico.

Hay dos tipos de paneles, sin rejilla que no dejan salir el aire y sirven para las zonas de paso y ubicaciones de los rack. Los otros tipos de paneles son con rejilla que dejan salir el aire para refrigerar la parte delantera de cada rack [2.4].

Los principales beneficios de estos suelos son:

- Facilidad para realizar instalaciones eléctricas, de refrigeración, agua y antincendios, gracias al hueco que hay en el falso suelo.
- Máxima resistencia al soportar cargas de peso de rack y equipos.

- Alta clasificación al fuego de acuerdo a normativas y estándares europeos.
- Flexibilidad en el intercambio de baldosas unas por otras.
- Eficiencia al evitar pérdidas de refrigeración.
- Control electrostático.

2.3.2 Infraestructura física

Un Centro de Datos dispone de un conjunto de sistemas y elementos que proporcionan todos los recursos necesarios para la puesta en marcha de equipos informáticos con seguridad y alta disponibilidad. Este conjunto se le denomina en el área de TI como infraestructura física de un Centro de Datos también se le conoce como el hardware de un Centro de Datos.

A continuación, se explica en detalle cada uno de los sistemas y elementos que componen un Centro de Datos.

2.3.2.1 Sistemas de energía [2.5]

El principal propósito de un sistema de energía eléctrica en un Centro de Datos es transmitir energía a cada fuente de alimentación que necesite energía eléctrica para su funcionamiento. Es evidente, que este suministro no puede producir cortes para garantizar el correcto funcionamiento del resto de elementos de un Centro de Datos que necesitan suministro eléctrico.

Este sistema se implanta por la comercializadora de la red eléctrica y por la empresa constructora de la obra civil. La comercializadora lleva las acometidas desde la estación eléctrica más cercana hasta las tomas principales de energía eléctrica del edificio y la empresa constructora conecta las acometidas que van desde la sala del Centro de Datos hasta las tomas principales.

Todos elementos usados en esta instalación como los cables, conectores, cuadros de energía, etc, cumplen normativas nacionales e internaciones y están certificados para soportar la carga de energía eléctrica contratada y demandada por el consumo del edificio del Centro de Datos de Alto Rendimiento.

2.3.2.2 Sistema de alimentación ininterrumpida (SAI) [2.6]

Un SAI o UPS (Uninterruptible Power Supply) es un dispositivo que proporciona energía eléctrica continua a todos los elementos que estén conectados a este, y tras un corte de suministro de la red eléctrica es capaz de suministrar energía eléctrica durante un tiempo limitado a todos los elementos, porque está dotado de unas baterías que suministran esa energía. Los SAI son de diferentes capacidades desde unidades pequeñas diseñadas para proteger una sola computadora (alrededor de 200 voltios-amperios nominales) hasta sistemas grandes que alimentan centros de datos o edificios completos.

Los distintos elementos no se conectan directamente a las tomas de alimentación de la red eléctrica, sino que se conectan al SAI que es quien está conectado a las tomas de corriente, haciendo de intermediario entre la red eléctrica y los elementos con necesidades de alimentación. Esto proporciona a todos los elementos conectados una protección porque una interrupción de energía inesperada podría causar lesiones, muertes, interrupciones comerciales graves o pérdida de datos.

El tiempo limitado de funcionamiento con baterías de un SAI suele ser de unos minutos, pero es tiempo suficiente para encender otra fuente de energía de respaldo o para apagar correctamente los elementos conectados a la red eléctrica si esta no se ha restablecido.
A continuación, se enumeran los problemas comunes de la red eléctrica que es capaz de corregir un SAI:

1. Pico de voltaje o sobrevoltaje sostenido.
2. Reducción momentánea o sostenida de la tensión de entrada.
3. Caída de voltaje.
4. Ruido, definido como un transitorio u oscilación de alta frecuencia, generalmente inyectado en la línea por equipos cercanos.
5. Inestabilidad de la frecuencia de la red.
6. Distorsión armónica, definida como una desviación de la forma de onda sinusoidal ideal esperada en la línea.

Existen diferentes tipos de SAI que afectan a su funcionamiento. Los más importantes son tres tipos de SAI: offline/standby, inline/línea interactiva y on-line/doble conversión. A continuación, se describen sus principales características:

SAI OFFLINE / STANDBY

Son los SAI más sencillos, solo entran en funcionamiento cuando se produce un corte de corriente, su funcionamiento es muy simple y por este motivo solo se recomienda su uso para pequeños equipos informáticos. Cuando se produce un corte de corriente el SAI casi de forma instantánea comienza a suministrar energía que acumula en sus baterías, para mantener en funcionamientos los dispositivos conectados. Este tipo de SAI está recomendado para sitios que disponen de una red eléctrica bastante estable y de buena calidad porque carecen de filtros y dispositivos de protección.

SAI INLINE / LINEA INTERACTIVA

Este tipo de SAI es parecido al anterior, pero con la diferencia que incorpora un AVR (Regulador de voltaje automático) que controla las posibles fluctuaciones de la red en ±15% regulando la tensión o corriente de salida, como en la tecnología Offline las baterías solo entran en funcionamiento en el caso de corte de corriente. Esta mejora la tensión de salida lo que proporciona un nivel más de seguridad para los dispositivos conectados a este, la recomendación es utilizar este tipo SAI para equipos de gama media baja, equipos de oficina, electrónica de red, etc.

SAI ONLINE / DOBLE CONVERSIÓN

Un SAI Online siempre está suministrando energía de las baterías, incluso cuando no existe corte de corriente. Esto es una gran ventaja porque garantiza una estabilidad total en la corriente de salida de energía eléctrica y no existe conmutación a modo baterías evitando el riesgo de que los elementos o dispositivos se puedan apagar o dañar en el tiempo de conmutación. Este tipo de SAI son los que mejor rendimiento dan porque son más seguros y tienen una mejor protección.

Un SAI Online realiza una doble conversión de la energía eléctrica, de ahí su nombre, que recibe en su entrada, transformándola en energía eléctrica continua para cargar las baterías y después la vuelve a pasar a alterna, porque es el tipo de corriente que necesitan los elementos conectados. Así proporciona una línea completamente estable con una onda de salida sinusoidal pura protegiendo a los equipos de cualquier anomalía eléctrica.

Los SAI con tecnología Online son de gran fiabilidad y por este motivo, se suelen implantar en sectores profesionales, equipos industriales, equipamiento activo delicado, equipos de TI.

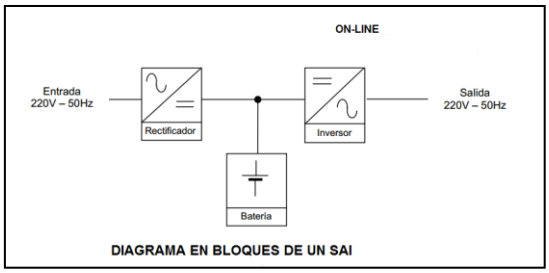


Ilustración 4 -Diagrama de un SAI Online

En definitiva, a la hora de elegir un SAI los factores a tener en cuenta que afectan a su funcionamiento en distintos entornos son: la autonomía de la batería, el coste, el tamaño, el fabricante, el número de tomas o la capacidad de gestión y la tipología de un SAI.

2.3.2.3 Sistema de grupos electrógenos [2.7]

En un caso de corte eléctrico y que los SAI se agoten, se necesita de una fuente de alimentación externa esto se consigue con grupos electrógenos o generadores. Estos proporcionan al Centro de Datos un Alta Disponibilidad porque dichos generadores en caso de un corte de servicio y agotamiento de los SAI, seguirían alimentando por tiempo limitado dependiendo de su autonomía y potencia, evitando así una caída del servicio.

Un generador se compone por un motor primario alimentado por un depósito de combustible diésel, un alternador y un regulador. Además, tiene un sistema de arranque automático, que cuando detecta que no hay suministro de energía, este activa un relé que enciende el grupo electrógeno dando servicio de red eléctrica desde ese momento.

Ilustración 5 - Tres grupos electrógenos industriales

2.3.2.4 Sistema de ventilación y climatización [2.4] [2.5] [2.8]

La producción de calor de los elementos que conforman un Centro de Datos es uno de los principales problemas y uno de los que más preocupan. El exceso de calor en una sala de equipos informáticos afecta negativamente al rendimiento de los equipos y acorta su vida útil, además de suponer un peligro en el caso de alcanzar niveles elevados. Por este motivo, es de vital importancia el diseño de un buen sistema de refrigeración en los Centros de Datos que refrigere manteniendo una temperatura y humedad óptima para el funcionamiento de los equipos con el menor gasto energético.

Según la normativa ASHRAE (American Society of Heating Refrigeration and Air conditioning Engineers) los límites de temperatura recomendados van desde los 18°C hasta los 27°C, la humedad está limitada a menos del 60%, dado que la refrigeración puede provocar la condensación de vapor de agua y en consecuencia pérdida de humedad, es necesario contar con una humidificación suplementaria para mantener el nivel de humedad recomendado.

De manera general, existen tres tipos de climatización de un Centro de Datos:

- **A través del aire**: el objetivo principal de este método es separar el aire caliente del frío; se bombea aire frío hacia los equipamientos y luego se recoge el aire caliente que sale de estos. Es un sistema sencillo, pero requiere un gran consumo de energía.

- **A través del agua**: este tipo de sistemas funcionan con grandes contenedores de agua fría, la cual se bombea a través de tuberías que pasan entre los racks o bastidores y también entre dispositivos. Siempre se mantiene una barrera entre los dispositivos y el agua que circula.

- **Inmersión**: este tipo de sistema funciona mediante la inmersión de los equipos de IT en un fluido dieléctrico que no conduce la electricidad, pero si es capaz de llevarse el calor de los chips de los equipos. Este es el sistema desarrollado más eficiente para refrigerar equipos.

Para evitar un alto consumo de energía, estos sistemas cuentan con una configuración de pasillo frio y pasillo caliente, se calcula que esto puede ahorrar alrededor de un 30% de consumo energético. Este aislamiento de pasillo frio, separa las áreas frías y las calientes sin necesidad de realizar cambios estructurales en la sala del Centro de Datos [2.9].

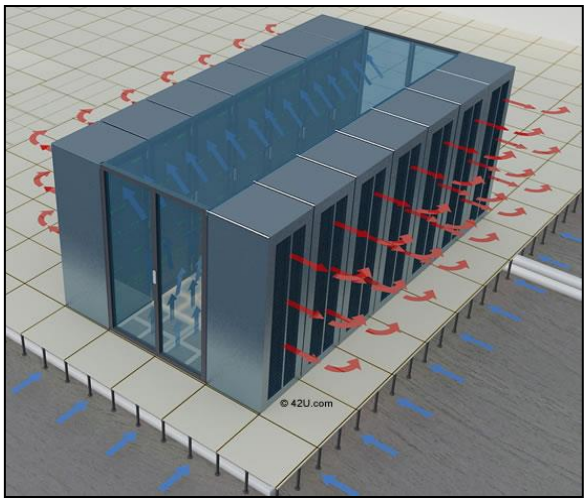


Ilustración 6 - Circuito de aire en un pasillo frio

El sistema de ventilación impulsa el aire frío por el falso suelo y este sale por las rejillas del falso suelo que están dentro del pasillo frío y es donde se absorbe el aire con los ventiladores de los equipos instalados en el rack. El aire caliente luego es expulsado por los propios equipos por detrás de los rack donde está el pasillo caliente.

2.3.2.5 Sistema de seguridad física [2.10]

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control para evitar y prevenir amenazas a los recursos y a la información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor de la capa física de los sistemas informáticos, así como los medios de acceso remoto al sistema y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

Cada sistema es único, por lo tanto, la política de seguridad a implementar no será única es por ello que siempre se recomendarán pautas de aplicación general y no procedimientos específicos.

La seguridad física está enfocada a cubrir las amenazas ocasionadas por las acciones del hombre y por las propias de la naturaleza del medio físico donde se encuentra ubicado el centro. Las principales amenazas que se ven en la seguridad física son amenazas ocasionadas por el hombre como robos, destrucción de la información, disturbios, sabotajes internos y externos, incendios accidentales, tormentas e inundaciones.

Este sistema cuenta con subsistemas que garantizan la seguridad física de un Centro de Datos, algunos como el sistema contra incendios son obligatorios por normativa.

2.3.2.6 Rack

Un rack es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones, tiene cierto parecido con un armario. Tienen una puerta con cerradura para permitir el acceso al interior del mismo. El equipamiento se aloja en el rack mediante guías metálicas que facilitan la extracción del mismo o la sustitución de piezas [2.11].

También suelen contar con PDUs para proporcionar alimentación eléctrica al equipamiento que se instale sobre el rack.

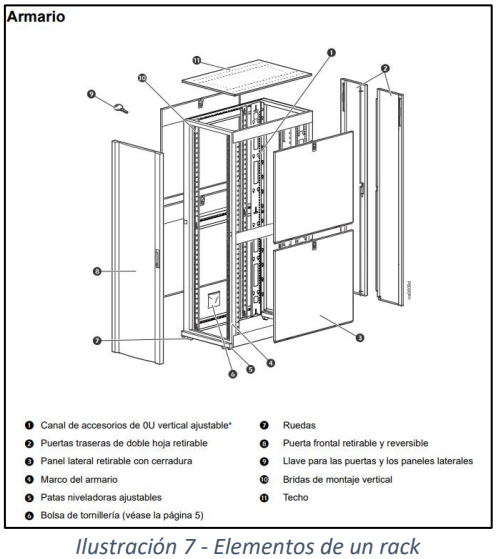


Ilustración 7 - Elementos de un rack

2.3.2.7 Patch Panel [2.12]

Es el elemento encargado de recibir todos los cables de red de cualquier Centro de Datos y de organizar las conexiones de la red. Estos elementos se usan para conectar fácilmente equipos relacionados con la red de área local (LAN) e incorporados al sistema sin dañar los puertos finales de los equipos más delicados y costosos.

Es decir, en estos paneles es donde se ubican los puertos o extremos (analógicos o digitales) de una red, normalmente localizados en un bastidor o rack de comunicaciones. Todas las líneas de entrada y salida de los equipos (computadoras, servidores, impresoras, entre otros) tienen su conexión a uno de estos paneles.

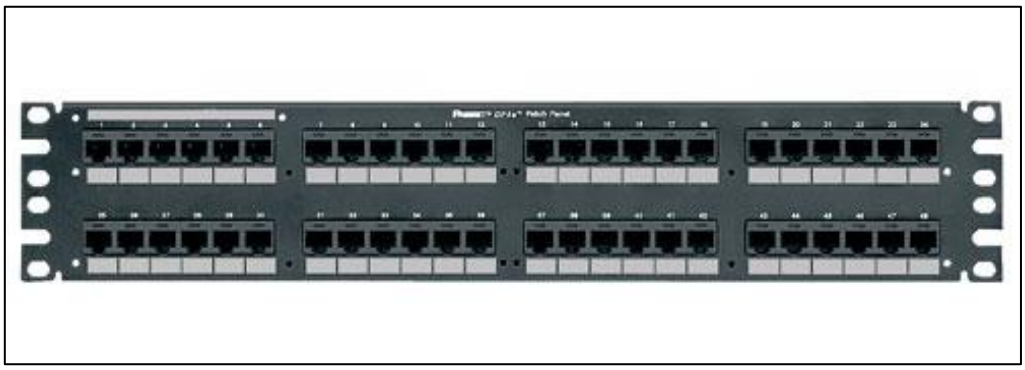


Ilustración 8 - Patch panel de 48 puertos UTP Cat 5

2.3.2.8 Sistema de cableado

El sistema de cableado de un Centro de Datos es un conjunto de cables que, dependiendo del tipo de cable, permite la alimentación eléctrica o la comunicación entre los equipos del Centro de Datos y la comunicación con el exterior del mismo.

A continuación, vamos a detallar según la tipología, el cableado que se usa en un Centro de Datos y que cumple con la normativa TIA-942.

CABLEADO ELÉCTRICO

En la mayoría de los Centro de Datos la distribución desde los cuadros de los sistemas de alimentación ininterrumpida hacia los rack de equipos informáticos, se realiza mediante conductores RZ1 0.6/1kV de cobre de sección adecuada. Cada conexión con los cuadros hasta cada una de las PDU de racks se realiza con conectores *cetac* y con los amperios adecuados al consumo de cada rack [2.5].

El resto de los cables eléctricos son estándar y suelen venir incluidos con el equipo que se instala en el rack que tiene conectores C14 para poder instalar cables de alimentación con conectores C13 a cada una de las fuentes de alimentación de los equipos y tener así redundancia eléctrica (N+1).

Ilustración 9 - Cable con conector C13

Ilustración 10 - Conector de chasis C14

Ilustración 11 - Conectores Cetac

CABLEADO DE RED COBRE

El cable de par trenzado o UTP/FTP, es un tipo de conexión usado en telecomunicaciones en el que dos conductores eléctricos aislados son entrelazados para anular las interferencias de fuentes externas y diafonía de los cables adyacentes. Este se usa para conectar los equipos de comunicaciones con los servidores o entre ellos mismos, siendo el cableado UTP categoría 6 (10mb/s,100mb/s,1gb/s) con conector rj45 es el más usado, aunque cada día menos [2.13].

En la actualidad los conectores SFTP+ tienen un uso más extendido porque son capaces de dar velocidades por encima de 1gb/s.

Ilustración 12 - Conector RJ45

CABLEADO DE FIBRA [2.14]

La fibra óptica es un medio de transmisión, empleado habitualmente en redes de datos, consistente en un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. El haz de luz queda completamente confinado y se propaga por el interior de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, en función de la ley de Snell, la fuente de luz puede provenir de un láser o un diodo LED.

Las fibras se utilizan ampliamente en telecomunicaciones, ya que permiten enviar gran cantidad de datos a una gran distancia, con velocidades similares a las de la radio y superiores a las de un cable convencional. Son el medio de transmisión por excelencia, al ser inmune a las interferencias electromagnéticas, y también se utilizan para redes locales donde se necesite aprovechar las ventajas de la fibra óptica sobre otros medios de transmisión.

El cable de fibra multi-modo (MM) permite más de un camino (o modo) de transmisión de la luz a través de la fibra. Los diámetros de este tipo de fibra son de 50 µm y 62,5 µm. Estos suelen usarse para conectar los servidores a cabinas de almacenamiento y backup, usando un cableado de fibra multimodo con conectores LC conectado a una SAN Fibre Channel. También se suele conectar dos cables a cada servidor para guardar la redundancia y cumplir con la normativa TIA-942 en referente a cableado.

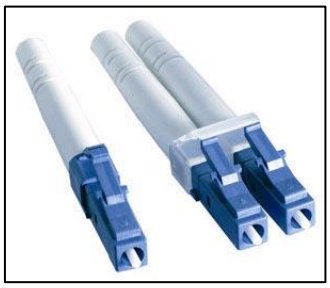


Ilustración 13 - Conector LC monomodo y multinodo.

2.3.2.9 Equipos informáticos

Los equipos informáticos se dividen en tres grandes grupos: equipos para las comunicaciones informáticas, equipos para almacenamiento de datos y equipos para cómputo que también se les llama servidores físicos.

Equipos de comunicaciones

Un equipo de comunicaciones es aquel dispositivo que participa en la comunicación entre dos dispositivos, pero que no es receptor final ni emisor original de los datos que forman parte de esa comunicación. También es el componente del circuito de datos que transforma o adecua las señales para poder utilizar el canal de comunicaciones.

Hay diferentes tipos o categorías dependiendo de la finalidad de la comunicación, estos son los tres tipos más importantes:

- **Firewall:** proporciona seguridad a las comunicaciones permitiendo o negando el tráfico de red que genera una comunicación entre dos dispositivos [2.15].

- **Router:** permite enrutar el tráfico de red entre redes diferentes que se genera en una comunicación entre varios dispositivos [2.16].

- **Switch:** permite comunicar varios dispositivos retransmitiendo el tráfico de red que generan en su red [2.17].

Equipos de cómputo [2.18]

Los equipos de cómputo también se les conoce como servidores físicos o máquinas físicas, pero en realidad son con una arquitectura y elementos parecidos a un ordenador personal, pero con características diferentes para ser más resistentes y potentes que estos.

Estos equipos están diseñados para poder ser montados en un rack y absorben el aire frio por delante expulsando el aire caliente por detrás. Esto supone un ahorro de espacio frente a otros tipos o formatos, es escalable pero su principal problema radica en la dificultad que existe para refrigerarlos.

Equipos de almacenamiento de datos

Según el fabricante HPE (Hewlett Packard Enterprise), “El almacenamiento de datos refiere al uso de medios de grabación para conservar los datos utilizando PC y otros dispositivos. Las formas más frecuentes de almacenamiento de datos son el almacenamiento de archivos, el almacenamiento en bloque y el almacenamiento de objetos, cada uno de los cuales resulta adecuado para un fin diferente.”

Un equipo de almacenamiento o cabina de almacenamiento, es físicamente un rack o varios llenos de discos duros que gracias a su tecnología y una red SAN (*Storage Area Network*) o red Ethernet proporcionan almacenamiento a los equipos de cómputo y a clientes que tienen acceso a estas cabinas. Una SAN es escalable y está diseñada para conectar servidores con las cabinas de almacenamiento con cables de fibra [2.19].

El crecimiento constante del volumen de datos que generan las empresas y la actual tendencia a trabajar con entornos virtuales, han hecho que las necesidades de almacenamiento sean superiores a cualquier estimación. En consecuencia, los fabricantes de cabinas de discos han ampliado su oferta y han hecho que estas soluciones, sean económicamente más asequibles para organizaciones pequeñas y medianas.

Algunas ventajas del almacenamiento compartido respecto al local, son:

- Mejora de utilización de la capacidad de disco.
- Aumento del rendimiento de los discos.
- Equipamientos redundados (fuente alimentación, discos, controladora de disco, caminos de acceso, interfaz de gestión, etc.)
- Gestión de Raid de discos por hardware.
- Gestión centralizada del almacenamiento.
- Copias centralizadas a través de la propia red SAN, liberando de carga la LAN.
- Escalabilidad para aumentar la capacidad de almacenamiento.

Capítulo 3 Tecnologías Software de un Centro de Datos

En el capítulo anterior hemos visto todos los elementos físicos (hardware) que suelen encontrarse en un Centro de Datos, estos elementos por sí solos no aportan valor ni sirven para lo que se han diseñado. Así pues, es necesario un software que gestione, integre y comunique todos estos elementos para que el Centro de Datos ofrezca servicios.

3.1 Software

"*Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación*", según las fuentes de Wikipedia [3.1].

Existen muchos tipos de software, algunos buscan una solución concreta a un problema o soluciones más complejas y holísticas donde una plataforma de Software proporciona una solución a muchos problemas de un mismo ámbito.

Se pueden clasificar en tres tipos, aunque a veces un software no solo pertenece a un tipo, los tres tipos son [3.1]:

- **Software de sistema:** es el software más necesario en un Centro de Datos. Proporciona al usuario y/o programador interfaces de alto nivel, controladores, herramientas y utilidades de apoyo que permiten el mantenimiento del sistema global. Un ejemplo, es Windows 10 que es un sistema operativo.

- **Software de programación:** Es un conjunto de herramientas que permiten a los programadores desarrollar programas informáticos, usando diferentes alternativas y lenguajes de alto nivel de programación, de una manera más práctica y legible para un humano. Un ejemplo es el programa Eclipse que permite desarrollar aplicaciones en varios lenguajes de programación.

- **Software de aplicación:** Está orientado a los usuarios porque realiza una o varias tareas específicas, en cualquier ámbito para cualquier actividad que sea susceptible de ser automatizada, son aplicaciones que aportan valor al negocio. Un ejemplo es Microsoft Word que es un procesador de textos.

3.2 Sistema Operativo

Es un Software de sistema y probablemente el más importante. Este es el software principal o conjunto de programas de un equipo informático que se encarga de gestionar el hardware sobre el que está instalado. Se ejecuta en modo privilegiado para asegurarse que solo él gestiona el hardware y que solo él proporcionar servicios o recursos al resto de programas o software.

Según las fuentes de Wikipedia: "El sistema operativo de escritorio dominante es Microsoft Windows con una cuota de mercado de alrededor del 82,74%. MacOS de Apple Inc. ocupa el segundo lugar (13,23%), y las variedades de GNU/Linux están en tercer lugar (1,57%). Las distribuciones Linux son dominantes en los sectores de servidores y supercomputación [3.1].

3.3 Virtualización

La virtualización es una tecnología software que simula la funcionalidad del hardware, realizando una abstracción para crear servicios de TI basados en software como servidores de aplicaciones, almacenamiento y redes. Es la forma más eficaz de reducir gastos porque aumenta la eficiencia y la agilidad de las organizaciones, aunque son muchas más las ventajas que proporciona este tipo de tecnología imprescindible hoy en día en un Centro de Datos.

Actualmente los cuatro tipos más importantes de virtualización completa son: virtualización de servidores, virtualización de red, virtualización de almacenamiento y virtualización de escritorio de usuario [3.2].

3.3.1 Virtualización de servidores físicos

La virtualización de servidores es una arquitectura de software que permite ejecutar más de un sistema operativo en un servidor como invitado o máquina virtual, en un host o servidor físico específico. El software del servidor de la máquina física se le llama hipervisor y se encarga de abstraer el hardware separando la capa física del servidor a las máquinas virtuales que estén ejecutándose. Estas máquinas virtuales se ejecutan dando por supuesto, que usan exclusivamente los recursos de memoria y de computación, aunque realmente se están ejecutando en una simulación virtual del hardware del servidor que proporciona el hipervisor [3.3].

La virtualización de servidores proporciona un uso más eficiente de los recursos de TI porque se pueden trasladar cargas de trabajo entre diferentes máquinas virtuales y diferentes servidores físicos según la demanda de la carga. El mismo servidor físico puede ejecutar múltiples configuraciones y sistemas operativos lo que significa un aumento de la eficiencia y agilidad.

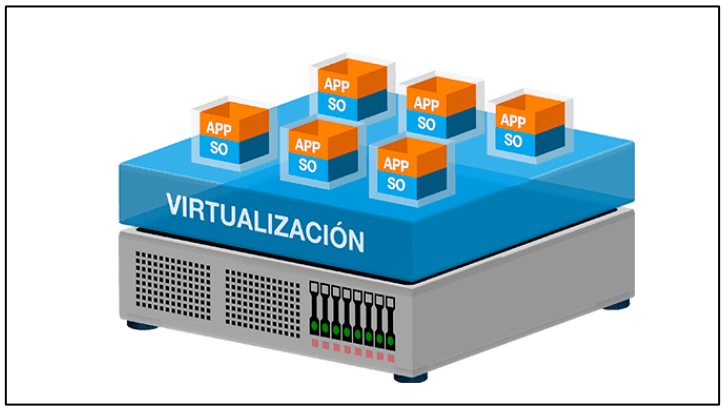


Ilustración 14 - Virtualización de servidor físico

3.3.2 Virtualización de red

La virtualización de red se refiere a la desvinculación de los recursos de red que tradicionalmente se proporcionaban en forma física como hardware. Esta virtualización puede abstraer varias redes físicas en una red virtual o dividir una red física en redes virtuales independientes y separadas, mediante redes definidas por software o SDN (*Software Define Network*) [3.4].

La virtualización de red desvincula los servicios de red del hardware y permite un aprovisionamiento virtual de toda la red. Los recursos de la red física, tales como conmutadores y enrutadores, se agrupan y están accesibles para cualquier usuario a través de un sistema de gestión centralizado. La virtualización de red también hace posible la automatización de muchas tareas administrativas, lo que reduce los errores manuales y el tiempo de aprovisionamiento. Puede aumentar la productividad y la eficiencia de la red.

3.3.3 Virtualización de almacenamiento

La virtualización de almacenamiento se puede definir como una agrupación de los recursos de almacenamiento físico y almacenamiento lógico. Esto proporciona una gestión centralizada de múltiples elementos de almacenamiento en red implicándolos en un único almacén de datos. Gracias a esta tecnología se pude ofrecer recursos de almacenamiento por Software, es decir, almacenamiento definido por Software (SDS) [3.5].

Estos tres tipos de virtualización proporcionan recursos virtuales definidos por software como se ha comentado anteriormente, gracias a estos, se puede definir todo un centro de datos por Software (SDDC). Este concepto se refiere a un centro de datos donde toda la infraestructura se virtualiza y se entrega como un servicio [3.6].

El control del centro de datos está completamente automatizado por el software, es decir, la configuración del hardware o elementos físicos se mantiene a través de los sistemas de software inteligentes. Esto contrasta con los centros de datos tradicionales, donde la infraestructura se define típicamente por hardware y sus elementos físicos se mantienen por personal técnico que usan diferentes tipos de herramientas para cada caso.

Las principales ventajas son [3.6]:

- Simplifica la gestión del centro de datos.
- Mayor eficiencia con menos costes.
- Aplicaciones y servicios desplegados en minutos.
- Disponibilidad y seguridad a la medida de las aplicaciones y servicios.
- Distribución de las cargas de trabajo a través de cualquier plataforma.

3.4 Contenedores y Kubernetes

En la actualidad se confunde el término “contenedores” con “Docker”, porque la empresa Docker fue pionera en la tecnología de contenedores, pero no es un estándar. Los contenedores constituyen un mecanismo de empaquetado lógico en el que las aplicaciones pueden abstraerse del entorno en que realmente se ejecutan. Este mecanismo facilita el despliegue uniforme y estandarizado de aplicaciones con independencia del entorno en el que sea desplegado. Es decir, un contenedor que contiene una aplicación se despliega, actualiza, configura y mantiene igual, aunque lo sistemas operativos sean diferentes.

La creación de contenedores permite separar las áreas de trabajo, porque los desarrolladores se centran en la lógica de negocio y las dependencias de sus aplicaciones y los equipos de operaciones se dedican a la administración. Así pues, el equipo de operaciones IT no tiene que preocuparse por detalles de las versiones de software específicas o las configuraciones determinadas de las aplicaciones o los pasos que hay que realizar en un despliegue.

Los contenedores no virtualizan la pila de hardware como ocurre con las máquinas virtuales, los contenedores se virtualizan a nivel del sistema operativo y para ello utiliza varios contenedores en ejecución encima del *kernel* que es el software más fundamental del sistema operativo. Esto proporciona que los contenedores sean mucho más ligeros porque comparten el *kernel* del sistema operativo, se inician mucho más rápido y utilizan una fracción de la memoria en comparación con el inicio de un sistema operativo completo. En la siguiente imagen se puede observar las diferencias entre ambos conceptos [3.7].

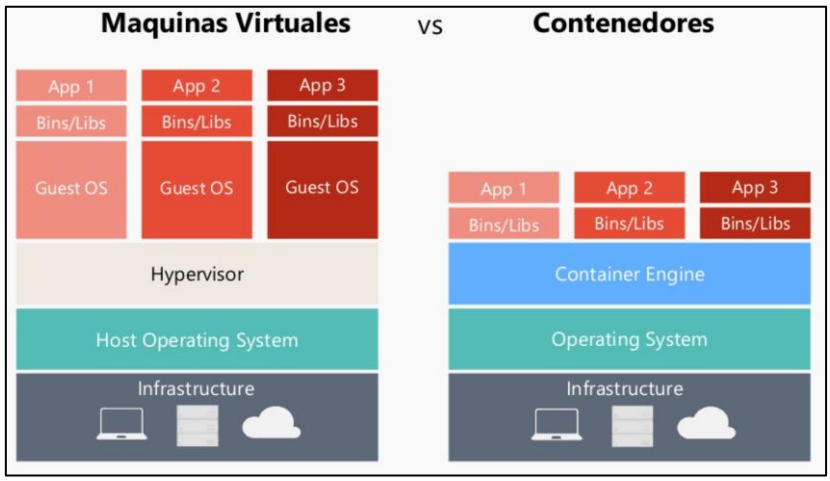


Ilustración 15 - Máquinas virtuales VS Contenedores

Los contenedores tienen muchas ventajas, pero tiene algunos problemas cuando se necesita alta disponibilidad, balanceos de carga, escalar y desescalar carga, persistencia de datos entre diferentes host, etc.

Ante esta necesidad los ingenieros de Google desarrollaron y diseñaron Kubernetes que es una palabra que proviene del griego y significa timonel o piloto. Google fue unos de los primeros colaboradores de la tecnología de contenedores de Linux, además han comunicado públicamente que todo en Google se ejecuta en contenedores (Esta es la tecnología detrás de los servicios de toda la nube de Google).

Kubernetes explicado de forma muy simple es un orquestador de contenedores, proporcionando una gestión centralizada de los contenedores y dotando a estos de la posibilidad de estar en alta disponibilidad en varios host físicos. También dota de la capacidad de escalar un servicio (añadir más contenedores) o desescalar un servicio (quitar los contenedores añadidos) dependiendo de la carga que tengan en cada momento [3.8].

La arquitectura de Kubernetes cuenta dos tipos de nodos: Master y Worker, un nodo puede ser un host físico o una máquina virtual ambos con un sistema operativo. Los nodos master tienen que ser 3 o más nodos y se encargan de la administración de todos los recursos de cómputo, red y almacenamiento gestionados por Kubernetes. Los nodos Worker son gestionados por los nodos master y es donde se ejecutan los contenedores [3.9].

Así pues, se forma un *cluster* se llama así porque todos los nodos están unidos entre sí con una red de alta velocidad y que se comportan como si fuesen un único servidor.

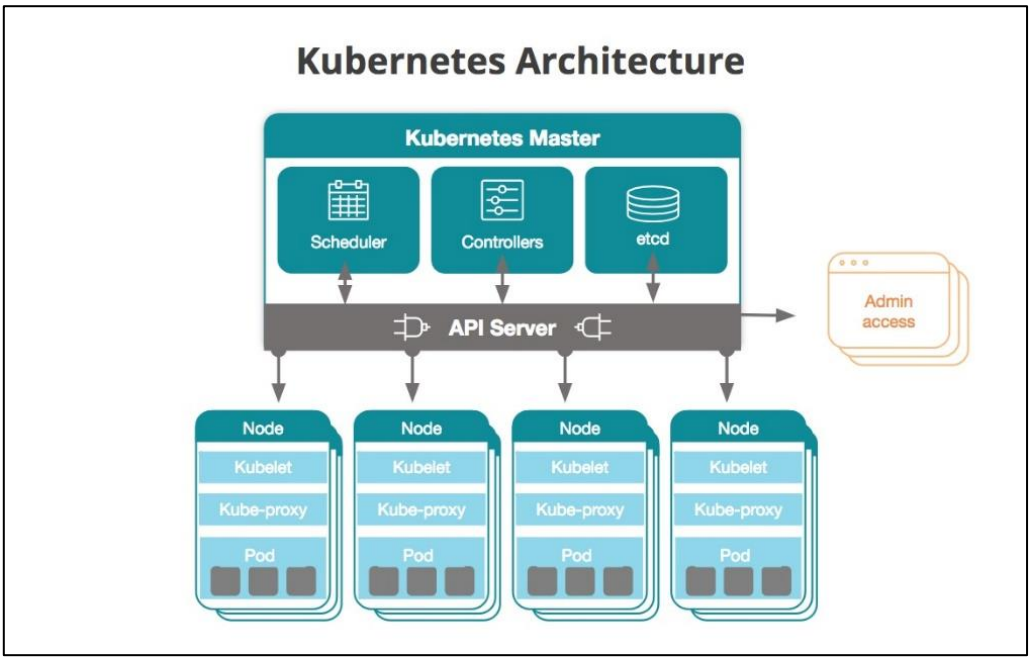


Ilustración 16 - Arquitectura de Kubernetes

3.5 Cloud

3.5.1 Definición [2.2]

El término “Cloud” hoy en día está muy extendido, aunque todavía hay mucha confusión y desconocimiento entre los usuarios acerca de qué es exactamente. El termino más preciso para referirse a este, según su significado, es “computación en la nube”.

Así pues, según Wikipedia: “la computación en la nube es la disponibilidad bajo demanda y en periodos de tiempo, de recursos y/o servicios informáticos, especialmente de almacenamiento de datos y de potencia de cómputo, sin la necesidad de una gestión activa directa por parte del usuario.

Hay dos tipos de Cloud, el Cloud privado que suele estar limitado solo a una organización y el Cloud público que está disponible para cualquier organización o público que tenga acceso a Internet.

Los servicios que provee un Cloud pueden ser usados por usuarios con acceso a Internet con dispositivos móviles o fijos, pero también otros servicios que residan en otros Cloud o Centro de Datos. En los Cloud públicos se pueden usar estos servicios en la modalidad pago por uso, es decir, se paga por el recurso o servicio que se ha usado durante un periodo de tiempo determinado.

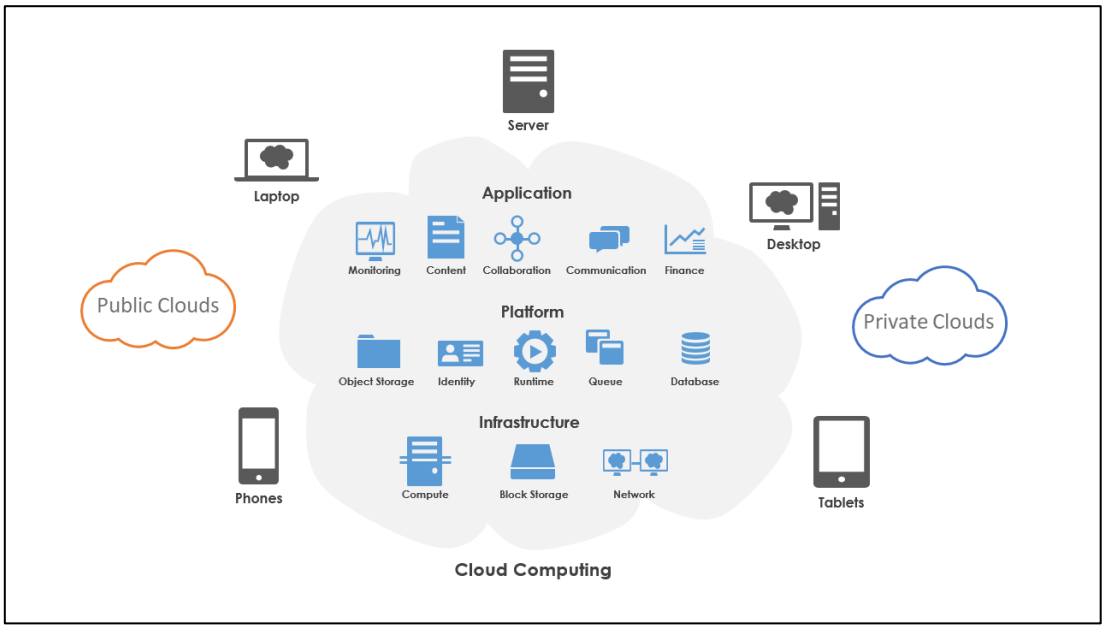


Ilustración 17 - Esquema básico de un Cloud

3.5.2 Características

El Instituto Nacional de Estándares y Tecnología (NIST) identifica cinco características esenciales en un Cloud [3.10]:

1. Un auto servicio en la demanda. Un cliente de un proveedor Cloud puede proporcionarse unilateralmente servicios informáticos o ampliación del mismo, según sea necesario, de forma automática, sin necesidad de una interacción humana.

2. Un amplio acceso a la red. Las capacidades están disponibles a través de la red de Internet y la propia red del proveedor del Cloud. Se accede a ellas a través de mecanismos estándar que promueven el uso de clientes web poco pesados que son fáciles y accesibles.

3. Los Tenant. Los servicios informáticos del proveedor se agrupan para atender a múltiples consumidores mediante un modelo de múltiples clientes, con diferentes recursos físicos y virtuales que son asignados o reasignados dinámicamente según la demanda del consumidor.

4. Una elasticidad rápida. Las capacidades se pueden aprovisionar y liberar elásticamente, en algunos casos de forma automática o programada, para escalar rápidamente verticalmente u horizontalmente de acuerdo con la demanda en cada momento. Esto produce la idea de que, las capacidades disponibles para el aprovisionamiento son ilimitadas y pueden disponerse en cualquier momento.

5. Un servicio automatizado y medido. El uso de servicios se puede monitorizar, controlar y reportar, proporcionando una transparencia tanto para el proveedor como para el cliente del servicio utilizado.

3.5.3 Modelo de servicio

En un Cloud "todo es un servicio" y para ello tiene un modelo de servicio propio. El NIST identifica tres tipos [3.10]:

1. ***IaaS***: Se entiende como ofrecer infraestructura como servicio y el NIST lo define como "el servicio donde el cliente del Cloud puede implementar y ejecutar software arbitrario, que puede incluir sistemas operativos y aplicaciones. El cliente no gestiona toda la infraestructura del Cloud porque está abstraído, pero tiene control sobre los sistemas operativos, almacenamiento y aplicaciones desplegadas". El ejemplo más sencillo de IaaS, es una máquina virtual en un Cloud.

2. ***PaaS***: es un servicio como plataforma y el NIST lo define como "el servicio que un cliente puede implementar sobre IaaS, aplicaciones del cliente utilizando lenguajes de programación, bibliotecas, servicios y herramientas compatibles con el proveedor". El ejemplo más sencillo de PaaS, es un servicio de contenedores para aplicaciones.

3. ***SaaS***: es un servicio como servicio y el NIST lo define como "El uso que puede hacer un cliente de los servicios publicados del propio proveedor del Cloud, sin la necesidad de que el cliente tenga que gestionar nada, solo tiene que preocuparse de cómo usar el servicio ofrecido". El ejemplo más sencillo de SaaS, es un servicio de correo como GMAIL.

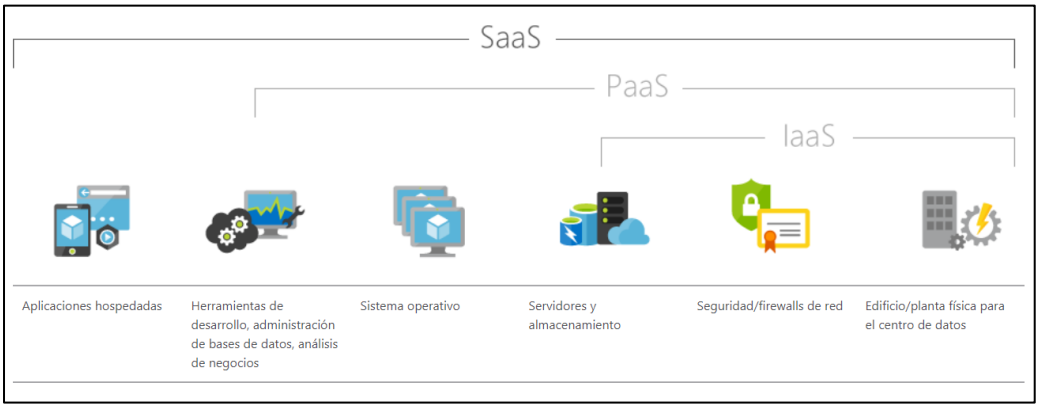


Ilustración 18 - Modelo de servicio de un Cloud

Capítulo 4 Normativas de un Centro de Datos

Los Centros de datos se basan en normas y estándares nacionales e internacionales para garantizar su funcionamiento y seguridad en la gestión de la información. Las Normas más importante son: IEEE 802.3 y ANSI/TIA-942. Este último, gracias al estándar TIER de Uptime Institute establece 4 niveles Tier para clasificar un Centro de Datos según la disponibilidad que proporciona.

4.1 IEEE 802.3

La IEEE es la asociación profesional dedicada al avance de la innovación tecnológica y la excelencia para el beneficio de la humanidad, dentro de ella existe la normativa 802.3 que es una especificación estándar que define qué tipo de cableado para las comunicaciones en un Centro de Datos se permite y cuáles son las características de la señal que transporta [4.1] [4.2].

La especificación 802.3 original utilizaba un cable coaxial grueso de 50 ohm, que permite transportar una señal de 10 Mbps a uno 500 metros. Luego se añadió la posibilidad de utilizar otros tipos de cables como: Coaxial delgado; pares de cables trenzados, y fibra óptica.

En la actualidad, hay cuatro tipos de datos que están definidos para la operación a través de cables de fibra óptica y cables de par trenzado [4.1]:

- 10 Mbps – 10Base-T Ethernet (IEEE 802.3)
- 100 Mbps Fast Ethernet (IEEE 802.3u)
- 1000 Mbps – Gigabit Ethernet (IEEE 802.3z)
- 10-Gigabit – Ethernet de 10 Gbps (IEEE 802.3ae)

4.2 ANSI/TIA-942

En Abril de 2005, Telecomunication Industry Association (TIA) publica su estándar TIA-942 con la intención de unificar criterios en el diseño de áreas de tecnología y comunicaciones. Este estándar en sus orígenes se basaba en una serie de especificaciones para comunicaciones y cableado estructurado [4.3].

Esta norma define los subsistemas de infraestructura generando las líneas base que se deben seguir para clasificar estos subsistemas en función de los distintos grados de disponibilidad que se pretende alcanzar. Los subsistemas son cuatro [4.2]:

- Telecomunicaciones
- Arquitectura
- Sistema Eléctrico
- Sistema Mecánico

La clasificación se realiza según el estándar desarrollado por el Uptime Institute, aceptado a nivel mundial, describe dentro de la normativa 4 niveles (Tiers) de centros de datos en función de su redundancia y disponibilidad de hasta el 99.995% al año.

Los cuatro niveles son:

Nivel I o Tier I

Es el nivel de certificación más básico con una disponibilidad del 99,671% al año, este proporciona una infraestructura para respaldar la tecnología de la información para un entorno de oficina. Los requisitos para una instalación de Nivel I incluyen:

- Una fuente de alimentación ininterrumpida (UPS) para cortes de energía, cortes y picos.
- Un espacio para sistemas informáticos.
- Equipo de enfriamiento dedicado que funciona fuera del horario de oficina.
- Un generador de motor para cortes de energía.

La instalación no tiene componentes redundantes en la distribución eléctrica y ni de equipos de refrigeración. Por lo tanto, pierde capacidad de operación ante el fallo de cualquiera de ellas.

Nivel II o Tier II

Las instalaciones de Nivel II con una disponibilidad del 99,741% al año, cuentan con componentes redundados para el suministro de energía y refrigeración, proporcionando ventanas de mantenimiento y seguridad contra interrupciones. Al igual que en una instalación de Nivel I, el cierre inesperado de un centro de datos de Nivel II afectará al sistema porque solo cuenta con una única línea de suministro eléctrico.

Nivel III o Tier III

Un centro de datos de Nivel III cuenta con una disponibilidad del 99,982% al año, tiene niveles importantes de tolerancia a fallos al contar con todos los equipamientos básicos redundados (N+1) incluido el suministro eléctrico, permitiéndose una configuración Activo / Pasivo. Todos los servidores deben contar con doble fuente y en un principio el Datacenter no requiere paradas para operaciones de mantenimiento básicas. Está conectado a múltiples líneas de distribución eléctrica y de refrigeración.

Nivel IV o Tier IV

Un centro de datos de Nivel IV cuenta con una disponibilidad del 99,995% al año, tiene varios sistemas independientes y físicamente aislados que actúan como componentes redundados y suministro eléctrico redundado. La separación es necesaria para evitar que un evento comprometa ambos sistemas. Sin embargo, si los componentes redundados se apagan por mantenimiento, el entorno puede experimentar un mayor riesgo de interrupción si ocurre un fallo.

Las instalaciones de Nivel IV añaden tolerancia a fallos a la topología de Nivel III. Cuando falla un equipo o hay una interrupción en el suministro eléctrico, las operaciones de TI no se verán afectadas. Los centros de datos de nivel IV también requieren enfriamiento continuo para que el entorno sea estable.

Capítulo 5 Marcos de trabajo

Wikipedia define como marco de trabajo “un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar”.

A continuación, se explica brevemente los marcos de trabajo más importantes en el ámbito de las tecnologías de la información.

5.1 COBIT

COBIT está administrado por ISACA y suele mantener el estándar actualizado con la tecnología más reciente. Está pensado para abordar el crecimiento de TI en las empresas realizando reformulaciones de cómo funcionan los estándares existentes. Es una norma aceptada mundialmente y abarca mucho más que el ámbito de la seguridad de la información al que se limitan otras normas (incluye gestión de riesgos y gobierno TI).

Es más fácil de aplicar de forma parcial sin la necesidad de realizar un análisis de espectro completo y sin requerir un compromiso por parte de la organización. Si bien el hecho de poseer un alcance tan amplio puede ser visto como una fortaleza clave, esta misma característica puede también suponer un obstáculo durante la implementación. Además, al no estar limitado por su diseño a una sola área, a menudo da lugar a lagunas en la cobertura [5.2].

Su objetivo más importante es que las empresas controlen la TI empresarial y establezcan una dirección nítida para ello. Esto significa alinear los objetivos comerciales con los objetivos de TI, gestionar recursos y manejar los riesgos. Desde esta perspectiva, el modelo se postula como un marco adecuado para compañías grandes y más maduras en TI, con muchos procesos y una TI empresarial sustancial.

Tabla 1 - Marco de trabajo COBIT

COBIT (Control Objectives for Information and related Technology) [5.1]	
Creador:	ISACA (Information Systems Audit and Control Association)
Fecha de creación:	La primera edición fue publicada en 1996
Definición:	Es un modelo para garantizar el control y el seguimiento de la gobernabilidad de los SI/TI a largo plazo a través de auditorías
Objetivos:	Los objetivos de COBIT 5 son: agilizar el intercambio de información entre toda la organización, alcanzar objetivos corporativos incluyendo TI en la estrategia, minimizar y controlar la seguridad de la información y gestión de riesgos y optimizar el coste de TI

Características más importantes:	• Marco de alto nivel (con respecto a ITIL, ISO 27002 y NIST) • Diseñado como un estándar ajustable a las buenas prácticas • Suministra herramientas al responsable de los procesos para facilitar su control • Ayuda a la gerencia a comprender y administrar los riesgos asociados con TI y a ejecutar con éxito las políticas clave • Disminuye las brechas existentes entre control, riesgos de negocio y aspectos técnicos
Fases o etapas:	Formado por 4 dominios, cada uno de los cuales están organizados en procesos (34 en total): 1. ***Planificación y organización***: Actividades que definen las estrategias de TI para que la compañía logre sus objetivos 2. ***Adquisición e implementación***: Define, ajusta e implementa el plan de TI en línea con los procesos de negocio de la organización 3. ***Entrega y soporte***: Comprende la entrega de los servicios requeridos garantizando la efectividad y eficiencia de los sistemas 4. ***Monitoreo y evaluación***: Actividades de inspección de los procesos de TI con el fin de verificar que la solución corresponde con las necesidades de la organización desde una perspectiva estratégica
Puntos Fuertes:	• Suministra un lenguaje común para ejecutivos, auditores y otro tipo de profesionales • Proporciona roles y responsabilidades • Ideal para todo tipo de empresa, PYME o gran empresa • Expande la base de conocimiento a todos los sectores productivos de la industria • Centrado en los documentos • Mejora los criterios para la toma de decisiones • Define los planes estratégicos de TI basados en la arquitectura • Asegura el servicio continuo • Ayuda en los procesos de auditoría
Puntos Débiles:	• Presenta un modelo bastante ambicioso que exige previamente un estudio en profundidad • Se necesita un esfuerzo significativo en la organización para implantar sus estándares • Se limita a temas particulares y hay que adoptarlos por separado (gestión, seguridad, calidad, desarrollo, continuidad, etc.) • Acentúa el abismo entre gerencia y operaciones

5.2 ITIL

ITIL es administrado por el gobierno del Reino Unido (UK), y en sus inicios se utilizaba principalmente en las organizaciones afines a ese país. Sin embargo, hoy en día es un marco global que puede ser considerado por cualquier compañía con independencia de su ubicación geográfica. ITIL destaca en el aumento de la visibilidad y la gestión de los procesos internos para impactar positivamente en la eficiencia y la economía.

Este marco permite entregar el valor máximo a los clientes, optimizar el uso de recursos y capacidades, entregar servicios útiles y confiables, y finalmente, planificar procesos con objetivos tangibles y roles claramente definidos. No obstante, carece de detalles específicos para proporcionar una implementación detallada [5.2].

Aunque su objetivo principal es organizar los servicios de TI en general y el trabajo de los departamentos de TI en particular, no hay que olvidar que también proporciona conceptos básicos "estratégicos" para la organización de servicios de IT. Estas características pueden ayudar a cubrir la mayoría de las necesidades en aquellas empresas modestas en fase de crecimiento. Por otro lado, su carácter altamente orientado al cliente también puede hacerlo interesante en compañías cuya actividad principal tiene una gran dependencia externa.
Además, puede encajar en empresas de outsourcing de TI que prestan servicios a terceros, dado que este modelo está centrado en la gestión de servicios de TI (cómo se tiene gestionar y ofrecer un servicio de TI).

Tabla 2 - Marco de trabajo ITIL

ITIL (Information Technology Infrastructure Library) [5.3] [5.4]	
Creador:	CCTA (Central Computer and Telecommunications Agency) del gobierno británico
Fecha de creación:	Se desarrolló durante los años 80, pero no fue ampliamente adoptada hasta mediados de 1990
Definición:	Es un conjunto de conceptos y mejores prácticas para la gestión y administración efectiva de los servicios de TI
Objetivos:	Su objetivo es proporcionar a los administradores de sistemas de TI las mejores herramientas y documentos que les permitan mejorar la calidad de sus servicios, es decir, mejorar la satisfacción del cliente mientras se alcanzan los objetivos estratégicos de la organización. Para lograrlo, el departamento de TI debe ser considerado como un conjunto de procesos vinculados entre sí
Características más importantes:	• Es un marco de trabajo de procesos IT no propietario basado en las mejores prácticas • Es independiente de la industria, de los proveedores y de la tecnología empleada • Describe los procesos críticos en la administración de servicios de TI poniendo especial énfasis en la seguridad • Garantiza los niveles de servicio establecidos previamente • Produce documentación de procesos, tareas y listas de verificación no específicas de la organización con el objetivo de poder implantar controles y medir el éxito
Fases o etapas:	Ciclo de vida del servicio (V3): 1. ***Estrategia del servicio***: Alinear los servicios proporcionados por TI a los objetivos estratégicos del negocio y definir los requisitos base 2. ***Diseño del servicio***: Análisis de la viabilidad del servicio en función de diferentes factores (económicos, técnicos, políticos, etc.) 3. ***Transición del servicio***: Se desarrollan las capacidades de los servicios asegurando los requisitos y acotando los riesgos (pruebas, evaluación de expectativas y puesta en marcha definitiva) 4. ***Operación del servicio***:

	Monitorización del servicio y registro de la percepción del cliente (se garantiza la eficacia con el fin de generar valor para el cliente y el proveedor del servicio) **5.** ***Mejora Continua del servicio***: Medición y feedback para documentar y evolucionar el servicio
Puntos Fuertes:	• La entrega de servicios TI está muy orientada al cliente • Los servicios se describen en un lenguaje más natural • Mejora la comunicación con la organización al establecer un acuerdo en los puntos de contacto • Conecta las TI y el negocio con seguridad, precisión, velocidad y disponibilidad en la entrega de servicios • Enfocado a los procesos de negocio • Más sencilla de adaptar al ser más flexible • Mejora la comunicación entre usuarios finales, clientes y empleados de la organización • Incrementa la seguridad en la entrega de servicios de TI • Fomenta la productividad y la eficiencia provocando un impacto positivo en los recursos financieros de la empresa • Se puede usar como guía práctica para obtener una mejora continua en la organización
Puntos Débiles:	• Requiere tiempo y esfuerzo para lograr una implantación completa en la cultura organizacional • Los procedimientos pueden convertirse en obstáculos burocráticos y entorpecer la adopción • No siempre se ven las reducciones de coste y la mejora en la entrega de los servicios • Requiere un compromiso real por parte de todos los empleados y niveles de la organización

5.3 COSO

Se creó en 1985 y surgió como una iniciativa para combatir las malas prácticas empresariales que ya en aquellos años empezó a preocupar a organizaciones, países y ciudadanos. Se dedica a estudiar aquellos factores que arrojan información financiera sospechosa o fraudulenta y elabora recomendaciones en forma de textos para las organizaciones y otras entidades reguladoras.

Se estableció en EEUU por cinco organizaciones: el Instituto de Contadores Administrativos (IMA), la Asociación Americana de Contabilidad (AAA), el Instituto Americano de Contadores Públicos Certificados (AICPA), el Instituto de Auditores Internos (IIA) y Financial Executives International (FEI). Fue diseñado para ayudar a las empresas a establecer, evaluar y mejorar su control interno.

La importancia del control interno en las operaciones y la información financiera de una entidad no se puede menospreciar, dado que la existencia o ausencia del proceso determina la calidad de la producción realizada en los estados financieros. Un proceso de control interno actual y en funcionamiento proporciona a los usuarios una "garantía" de que los resultados presentados son precisos y de confianza.

El marco propuesto de COSO ERM (2017) eleva el papel del riesgo en el debate del liderazgo sobre el futuro de la empresa. También enfatiza las conexiones entre riesgo, estrategia y valor.

La actualización proporciona una nueva lente para evaluar cómo el riesgo informa las decisiones estratégicas, que finalmente afectan el desempeño de una organización. Además, el papel del riesgo se enfatiza más al establecer y ejecutar la estrategia, porque al alinear el riesgo y el rendimiento, las organizaciones estarán mejor posicionadas para aprovechar las oportunidades y orientarse hacia el futuro con mayor confianza [5.6].

Tabla 3 - Marco de trabajo COSO

COSO (Committee of Sponsoring Organizations) [5.5] [5.7]	
Creador:	Patrocinada y financiada conjuntamente por 5 importantes asociaciones e institutos profesionales de contabilidad con sede en los Estados Unidos: *Instituto Americano de Contadores Públicos Certificados* (AICPA), *Asociación Americana de Contabilidad* (AAA), *Financial Executives International* (FEI), *Instituto de Auditores Internos* (IIA) e *Instituto de Contadores Administrativos* (IMA)
Fecha de creación:	En 1985 se formó el Comité de Organizaciones Patrocinadoras (COSO)
Definición:	Es un conjunto de directivas para ayudar a que las entidades evalúen y mejoren sus sistemas de control interno aplicando un enfoque orientado a la gestión de riesgos: COSO alinea los objetivos del grupo con los objetivos de las diferentes unidades de negocio, así como los riesgos asumidos y los controles puestos en acción
Objetivos:	• Establecer una definición común del control interno • Proporcionar un marco para cualquier tipo de organización con el fin de que ésta pueda evaluar sus sistemas de control y decidir cómo mejorarlos • Ayudar a la dirección de las empresas a mejorar el control de las actividades de sus organizaciones
Características más importantes:	Los puntos estratégicos más cruciales del marco son: • ***Gobierno y cultura***: Garantiza transparencia en todas las actividades diarias • ***Estrategia y fijación de objetivos***: Requiere que los riesgos se evalúen objetivamente • ***Rendimiento***: Garantiza una notificación efectiva de los riesgos • ***Revisión y corrección***: Auditoría interna y el monitoreo de varios controles. • ***Información, comunicación e informes***: Dicta que debe haber un mecanismo de comunicación confiable entre los miembros internos y externos
Fases o etapas:	A continuación, se detalla un borrador inicial del plan de acción de alto nivel para implementar el enfoque de COSO-ERM: 1. *Buscar la participación y supervisión de la junta directiva y la alta dirección* 2. *Identificar y elegir a un líder para impulsar la implantación* 3. *Establecer un grupo de trabajo de gestión* 4. *Realizar un inventario de las prácticas actuales de gestión de riesgos de la organización* 5. *Ejecutar una evaluación inicial de las estrategias clave y de los riesgos estratégicos relacionados* 6. *Desarrollar un plan de acción consolidado con el respaldo de la alta dirección de la organización* 7. *Desarrollar y mejorar los informes de riesgos* 8. *Desarrollar la próxima fase del plan de acción y poner en marcha las comunicaciones*

Puntos Fuertes:	• Aumenta el alcance de las oportunidades considerando los aspectos de los riesgos positivos y negativos • Aumenta los resultados positivos y el negocio evitando sorpresas negativas • Responde de manera proactiva ante los riesgos, y no con respuestas reactivas • Mejora la capacidad de identificar y gestionar los riesgos en toda la organización • Reduce las irregularidades del rendimiento • Mejoras en la implementación de recursos • Fomenta la comunicación fluida y constructiva con la alta dirección de la organización
Puntos Débiles:	• El control interno no debe costar más de lo que recibe a través de sus beneficios; esto quiere decir que necesariamente se revisan los registros del costo-beneficio • Establece que el control interno sólo está dirigido a cuestiones rutinarias, por lo que no se amolda a situaciones globales • El control interno no debería tener errores; sin embargo, es propenso a quebrarse por los errores humanos que ocurren debido a la desinformación o confusiones durante la interacción de los empleados • Cuando no es aplicado de forma adecuada, el control interno puede verse afectado por los abusos de poder

5.4 DevOps

Es un término que está de moda en la actualidad en el mundo TI, pero no se puede decir que sea un marco de trabajo, aunque está en la línea de ser un conjunto de buenas prácticas y un marco de trabajo. DevOps es un conjunto de prácticas que automatiza los procesos entre el desarrollo de software y los equipos de operaciones TI, con el fin de construir, probar y ejecutar software de manera más ágil y confiable.

El concepto de DevOps se basa en la creación de una cultura de colaboración entre equipos que históricamente funcionaban en silos aislados uno del otro. Los beneficios prometidos incluyen una mayor confianza, lanzamientos de software más rápidos, capacidad para resolver problemas críticos rápidamente y gestionar mejor el trabajo no planificado. Une la entrega ágil y continua, la automatización y mucho más, para ayudar a los equipos de desarrollo y operaciones a ser más eficientes, innovar más rápido y ofrecer un mayor valor a las empresas y los clientes.

Actualmente, en la mayoría de las organizaciones el equipo de operaciones no es consciente de los trabajos de los equipos de desarrollo y viceversa, por este motivo, DevOps alinea los equipos para formar un único grupo de trabajo que trabajen de forma coordinada y con objetivos comunes, además de ofrecer mantenibilidad, previsibilidad, mayor calidad, rentabilidad y tiempo de comercialización.

El ciclo de vida de la metodología de DevOps incluye [5.8]:

- Desarrollo
- Pruebas
- Integración
- Implementación
- Monitorización

Capítulo 6 Diseño de un Centro de Datos de Alto Rendimiento

Son muchos los motivos que justifican la necesidad de adoptar un nuevo Centro de Datos, estas razones son: económicas, culturales, sociales o medioambientales. A continuación, se exponen los motivos principales que acreditan la necesidad de un Centro de Datos de Alto Rendimiento.

Uno de los motivos, es que, en los últimos años, los datos son imprescindibles para cualquiera en su día a día, por ejemplo, muchas personas usan *Gmail o Facebook*. Esta información se encuentra en Centros de Datos o Data Center que pueden ser públicos, porque ofrecen servicios desde Internet, (llamados comúnmente "Cloud públicos") o, privados porque están al servicio de la organización que lo gestiona.

Otro motivo más, son los avances en las tecnologías como la inteligencia artificial y minería de datos cada día son más exigentes con las capacidades de computación. La aparición de nuevos paradigmas ha supuesto la utilización de los servicios que prestan los Cloud públicos como desarrollos continuos (DevOps) o microservicios basados en contenedores. Estas nuevas tendencias, en el sector de las TI, empujan cada vez más a las organizaciones a realizar cambios con la implantación de estos nuevos servicios. En consecuencia, las organizaciones necesitan un Centro de Datos para ser capaces de soportar de forma eficiente, ágil y con el mayor rendimiento posible dichos servicios.

Por estos motivos, estas infraestructuras cada día son más complejas e imprescindibles dado que el negocio de cualquier organización depende del buen funcionamiento del mismo, pero también cada vez es más necesario que puedan interoperar entre ellos. Las organizaciones tienen la necesidad de orientarse a la provisión de servicios que demanden las necesidades de su negocio y aporten valor al mismo, estos servicios son: IaaS, PaaS y SaaS. En los Centros de Datos de años atrás no se diseñaron o no se tenía en cuenta una visión holística de la organización, si no únicamente las necesidades de aplicaciones o repositorios de datos que eran demandados por cada departamento de la organización.

En este documento, se definen los diferentes elementos y aspectos que son necesarios en un diseño de un Centro de Datos de Alto Rendimiento con Alta Seguridad y Alta Disponibilidad. Este diseño sirve, tanto a organizaciones como instituciones, para garantizar la capacidad y disponibilidad de los servicios que presten en forma de IaaS, PaaS o SaaS.

El Centro de Datos tiene que tener la posibilidad de ofrecer estos servicios (IaaS, PaaS y SaaS) como públicos o privados, además de integraciones con cualquier servicio de Cloud público. El diseño de alto nivel se centrará en saber cómo se auto provisionarán los servicios que proporciona un Cloud privado en un Data Center.

Los proyectos se dividen en fases con objeto de facilitar su gestión, mejorar el control, y mantener el proyecto alineado con los objetivos. El conjunto de las fases de un proyecto se denomina ciclo de vida del proyecto. Este ciclo define cinco etapas: inicio, planificación, ejecución, seguimiento y cierre. En consecuencia, es necesario dada la magnitud de este proyecto, dividirlo en varias fases para favorecer el trabajo y la revisión de cada fase. Se han definido tres fases basándose en las etapas del ciclo de vida del proyecto, dado que en el alcance de este proyecto no están contempladas todas las etapas. Las tres fases son:

1. **FASE de Diseño de un Centro de Datos de Alto Rendimiento**

   En esta fase se recopila documentación para luego definir los requisitos y características que debe tener el Centro de Datos. También se documentan los diferentes elementos y soluciones necesarias para satisfacer dichos requisitos y objetivos del proyecto. Por último, se describirán recomendaciones para elaborar un catálogo de servicios y un marco de trabajo para el Centro de Datos.

2. **FASE de Implantación de un Centro de Datos de Alto Rendimiento**

   Una vez concluida la fase de diseño, hay que aplicar o hacer realidad todas las soluciones aportadas en la fase de diseño que satisfagan el nivel de disponibilidad, seguridad y *resiliencia*, que son exigidos por los objetivos y requisitos.

3. **Oferta económica, marco de trabajo y conclusiones**

   En esta fase final se presentará lo más claro posible con todos los importes desglosados de los diferentes elementos necesarios involucrados en las diferentes fases, por supuesto se presentará un resumen e importe total. También incluirá un modelo de trabajo necesario para gestionar y proveer servicios. Por último, se contarán las conclusiones del proyecto que se han podido extraer durante todo el desarrollo del mismo.

Capítulo 7 FASE de Diseño de un Centro de Datos de Alto Rendimiento

7.1 Recopilación de documentación

En la actualidad, no existen estándares o manuales que especifiquen cómo se debe crear un Centro de Datos. Así pues, antes de realizar un diseño, es necesario recopilar información de todas las buenas prácticas que deben y pueden aplicarse al Centro de Datos en base a unos requisitos definidos. Una vez revisada toda la información de los estándares relacionados con las infraestructuras del Centro de Datos, se buscaron proyectos de soluciones de distintos fabricantes y así tener un punto de partida como referencia para realizar dicho diseño.

También se ha realizado una búsqueda de los servicios más demandados y necesarios que actualmente soporta un Centro de Datos de una organización media o grande. Se ha observado que la gran mayoría de las organizaciones están apostando por dar servicios: IaaS, PaaS y SaaS. Esto ha llevado a realizar un análisis y estudio de las herramientas actuales que se pueden implantar en un Centro de Datos para ofrecer estos servicios.

A continuación, se describen algunas normativas y documentación que se han revisado y analizado:

- Estándar internacional *TIA 942* [7.1].
- ISO / IEC 27001 [7.2].
- Esquema de Seguridad Nacional [7.3].
- Reglamento General de Protección de Datos de la Unión Europea (GDPR) [7.4].
- VMware Cloud Foundation Product Documentation [7.5].

7.2 Requisitos de la ubicación para el Centro de Datos

Antes de ejecutar la construcción de un Centro de Datos es necesario evaluar y estudiar la ubicación física tanto del edificio como de la propia sala que custodie los datos. No es válida cualquier ubicación física, es necesario que se cumplan un mínimo de requisitos para garantizar la protección de la información que debe custodiar y proteger. Recordemos que esta información es el mayor activo para cualquier organización en la actualidad.

Por este motivo, cualquier edificio que tenga que albergar un Centro de Datos debe cumplir un mínimo de requisitos que define el estándar internacional *TIA 942*, estos son:

- ❒ El edificio tiene que estar en una ubicación donde las catástrofes naturales se produzcan en el menor grado posible y en el caso de que se puedan producir se deben dotar de medios al edificio para resistir y/o mitigar los daños. Estos fenómenos son: terremotos, inundaciones, erupciones volcánicas y fenómenos atmosféricos extremos como los tornados o huracanes.

- ❒ Es aconsejable que el edificio que contenga el Centro de Datos, esté dotado de dos accesos diferentes al edificio desde calles o carreteras separadas, aunque estas últimas no son aconsejables.

- ❒ Lo recomendado es que sea un único edificio de una planta solamente dedicado exclusivamente al Centro de Datos.

- ❒ Si hay edificios colindantes al edificio que contendrá el Centro de Datos, las empresas de los mismos no deberán dedicarse a actividades industriales.

- ❒ La sala del Centro de Datos no puede estar cerca de fuentes de radiaciones electromagnéticas y/o de radiofrecuencia ya que produce mucho ruido en las señales de las comunicaciones de un Centro de Datos.

- ❒ Es aconsejable que el Centro de Datos se encuentre por encima de los niveles de agua del edificio, por eso hay que evitar instalar sistemas críticos en los sótanos.

- ❒ NO se puede ubicar la sala bajo instalaciones de fontanería que puedan inundar la sala por una rotura en una tubería.

- ❒ Es muy aconsejable y recomendable que la ubicación física de un Centro de Datos esté fuera del alcance de centros urbanos y además esté lo más retirado posible de los mismo.

- ❒ Tampoco es aconsejable que esté cerca de aeropuertos de las zonas de despegue y aterrizaje de los mismos.

Ilustración 19 - Imagen del Datacenter de Telefónica en Alcalá de Henares.

7.3 Características físicas para el Centro de Datos

En apartados anteriores, se ha indicado que la construcción o proyecto de la obra civil que alberga la sala del Centro de Datos está fuera del alcance de este proyecto. Las empresas que se dedican a realizar estas construcciones saben cómo diseñar y realizar estas obras teniendo en cuenta todas las normativas que tienen que cumplir. A continuación, se describen las más importantes [2.5]:

- Código Técnico de la Edificación (CTE). Real Decreto 314/2006 de 17 de Marzo.
- Reglamento Electrotécnico para Baja Tensión aprobado por Decreto 842/2002 de 2 de Agosto (B.O.E. nº 224 de 18.09.02).
- Normas UNE de aplicación en los conceptos que se consideren.
- Normas IEC de aplicación en los conceptos que se consideren.
- Recomendaciones UNESA de aplicación en los aspectos que se consideren.
- NFPA 101- Life Safety Code.
- ANSI/TIA-942-2005 Telecommunications Infrastructure Standard for Data Center.
- Real Decreto 1627/1997 sobre disposiciones mínimas de seguridad en las obras de construcción que obliga a la elaboración de Estudios de Seguridad y Salud.
- Ley de Prevención de Riesgos Laborales.

Sin embargo, es muy usual que la obra esté supervisada por el personal de TI y por este motivo, es necesario detallar una serie de requisitos que la sala del Centro de Datos debe cumplir y este personal debe verificar que cumple. Es importante tener siempre presente que la seguridad es uno de los principales problemas en cualquier Centro de Datos.

A continuación, se detallan una serie de recomendaciones que la empresa constructora debe cumplir cuando realice la obra civil:

- ❒ Los elementos de obra civil como: paredes, techos, suelos y puertas tienen que cumplir la normativa para la protección contra incendios e inundaciones.
- ❒ El Centro de Datos debe cumplir la normativa a lo que se refiere a resistencia antirrobo, estos elementos tienen que resistir dependiendo la herramienta usada, según lo que especifique la normativa aplicada.
- ❒ El Centro de Datos no puede tener ventanas, en caso contrario por razones que están fuera del alcance de este proyecto, las ventanas deben cumplir las normativas anteriormente descritas en cuanto a resistencia de fuego, agua y robo. Es importante que las ventanas no dejen pasar calor, frio y luz del exterior.
- ❒ La altura de la sala del Centro de Datos debe tenerse en cuenta, ya que necesitamos que esta sala albergue el equipamiento necesario sin problemas de espacio o capacidad. Con unos 3 metros o 3 metros y medio de altura en la sala sería suficiente, teniendo en cuenta que la mayoría del cableado irá colgado del techo sobre unas bandejas de rejilla de acero.

- El edificio que contenga la sala del Centro de Datos, debe tener un muelle de carga y descarga que de acceso al edificio y a la sala, sin saltos de planta. Así pues, de esta manera se puede introducir mercancía voluminosa y pesada en sala con montacargas portátiles sin requerir un sobre esfuerzo humano.

- La Sala del del Centro de Datos dispondrá de suelo técnico elevado unos 40 cm del suelo de la sala que deberá cumplir la normativa contra incendios. Tiene que estar formado por baldosas de 60x60 cm con una superficie antiestática, permitiendo soportar 2000 kg/m2 en carga repartida y 400 kg en carga puntual. También se suministrarán rejillas de ventilación que se colocarán delante de cada rack que necesite ventilación aparte de las baldosas.

- No es necesaria la instalación de un falso techo ya que la altura de la sala es suficiente. Todo el espacio disponible que quede entre el techo y los pasillos fríos, se aprovechará para el montaje de las instalaciones de iluminación, de extinción y detección de incendios, de canalizaciones, de cableado de datos y eléctrico, y de conductos del circuito de renovación de aire frio y caliente.

- Las canalizaciones y parte del sistema de extinción contra incendios que contiene agua, se instalarán debajo del falso suelo. Por este motivo, queda prohibido instalar cableado eléctrico ni de datos en el falso suelo, dado que ante cualquier fuga del sistema de extinción podría afectar a dicho cableado sensible al agua.

- La refrigeración es una de las principales preocupaciones en el sector de los Centros de Datos, el aislamiento de pasillos puede mejorar el funcionamiento de la refrigeración en estos. Por este motivo, la sala tiene que contar con un pasillo frio, como se ilustra en el plano de la sala del Centro de Datos en el ANEXO II. Además, tiene que poder albergar un total de 16 rack, aunque en esta primera fase solo se ocupen 8 huecos.

- Las paredes que delimitan la sala con el resto del edificio, deben ser con un tabique formado por dos placas de yeso FOC/15 mm (15+15+70+15+15) atornilladas a cada lado de una estructura metálica de acero galvanizado de 70 mm de ancho, relleno interior de aislante.

- La sala tiene que contar con dos puertas metálicas de acceso, tiene que ser cortafuegos de dos hojas pivotantes de 1,00 x 2,10, homologadas RF-90, con una barra antipánico y retenedor automático.

- Los dos cuadros generales de la sala dispondrán de protecciones magnéticas, térmicas y diferenciales, independientes para cada una de las salidas.

- La sala cuando sea entregada como método llave en mano por la constructora, esta se compromete a entregar la sala en perfecto estado de limpieza y orden para poder realizar la instalación del equipamiento sin problemas de polución o suciedad.

- Se instalará por parte de la constructora como se indica en el plano en el ANEXO II, una esclusa unipersonal con supervisión electrónica y con lector de huella, esta solución evita que personas no autorizadas puedan acceder.
  También contará con un sistema de báscula en el interior de la esclusa, para evitar que varias personas a la vez pasen por la esclusa. El acceso a la esclusa se realiza con la instalación de un sistema de identificación biométrico que identifique unívocamente a la persona que acceda a la sala.

Ilustración 20 - Esclusa unipersonal de alta seguridad.

En el ANEXO II se representa un plano de la sala del Centro de Datos una vez finalizadas las obras.

7.4 Equipamiento

A continuación, se detalla el equipamiento que es necesario en el Centro de Datos de Alto Rendimiento, este contribuirá a proporcionar Alta Disponibilidad y Alta Seguridad, además de una flexibilidad en un posible crecimiento.

7.4.1 Sistema de energía eléctrica [2.5]

El diseño básico de la instalación eléctrica del Centro de Datos se fundamenta en la creación de dos ramas (A y B), cada una de ellas dotada con un Sistema de Alimentación Ininterrumpida (en adelante, SAI), en redundancia (N+1). Desde cada una de estas ramas de SAI, se alimentará al correspondiente Cuadro de Distribución de Sala (PDU) y, desde éstos, se realizará la conexión con cada una de las fuentes de los equipos informáticos instalados en el Centro de Datos.

Para la alimentación eléctrica de las máquinas de climatización de la Sala de Centro de Datos, están previstas dos alimentaciones diferentes. Cada una de las máquinas contará con un conmutador que cambiará de fuente de alimentación en caso de fallar la que tiene asignada.

Es necesario dos cuadros eléctricos alimentados por distintos SAI, para que en caso de corte eléctrico no tengamos perdida de servicios o algún equipo quede dañado. La redundancia es (N+1) y cumple con la norma TIER 3, cada cuadro tendrá un diferencial por cada toma eléctrica que vaya a cada rack y por supuesto el etiquetado correspondiente en cada diferencial del cuadro y a cada toma de los rack.

7.4.2 Sistema de alimentación ininterrumpida (SAI)

Es necesario el suministro de dos SAI de tipo en línea u on-line. Este tipo de SAI, es la topología más sofisticada de todas, dado que ofrece protección completa contra los nueve problemas que puede producirse en el suministro eléctrico [2.6]:

1. Corte de electricidad
2. Sobretensión
3. Picos de tensión
4. Bajada de tensión
5. Baja y alta tensión continuada
6. Ruidos o interferencias radioeléctricas o electromagnéticas en la línea
7. Variaciones de frecuencia
8. Microcortes y conmutaciones
9. Distorsiones armónicas en la forma de onda

El dispositivo genera continuamente una alimentación limpia con una onda sinusoidal perfecta, gracias a la tecnología de doble conversión. Este sistema funciona pasando la electricidad de la red eléctrica (AC) a corriente continua (DC) mediante una primera conversión realizada por un rectificador. Este alimenta un bus interno y el cargador de las baterías.

Mediante una segunda conversión realizada por un inversor DC/AC se transforma la electricidad del bus interno y a salida sinusoidal perfecta, quedando la carga protegida de cualquier anomalía de la red eléctrica. Como las baterías también están conectadas al bus interno, al producirse un corte de luz, el inversor pasa a alimentarse a partir de ellas sin cortes ni conmutaciones.

Es recomendable que en caso de corte las baterías como mínimo puedan suministrar energía al Centro de Datos unos 10 minutos, tiempo suficiente para que se restablezca el suministro eléctrico o para activar los grupos de respaldo.

En definitiva, en caso de fallo o corte en el suministro eléctrico, los dispositivos protegidos no se ven afectados en ningún momento porque no hay un tiempo de conmutación. Además, se debe tener en cuenta un contrato de mantenimiento para la sustitución de las baterías de los SAIs ya que su principal inconveniente son que las baterías trabajan constantemente y tienen un mayor desgaste.

El modelo de SAI con el que contaremos, independientemente de la marca, tendrá las siguientes especificaciones generales [2.5]:

Tabla 4 - Características del SAI

ESPECIFICACIONES SAI	
Topología del SAI	ON-LINE permanente
Tipo de conversión	Doble conversión
By-pass estático	Integrado
Paralelable	Hasta 4 módulos
Características de carga	DIN 41773
Temperatura ambiente	0 – 40º C
Humedad relativa	95% sin condensación
Clase de protección	IP30 estándar, IP31 opcional
Diseñado y fabricado según normas	Calidad: ISO 9001
Seguridad	EN50091-1; UL1778; marca CE
Radiofrecuencia e inmunidad	EN50091-2
Protección al medio ambiente	ISO 14001
Gestión avanzada de las baterías	Programable
Rearranque automático	Programable
Tensión de entrada	3x380/400/415 V
Tolerancia de tensión	+/- 10%
Frecuencia de entrada	50 Hz
Distorsión armónica de la corriente de entrada	<5%
Régimen de entrada de potencia	0 a 100% en 10s. (programable de 0 a 40s.)
Corriente de cortocircuito	10 kA
Tensión de salida	3x380/400/415 V
Tolerancia de tensión	1% estática, carga simétrica
	3% estática, carga asimétrica
	5% dinámica con escalones de carga del 0 al 100%
Distorsión de la tensión	< 3% con carga lineal y < 5% con carga no lineal
Frecuencia de entrada	50 Hz. (_6% sincronizado con red; _ 0,1% sin red
Capacidad de sobrecarga	Funcionamiento con red (125% - 10min o 200% - 60seg).
	Funcionamiento en baterías (150% - 30seg).
	Funcionamiento en by-pass (125% - permanente).
	Capacidad de cortocircuito: 10 kA con by-pass sin daño para los equipos.

Los SAI deben proporcionarse con todo el equipamiento auxiliar y complementario que cumpla la normativa para su perfecta instalación y funcionamiento.

7.4.3 Grupos electrógenos

Aunque este fuera del alcance del proyecto, es recomendable detallar las necesidades que debe cubrir los grupos electrógenos dado que es un punto importante, al ser una contingencia en caso de corte o fallo eléctrico y agotamiento de los SAI.

El Centro de Datos necesitan dos grupos electrógenos que tienen que ser instalados por la empresa constructora y estar disponibles y certificados cuando se finalice la obra. Estos en caso de fallo o corte eléctrico tienen que tener la capacidad de suministro para dar servicio de energía a todo el edificio. Es recomendable que se instalen en la azotea ya que al entrar en funcionamiento genera mucho ruido y gases de combustión, porque son motores que se alimentan de gasoil.

Los grupos tienen que estar conectados cada uno directamente a los dos cuadros generales del Centro de Datos. Así pues, se consigue alta disponibilidad en el suministro eléctrico, porque cuando se produzca un corte y los SAI se agoten, se activan los grupos electrógenos y el sistema puede tolerar un fallo de uno de los dos grupos electrógenos. Por este motivo es muy importante, que cada grupo electrógeno disponga de una potencia lo suficiente para cubrir el 100% del consumo del Centro de Datos solo con un grupo electrógeno, considerando este consumo de modo prioritario.

El funcionamiento de los grupos tiene que ser automático, es decir, la conmutación tiene que ser automática, como se ha comentado antes. Los grupos entrarán en servicio cuando se produzca una desviación de los parámetros de red eléctrica respecto a sus valores nominales. El arranque de los grupos y su entrada con suministradores de potencia al sistema tendrá un tiempo máximo de 20 segundos, comprendiendo en este tiempo la detección del fallo, su comprobación, arranque, cierre de conmutaciones y suministro de energía.

7.4.4 Grupos de ventilación y climatización

Los grupos de ventilación y climatización tienen que conectarse a diferentes suministros o líneas de red eléctrica independientes para tener alta disponibilidad. Los grupos tienen que ser de impulsión a la canalización del falso suelo, de expansión directa, con control estricto de temperatura y humedad.

A continuación, se describen las características más importantes que tienen que tener estos equipos [2.5]:

- Potencia total 41,2 Kw y potencia sensible 41,2 Kw
- Caudal de aire 12.950 m3/h
- Un compresor de expansión directa
- Temperatura ext. 35ºC
- Condensadora Exterior
- Caudal 14.900 m3/h
- Ventilador 1,69 kW
- Impulsión A falso suelo
- Retorno Superior
- Presóstato filtros, sistema de humectación, filtros de alta eficacia EU4, refrigerante R407C y bancada con amortiguadores

Dada la proximidad que puede haber entre las unidades, cada una de ellas estará dotada de compuerta antirretorno. Por otro lado, el conjunto debe disponer de un microprocesador de control en una de las unidades y un display en cada una de las restantes que estarán comunicados entre sí. Esto sirve para controlar el estado de funcionamiento, realizando en caso necesario una función secuenciadora.

Adicionalmente, se dota de un pasillo frío que depende la instalación por parte de la constructora de la obra civil y está fuera del alcance del proyecto.

Este mecanismo mejora la eficiencia energética, porque el aire caliente se expulsa fuera del pasillo frío y el aire frío se impulsa directamente a los pasillos fríos través de la canalización del falso suelo. El aire frío sale por unas rejillas en el pasillo frío, que es donde están los equipos succionando el aire para ventilarse. Así pues, con este método no es necesario mantener los 20-21 °C ni una humedad de entre 40-60 % en toda la sala.

7.4.5 Sistema de seguridad física

Es necesario un conjunto de sistemas para la aplicación de barreras físicas y procedimientos de control que puedan evitar y prevenir amenazas a recursos del Centro de Datos y a la información confidencial que este custodia.

7.4.5.1 Sistema de protección contra incendios [2.5]

El sistema de detección de incendios permite la localización de un incendio y activa la alarma correspondiente. El sistema de incendios puede estar controlado por personal adecuado o puede que esté programado para realizar determinadas acciones que son susceptibles de ser automáticas.

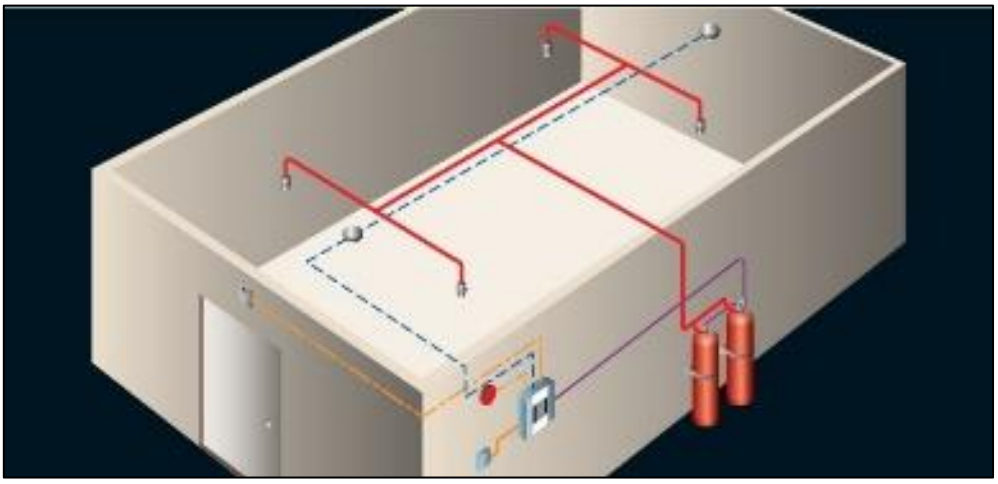


Ilustración 21 - Imagen de un sistema básico contra incendios.

Es necesario e imprescindible así lo indica la normativa, realizar detección y extinción automática de incendios en la sala del Centro de Datos, con una centralita independiente para cada sala. La protección contra incendios de este sistema la realiza mediante un sistema automático de extinción, utilizando como agente extintor el gas FE-13 y agua nebulizada.

Este gas es un agente extintor limpio de alta presión que extingue los incendios principalmente por absorción del calor, presentando ventajas tanto para los propios equipos informáticos instalados en la sala como para el posible personal que se pueda encontrar en la instalación:

- No deja residuos tras su aplicación, ya sea por una descarga fortuita por falsa alarma o por la existencia de un fuego, no afectando por tanto a los equipos sensibles.

- Es totalmente seguro para su aplicación en áreas ocupadas, dado que el NOAEL es del 50%, superior a los valores de todos los demás agentes extintores actualmente empleados.

Las salas son estancas por normativa y los conductos de renovación de aire dispondrán de compuertas cortafuegos en todos los puntos donde éstos atraviesen diferentes sectores de incendios. Los cilindros de agente extintor tienen que ir ubicados en una sala propia y exclusiva para ese fin. Además, se instalarán extintores portátiles en el vestíbulo de acceso y en cada sala.

Los detectores de incendios convencionales (detectores de humo y sensores de calor) se disponen por toda la sala. De forma muy general, considerando techos planos, los detectores de humos cubrirán 80 m2 si se sitúan entre una altura de entre 6 y 12 metros. Si la altura de instalación es inferior a 6 metros, la superficie de cobertura será de 60 m2. En el caso de detectores de calor, en general, la superficie de cobertura es de 20 m2.

7.4.5.2 Sistema de alarma

En la *Wikipedia* se define un sistema de alarma como: *"Un sistema que es un elemento de seguridad pasiva. Esto significa que no evitan una situación anormal, pero sí son capaces de advertir de ella, cumpliendo así, una función disuasoria frente a posibles problemas"* [7.6].

Es necesario dotar al Centro de Datos, con sistema de alarmas diferente según el tipo de situación que queremos que detecte y avise. Este sistema de alarmas debe ser capaz de avisar cuando se produzca: fuego, fuga de agua, una temperatura anormal (menos de 15 ºC o más de 25 ºC) o una intrusión de personal no autorizado.

Por este motivo, es necesario equipar con los diferentes sensores en los lugares recomendados para la detección de anomalías. Este sistema se integrará con el del propio edificio y tendrá avisadores acústicos, además de la posibilidad de habilitar mensajería para avisar mediante SMS, email, o alertas al servidor de monitorización. Este registra las alarmas enviadas y toma acciones adecuadas según el tipo de alarma que recibe.

7.4.5.3 Sistema de CCTV [7.7]

Es un sistema de circuito cerrado de video cámaras de vigilancia que aparte de las cámaras y monitores, tiene un dispositivo de almacenamiento de video, dependiendo del circuito puede ser analógico o basado en redes IP. Aunque se pueden realizar combinaciones dependiendo las necesidades del sitio.

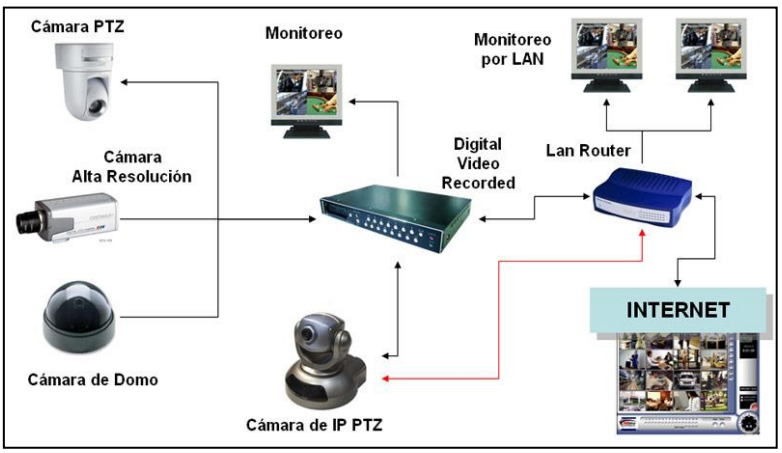


Ilustración 22 – Esquema de soluciones de un CCTV

Las cámaras deben ser móviles con zoom, las cámaras con posicionador, pueden ser remotamente movibles, este movimiento se puede hacer mediante una consola o teclado mediante el cual remotamente se pueden manejar las diversas opciones del software instalado en ésta. También permiten según los modelos, en total oscuridad captar imágenes térmicas o imágenes normales con infrarrojos que la vista de una persona no es capaz de ver.

Este sistema al igual que el sistema de alarmas estará integrado con el propio del edificio para que el personal de seguridad privada que gestiona la seguridad de todo el edificio, pueda vigilar la sala del Centro de Datos con el sistema CCTV.

7.4.5.4 Control de accesos físicos al Centro de Datos

El control de acceso tiene la capacidad de identificar y asociar la apertura o cierre de puertas, permitiendo o negando el acceso, basándose en restricciones de tiempo, un área o un sector que pertenece a una organización. Es decir, se verificará el nivel de acceso de cada persona mediante aplicación de barreras (llave, tarjeta, contraseñas, etc.) [2.10].

Ilustración 23 - Control de acceso de un CPD

El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz de ingreso y salida del personal es necesario un detector de huella digital para abrir la esclusa que da acceso a cada persona autorizada a la sala del Centro de Datos.

También se contará con otro detector de huella digital para abrir la puerta que da acceso a la sala fría. Para abrir la puerta de entrada de mercancía o de emergencia será necesario estar autorizado para deshabilitar el sistema de alarmas y un lector de tarjeta corporativo, además de estar un vigilante de seguridad privada del edificio en persona hasta que se termine con la intervención.

7.4.5.5 Sistema de monitorización del Centro de Datos [7.8]

Son sistemas de monitorización y control capaces de obtener información del entorno donde tienen acceso, para su posterior análisis. En base a este análisis, se realizan las acciones pertinentes o que se le han programado previamente al sistema. Para obtener la información de su entorno hacen uso de una red de sensores. Estos sistemas se pueden clasificar en dos tipos:

- Los sistemas de monitorización, que permiten hacer un seguimiento de los valores recopilados por todos los sensores que forman la red.

- Los sistemas de control, que permiten una vez recopilada y analizada la información del entorno, la puesta en funcionamiento de las acciones más adecuadas. Se puede decir que estos tipos de sistemas, son reactivos, ya que el análisis de los datos y posterior control se realiza de forma automática.

Es fundamental que un Centro de Datos cuente con un sistema integral de monitorización y control certificado.

7.4.6 Racks [2.11]

Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de distintos fabricantes. Es posible que la sala del Centro de Datos necesite tres tipos diferentes de RACK, dependiendo de los equipos o elementos que alberguen, pero siempre cumpliendo las normativas: DIN 41494 parte 1 y 7, UNE-20539 parte 1 y parte 2 e IEC 297 parte 1 y 2, EIA 310-D y la normativa medioambiental RoHS.

7.4.6.1 Racks para servidores de computo

Son RACK de 48U, más altos de lo normal para poder alojar más servidores y así poder ahorrar espacio. Los servidores son enracados ocupando de 4 a más U cada uno, de tal manera que es recomendable contar con el mayor número de servidores usando el menor número de U.

7.4.6.2 Racks para equipos de comunicaciones

Para todos los equipos y elementos de comunicaciones se suele usar Rack de 42 U, para los patch panel se usa un Rack independiente y los otros para los equipos de comunicaciones que suelen instalarse en cluster, así las comunicaciones están redundadas en caso de fallos.

7.4.6.3 Racks para equipos de almacenamiento

Los equipos de almacenamiento suelen proporcionarse con el rack, estos equipos se les conoce como cabinas de almacenamiento y están diseñadas para poder ser escalables. Dependiendo del fabricante serán de unas medidas determinadas, pero siempre cumpliendo la normativa.

7.4.7 Patch Panel [2.12]

Como mínimo es necesario instalar dos rack en un Centro de Datos para tener redundancia (N+1), pacth panels de 24 o 48 bocas de UTP (cables de cobre) o FC (cables de fibra) para las conexiones entre equipos, y según demanda. Es un sistema escalable de bocas y siempre suele haber sitio en el rack para ampliar el número de puertos. Para facilitar la tarea de instalación y peinado de cables se deben instalar pasahilos y organizadores de cableado en los armarios, a través de los que se encaminarán los cables.

7.4.8 Tipos de cableado

A continuación, se detallan los diferentes tipos de cableados con sus características.

7.4.8.1 Cableado eléctrico [2.5]

La distribución desde los dos cuadros de los sistemas de alimentación ininterrumpida hacia los racks de sistemas informáticos, se debe realizar mediante conductores RZ1 0.6/1kV de sección adecuada. Cada conexión con los cuadros hasta cada una de las PDU de racks se realiza con conectores cetac y con los amperios adecuados al consumo de cada rack.

Estos circuitos discurrirán por soportes instalados en el techo que están en la parte superior de los racks. No es recomendable guiarlos por el faso suelo ya que la instalación del sistema contra el fuego funciona con un circuito de agua que discurrirá por el falso suelo y hay que evitar cortocircuitos con estos cables ante una fuga de agua de este circuito.

Para cumplir la normativa y el nivel de Tier III, cada rack estará alimentado por dos cables de alimentación que van a diferentes cuadros eléctricos para evitar cortes de alimentación en los equipos que están instalados en estos. Cada rack tiene conectores C14 para poder instalar cables de alimentación con conectores C13 a cada una de las fuentes de alimentación de los equipos y tener así redundancia eléctrica (N+1).

Los equipos que se conecten a las PDU de los rack se conectarán con un cable estándar que cumpla todas las normativas de la Unión Europea. Este cableado suele proporcionarlo los propios equipos que se conectan a cada rack.

7.4.8.2 Cableado de red cobre [7.9]

El cable de red cobre recomendado es el FTP categoría 7 con clavija RJ45 y una frecuencia de 600 MHz según la norma internacional ISO-11801, (10 Gigabit Ethernet de la norma IEEE 802).

Los equipos informáticos que usan este tipo de cableado nunca se deben conectar directamente, es recomendable usar los patch panel y los switch que estarán en sus rack correspondientes. Así pues, la interface de un servidor físico se conecta con este cableado a una boca libre del patch panel y esta boca se conecta a la interface del switch que da acceso al servidor físico.

Cada equipo de comunicaciones debe estar en cluster, cada servidor físico como mínimo debe tener dos interfaces de red para conectar dos cables de red a cada interface del servidor físico conectados a una interface de un equipo diferente de comunicaciones. Este mecanismo es necesario para disponer de una redundancia de la comunicación en caso de fallo o caída.

Este tipo de cableado solo será usado para conectar las interfaces de red de los servidores físicos o cabinas de almacenamiento a los path panel y los puertos de acceso de los switch a los patch panel.

En ningún caso este tipo de cable se usa para cableado troncal u horizontal, es decir, para conectar equipos de comunicaciones entre sí. El máximo de distancia que podemos usar con este cable es de 50 metros para asegurar su correcto funcionamiento, para distancias más largas se tendrá que usar cableado de fibra.

Siempre se debe instalar según normativa TIA-942, por eso el cableado entre equipos se realizará por el techo peinado correctamente sobre los soportes montados para tal fin, por detrás del rack el cableado tiene que estar correctamente sujeto y organizado. También se cuidará el correcto etiquetado siguiendo la normativa TIA-942.

7.4.8.3 Cableado de Fibra [2.14]

El cableado de fibra es necesario para conectar equipos de comunicaciones entre sí y para la red SAN de almacenamiento. También se puede usar para la red Ethernet cuando la distancia entre dispositivos sea mayor de 50 metros o los servidores físicos necesiten velocidades de red Ethernet superiores a los 10gbs.

El tipo de cableado de fibra recomendado es LC OM4, Multimodo 50/125µm 40Gigabit, es insensible a la curvatura multimodo, tiene menos atenuación cuando está doblado o retorcido en comparación con los cables de fibra óptica tradicionales y, hace más eficientes la instalación y el mantenimiento de los cables de fibra óptica. También ahorra más espacio en el cableado de alta densidad del Centro de Datos.

Este tipo de cable de fibra óptica sirve para conectar transceptores 40G BIDI SR, 10G SR, QSFP+, SFP+ etc. También para conexiones Ethernet 10G/40G/100G y es la especificación de fibra preferida para aplicaciones 40G/100G [7.10].

Tabla 5 - Especificaciones técnicas del cable de fibra

Tipo de conector	LC a LC	**Tipo de pulido**	UPC a UPC
Modo de fibra	OM4 50/125µm	**Longitud de onda**	850/1300nm
Distancia 40G Ethernet	150m en 850nm	**Distancia 100G Ethernet**	100m en 850nm
Pérdida de inserción	≤0.3dB	**Pérdida de retorno**	≥30dB
Grado de fibra	Insensible a la curvatura	**Radio mínimo de curvatura**	7.5mm
Atenuación en 850nm	3.0 dB/km	**Atenuación en 1300nm**	1.0 dB/km
Cantidad de fibra	Dúplex	**Diámetro de cable**	2.0mm
Chaqueta	PVC	**Polaridad**	A(Tx) a B(Rx)
Temperatura de funcionamiento	-20~70°C	**Temperatura de almacenamiento**	-40~80°C

7.4.9 Equipos de comunicaciones

Se recomienda contar con cuatro firewall físicos o virtuales para cumplir con el Esquema Nacional de seguridad, separando la red interna de la red externa. También es recomendable cuatro switch (dos para la capa Core y dos para la capa de distribución), y dos switch Brocade de fibra para la red SAN.

Para todos los equipos de comunicaciones es recomendable contar con 2 Rack diferentes de 42 U, juntos pared con pared a los rack de los path panel para facilitar el cableado entre ellos, los equipos de comunicaciones deben estar en cluster para tener las comunicaciones redundantes en caso de fallos.

En capítulos anteriores se ha explicado la necesidad de porqué estos equipos deben prestar servicio en cluster y tener redundancia lógica entre ellos, de tal manera si uno se apaga o falla el otro equipo asume todo el servicio.

7.4.10 Equipos de cómputo

Se recomienda usar servidores en rack, frente a los servidores tipo Blade. Estos se basan en un servidor modular diseñado para minimizar el uso de espacio físico, un chasis Blade contiene múltiples servidores y mecanismos de ventilación y alimentación redundados. Es tipo de servidores es altamente escalable, pero requiere de mecanismos de refrigeración adicionales y un mayor consumo de energía frente a los servidores en rack, todo esto incrementa su coste a largo plazo. Por este motivo, no se recomiendan este tipo de servidores [7.14].

A priori no se han definido los requisitos y las necesidades respecto al hardware de los servidores. Independientemente de la marca, la recomendación es alojar servidores enracados que no ocupen más de 8U, dado que los racks para los servidores se recomiendan de 48U más altos de lo normal. Estos pueden alojar más servidores y ahorrar espacio, de tal manera que en cada rack entran 6 servidores con tecnología hiperconvergente [7.15].

Estos servidores están diseñados para usar la virtualización, y algunos cuenta con GPUs que proporcionan recursos de cómputo de alto rendimiento a los análisis de datos pesados. Si fueran necesarios más servidores físicos, se han previsto de espacio en la sala para que pueda crecer la infraestructura.

7.4.11 Cabinas de almacenamiento de datos

El Centro de Datos necesita un alto rendimiento, escalabilidad y una alta disponibilidad, para poder soportar servicios de datos avanzados de todas las aplicaciones de misión crítica que ofrezca. En la actualidad, las cabinas de almacenamiento están diseñadas para optimizar la tecnología de unidades flash, que sirve para enfrentarse y resolver todos los retos que plantea el Centro de Datos.

Por este motivo, es necesario contar con una red SAN, pero se recomienda que la cabina proporcione almacenamiento a los servidores por la red Ethernet (NAS), generalmente con tecnología iSCSI. Esta cabina tiene que permitir conectar diferentes servidores independientemente del tipo red necesaria y cumplir los siguientes objetivos [7.11]:

- ✓ **Rendimiento**: independientemente de la carga de trabajo y de la utilización de la capacidad de almacenamiento, debe proporcionar un alto rendimiento predecible de manera coherente al Centro de Datos empresarial y ofrecer hasta 4 millones de IOPS con una latencia inferior a 0.5 ms a un ancho de banda de 150 Gb/s.

- ✓ **Alta disponibilidad y resistencia**: con una arquitectura confiable que no tiene puntos únicos de fallo y tiene una disponibilidad comprobada de seis nueves (99,9999%). La capacidad de replicación de múltiples sitios para lograr una recuperación ante desastres y un reinicio rápido.

- ✓ **Compresión en línea**: la compresión es una función que ahorra espacio y está diseñada para permitir que se administre la capacidad de la manera más eficiente posible. La compresión se realiza dentro del sistema y utiliza múltiples rangos de compresión a fin de lograr el promedio de 2:1 para el sistema.

- ✓ **Mejoras en la resistencia del disco flash**: tiene funcionalidades únicas para minimizar significativamente la amplificación de escritura en los discos flash.

- ✓ **Densidad de flash**: mediante discos flash de alta capacidad.

- ✓ **Escalabilidad**: las configuraciones están diseñadas con componentes modulares básicos llamados “bricks”. La capacidad del Brick se puede escalar verticalmente en incrementos específicos de capacidad útil denominados paquetes de capacidad flash.

- ✓ **Consolidación**: almacenamiento All-flash que pueda consolidar almacenamientos de bloques y archivos de sistema. Compatible con muchas opciones de conectividad front-end, incluidos Fibre Channel, iSCSI y FICON para mainframe.

- ✓ **Facilidad de administración**: una interfaz de administración intuitiva que permite a los administradores de TI maximizar la productividad reduciendo considerablemente el tiempo necesario para aprovisionar, administrar y monitorizar los recursos de almacenamiento.

Se recomienda dotar al Centro de Datos con dos cabinas de almacenamiento con las características descritas, que estén dotadas con su propio rack. Todos los cables se instalarán según normativa por encima del rack en los soportes instalados para ello en el techo.

7.5 Diseño de red física Ethernet

Toda organización necesita unas comunicaciones para dar cobertura a sus necesidades, este punto es clave en un buen diseño de un Centro de Datos. Un fallo en este punto del diseño puede hacer fracasar todo el proyecto y hacer inservible el Centro de Datos. El principal propósito de un Centro de Datos es ofrecer servicios, estos se ofrecen gracias a las comunicaciones por este motivo es tan importante este punto.

En el ANEXO III se representa el diseño lógico de red, para las comunicaciones del Centro de Datos de Alto Rendimiento, donde se ha definido una arquitectura recomendada por Cisco, que es el fabricante líder del mercado en las comunicaciones informáticas durante muchos años. Esta arquitectura dispone de tres capas: Core, Distribución y Acceso. También se representa la capa de seguridad que garantiza solo el acceso a la red permitido [7.12].

La capa Core, proporciona un transporte óptimo entre sitios y enrutamiento de alto rendimiento, la criticidad de esta capa hace necesario que los principios de diseño de esta capa proporcionen un nivel adecuado de resiliencia. Así pues, tiene que ofrecer la capacidad de recuperarse rápida y fácilmente después de cualquier evento de fallo de red que se produzca en esta capa.

La capa de Distribución, proporciona conectividad basada en políticas y control de límites entre las capas de acceso y núcleo.

La capa de Acceso, proporciona el acceso al recurso de red a los dispositivos finales que se conectan a ella, es decir, todos los servidores tienen acceso a la red gracias a esta capa.

Es muy común que la capa de Core y Distribución sea una única capa, pero no se ha optado por esto, porque en la capa de acceso se usarán switch virtuales.

Aunque no se sabe la demanda de tráfico que es necesario para el Centro de Datos, se han recomendado unos anchos de banda de cada conexión. Se ha dado por supuesto que las

conexiones a servidores son a 10G y todas las conexiones a los SW CORE son a 40G para garantizar que no haya cuellos de botella.

Este diseño garantiza el cumplimiento del esquema nacional de seguridad si el Centro de Datos fuera evaluado como categoría ALTA, dado que dispone de dos o más equipos de firewall de distinto fabricante con sistemas redundantes que garanticen la continuidad en caso de fallo técnico y aíslan los tráficos entre las redes internas y externas.

Por este motivo, se recomienda contar con una red DMZ que es una zona desmilitarizada que permite agregar una capa adicional de Seguridad a la red entre una red de área local (LAN) y una red menos segura que sea Internet [7.13].

7.6 Diseño de red SAN

Una SAN (Storage Área Network), es una red de área de almacenamiento integral y dedicada a proporcionar recursos de almacenamiento, está diseñada para conectar servidores y librerías de almacenamiento o backup, están basadas en tecnología Fibre Channel y/o SCSI. Su principal función es conectar de forma rápida y segura los distintos elementos que la conforman, esta red transporta los datos entre los servidores y cabinas de almacenamiento, actuando de manera independiente de red LAN, pero coexistiendo con ella [7.16].

Se representa el siguiente diseño lógico de red SAN en el ANEXO IV, para red de almacenamiento del Centro de Datos de Alto Rendimiento, donde se ha definido una arquitectura en malla y redundancia de caminos que son los cables de fibra que se representan.

Así pues, cada cabina está conectada con cuatro cables de fibra a cada Brocade y cada servidor está conectado con cable de fibra a cada Brocade consiguiendo múltiples caminos para acceder al almacenamiento. También se representa cómo se conecta el componente NAS que ofrece almacenamiento a través de la red Ethernet.

Aunque no se sabe la demanda de tráfico de almacenamiento que es necesario para el Centro de Datos, se han recomendado unos anchos de banda de cada conexión. Se ha dado por supuesto que las conexiones a servidores con fibra son a 8G y todas las conexiones de las cabinas a los Brocades se realizan a 16G para garantizar que no haya cuellos de botella.

7.7 Tecnologías Software

El soporte lógico que necesita un servidor para dar un determinado servicio podemos decir que eso es un software, podemos diferenciarlo en diferentes tipos:

- Sistemas Operativos.
- Aplicaciones.
- Herramientas.
- Embebido.

En los últimos años se ha avanzado mucho en la virtualización de servidores y redes, porque son muchos los beneficios que proporciona a una organización. Por este motivo, la estrategia

que se recomienda es virtualizar los servidores, el almacenamiento y la red con la solución líder en el mercado de Vmware. Se han descartado productos *opensource* (software libre, sin coste de licencias y mantenido por una comunidad) debido a que son más complejos de implantar y mantener, además de la ausencia de un soporte oficial ante problemas.

A continuación, se detallan las siguientes ventajas [7.17]:

- Optimizar el aprovechamiento de todos los recursos de hardware.
- Rápida incorporación de nuevos recursos.
- Reducción de los costes de espacio y consumo (Estimación media 10:1).
- Administración global centralizada y simplificada.
- Nos permite gestionar nuestro CPD como un pool de recursos.
- Mejora en los procesos de clonación y copia de sistemas.
- Aislamiento.
- Flexibilidad.
- Alta Disponibilidad.
- Reduce los tiempos de parada.
- Migración en caliente de máquinas virtuales.
- Balanceo dinámico de máquinas virtuales entre los servidores físicos.
- Contribución al medio ambiente.
- Microsegmentación de la red.
- Balanceo de flujos de red.

Además, se recomienda el uso de software libre para reducir costes de licencias, aunque no se han definido los servicios necesarios que debe tener el Centro de Datos, se recomienda la siguiente lista provisional de software necesario para el portal de autoaprovisionamiento de servidores y para infraestructura del propio Centro de Datos.

- Sistemas Operativos.
    - VMware vSphere 7.0
    - Linux CentOS 7 (libre)
    - Windows 2019 Server.

- Bases de datos.
    - MySQL 8 (libre)
    - Oracle 19g
    - PostgreSQL 13 (libre)
    - SQL Server 2019

- Aplicaciones.
    - Apache 2.5 (libre)
    - Servidor de correo PostFix (libre)
    - Bind DNS (libre)
    - DHCP3 (libre)
    - Aplications Server Jboss 6.5 (libre)

- OpenLDAP (libre)
- Proxy Squid (libre)
- Docker (libre)

- Herramientas.
  - Vmware vCloud Foundation
  - Vmware Tanzu
  - Monitorización del sistema con Zabbix (libre).
  - Herramienta de backup: Veeam.
  - Una Wikipedia de conocimiento del proyecto (libre).
  - Centralita Asterisk con FreePBX (libre).
  - Gestor de incidencias con Mantis (libre).
  - Antivirus TrendMicro.

Con este software cubrimos las principales demandas de un Centro de Datos de Alto Rendimiento, al disponer de una plataforma virtual, se está preparado para satisfacer cualquier demanda de nuevos servicios o ampliaciones de los existentes. Todo esto no sería posible si no se contara con la solución de Vmware para desplegar un Cloud on-premise, en el siguiente apartado detallaremos más esta solución.

7.8 Vmware vCloud Foundation

VMware Cloud Foundation, en adelante VCF, es una nueva plataforma de Centro de Datos definido por software (SDDC) del fabricante VMware para Cloud públicas y privadas. Esta plataforma se compone de la virtualización con VMware vSphere (servidores), vSAN (almacenamiento) y NSX (red). Así, se consigue una pila integrada de forma nativa, gracias a las funciones de automatización y gestión del ciclo de vida con el nuevo VMware SDDC Manager.

La implantación de esta plataforma se puede desplegar de forma Cloud local (on-premise) o bien ejecutarse como servicio en Cloud pública. En la siguiente imagen podemos observar un esquema lógico de VCF [7.17].

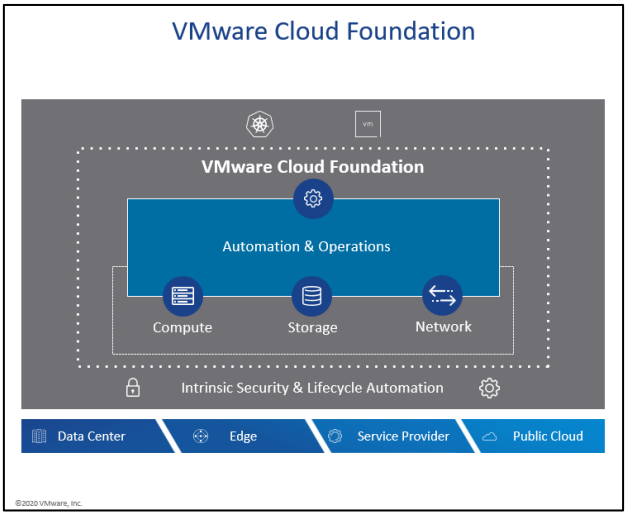


Ilustración 24 - Esquema lógico de VCF

También es una plataforma de nube híbrida para gestionar máquinas virtuales y coordinar contenedores, además de la red y el almacenamiento. Se basa en tecnología de infraestructura hiperconvergente (HCI) de pila completa. VCF, es fácil de implementar porque solo posibilita una única arquitectura y unas operaciones e infraestructura uniformes que son seguras en cualquier entorno Cloud, proporcionando un aumento en la agilidad y la flexibilidad de las organizaciones.

La integración de pila completa de la capa de infraestructura de HCI junto con las capacidades nativas de Kubernetes integradas en la pila proporciona una solución de nube híbrida llave en mano automatizada para administrar entornos complejos de Kubernetes, brindando una experiencia de desarrollador que reduce en gran medida el riesgo y aumenta la eficiencia operativa de TI.

La arquitectura de VCF crea grupos completos de infraestructura bajo demanda a través de "Workload Domains" que brinda a los equipos de TI la capacidad de aprovisionar infraestructura de nube privada de forma ágil y consistente.

Las tareas de parchear y actualizar pueden ser tareas pesadas y complicadas en el Centro de Datos, con el riesgo de errores en las configuración y errores humanos. El ciclo de vida de VCF, gestiona las actualizaciones disponibles para todos los componentes se prueban para la interoperabilidad y luego se empaquetan con la lógica necesaria para el orden de instalación adecuado.

VCF ofrece gestión automatizada del ciclo de vida por clúster. Luego, los paquetes de actualización se programan para la instalación automática que se pueden aplicar a cualquier clúster dentro de cualquier dominio de carga de trabajo. El administrador VCF puede lanzar actualizaciones independientemente a cargas de trabajo o entornos específicos (desarrollo frente a producción, por ejemplo).

Esto permite que la infraestructura definida por software sea administrada, parcheada y actualizada durante el ciclo de vida como una entidad completa, en lugar de componentes individuales sin pérdidas de servicio [7.5].

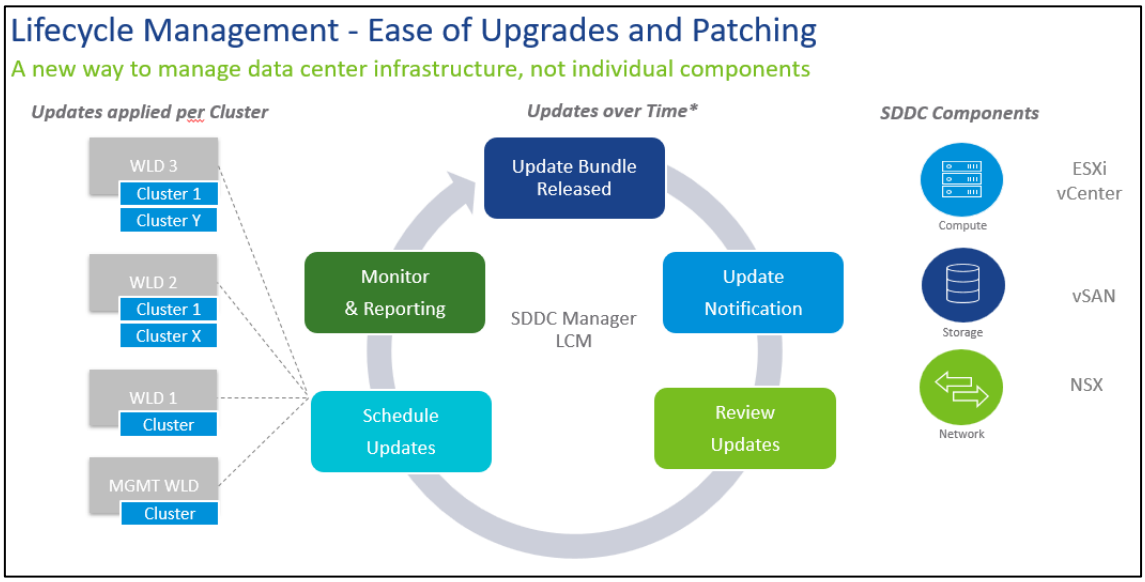


Ilustración 25 - Ciclo de vida de VCF

Anteriormente se ha explicado que VCF se compone de un paquete de soluciones de Vmware que son: VMware vSphere (servidores), vSAN (almacenamiento), NSX (red), vRealize Suite (automatización). Todas estas soluciones son instaladas por VCF en una única instalación sin la necesidad de tener que ir instalando e integrando cada una de estas, esto significa ahorro de costes en la implantación y mantenimiento al contar con una arquitectura estándar.

En los próximos apartados se detallan las funcionalidades de cada una de estas soluciones.

7.8.1 VMware vSphere [7.18]

La última versión en el momento que se está escribiendo este documento, es VMware vSphere 7, es una plataforma de virtualización que transforma los centros de datos en infraestructuras de computación agregadas que incluyen recursos de redes, CPU y almacenamiento. vSphere administra estas infraestructuras como un entorno operativo unificado y proporciona las herramientas para administrar los centros de datos que participan en dicho entorno.

A continuación, veremos en detalle las herramientas que incluye vSphere con su licencia Enterprise Plus.

7.8.1.1 VMware ESXi

Es un hipervisor y es la solución más esencial de la estructura vSphere, es básicamente un sistema operativo ligero que implementa en su núcleo la funcionalidad de virtualizar que permite ejecutar varios sistemas operativos (máquinas virtuales) sobre la misma máquina física. Este hipervisor es de tipo “Bare-metal”, esto quiere decir que se instala directamente sobre el hardware sin necesidad de un sistema operativo HOST (Windows o Linux).

La potencia de este sistema Hipervisor es precisamente que, al estar directamente instalado en un servidor físico, utiliza el hardware disponible en él para distribuirlo entre las máquinas virtuales que estén arrancadas.

Características

- Consolidar el hardware para mejorar la utilización de la capacidad.
- Aumentar el rendimiento para lograr una ventaja competitiva.
- Optimizar la administración de TI mediante una gestión centralizada.
- Reducir la inversión en capital y los gastos operativos.
- Reducir al mínimo los recursos de hardware necesarios para ejecutar el hipervisor, lo que se traduce en una mayor eficiencia.

7.8.1.2 VMware vCenter

Es una plataforma centralizada y extensible para gestionar la infraestructura virtual. vCenter Server gestiona entornos de VMware vSphere y proporciona a los administradores de TI un control sencillo y automático sobre el entorno virtual para distribuir la infraestructura con seguridad. vCenter Server ofrece una gestión centralizada de los hosts virtualizados (ESXi) y de las máquinas virtuales desde una única consola.

Proporciona a los administradores monitorización y visibilidad detallada de la configuración de los componentes fundamentales de la infraestructura virtual, todo desde una única consola web. Un solo administrador puede gestionar cientos de cargas de trabajo, lo que duplica con creces la productividad cuando se gestiona una infraestructura física. El vCenter Server Appliance se basa en Photon OS, por lo que la aplicación de parches y actualizaciones no depende de terceros.

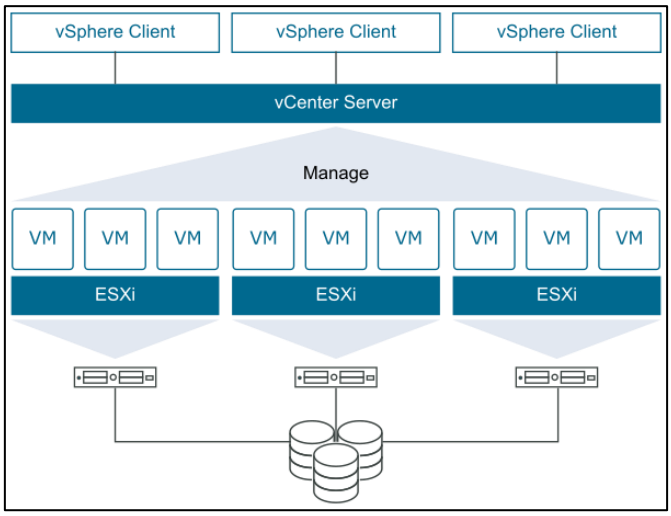


Ilustración 26 - Arquitectura VMware vSphere

Las principales funciones de vCenter Server son:

- **VMware vSphere vMotion**: permite migrar máquinas virtuales sin la necesidad de apagarlas entre diferentes ESXi.

- **VMware vSphere Distributed Resource Scheduler (DRS)**: es una utilidad que equilibra las cargas en los ESXi con los recursos disponibles, dependiendo de las reglas configuradas.

- **VMware vSphere High Availability (HA)**: es un cluster formado por dos o más ESXi, en caso de caída de un ESXi las máquinas virtuales arrancadas en este, automáticamente se arrancan en el ESXi menos cargado o según las políticas del DRS.

- **VMware vSphere Fault Tolerance (FT)**: es un cluster formado por dos o más ESXi, pero en caso de caída de un ESXi las máquinas virtuales arrancadas en este, automáticamente dan servicio sin apagarse en el ESXi configurado con FT.

- **VMware vRealize Orchestrator** (vRO): es un software de flujo de trabajo de arrastrar y soltar que simplifica la automatización de las tareas complejas de TI.

- **Distributed Switch**: proporciona una administración y supervisión centralizada de la configuración de red de todos los hosts (ESXi) asociados con el switch.

7.8.2 VMware vSAN [7.18]

Es un software que define almacenamiento (SDA) mediante la virtualización del almacenamiento que combinado con vSphere, permite gestionar los recursos informáticos y el almacenamiento con una única plataforma, la consola de vCenter. Esta tecnología, puede reducir la complejidad y los costes asociados al almacenamiento tradicional y facilitar la transformación hacia la infraestructura hiperconvergente y nube híbrida.

Es una solución de almacenamiento convergente, que abstrae los recursos de almacenamiento de los servidores (ESXi) que forman parte de una infraestructura virtual. Utiliza los discos HDD y SDD de dichos servidores para crear una capa de almacenamiento resistente y de alto rendimiento, en la capa del hipervisor, para proporcionar volúmenes de almacenamiento a las máquinas virtuales que estén alojadas en esos hipervisores.

Características

- Storage Convergente con el Hipervisor.
- Automatización y administración basa en políticas centradas en las máquinas virtuales.
- Storage Policy Based Management.
- Cache de lectura/escritura en el Servidor.
- Tolerancia a fallos.
- Administración centralizada.
- Crecimiento scale-up y scale-out.
- Independiente del hardware.
- Interoperabilidad con Vmware.

7.8.3 VMware NSX [7.19]

La visión del Centro de Datos definido por el software (SDDC, Software Defined Data Center) de VMware aprovecha las principales tecnologías de virtualización del centro de datos para transformar el centro de datos y ganar agilidad del negocio mediante la automatización. Los centros de datos ya están aprovechando las importantes ventajas de las soluciones de virtualización de almacenamiento y servidor.

Sin embargo, la red del centro de datos no ha evolucionado de la misma manera y sigue siendo rígida, compleja, propietaria y cerrada a la innovación, lo que es un obstáculo para aprovechar todo el potencial de la virtualización y el SDDC. La plataforma de virtualización de redes de VMware NSX ofrece el tercer pilar fundamental de la arquitectura del centro de datos definido por software reduciendo el costo total de propiedad (TCO, Total Cost of Ownership).

La virtualización de redes de NSX permite crear, guardar, eliminar y restaurar redes virtuales según la demanda, sin necesidad de realizar ninguna reconfiguración de la red física. El resultado esencialmente transforma el modelo operacional de la red del centro de datos, reduce el tiempo de aprovisionamiento de la red de días o semanas a minutos y simplifica considerablemente las operaciones de red.

Esta plataforma ofrece todo un conjunto de elementos virtuales y servicios de red lógicos, como switch lógicos, router, firewall, balanceadores de carga, VPN, calidad de servicio (QoS) y supervisión. Estos servicios se implementan en redes virtuales mediante cualquier plataforma Cloud que aproveche las API de gestión del NSX. La solución a estos desafíos es virtualizar la red y hacer con las redes lo mismo que se ha hecho con el procesamiento y el almacenamiento, de hecho, la virtualización de la red es conceptualmente, muy similar a la virtualización de servidor.

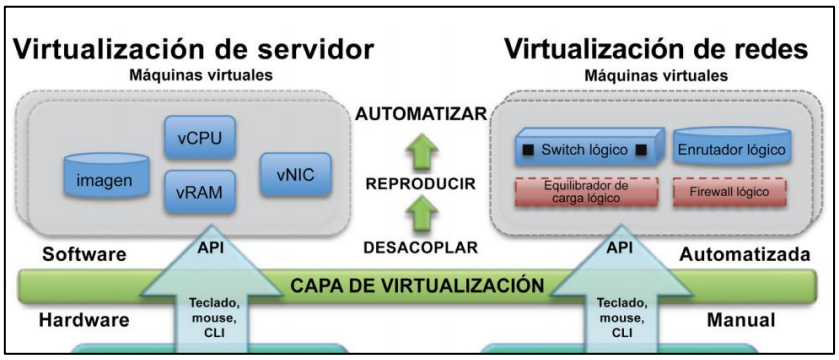


Ilustración 27 - Virtualización de servidor VS virtualización de redes

NSX es una solución no disruptiva que se implementa en cualquier red IP, incluidos los diseños existentes de redes de centro de datos o las arquitecturas de siguiente generación de cualquier proveedor de redes. Las redes virtuales se implementan sin interrupciones en cualquier hardware de red existente.

Características

Tabla 6 - Características VMware NSX

Conmutación	Permite las extensiones de superposición de capa 2 lógicas en una estructura enrutada (capa 3) dentro y a través de los límites del centro de datos. Compatibilidad con superposiciones de redes basadas en VXLAN.
Enrutamiento	Enrutamiento dinámico entre redes virtuales de una manera distribuida en el kernel del hipervisor, enrutamiento de escalabilidad horizontal con conmutación por error activo-activo con routers físicos. Compatibilidad con protocolos de enrutamiento estático y dinámico (OSPF, BGP).
Firewall distribuido	Firewall con estado distribuido, incorporado en el kernel del hipervisor, compatible con Active Directory y supervisión de actividad. También puede proporcionar funciones de firewall de norte a sur a través de NSX Edge
Balanceadores de carga	Funcionan en las capas de la 4 a la 7 con descarga y traspaso de SSL, comprobación del estado del servidor y reglas de aplicaciones para programación y manipulación del tráfico.
VPN	Funciones VPN de acceso remoto y de sitio a sitio, VPN no gestionado para servicios de puerta de enlace a la Cloud.
Puerta de enlace de NSX	Compatibilidad de conexión entre VXLAN y VLAN para una conexión perfecta con las cargas de trabajo del entorno físico.
API de NSX	API de RESTful para la integración en cualquier plataforma de gestión de la Cloud o automatización personalizada.
Operaciones	Funciones de operaciones nativas, como CLI central, Traceflow, SPAN e IPFIX para la solución de problemas y la supervisión proactiva de la infraestructura. Integración con herramientas como VMware vRealize Operations y vRealize Log Insight para técnicas de análisis y solución de problemas avanzadas.

Política de seguridad dinámica	NSX Service Composer permite la creación de grupos de seguridad dinámicos. Más allá de la dirección IP y MAC, la pertenencia a grupos de seguridad se puede basar en etiquetas y objetos de VMware vCenter, el tipo de sistema operativo y las funciones de Active Directory para habilitar una función de aplicación de seguridad dinámica.
Gestión de la Cloud	Integración nativa con vRealize Automation y OpenStack
Integración con otros partners	Soporte de la integración de la gestión, el plano de control y de datos con otros partners en una gran variedad de categorías, como firewall de nueva generación, sistema de prevención y detección de intrusiones (IDS/IPS), antivirus sin agente, controladores de despliegue de aplicaciones, conmutación, operaciones y visibilidad, seguridad avanzada, entre otros.
Gestión de registros	Ayuda a resolver problemas más rápidamente con la mayor visibilidad de vRealize Log Insight para NSX. Visualización de tendencias de eventos, active alertas, etc., todo ello en tiempo real.

Ventajas

- Microsegmentación y seguridad detallada proporcionada a la carga de trabajo individual.
- Menor tiempo de implementación de la red, de días a segundos, además de mejor eficiencia operativa a través de la automatización.
- Movilidad de la carga de trabajo independiente de la topología de la red física en los centros de datos y entre ellos.
- Mayor seguridad y servicios de red avanzados a través de un ecosistema formado por los principales proveedores.

Arquitectura y componentes

NSX-T mediante software reproduce los servicios de red al completo. Estos se pueden montar mediante programación para producir redes virtuales únicas y aisladas en cuestión de unos pocos segundos. NSX-T funciona mediante la implementación de tres planos separados pero integrados: gestión, control y datos. Los planos se implementan como conjuntos de procesos, módulos y agentes que residen en tres tipos de nodos: administrador, controlador y transporte.

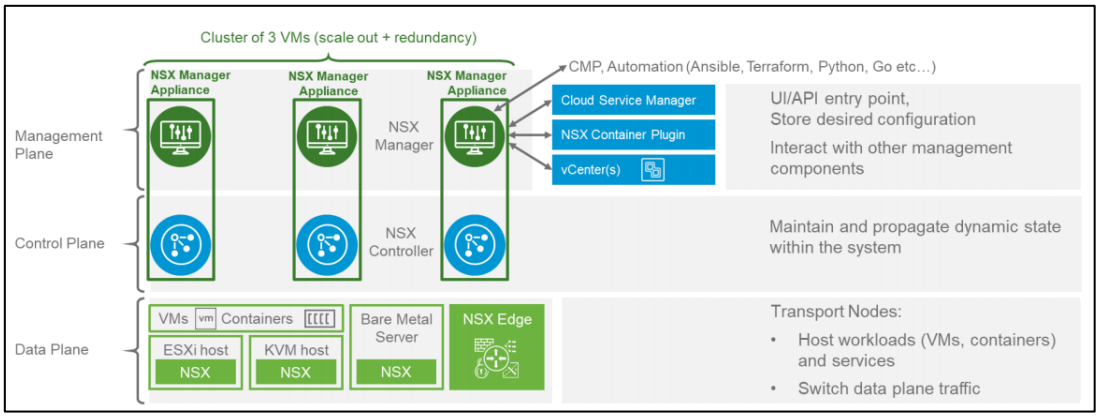


Ilustración 28 - Arquitectura y componentes de NSX

1. **Plano de gestión (Management Plane)** proporciona la interfaz de interacción del usuario final con la solución NSX-T por medio de REST-API, GUI o Cloud Service Manager. Esta interfaz permite tareas de configuración y administración en el management plane, control plane o data plane, desde un punto central de administración por medio de NSX-T Manager. Sus componentes son:

    - NSX-T Manager: es la consola central de administración de todos los componentes de NSX-T.

    - Cloud Service Manager (CSM): proporciona una vista completa de todos los endpoints desplegados en nuestras nubes públicas, permite realizar tareas de configuración, monitoreo y administración de mi inventario en Cloud por medio de UI y REST APIs.

    - NSX Container Plugin (NCP): convierte recursos de Kubernetes en objectos de NSX-T para administración centralizada de contenedores. Proporciona integración entre NSX-T y orquestadores de contenedores.

2. **Plano de Control (Control Plane)** proporciona capacidades de control y configuración para funcionalidades de red como logical switching y routing, Este plano está segregado en dos partes, una por el Central Control Plane (CCP) y otra por el Local Control Plane (LCP). Su único comente es**:**

    - NSX Controller: son desplegados e integrados desde NSX-T Manager como máquinas virtuales de Linux, uno por cada NSX-T manager.

3. **Plano de Datos (Data Plane)** realiza el reenvío sin estado o la transformación de paquetes basados en tablas utilizando las tablas publicadas por el CCP. También mantiene estadísticas para informar al NSX-T Manager acerca de eventos**.** Sus componentes son:

    - Los hipervisores nodos de transporte: son hipervisores preparados y configurado para NSX-T.

    - NSX Edge: son máquinas virtuales dedicados a servicios centralizados en el data plane como: Load Balancing, NAT, Edge Firewall, VPN, DHCP y conectividad a la red física.

7.8.4 VMware vRealize [7.20]

VMware vRealize Suite es una plataforma de gestión para Cloud destinada para ayudar a los equipos de TI y a los proveedores de servicios. Estos equipos con vRealize pueden capacitar a cualquier demandante para crear de manera rápida y sencilla aplicaciones basadas en contenedores y máquinas virtuales en cualquier Cloud privada, pública o híbrida con operaciones seguras y coherentes.

Proporciona una pila de gestión completa y unificada para servicios de TI en tecnologías de VMware vSphere y otros hipervisores, pero también para un amplio grupo de tecnología como: infraestructura física, contenedores, OpenStack y Cloud externas, como VMware Cloud™ o AWS, Azure y Google Cloud Platform.

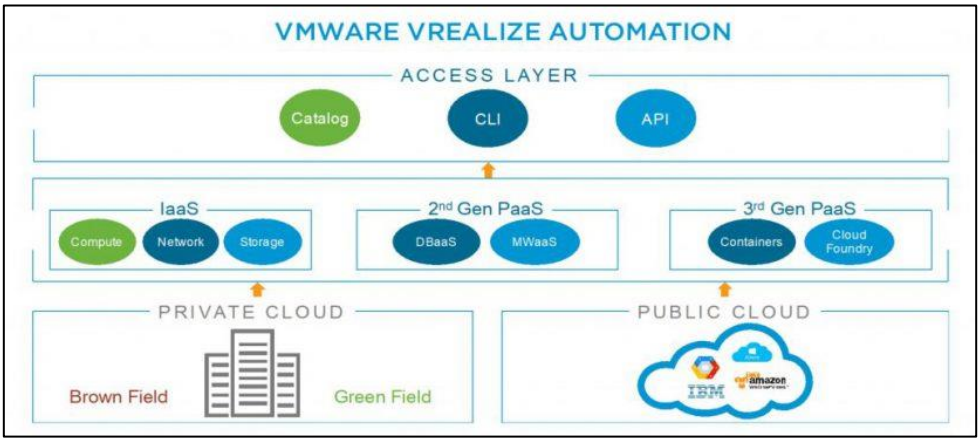


Ilustración 29 - VMware vRealize Automation

La suite de VMware vRealize Enterprise es un conjunto de herramientas y componentes que proporcionan funcionalidades para gestionar la infraestructura como servicio (IaaS), gracias a la integración completa con vCenter vSphere. También proporciona herramientas como Tanzu que se integran perfectamente con vRealize y NSX, para ofrecer la posibilidad de proporcionar plataforma como servicio (PaaS).

Por último, vRealize cuenta con un portal Web de autoaprovisionamiento donde además de obtener los servicios IaaS y PaaS, se podrán publicar servicios como servicios (SaaS) a usuarios de la organización.

Características

- Operaciones de aplicaciones: permite a los desarrolladores publicar versiones rápidamente, solucionar problemas y optimizar el rendimiento en tiempo real de las aplicaciones de Cloud basadas en microservicios y altamente distribuidas.

- Aprovisionamiento programable: ayuda a los desarrolladores y al equipo de TI a acceder fácilmente a la infraestructura y a los recursos de las aplicaciones en cualquier Cloud a través de API, catálogo o CLI con gestión completa del ciclo de vida.

- Operaciones autónomas: ayuda al equipo de TI a optimizar continuamente la capacidad y el rendimiento en función de la intención operativa y empresarial. vRealize Suite también permite a las organizaciones abordar los casos de uso anteriores para conocer el coste de las opciones de infraestructura y la utilización de los recursos por parte de los usuarios finales a fin de rentabilizar al máximo la inversión en capital.

VENTAJAS

- Agilidad: acelera la distribución de servicios de TI, permitiendo que el equipo de TI responda por completo a las expectativas de los desarrolladores.

- Control: proporciona el nivel adecuado de control para dar soporte a las necesidades de los equipos de TI equilibrando los objetivos entre las dimensiones de agilidad, riesgo y coste.

- Eficiencia: aumenta la eficiencia del personal de TI y del uso de recursos de Cloud pública y privada, con lo que se reducen tanto los gastos operativos como la inversión en capital.

- Opciones: capacita a los desarrolladores para utilizar recursos a través de API, CLI o catálogos y emplear las herramientas de desarrollador que prefieran.

VMware vRealize Suite ofrece una plataforma de gestión de Cloud híbrida acreditada en el ámbito empresarial que se compone de los siguientes productos:

- vRealize Automation: distribución automatizada de la infraestructura, las aplicaciones y los servicios de TI personalizados.

- vRealize Operations: optimización continua del rendimiento basada en intención, gestión eficiente de la capacidad, planificación proactiva y corrección inteligente.

- vRealize Log Insight: gestión y técnicas de análisis de registros eficaces en tiempo real.

- vRealize Business for Cloud: cálculo de costes, medición del uso y asignación de precios de los servicios de la infraestructura virtualizada automatizados.

- vRealize Lifecycle Manager: instalación, configuración, actualización, mantenimiento y gestión de contenido de vRealize automatizados.

7.8.5 Tanzu [7.21]

Un clúster de Tanzu Kubernetes Grid (TKG) es un clúster de Kubernetes (K8s) que se ejecuta dentro de máquinas virtuales en la capa Supervisor y no en vSphere Pods. Se habilita a través del servicio Tanzu Kubernetes Grid para vSphere. Dado que un clúster de TKG es totalmente compatible con Kubernetes de código abierto, se garantiza que funcionará con todas sus aplicaciones y herramientas de K8. También puede ejecutarse además de vSphere nubes pública como Amazon EC2 y Microsoft Azure.

Los clústeres de Kubernetes aprovisionados por Tanzu son totalmente compatibles, y sé puede implementar todos los tipos de cargas de trabajo que en un Kubernetes nativo. Con vSphere with Tanzu se aprovecha muchas características confiables de vSphere para mejorar la experiencia de Kubernetes, incluyendo vCenter SSO, la biblioteca de contenido para distribuciones de software de Kubernetes, redes vSphere, almacenamiento vSphere, vSphere HA y DRS y seguridad vSphere.

La solución vSphere with Tanzu requiere una configuración de redes específica para habilitar la conectividad necesaria entre todas sus instancias de Clúster supervisor y de los recursos que usan los contenedores, por este motivo, es necesario instalar y configurar el NSX-T para vSphere with Tanzu para proporcionar esta capa SDN a Tanzu.

Esta herramienta es pieza clave para los desarrolladores dado que les proporciona herramientas para realizar desarrollos ágiles y automatizados, como describe la metodología DevOps. También es una pieza clave a para los administradores de TI porque con esta herramienta son capaces de monitorizar y proveer recursos de forma ágil y dinámica desde una gestión centralizada. Tanzu fomenta la colaboración entre los departamentos de desarrollo y operaciones.

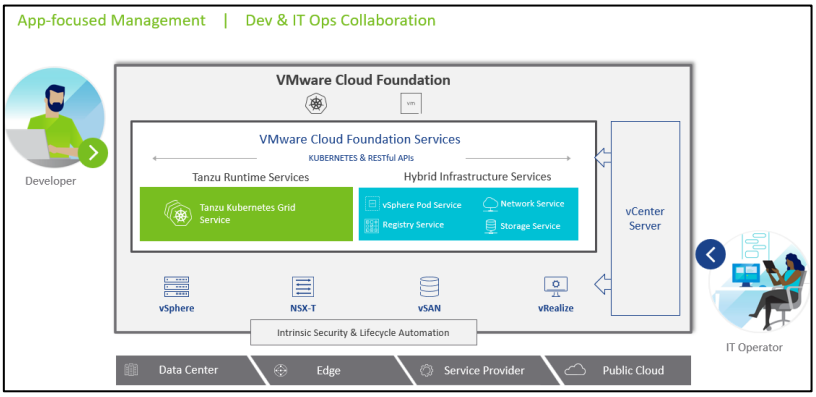


Ilustración 30 - VCF con Tanzu

7.8.6 Arquitectura de VCF [7.5]

En VMware Validated Design, un dominio de carga de trabajo o Workload Domain (WLD) representa una unidad lógica que agrupa hosts ESXi administrados por una instancia de vCenter Server con características específicas de acuerdo con las mejores prácticas de VMware SDDC.

Esta segmentación lógica con WLD permite crear entornos dedicados a diferentes tipos de carga de trabajo, como máquinas virtuales, contenedores, virtualización de escritorios, etc. Las opciones de diseño son bastante amplias, al disponer de diferentes perfiles de hardware para temas de rendimiento, SLAs, distribución entre racks, etc.

Existe un dominio de carga de trabajo en los límites de una región SDDC. Una región puede contener uno o más dominios. Un dominio de carga de trabajo no puede abarcar varias regiones.

Cada dominio de trabajo contiene al menos, los siguientes componentes:

- Una instancia de vCenter Server conectada a un par de instancias de Platform Services Controller en el mismo dominio de carga de trabajo o en otro.
- Al menos un clúster de vSphere con vSphere HA y vSphere DRS habilitados.
- Un conmutador distribuido de vSphere para la gestión del tráfico y la conmutación lógica de NSX.
- Componentes de NSX que conectan las cargas de trabajo en el clúster para conmutación lógica, enrutamiento lógico dinámico y equilibrio de carga.
- Una o más asignaciones de almacenamiento compartido.

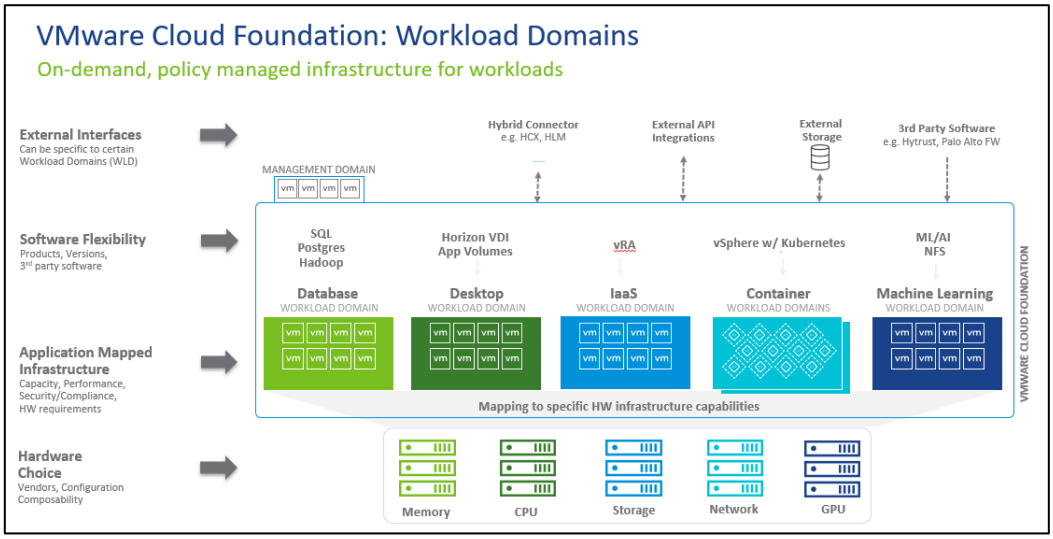


Ilustración 31 - Dominios de cargas de trabajo de VCF

SDDC Manager

Es la herramienta que integra todos los componentes de VCF, desde SDDC Manager se entregan todos los Workload Domain, e instala y gestiona el ciclo de vida de componentes de software de la misma plataforma. Este realiza cambios de configuración en objetos gestionados, gestión de certificados, passwords, parches de actualización, etc.

Management Workload Domain

Es un dominio de carga de trabajo de propósito especial dedicado a la infraestructura y las tareas de gestión. Es donde se ejecutan todos los componentes de administración, como SDDC Manager, vCenter, la instancia de NSX Manager y un clúster de NSX Edge.

Se requieren algunas consideraciones para el WLD de Management:

- Se requieren al menos 4 hosts ESXi para este WLD.
- Este WLD tiene como almacenamiento principal vSAN.
- Se puede tener NFS como almacenamiento secundario, para crear Datastores de NFS.

Contiene los siguientes componentes de gestión:

- Administrador de SDDC
- Controladores de vCenter Server y Platform Services
- vRealize Log Insight
- NSX

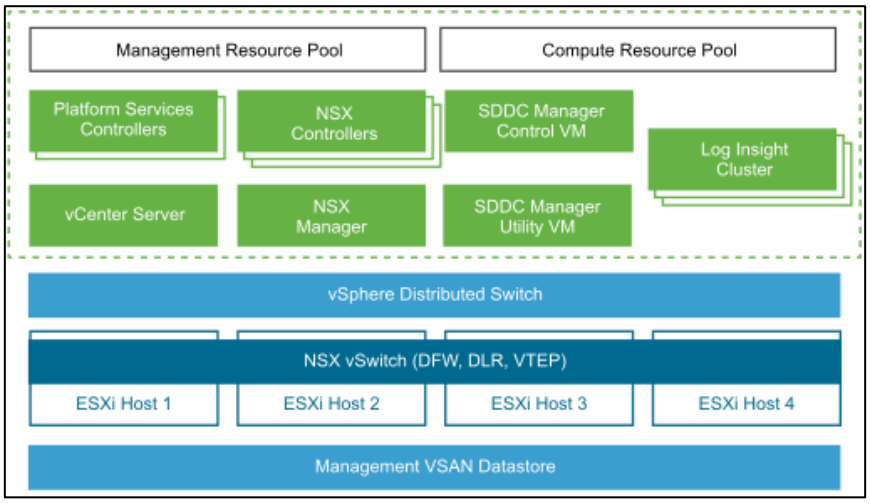


Ilustración 32 – Componentes de un dominio de gestión

Compute Workload Domain

Los dominios de carga de trabajo de cómputo pueden ser para infraestructura virtual (VI) o para infraestructura de escritorios virtuales (VDI). Es necesario un mínimo de tres hosts ESXi para poder aprovisionarlo. Cada dominio de carga de trabajo se crea de acuerdo con el tamaño, el rendimiento y la disponibilidad especificados por el usuario.

Los dominios de una carga de trabajo de cómputo contienen los siguientes componentes de software:

- vCenter Server
- NSX

Además de los componentes anteriores, los dominios de carga de trabajo de VDI también contienen el software VMware Horizon.

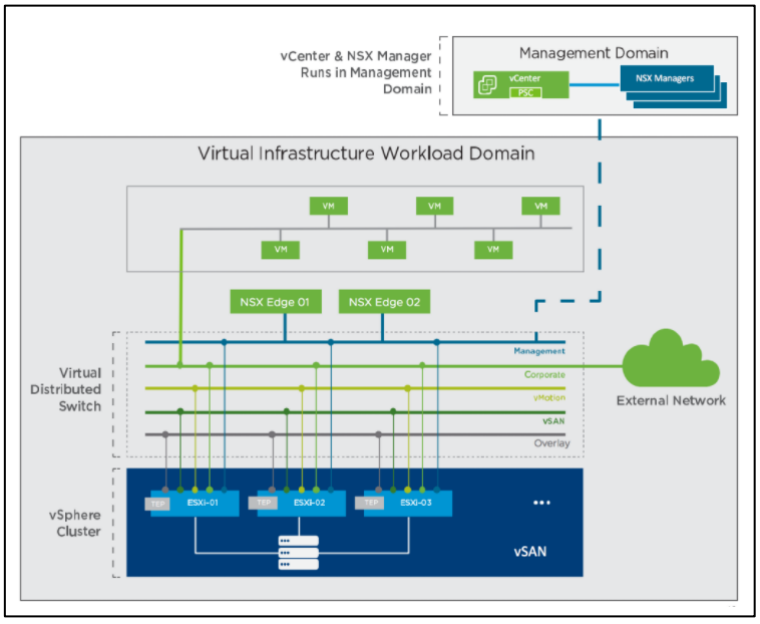


Ilustración 33 - Dominio de cómputo

Modelo de arquitectura estándar

Con el modelo de arquitectura estándar, las cargas de trabajo de administración se ejecutan en un dominio de administración dedicado y las cargas de trabajo de los usuarios se implementan en dominios de cargas de trabajo de infraestructura virtual (VI) separados. Cada dominio de carga de trabajo es administrado por una instancia de vCenter Server separada que proporciona escalabilidad y permite la administración autónoma de licencias y ciclo de vida.

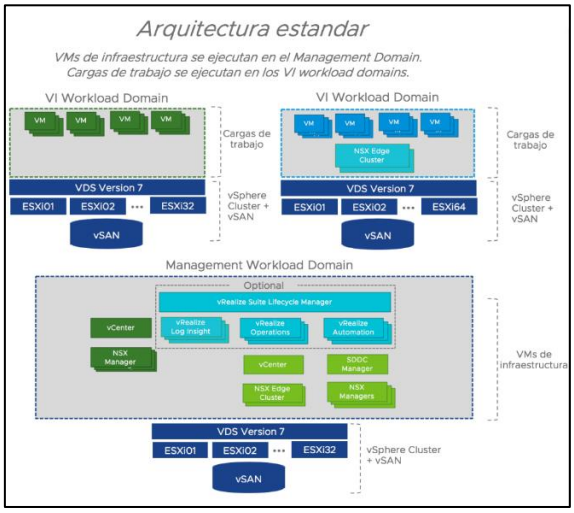


Ilustración 34 - Arquitectura estándar VCF

Modelo de arquitectura consolidada

En este diseño, los dominios de carga de trabajo de administración y de usuario se ejecutan juntos en un dominio de administración compartido. El entorno se administra desde un solo vCenter Server y los grupos de recursos de vSphere brindan aislamiento entre la administración y las cargas de trabajo de los usuarios.

En un modelo de arquitectura consolidada, se debe tener cuidado para garantizar que los grupos de recursos estén configurados correctamente, porque el dominio es compartido. Por este motivo este modelo se recomienda en implementaciones pequeñas de VCF y casos de uso especiales.

Existe la opción que un sistema VMware Cloud Foundation implementado en una arquitectura consolidada, pueda convertirse en una arquitectura estándar creando un dominio de carga de trabajo VI.

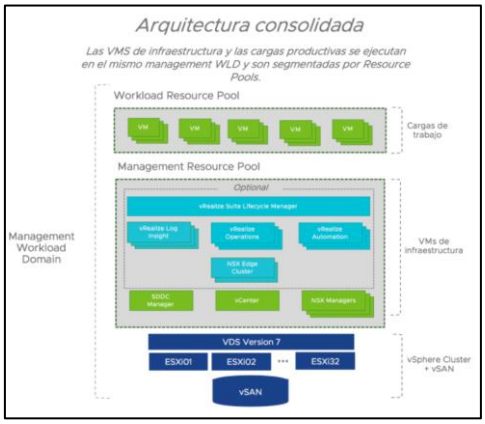


Ilustración 35 - Arquitectura consolidada VCF

7.8.7 Vmware HCX [7.22]

Es una solución software diseñada para facilitar migraciones de aplicaciones, cambios de plataforma, reequilibrio de cargas de trabajo, continuidad del negocio y las operaciones de comunicaciones en la nube. Simplifica el movimiento a gran escala de máquinas virtuales entre centros de datos basados en Vmware vSphere y nubes públicas con VCF. Esta herramienta dota de la capacidad de recuperar todo un Centro de Datos ante un desastre combinado con Site Recovery Manager (SRM) de Vmware.

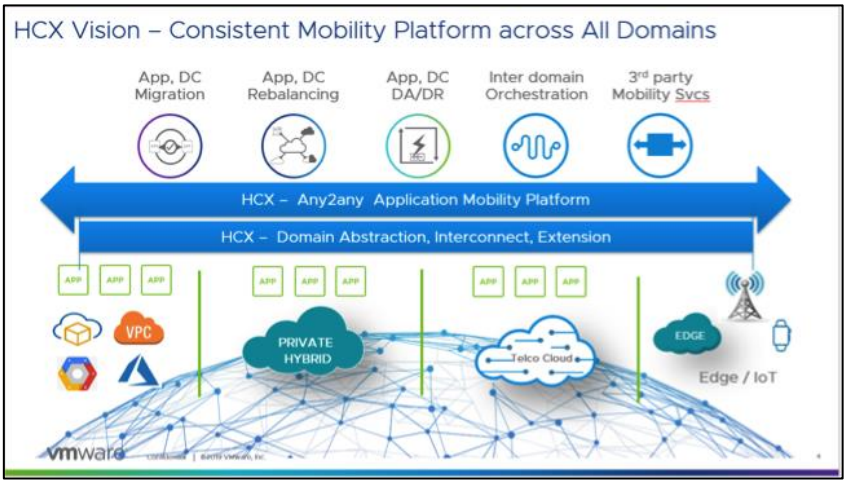


Ilustración 36 - VMware HCX

Características

- Migración de máquinas virtuales o dominios de carga de trabajo entre Centro de Datos, con poco esfuerzo y sin pérdidas de servicio.

- Interconexión híbrida diseñada para el tráfico de red que automatiza la creación de una extensión de red, proporciona equilibrio de carga, optimización para WAN, alto rendimiento, comunicaciones cifradas y seguras.

- Planificación y migración de aplicaciones fácilmente sin necesidad de reiniciar.

- Migración a versión actualizada sin necesidad de actualizar, realizando migraciones en bloque de entornos con versión antigua entre centros de datos o nubes a los entornos actuales.

- Equilibrio de cargas de trabajo extendiendo los componentes de las aplicaciones en un entorno multicloud, para responder a picos de recursos informáticos y almacenamiento adicionales.

- Continuidad del negocio proporcionando protección en las cargas de trabajo esenciales según las necesidades o de forma programada, para planificar la recuperación ante desastres de forma eficaz y segura, sin necesidad de reconfigurar direcciones IP.

- Acelera los procesos de replicación eliminando los problemas de incompatibilidad entre redes y almacenamiento.

7.9 Catálogo de servicios [7.23]

El Centro de Datos de Alto Rendimiento su principal función es ofrecer servicios a organizaciones para uso privado o público, como se ha mencionado anteriormente. Así pues, es imprescindible que este cuente con un catálogo de servicios alineados con el negocio de la organización.

Un catálogo de servicios es una lista que contiene los servicios que una organización o empresa ofrece a ella misma de forma privada, a modo particular, o pública para otra empresa. Esta herramienta es muy útil porque tanto el proveedor como el consumidor conocen todas las condiciones con las que se presta el servicio.

A continuación, se detallan unas recomendaciones que ayudarán a implantar un Catálogo de servicios.

- ✓ Definición, creación e implantación de un catálogo de servicios dinámico y alineado con el negocio, aceptado por la dirección de la organización que presta el servicio.

- ✓ Cada servicio tiene que definir unos niveles de servicio, mediante SLA, que el departamento IT tiene que cumplir en cada caso. Y que además se podrán revisar con sus indicadores clave (KPI).

- ✓ Los servicios incluidos en el catálogo tendrán sus costes asociado o vinculados, tiempos de disponibilidad, capacidad del servicio y el propietario del mismo.

- ✓ Todo servicio que esté en el catálogo tendrá su contingencia.

- ✓ El soporte a cada servicio se realizará a través de un CAU centralizado.

- ✓ Es necesario que anualmente se revise el plan de cada servicio para aplicar las mejoras o correcciones en cada caso.

7.10 Organización y Marco de trabajo

Es recomendable y casi imprescindible en proyectos nuevos seleccionar un marco de trabajo y con ello definir una organización, para alinear a todos los miembros de la organización con el negocio. Este proyecto está orientado al servicio, luego en un primer momento el marco de trabajo ITIL podría ser el más adecuado, pero no están ágil y dinámico como requiere la actualidad. No es fácil para empresas muy grandes adoptar marcos de trabajo tan ágiles y asumir riesgos [7.24].

En consecuencia, Bimodal IT plantea como solución usar dos modelos:

- Modelo 1 para mantener los servicios heredados y más estables. (ITIL)
- Modelo 2 para realizar innovaciones o evoluciones de sus servicios o productos. (DevOps)

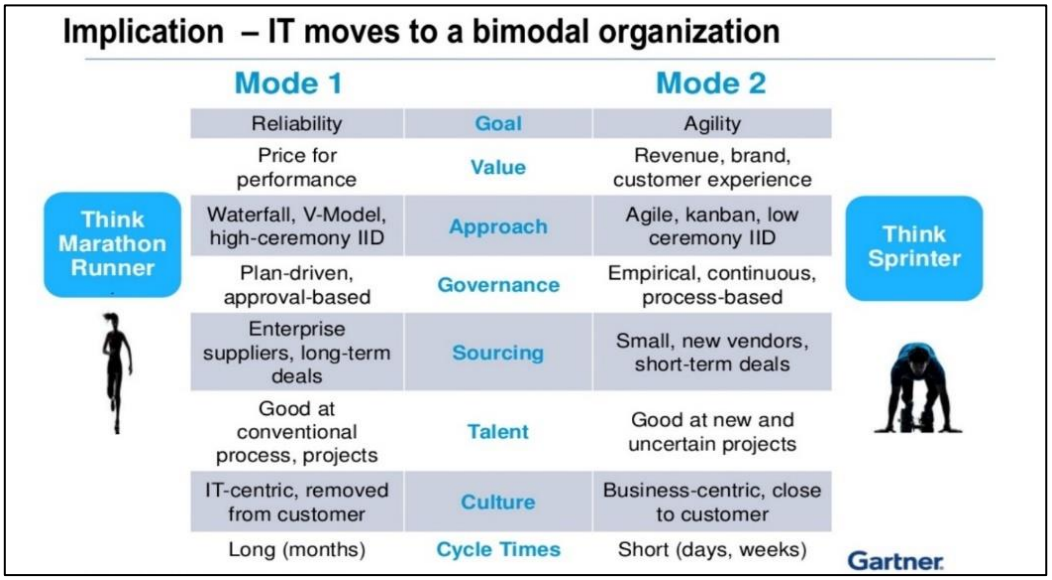


Ilustración 37 - Bimodal IT según Gartner

En los últimos tiempos se está demandando rapidez y agilidad en la ejecución de los procesos TI, por esta necesidad que tienen las empresas, nace Bimodal IT para realizar procesos más rápidos y ágiles. Es complicado para empresas que llevan años en el mercado evolucionar a un modelo donde se premia la rapidez y la agilidad, pero donde hay que asumir más riesgos y realizar un cambio culturar. Bimodal IT plantea como solución usar dos modelos: el modelo 1 para mantener los servicios heredados y más estables y el modelo 2 para realizar innovaciones o evoluciones de sus servicios o productos.

El gobierno tradicional de TI bloquea la agilidad y la rapidez que se intenta implantar con el modelo 2 por este motivo es muy importante realizar un cambio de gobierno TI en cada modelo teniendo en cuenta las prioridades competitivas y el entorno heredado. Se plantea que el modelo 1 sostenga los proyectos convencionales de la organización proporcionando un control más estricto o incluso una vez que un proyecto está estable en el modelo 2, es posible que se tenga que migrar la modelo 1 para asumir menos riesgos y dar más valor.

En cambio, en el modelo 2 se centra en obtener resultados para demostrar que se puede hacer de una manera rápida y ágil, en vez de consensuar todas las negociones, autorizaciones o riesgos que puedan derivar del trabajo que se está realizando. En este modelo premian los resultados y la velocidad con los que se obtienen. Aunque se asume que haya un alto porcentaje de fracaso en la mayoría de los proyectos que se realizan bajo el paraguas del modelo 2, se piensa que los proyectos que se obtienen con éxito compensarán las perdidas.

Es importante buscar un equilibrio en un modelo Bimodal IT, fomentar el cambio y la comunicación entre las personas de un modelo y otro. Es necesario dentro del gobierno de la organización apoyar el cambio de cultura para fomentar el cambio y un liderazgo para salvar las barreras u obstáculos que irán apareciendo según se implanta el modelo.

7.11 Cambios y riesgos.

En toda fase de diseño hay que contemplar los cambios que pueden aparecer debido a los cambios que puedan producir en los requisitos por parte del cliente o simplemente por imposibilidad del diseño, por esta razón tenemos que estar preparados para solventar y dar la mejor solución al nuevo problema que nos podamos enfrentar, de esta manera tenemos que asumir que esta fase es una fase dinámica y que estará constantemente expuesta a cambios que serán necesarios o que por el contrario no lo serán.

Es importante realizar reuniones de seguimiento con los diferentes responsables para minimizar el impacto de esos cambios en el proyecto ya que puede ser un riesgo muy alto para finalizar con éxito la implantación de nuestro Centro de Datos. Si se incluyen muchos cambios, esto afectaría a retrasar la fase de implantación y no entregar el Centro de Datos en la fecha acordada.

El éxito de la fase de diseño depende en identificar bien los riesgos que pueden poner en peligro nuestra fase de implantación.

A continuación, expondremos los que a priori pueden ocurrir, pero como he comentado antes este documento tiene que ser dinámico y luego sobre el terreno es posible que podamos identificar más:

- Retrasos en la obra de la sala del Centro de Datos.
- Retrasos de la administración pública para autorizar todas las licencias y células necesarias para el Centro de Datos.
- Retrasos en servir el diferente material para realizar la obra.
- Posibles problemas estructurales del edificio.
- Inclemencias meteorológicas que puedan impedir las obras.

Capítulo 8 FASE de Implantación de un Centro de Datos de Alto Rendimiento

Una vez finalizada la fase de diseño y analizados los riesgos del apartado anterior, se puede comenzar a desarrollar la fase de implantación. La solución que se propone en esta fase se basa en la documentación recopilada en apartados anteriores, lo estudiado a lo largo de mi carrera y mi experiencia personal adquirida en el área TI como arquitecto de sistemas informáticos.

A lo largo de los años, he podido participar en varios proyectos donde se han implantado y migrado un Centro de Datos, además de realizar auditorías para valorar el estado de un Centros de Datos. Por todas estas razones, se parte de una situación solvente para poder desarrollar esta fase con garantías.

En esta fase hay que tener en cuenta que se pueden introducir cambios, es posible que después de analizarlos, supongan un cambio importante en el diseño. En este caso, habría que realizar modificaciones en la fase de diseño y luego en fase de implantación.

La normativa que se debe cumplir es TIA-942 y un nivel TIER III, es importante tener presente el cumplimiento de estas normativas durante toda esta fase, porque la aplicación incorrecta de las normativas en algún parte de la fase, propiciará que el proyecto no acabe en éxito. La fase de implantación es muy importante y la que probablemente más riesgos entraña. Estos se analizarán en detalle por separado dada su importancia.

En la fase de diseño se ha explicado cada elemento que se debe utilizar o que es imprescindible para un Centro de Datos de Alto Rendimiento. El equipamiento que se adquiera en esta fase debe ser con las mismas características descritas en la fase de diseño, como se ha indicado antes, si se realizan cambios en el equipamiento descrito en fase de diseño, se tendría que revisar la fase de implantación.

En consecuencia, se plantea una solución de un caso ficticio que cumpla todos los requerimientos y normativas que se han definido en apartados anteriores. Se recuerda que según se definió en el alcance del proyecto hay elementos que no se contemplan en esta fase y se darán por supuesto, que su implantación se ha realizado cumpliendo todas la normativas y estándares internacionales.

8.1 Descripción del caso ficticio

La implantación del Centro de Datos de Alto Rendimiento se propone sobre un caso ficticio, esto no quiere decir que esté alejado de la realidad del mercado o las necesidades del mismo, si no todo lo contrario, está basado en una mezcla de casos reales y que por lo tanto sería plenamente funcional.

El motivo por el cual no se ha propuesto un caso real, es porque no se ha podido autorizar la cesión y utilización de información de una organización que esté con la necesidad de implantar un Centro de Datos, además de los contratos de confidencialidad que he firmado a lo largo de mi carrera. También se ha descartado realizar una implantación sobre un escenario que ya se implantó un Centro de Datos porque se entendería como una falta de originalidad.

El caso ficticio parte de la necesidad de una organización en implantar un Centro de Datos de Alto Rendimiento, esta organización antes de comprometer un presupuesto y licitar una oferta, necesita información para implantar un Centro de Datos. Esta organización propone el alcance y los requisitos descritos a lo largo de todo el documento en anteriores fases, también acepta el diseño propuesto para su futuro Centro de Datos. Aunque no es una propuesta formal para adjudicar la implantación, la organización quiere que sea lo más realista posible y recoja todos los requisitos en base a sus necesidades de negocio actuales.

Los requisitos que se proporcionan para la fase de implantación son los siguientes:

- ✓ Todos los elementos que se propongan tienen que ser instalados, certificados y mantenidos por el fabricante.
- ✓ Todos los elementos se implantarán en Alta Disponibilidad para lograr un nivel TIER III.
- ✓ Se propondrá para los equipos de comunicaciones los siguientes equipos: dos firewall, dos switch para la capa CORE, dos switch para la capa de Distribución y dos switch de fibra para red SAN. Los switch de la capa CORE y los firewall, contarán con puertos de alta velocidad QSFP+.
- ✓ Se propondrá para el almacenamiento dos cabinas de almacenamiento All-Flash.
- ✓ Se pretende desplegar varios dominios de carga para escritorios virtuales, máquinas virtuales, cluster de Kubernetes (Tanzu) y proveer servicios SaaS. Por este motivo, se plantea un alto número de servidores, unos 34 servidores físicos en total.
- ✓ Todo el equipamiento descrito anteriormente se instalará solo en 8 rack.
- ✓ Los equipos de red y almacenamiento propuestos tienen que ser altamente escalables, ampliables y de fabricantes líderes del mercado.
- ✓ Todos los servidores físicos contarán con 4 RJ45 a 10G y con 4 puertos FC a 16G, con dos CPU como mínimo. Además de proporcionar un sistema de hiperconvergencia.
- ✓ Los servidores físicos dedicados a los dominios de cargas de trabajo contarán con GPUs.
- ✓ Proporcionar un presupuesto económico de todos los elementos implantados, así como los servicios y licencias que son necesarios.
- ✓ La dirección de la organización valorará positivamente propuestas de soluciones a problemas actuales que estén argumentas y consensuadas.
- ✓ Proponer un organigrama y marco de trabajo para la gestión del Centro de Datos.
- ✓ Proporcionar planos de la sala con la ubicación y distribución de cada rack y una planificación con el tiempo necesario para realizar la implantación.

8.2 Instalación de elementos físicos

A continuación, se detalla el equipamiento necesario para cumplir con todos los requisitos y realizar la implantación del Centro de Datos de Alto Rendimiento en el orden correcto.

Antes de instalar cualquier elemento en la sala es importante realizar una inspección de la misma una vez que ha sido entregada por la empresa constructora, para verificar el cumplimiento de todos los requisitos descritos en la fase de diseño. También es importante que la sala se entregue en condiciones óptimas de orden y limpieza.

8.2.1 Sistema de alimentación ininterrumpida (SAI)

El primer componente que hay que instalar son los dos SAI de tipo on-line, que se ubicarán en el lugar que indica el plano ANEXO V, cada SAI tiene una potencia capaz de asumir el 100% de la carga de los sistemas informáticos durante unos 10 minutos.

El sistema debe funcionar con las cargas conectadas permanentemente a través del SAI (on-line) y la línea directa de corriente alterna (*by-pass*) que servirá para sobrecargas, anomalías y mantenimiento del equipo.

Con dos SAI el Centro de Datos cumple con el nivel TIER III, al tener una redundancia (N+1), cada SAI estará conectada a cada cuadro eléctrico general, recordamos que estos cuadros también estarán conectados a los generadores para que en caso de agotamiento de los SAI puedan suministrar energía.

8.2.2 Grupos de ventilación y climatización

Una vez se ha finalizado la implantación de los SAI y se han conectado al suministro eléctrico, se puede comenzar con la instalación de dos máquinas de ventilación en el lugar que indica el plano ANEXO V. Estas funcionarán en paralelo redundante y tendrán una potencia frigorífica de 41,2 kW cada una.

Estas máquinas son unidades de aire acondicionado de precisión de expansión directa e impulsan el aire frío hacia el falso suelo que solo saldrá hacia el pasillo frío como se explicó en la fase del diseño. También se impulsará al ambiente en las dos salas para asegurar el confort de trabajo, realizándose el retorno del aire caliente a las mismas por su parte superior. El retorno hasta las unidades de aire acondicionado se realizará de forma natural por la parte superior de la Sala.

Este sistema presenta la ventaja de la individualidad de las máquinas, ya que cada una va asociada a una unidad exterior con su propio circuito frigorífico, de manera que, en caso de producirse cualquier anomalía en algún elemento de una máquina, las restantes no se ven afectadas. Así puede realizarse la instalación con una redundancia en máquinas (N+1). Las máquinas de climatización del Centro de Datos se alimentan directamente desde el Cuadro General y para proporcionar redundancia eléctrica de alimentación a los equipos.

El sistema de renovación de aire, tanto para la sala de SAI (por la presencia de baterías) como en la sala del Centro de Datos (garantiza una sobrepresión en la sala, así como la renovación del aire tras la descarga de agente extintor, en caso de detectarse un incendio). El sistema de impulsión-extracción garantiza entre 1,5 y 2 renovaciones por hora, al tiempo que evita la entrada de una elevada carga térmica en forma de aire a una gran temperatura.

8.2.3 Sistema de protección contra incendios

La implantación del sistema de detección de incendios se debe realizar en base a la Fase de Diseño, este sistema se tiene que instalar en la Sala fría y en otra Sala independiente de cuadros o máquinas. Este sistema cuenta con una central de incendios para recibir la información de los detectores y producir, en su caso, la señal correspondiente. Esta central está integrada con el sistema central del edificio, para enviar señales en caso de detección y/o salto de la extinción.

Este sistema cuenta con una fuente de alimentación y un cargador para las baterías internas, de manera que, cuando se produce un fallo en el suministro eléctrico, entran en servicio estas baterías para alimentar a todo el sistema. Los detectores de incendios convencionales (detectores de humo y sensores de calor) estarán presentes en las dos salas. En el plano ANEXO V se indica la cantidad y posición de los detectores.

Además, la sala del Centro de Datos contará con el sistema convencional de detección y extinción de incendios un sistema de detección precoz por aspiración (ASD). Este sistema se instala en el falso suelo de la sala, así como en el retorno del sistema de ventilación.

Este sistema cuenta con la implantación de un sistema de detección de agua con cable sensor para garantizar el aviso en caso de una fuga de agua en el Centro de Datos. El sistema generará de manera automática una alarma cuando el cable sensor se humedezca. Este cable se instalará por el suelo técnico, extendiéndolo alrededor de la sala por la parte frontal de los equipos de climatización.

8.2.4 Sistema CCTV

El sistema cerrado de cámaras como se explicó en la Fase de Diseño se tiene que integrar con el sistema de CCTV de todo el edificio, por este motivo, sólo se contempla la instalación de ocho cámaras móviles que se tienen que conectar al sistema de seguridad de todo el edificio. La ubicación aproximada de todas las cámaras está indicada en el plano ANEXO V.

8.2.5 Sistema de monitorización.

Para supervisar los equipos existentes en el Centro de Datos se instalará un sistema de control y gestión, que es compatible con el sistema existente del resto del edificio. Este sistema permitirá la monitorización de los siguientes elementos:

- ❒ SAI.
- ❒ Equipos interiores de climatización.
- ❒ Grupos Electrógenos.
- ❒ Cuadros Eléctricos.
- ❒ Sistema de incendios.
- ❒ Central de detección de agua.
- ❒ CCTV.
- ❒ Sistema de alarmas.

El técnico del fabricante tendrá que contemplar la instalación del software necesario para supervisar todas las alarmas y controlar el consumo eléctrico de todas las salidas y de todos los Racks del Centro de datos desde un PC exterior.

8.2.6 Instalación de Rack

Se suministrarán e instalarán los armarios racks necesarios para completar la disposición prevista del plano ANEXO V. Estos rack son los siguientes:

- 2 rack de 48U para los servidores.
- 2 rack de 42U para equipos de comunicaciones.
- 2 rack de 42U para los patch panel.

Es importante seguir la normativa TIA-942 para instalación del cableado de alimentación, cada rack contará con dos líneas de alimentación o PDU verticales con hembras C13. Cada PDU irá conectada directamente a una línea diferente de alimentación que sale del cuadro general de la sala con los conectores cetac. Estos cables irán por encima de los rack, organizados y correctamente etiquetados en origen y destino.

Ilustración 38 - Organización del cableado por encima de un rack

En el plano ANEXO V viene reflejado la disposición y ubicación para cada tipo de rack. No se incluyen los rack para equipos de almacenamiento porque estos vienen instalados en sus propios rack por el fabricante que proporciona el equipamiento con el rack.

8.2.7 Patch panel.

Se instalarán en una primera fase y ampliable según la demanda, dos patch panel de 48 puertos UTP y dos patch panel de 48 puertos Fiber Channel. Cada patch panel de UTP y fibra se enracará en un rack diferente como muestra el plano ANEXO VI. El cableado que se instale aquí se debe realizar siguiendo la normativa TIA-942, se identificará tanto los latiguillos de parcheo, como el cableado en los paneles y en los extremos de los cables horizontales.

Cada etiquetación se realizará con identificadores apropiados para cada caso, que serán altamente legibles y que se mantendrán permanentemente sin riesgo de caerse o desvanecerse por el paso del tiempo.

8.2.8 Equipos de comunicaciones.

Todos los equipos de comunicaciones se deben enracar según las especificaciones del fabricante, el cableado de alimentación, de red y fibra se realizará en base a la normativa TIA-942. Es importante que los cables de alimentación con conectores C13 de los equipos se conecten a tomas diferentes de alimentación de los rack para tener redundancia ya que todos los equipos cuentan como mínimo con dos fuentes de alimentación con una redundancia de N+1.

Se propone unos equipos de red que sean escalables y de alto rendimiento en alta disponibilidad, los equipos que se proponen son:

- Para la capa de seguridad, 2 firewalls de Palo Alto modelo PA-5220 de 3U o similar con 4 puertos QSFP+ (40/100G) y 16 puertos SFTP+ (10/25G) cada equipo.

- Para la capa de CORE, 2 switch Cisco Nexus 9504 de 7U o similar con 64 puertos QSFP+ (40/100G) cada equipo.

- Para la capa de distribución, 2 switch Cisco Catalyst C9600 de 8U o similar con 96 puertos FTP 10G y 24 puertos QSFP+ (40/100G) cada equipo

En ANEXO VII, se detalla la ubicación y la distribución de los dos rack para los equipos de comunicaciones, su distribución por rack es la siguiente:

- 1 Firewall Palo Alto PA-5220 o similar que ocupa 3U.
- 1 Switch Cisco Nexus 9504 o similar que ocupa 7U.
- 1 Switch Cisco Catalyst C9404R o similar que ocupa 8U.
- 1 Brocade 6520 o similar que ocupa 4U.

El enracado lo realizará el fabricante siguiendo las indicaciones del ANEXO VII, todo el cableado de alimentación, de cobre y fibra se realizará en base a la normativa TIA-942.

Los firewall estarán en cluster y conectados por cable de fibra LC como muestra el esquema de red, así tendremos una redundancia de N+1 en las comunicaciones. Se conectarán a cada uno de los switch CORE con un cable de fibra QSFP+ de 40G y se conectara a cada equipo de acceso a Internet (ISP) instalado por el proveedor de internet con cables de fibra SFTP+ de 10G.

Los switch Core van conectados a los firewall como se ha indicado anteriormente y a los switch de distribución van conectados a cada uno con un cable de fibra QSFP+.

Los switch de distribución van conectados a cada boca RJ45 de los patch panel que conecta a una boca de RJ45 de un servidor físico, es decir, cada switch de distribución tiene 96 puerto en total, pues 48 puertos se conectan a un patch panel y los otros al otro patch panel de rack diferente.

Por último, se instalarán dos switch de fibra Brocade 6520 o similar de 4U con 96 puertos de 16G para la red SAN, cada uno irá en diferentes rack con el mismo método de enracado y cableado que los anteriores. En este dispositivo se conectará la cabina de almacenamiento que se explica en el siguiente apartado y también se conectará 48 puertos a las bocas del path panel de fibra que está en el rack de al lado y 48 puertos al patch panel de fibra de diferente rack.

8.2.9 Equipos de almacenamiento.

Se propone un sistema flexible de almacenamiento integrado dentro de VCF, escalable y de alto rendimiento, sin perder de vista la alta disponibilidad que necesita el Centro de Datos a la hora de acceder a los datos. Las cabinas de almacenamiento para la implantación son dos Dell EMC PowerMax 2000Pro o similares, que garantizan un alto rendimiento y una alta disponibilidad de los elementos hardware.

Estas cabinas tienen las siguientes características:

- 100TiBNetos efectivos, según configuración detallada
- 1 Brick de proceso con NVMe end to end
- Calidad de servicio por tiempo de respuesta
- Compresión y de duplicación inline
- Activo-Activo con SRDF/Metro
- Integración con VCF
- Cloud IQ
- Instalación y mantenimiento MissionCritical24x7
- Tipo de almacenamiento: bloque, archivo, sistema abierto, IBM i
- Máximo IOPS: 2,7 millones.
- Tiempos de respuesta (lecturas): Menos de 100 microsegundos.

La instalación de estos equipos la realiza el fabricante y se proporcionan con su propio rack de 40 o 42U facilitando la instalación del mismo, estos dos rack se instalarán según la normativa TIA-942 para instalación del cableado de alimentación, cada rack contará con dos líneas de alimentación o PDU verticales con hembras C13. Cada PDU irá conectada a líneas diferentes de alimentación para garantizar redundancia N+1, en el ANEXO VIII se indica la ubicación de cada rack.

Las conexiones de cada cabina son de fibra y cobre, dado que pueden suministra almacenamiento a través de la SAN o de la red Ethernet. Así pues, cada cabina de almacenamiento tiene dos controladoras cada una con 8 puertos de fibra y 3 puertos de cobre, uno puerto para la gestión y dos para exportar almacenamiento por red ethernet.

Los puertos de fibra de una controladora se conectan con cable LC-LC multimodo al Brocade y los puertos de fibra de la otra controladora se conectan al otro Brocade diferente. Lo mismo ocurre con los puertos de cobre, se conectan con cable FTP cat 7 al switch de distribución los puertos de RJ5 de una controladora y los puertos de RJ45 de la otra controladora se conectan a distinto switch de distribución.

8.2.10 Servidores de cómputo.

En base a la FASE de diseño donde se apuesta por VCF, es importante tener en cuenta que los servidores físicos que se implanten estén certificados y soportados por el fabricante Vmware propietario de la solución VCF. Este fabricante cuenta una matriz de compatibilidad en su página web para asegurar que los servidores físicos que se seleccionen están soportados o no. Es evidente que si no están soportados los servidores se implantan no servirán para el propuesto de este proyecto y será un fracaso.

En el diseño de VCF, se indica que se necesitan como mínimo cuatro servidores físicos certificados por Vmware para el Workload Domain Management y un mínimo de tres servidores físicos certificados para el resto de Workload Domain. Así pues, se implantarán los siguientes servidores físicos:

- 2 conmutador de consola Dell KVM 1081 o similar que ocupa 1U.
- 4 servidores Dell PowerEdge R640 o similar que ocupan 1U.
- 30 servidores Dell PowerEdge R940 o similar que ocupan 4U.

En ANEXO IX, se detalla la ubicación de los dos rack para servidores físicos y la distribución de los servidores físicos en cada rack, su distribución por rack es la siguiente:

- 1 conmutador de consola Dell KVM 1081 o similar que ocupa 1U.
- 2 servidores Dell PowerEdge R640 o similar que ocupan 1U.
- 15 servidores Dell PowerEdge R940 o similar que ocupan 4U.

El enracado lo realizará el fabricante siguiendo las indicaciones del ANEXO IX, todo el cableado de alimentación, de cobre y fibra se realizará en base a la normativa TIA-942. Es muy importante que los cables de alimentación con conectores C13 de los servidores se conecten a tomas diferentes de alimentación del rack para tener redundancia ya que los servidores cuentan dos fuentes de alimentación con una redundancia de N+1.

El cableado de red FTP categoría 7 se conectará a cada boca RJ45 de los servidores, distribuyendo cada boca a un patch panel diferente, como los servidores cuenta con 4 bocas RJ45, dos se conectarán a un patch panel y las otras dos bocas al otro patch panel. La otra boca de RJ45 es para la consola remota que irá conectada a un patch panel.

En el caso de los servidores que cuentan con dos tarjetas de fibra HBA, el cable de fibra LC-LC multinodo se conectará a cada boca de cada servidor y cada una irá conectada a cada boca de un patch panel diferente.

8.2.11 Equipamiento exento en la FASE de implantación.

En este apartado se menciona todo el equipamiento que no aparece en la FASE de implantación por estar fuera del alcance del proyecto. No se ha detallado la instalación de los siguientes elementos:

- ❒ Cuadros generales del Centro de Datos.
- ❒ Generadores.
- ❒ Exclusa y accesos de control.
- ❒ Sistema de Alarma y el sistema de CCTV, en este último solo se ha mencionado la instalación de las cámaras.

Se ha mencionado que los generadores, el sistema de alarmas, sistema de CCTV y controles de acceso, serán los mismos para todo el edificio. La instalación de los cuadros generales, el alumbrado y la exclusa de la Sala del Centro de Datos es realizada por la empresa responsable de la obra civil.

Es muy importante que se exija una certificación y pruebas de estos sistemas por parte de la empresa responsable antes de ser entregados.

8.3 Implantación de la solución de Vmware Cloud Foundation.

El propósito de este apartado no es detallar paso a paso cómo se realiza la instalación de la VCF, si no describir cómo es el proceso de implantación de la solución de VCF. Es recomendable cuando se adquieren las licencias de toda la solución negociar con el proveedor el soporte para la implantación una vez ya está implantado y certificado.

VCF es una plataforma unificada que proporciona: vSphere 7.0, VSAN 7.0, NSX-T 3.0, VRA 8.1 y SDDC Manager para administrar dominios de trabajo o Workload Domain. Además de la implementación de Kubernetes a través del administrador SDDC después de la implementación del dominio de administración.

Antes de comenzar con la instalación es necesario definir las siguientes redes, asignando a cada una su identificador de VLAN, su nombre del Portgroup, su dirección de red/mascara y su puerta de enlace:

- Management Network
- vMotion Network
- vSAN Network
- NSX-T Host Overlay (sin direccionamiento, ni puerta enlace)
- NSX-T Endge Uplink 1
- NSX-T Endge Uplink 2
- NSX-T Endge Overlay

También es necesario un servidor de directorio activo y DNS en alta disponibilidad, para que los ESXi puedan resolver los siguientes nombres de máquinas virtuales que se crearán con la instalación:

- vCenter
- NSX
- SDDC

Por último, es necesario que en los 4 servidores físicos Dell PowerEdge R640 esté instalado Vmware ESXi 7.0 y vSAN 7.0 que es la última versión en el momento que se está desarrollando este documento. Los ESXi tienen que tener configurada la red de gestión o Management Network.

Una vez se ha realizado lo anterior, hay que usar *Cloud Builder*, que es una herramienta proporcionada por VMware para crear entornos VCF en ESXi destino. En realidad, es una máquina virtual de uso único para despliegues automáticos de VCF, se puede apagar y borrar una vez realizada la implementación.

La implementación es sencilla con esta herramienta, gracias al portal web que provee *Cloud Builder* y su asistente, se despliega en pocas horas el dominio de gestión en los cuatro servidores ESXi. Después de la implementación, se puede usar SDDC Manager para administrar o crear dominios de cargas de trabajo adicionales y desplegar en cuestión de minutos un cluster de Kubernetes con Tanzu.

8.4 Seguridad lógica.

Es importante minimizar o evitar casi en la medida de lo posible, cualquier daño que pueda sufrir un sistema informático, tanto en la información almacenada como la información que se está procesando. Anteriormente se ha mencionado en varias ocasiones que esta información es el activo más importante para una organización.

Por este motivo deben existir técnicas más allá de la seguridad física que aseguren dicha información. La seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo permita acceder a estos a las personas que estén autorizadas para ello.

8.4.1 Red desmilitarizada o DMZ.

Una parte importante de seguridad lógica es la red ethernet de un Centro de Datos, para evitar intrusiones a los datos desde fuera del Centro de Datos, es fundamental configurar y mantener los equipos firewall que son los que permiten o deniegan el acceso a las redes del Centro de Datos tanto para el acceso desde fuera como el interno.

Para evitar intrusiones del exterior el Esquema Nacional de Seguridad, recomienda contar con una red desmilitarizada o DMZ situada entre dos firewall, para ofrecer servicios públicos, esto es obligatorio si el Centro de Datos es proveedor de servicios.

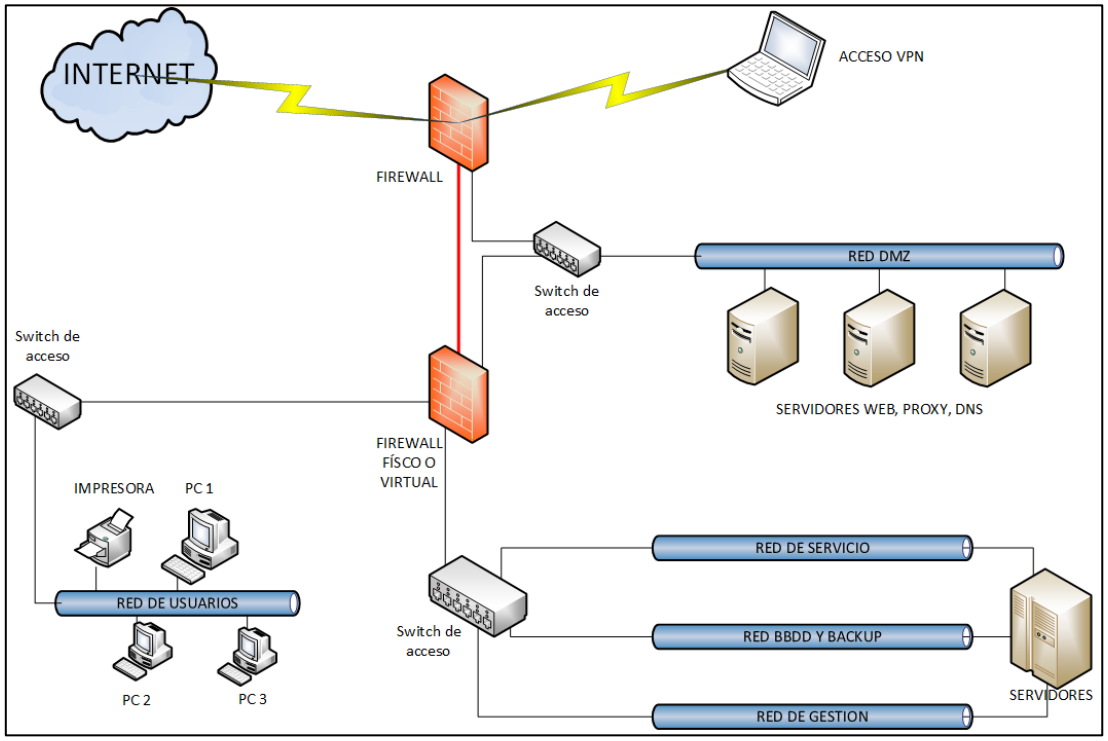


Ilustración 39 - Esquema de red lógico con DMZ

8.4.2 Control de accesos.

Estos controles se implementan a nivel lógico, por ejemplo, en la BIOS, sistemas operativos, sistemas de aplicación, en las DB, etc. Estos controles ayudan a proteger al sistema del acceso o modificaciones no autorizados y la no implantación de estos controles puede comprometer toda la seguridad del sistema.

A continuación, se detallan los más importantes:

- Todo acceso lógico tiene que estar protegido por una contraseña segura, que tenga más de 14 caracteres, combinación de números, letras y símbolos, es importante no usar frases o palabras. Está totalmente prohibido tener estas contraseñas apuntadas en un soporte físico como por ejemplo un cuaderno.

- El personal que tenga acceso al sistema tendrá asignado un rol dependiendo del grupo de trabajo al que pertenezca, así se asocia en base al rol que tipos de accesos tienes permitidos.

- Para salvaguardar la estabilidad y el rendimiento del servidor se pueden limitar los accesos a los servicios del mismo. Por ejemplo, un servidor web se puede limitar los accesos a menos 100 usuario concurrentes y así evitar un ataque de *denegación del servicio o DoS*[1].

- Los discos duros que están conectados a las cabinas de almacenamiento y a los servidores tendrán su contenido encriptado y solo se podrá acceder a la información que contienen a través del equipo al que desde un principio está conectado. Este mecanismo evita que si alguien substrae o realiza algún cambio de un disco duro del Centro de Datos no pueda acceder a la información que contiene conectándolo en otro equipo.

- Los servicios web tienen que cifrar la comunicación con los clientes con certificados electrónicos válidos y emitidos por una autoridad certificadora. Este mecanismo evita que alguien escuche la comunicación entre el servidor y el cliente pudiendo obtener información comprometida.

- No es recomendable que cualquier equipamiento del Centro de Datos tenga acceso directo a Internet, es necesario contar con un servidor Proxy que permita la salida a Internet a través de este. Esto evita que una persona en Internet pueda realizar ataques directamente a los servidores porque el único servidor que se expone ante las amenazas de Internet es el servidor Proxy.

[1] *Definición de Ataque de denegación de servicio en Wikipedia: también llamado ataque DoS (de las siglas en inglés Denial of Service) o DDoS (de Distributed Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.*

8.5 Certificación

Una vez finalizada la implantación es imprescindible realizar un proceso de evaluación al Centro de Datos de Alto Rendimiento para verificar qué requisitos cumple, cuales se pueden mejorar y cuales no cumple. Estos requisitos están relacionados con la eficiencia energética, tolerancia a fallo, seguridad, etc.

Este proceso es importante para verificar y certificar que todos los elementos con redundancia N+1 son tolerantes a fallos cuando se fuerza un fallo. Al forzar estos errores hardware se observa qué consecuencias tiene dicho error en el Centro de Datos y pueden tomarse medidas en el caso de producirse en un futuro.

Antes de realizar dicha evaluación, es importante verificar que todo el equipamiento descrito anteriormente está ubicado correctamente según los planos proporcionados e instalado físicamente según normativa TIA-942. También revisar que su correspondiente cableado está guiado por los soportes correspondientes y su etiquetado es el correcto sin ambigüedades.

El primer elemento que hay que certificar son los SAI, una vez se ha finalizado su instalación se suministra alimentación limpia y sin cortes. El fabricante tendrá que realizar pruebas que certifiquen que funcionan correctamente con o sin cortes de alimentación. Además de certificar el correcto funcionamiento del grupo electrógeno cuando se fuerza un corte de suministro eléctrico.

El segundo elemento que hay que certificar son los grupos de ventilación y climatización, una vez se ha finalizado su instalación y verificado que los equipos impulsan aire frio al falso suelo. El fabricante tendrá que realizar pruebas que certifiquen que funcionan correctamente con o sin cortes de alimentación. También realizará pruebas apagando un equipo y luego otro para observar si un solo equipo puede refrigerar toda la sala.

El sistema de incendios, control de acceso y sistema CCTV se debe certificar para todo el edificio dado que se integra con los sistemas de este. Se recomienda supervisar dichas certificaciones.

A continuación, una vez realizada la puesta en marcha del equipamiento de comunicaciones por el fabricante, es necesario volver a verificar que tienen todo el cableado correctamente instalado y cargada una configuración base que proporciona un cluster para tener redundancia N+1 en las comunicaciones. El fabricante realizará pruebas de carga y estrés sobre todos los elementos del equipamiento de comunicaciones para verificar que en ningún momento sufren degradación y no se pierde la comunicación con ningún elemento.

El proceso se repite con las cabinas de almacenamiento, es necesario volver a verificar que tienen todo el cableado correctamente, instalados y cargada la configuración base. El fabricante realizará pruebas de carga y estrés sobre las cabinas de almacenamiento para verificar que en ningún momento sufren degradación y no se pierde el acceso al almacenamiento.

Por último, el proceso se repite con los servidores físicos es necesario volver a verificar que tienen todo el cableado correctamente, instalados y cargada la configuración base. El fabricante realizará pruebas de carga y estrés sobre los servidores para verificar que en ningún momento sufren degradación y no se satura, respondiendo a las peticiones.

La certificación del Centro de Datos no termina aquí, después de certificar cada elemento es necesario realizar pruebas de carga y estrés, desconexiones de cables, forzado de corte de alimentación en los equipos, etc. Estas pruebas se deben realizar observando que ocurre en cada elemento y así verificar que el fallo de un equipo afecte a otro elemento y comprometa el servicio del Centro de Datos.

A continuación, se describen algunas pruebas que se recomienda realizar y sus resultados esperados:

Tabla 7 - Pruebas y resultados de la Certificación

Pruebas a realizar	Resultados esperados
1. Desconectar un cable de red de una interface RJ45 de todos los servidores físicos o ESXi	**ES CORRECTO**, si el tráfico de red es balanceado automáticamente al resto de interfaces de los ESXi y las VMs que contiene no pierden la conexión a la red. También si se verifica que en el vCenter reporta el error en el ESXi.
2. Desconectar dos cable de red de dos interface RJ45 de todos los servidores físicos o ESXi	**ES CORRECTO**, si el tráfico de red es balanceado automáticamente al resto de interfaces de los ESXi y las VMs que contiene no pierden la conexión a la red. También si se verifica que en el vCenter reporta el error en el ESXi.
3. Desconectar dos cable de red diferentes a los anteriores de las otras interface RJ45 de todos los servidores físicos o ESXi	**ES CORRECTO**, si el tráfico de red es balanceado automáticamente al resto de interfaces de los ESXi y las VMs que contiene no pierden la conexión a la red. También si se verifica que en el vCenter reporta el error en el ESXi.
4. Desconectar un cable de fibra de una interface de una hba todos los servidores físicos o ESXi	**ES CORRECTO**, si el tráfico de fibra es balanceado automáticamente al resto de interfaces de los ESXi y las VMs que contiene no pierden el acceso al almacenamiento. También si se verifica que en el vCenter reporta el error en el ESXi.
5. Desconectar dos cable de fibra de dos interface de una hba todos los servidores físicos o ESXi	**ES CORRECTO**, si el tráfico de fibra es balanceado automáticamente al resto de interfaces de los ESXi y las VMs que contiene no pierden el acceso al almacenamiento. También si se verifica que en el vCenter reporta el error en el ESXi.
6. Desconectar dos cable de fibra de dos interface de la otra hba todos los servidores físicos o ESXi	**ES CORRECTO**, si el tráfico de fibra es balanceado automáticamente al resto de interfaces de los ESXi y las VMs que contiene no pierden el acceso al almacenamiento. También si se verifica que en el vCenter reporta el error en el ESXi.
7. Apagado forzado de un ESXi del Workload Management	**ES CORRECTO**, si se pierde conexión con el ESXi y las VMs que contiene son movidas por HA a los ESXi que están vivos. También si se verifica que en el vCenter reporta el error de conexión con el ESXi
8. Apagado forzado de dos ESXi del Workload Management	**ES CORRECTO**, si se pierde conexión con los dos ESXi y las VMs que contienen son movidas por HA a los otro ESXi que están vivos. También si se verifica que en el vCenter reporta los errores de conexión a los ESXi

9. Desconectar un cable de fibra del Brocade que conecta con una controladora de la cabina de almacenamiento	**ES CORRECTO**, si el tráfico de fibra es balanceado automáticamente al resto de interface de la controladora, verificar si los servidores no pierden accesos a los discos.
10. Desconectar todos los cables de fibra del Brocade que conecta con una controladora de la cabina de almacenamiento	**ES CORRECTO**, si el tráfico de fibra es balanceado automáticamente a la otra controladora, verificar si los servidores no pierden accesos a los discos.
11. Desconectar todos los cables de fibra del Brocade que conecta con la otra controladora de la cabina de almacenamiento	**ES CORRECTO**, si el tráfico de fibra es balanceado automáticamente a la otra controladora, verificar si los servidores no pierden accesos a los discos.
12. Apagado forzado del Brocade	**ES CORRECTO**, si el tráfico de fibra es balanceado automáticamente al resto de interface del Brocade vivo y los servidores no pierden accesos a los discos.
13. Apagado forzado del otro Brocade	**ES CORRECTO**, si el tráfico de fibra es balanceado automáticamente al resto de interface del Brocade vivo y los servidores no pierden accesos a los discos.
14. Apagado forzado del firewall	**ES CORRECTO**, si el tráfico de red es balanceado automáticamente al otro firewall vivo y los servidores no pierden accesos a su puerta de enlace.
15. Apagado forzado del otro firewall	**ES CORRECTO**, si el tráfico de red es balanceado automáticamente al otro firewall vivo y los servidores no pierden accesos a su puerta de enlace.
16. Apagado forzado del switch de la capa CORE	**ES CORRECTO**, si el tráfico de red es balanceado automáticamente al otro switch vivo y los servidores no pierden accesos a su red.
17. Apagado forzado del otro switch de la capa CORE	**ES CORRECTO**, si el tráfico de red es balanceado automáticamente al otro switch vivo y los servidores no pierden accesos a su red.
18. Apagado forzado del switch de la capa de distribución	**ES CORRECTO**, si el tráfico de red es balanceado automáticamente al otro switch vivo y los servidores no pierden accesos a su red.
19. Apagado forzado del otro switch de la capa de distribución	**ES CORRECTO**, si el tráfico de red es balanceado automáticamente al otro switch vivo y los servidores no pierden accesos a su red.
20. Apagado forzado de una línea de suministro eléctrico.	**ES CORRECTO**, si todos los elementos del Centro de Datos siguen encendidos y funcionando correctamente, verificar los errores en las fuentes de alimentación de cada equipo al no estar llegando suministro de energía a la mitad de sus fuentes de alimentación.
21. Apagado forzado de la otra línea de suministro eléctrico.	**ES CORRECTO**, si todos los elementos del Centro de Datos siguen encendidos y funcionando correctamente, verificar los errores en las fuentes de alimentación de cada equipo al no estar llegando suministro de energía a la mitad de sus fuentes de alimentación.
22. Apagado forzado de las dos líneas de suministro eléctrico.	**ES CORRECTO**, si todos los elementos del Centro de Datos siguen encendidos y funcionando correctamente, suministrados energía por los SAI y después por los grupos electrógenos.

8.6 Planificación de la FASE de implantación

En el presente apartado se detalla la propuesta de planificación para la ejecución de la FASE de Implantación. Esta planificación se ha realizado en base a todos los requisitos recogidos en este documento y el detalle descrito a lo largo de la fase de implantación.

Se plantea cuatro fases que marcan los cuatro hitos de la planificación, estas tienen un tiempo estimado de finalización, en total la planificación de la implantación se estima en seis meses. En todo este tiempo será necesario el acompañamiento de dos procesos:

- La aceptación y apoyo de la dirección de los cambios necesarios que afectan a toda la organización.

- Mejora continua de cada uno de los procesos que intervienen en la planificación y ampliación del catálogo de servicios del Centro de Datos para que esté alineado con el negocio y cada día sea más completo.

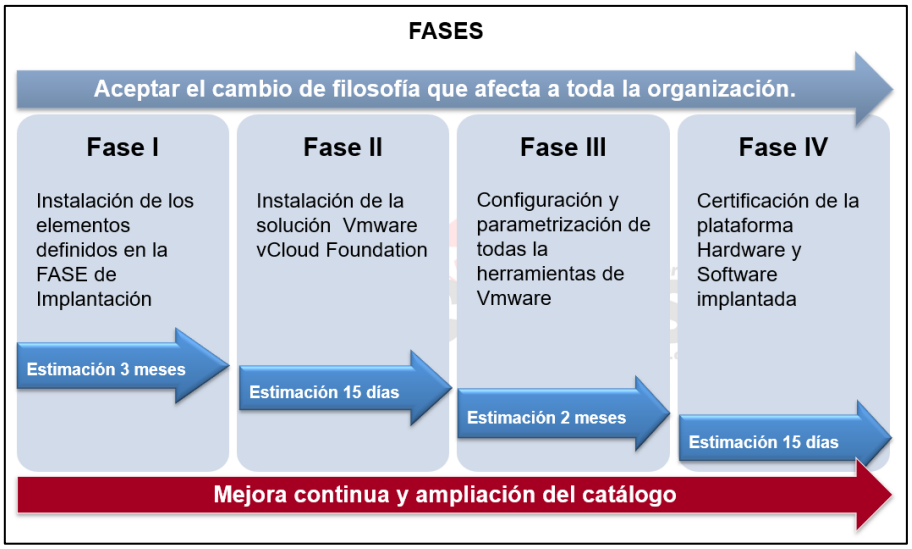


Ilustración 40 - Planificación de la FASE de Implantación

En la primera fase se estima un tiempo de desempeño de unos tres meses para realizar la instalación y configuración de los elementos físicos que participan en la FASE de implantación.

En la segunda fase se basa en la instalación de la solución de VCF, para lo que se estima unos 15 días dado que dicha instalación está automatizada por el fabricante.

La tercera fase se realizará la configuración y parametrización de todas las herramientas desplegadas de Vmware con una estimación de tiempo de unos 2 meses.

Por último, en la cuarta fase se realizarán todos los trabajos necesarios para certificar el Centro de Datos en tan solo 15 días.

Así pues, en el ANEXO X se propone una planificación con un diagrama de Gantt con las fases y estimación de tiempos descritas.

8.7 Organización y marco de trabajo

En la FASE de Diseño se recomienda que en proyectos nuevos seleccionar un marco de trabajo y con ello definir una organización, para alinear a todos los miembros de la organización con el negocio.

En base los requisitos de la FASE de Implantación y la experiencia que aporto de la participación en otros proyectos, se propone el siguiente organigrama a la dirección de la organización que sirva para cubrir toda la gestión y soporte del Centro de Datos de Alto Rendimiento que se va a implantar.

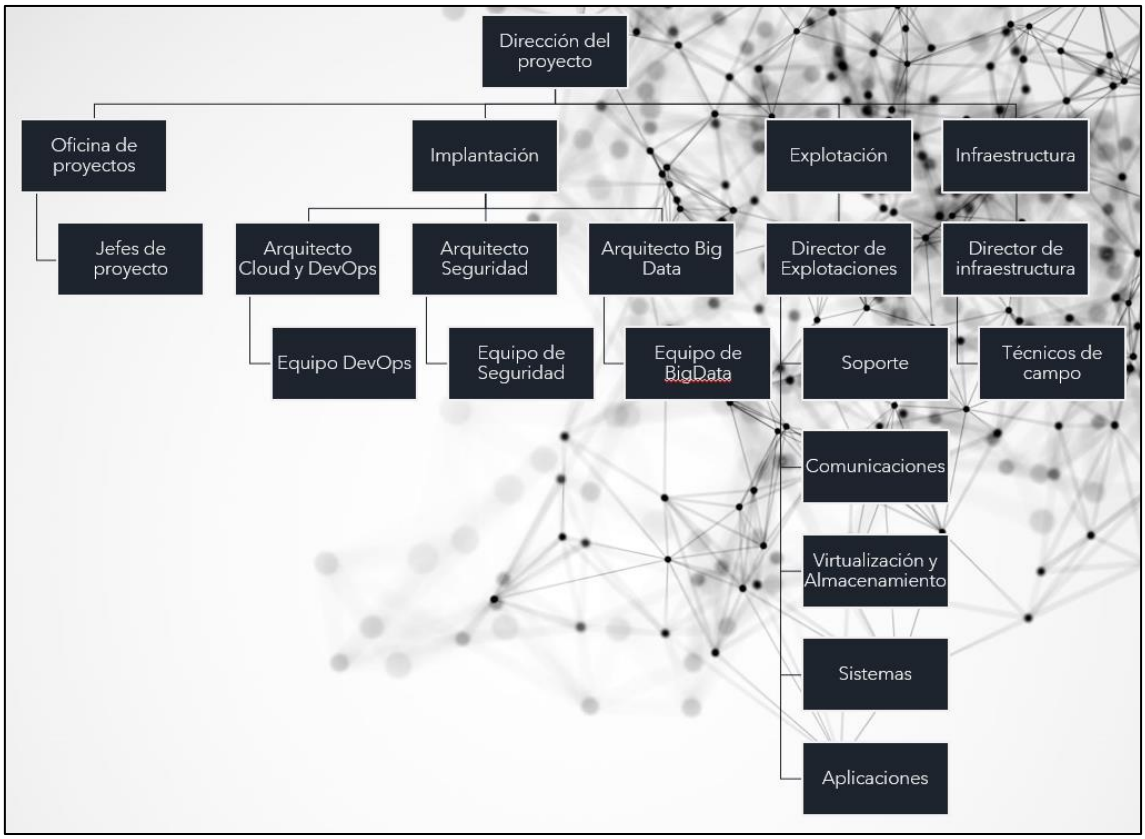


Ilustración 41 - Organigrama para la gestión del Centro de Datos de Alto Rendimiento

Es cierto que muchas áreas no son necesarias hasta que el Centro de Datos haya finalizado su implantación, pero el beneficio es muy alto por el conocimiento que se adquiere si hay ciertas áreas que participan desde el principio. Se recomienda que las áreas de Oficina de proyectos, Implantación e Infraestructura esté presente desde el inicio de la implantación para adquirir ese conocimiento muy valioso para luego dar un servicio ágil y de calidad.

Esta organización encaja con el modelo Bimodal IT descrito en la FASE de Diseño, porque el área de implantación está orientada a DevOps, esta implanta nuevos servicios que necesitan cambios ágiles hasta que se estabilicen. En cambio, las áreas de Explotación, Oficina de Proyectos e Infraestructura están más orientadas a procesos ITIL. Los servicios son entregados a estas áreas por el área de implantación cuando son estables y tiene pocos evolutivos, además de entregar todos los procedimientos y automatizaciones de los mismos.

8.8 Plan de riesgos

La fase de implantación se debe tener en cuenta los riesgos potenciales que pueden aparecer y afectar a la ejecución de esta etapa. En consecuencia, hay que tener presente que se debe realizar una evaluación permanente de los riesgos potenciales, asignándolos una prioridad, indicando si aplica o han dejado de aplicar.

En general, estos riesgos podrían incluir aspectos relacionados con:

Tabla 8 - Plan de riesgos en la FASE de implantación

Riesgos potenciales	Acciones para mitigarlos
Planificación demasiado optimista en la fase de implantación	Se recomienda realizar reuniones de seguimiento cada semana para revisar el cumplimiento de los plazos.
Un diseño incorrecto del Centro de Datos (inestable, no cumple las especificaciones, no puede prestar el servicio, etc.)	Se realizarán una prueba de concepto con el mínimo de funcionalidades para quien corresponda comprobar el funcionamiento del Centro de Datos.
Retrasos en la entrega e instalación del equipamiento.	Intentar trasladar al proveedor de la importancia que tiene realizar la entrega e instalación en la fecha indicada. También se recomienda firmar un contrato de compromiso que en caso de no cumplirse se pueda penalizar al proveedor.
Una mala instalación del equipamiento.	Es importante supervisar en todo momento todas las instalaciones que sean necesarias para verificar que cumplen todos los requisitos y están acorde con la normativa.
Material defectuoso.	Contaremos en todo momento con la garantía del fabricante para sustituir en el menor tiempo posible cualquier material.
Personal no cualificado.	Capacidad para poder decidir cuales personas realizarán las instalaciones y luego administrarán el sistema.
Sobre costes no contemplados en un primer momento.	Se identificarán e inmediatamente se tendrán que poner en conocimiento a quien corresponda.
No cumplir las expectativas ni del servicio.	Es importante realizar reuniones de seguimiento con quien corresponda para valorar sus inquietudes y sus valoraciones.
Realizar cambios constantes en los requisitos del Centro de Datos	Se recomienda comunicar los inconvenientes a quien corresponda en las reuniones de seguimiento.
Error al calcular la capacidad necesaria del Centro de Datos	Se identificarán e inmediatamente se tendrán que poner en conocimiento a quien corresponda.
No cumplir las expectativas de los clientes.	Se recomienda realizar reuniones de seguimiento con la dirección de la organización y clientes o usuarios para valorar sus inquietudes y sus valoraciones.

8.9 Buenas prácticas

Las buenas prácticas son un conjunto de normas o estándares de operación que guían a los usuarios de un Centro de Datos acerca de cómo desarrollar su trabajo de manera segura y correcta.

Es importante dar formación a todos los involucrados en la fase de implantación sobre las buenas prácticas que intervienen en cada proceso, muchas de estas buenas prácticas están definidas en los estándares TIA-942 y en la documentación de ITIL.

A continuación, se destacan las siguientes buenas prácticas que servirán como ejemplo para entender mejor este punto.

- Se documentará todo el equipamiento que se instala en el Centro de Datos, desde cómo se instaló, todas las pruebas realizadas y estos documentos tendrán que estar sujetos a los posibles cambios que surjan en un futuro.

- Es importante tener un inventario actualizado de todo el equipamiento con el nombre del fabricante, modelo y número de serie, además de incorporar los contratos de mantenimiento de los mismos.

- El personal que mantenga el sistema tendrá que recibir formación sobre las tecnologías implantada en el Centro de Datos que sirva como un valor añadido al mantenimiento del sistema.

- Se planificará el trabajo y se realizarán reuniones de seguimiento para evaluar la realización del trabajo del personal encargado en la administración.

Estas buenas prácticas son solo un ejemplo, pero es muy recomendable que se realicen documentos explicando con más detalle las buenas prácticas que hay que aplicar en cada caso y es de obligado cumplimiento por el personal a cargo de la gestión del Centro de Datos. Las buenas prácticas no sirven de mucho si una vez definidas y comunicas al personal no se realiza revisiones periódicas de su aplicación en el Centro de Datos, por este motivo es recomendable realizar auditorías para valorar la aplicación de las mismas.

8.10 Oferta económica

A continuación, se incluye la oferta económica de la FASE de Implantación, además de contemplar todos los elementos físicos se ha tenido en cuenta el coste de elementos no tangibles como el precio de licencias software, contratos de mantenimiento e instalación y horas del personal técnico involucrado en la implantación.

En la siguiente tabla, se presenta la oferta económica.

Tabla 9 - Presupuesto económico

Descripción	Uds.	Coste unidad (€)	PVP TOTAL
RACK de 48U	2	1.504,35	**3.008,70**
RACK de 42U	2	1.319,75	**2.639,50**
Patch Panel de UTP/FTP RJ45	2	300,50	**601,00**
Patch Panel de fibra LC-LC	2	250,50	**501,00**
Firewall PA-5220 (instalación incluida)	2	65.700,77	**131.401,54**
Switch Cisco Nexus 9504 (instalación incluida)	2	28.299,00	**56.598,00**
Switch Cisco Catalyst C9600 (instalación incluida)	2	19.199,05	**38.398,1**
Switch Brocade 6520 (instalación incluida)	2	10.800,99	**21.601,98**
Servidor Dell EMC PowerMax Pro 2000 (instalación incluida)	2	550.070,89	**1.100.141,78**
Servidor Dell Power Edge R640 (instalación incluida)	4	32.333,01	**129.332,04**
Servidor Dell Power Edge R940 (instalación incluida)	30	62.833,51	**1.885.005,3**
Cámaras CCTV (instalación incluida)	8	880,98	**7.047,84**
Sistema de incendios (instalación incluida)	1	27.148,47	**27.148,47**
Sistema de ventilación y clima, Hiref TADR0401 (41,2 Kw) (instalación incluida)	1	101.242,55	**101.242,55**
SAI EATON 9390 de 40 KVA (36 Kw) (instalación incluida)	2	17.093,99	**34.187,98**
Sistema de monitorización HONEYWELL (instalación incluida)	1	6.846,88	**6.846,88**
Cableado de cobre FTP 7 de 10/20/30 metros	-	102.000,98	**51.000,49**
Cableado de fibra LC multimodo de 10/20/30 metros	-	12,59	**3.120**
Licencias de Vmware Cloud Foundation (incluye soporte)	-	31.600,82	**2.148.855,76**
Mantenimiento de los equipos (hardware)	-	1.415.580,98	**1.415.580,98**
Dirección del proyecto	-	105.600,00	**105.600,00**
TOTAL			**7.269.859,89**

Capítulo 9 Conclusiones y discusiones

Nuestra sociedad vive en un mundo cada día más globalizado gracias a los dispositivos móviles y donde la información o el dato tiene cada vez más importancia en grandes organizaciones que prestan servicios a nivel mundial a través de Internet. La transformación digital necesita información para que cada organización pueda alinear su negocio con las tecnologías. La actual pandemia que vivimos, ha demostrado que las organizaciones que han realizado mejor una transformación digital son capaces de adaptarse mejor al nuevo escenario que ha traído la aparición de la Covid19.

En este escenario nace la necesidad de nuevos sistemas de información que demandan nuevas herramientas y métodos de trabajo dado que es inviable gestionarlos con las herramientas y métodos actuales. Estos sistemas demandan un Centro de Datos que cuente con equipamiento y herramientas, que agilicen la gestión y el mantenimiento de los sistemas de información. Un sistema *resiliente* preparado ante cualquier cambio que pueda comprometer a dicho sistema y lo suficientemente escalable para suministrar recursos ante cualquier demanda ya sea imprevista o circunstancial.

El diseño de un Centro de Datos de Alto Rendimiento, se basa en el modelo de negocio de un Cloud, proporciona funcionalidades y soluciones que demandan en la actualidad las organizaciones. Hay que tener en cuenta que la adopción de este Centro de Datos realiza cambios profundos sobre la organización que lo está adoptando, pero genera un aumento de su productividad y capacidad al ofrecer servicios a través de Internet.

La adopción e implantación de un Centro de Datos de Alto Rendimiento no es una tarea fácil al alcance de cualquier organización, la inversión es considerable y se debe contar con una gran experiencia en las TI. La solución de VMware Cloud Foundation facilita la adopción e implantación de un Cloud privado proporcionando un portal de autoservicio para ofrecer servicios IaaS, PaaS, SaaS, a la propia organización dueña del sistema u otras a través de Internet.

En la actualidad, se está debatiendo si los Cloud públicos serán los Centro de Datos del futuro para todas las organizaciones y como consecuencia estas no necesitarán tener un Centro de Datos para desempeñar su actividad. Sin embargo, el pago por uso de servicios Cloud públicos no es tan rentable y hay dudas en su seguridad. El cumplimiento de los marcos legales sobre todo en Europa y además de lo expuesto, hacen que a las organizaciones opten por un entorno híbrido donde puedan usar Cloud públicos, privados y su propia tecnología tradicional.

La implantación de un Cloud privado en un Centro de Datos de Alto Rendimiento no es una tarea fácil, hay pocas empresas en el mercado que cuenten con soluciones y experiencia en este tipo de proyectos. La mayoría de las organizaciones no están preparadas para mantener y explotar dicho sistema una vez implantado, y son pocas las compañías que tienen experiencia en el mantenimiento de un Cloud privado. Por este motivo, la decisión de adopción de un Centro de Datos de Alto Rendimiento, tiene que ser consensuada y analizada para valorar si realmente es necesario.

Hay que tener en cuenta, que la adopción de este sistema produce cambios en todos los niveles de la organización. Estos cambios pueden producir resistencias y tensiones en la organización y por este motivo, es muy importante tener el apoyo de la dirección de la organización desde el inicio del proyecto hasta final.

En el análisis de las soluciones software que proporcionan un Cloud privado, se han encontrado dificultades a la hora de acceder a información técnica donde se describen las funcionalidades y servicios que incluye cada solución. La mayoría de esta información no es pública y es necesario contactar con el fabricante de la solución. También se han tenido muchas dificultades para encontrar los costes de algunos elementos descritos en el presupuesto económico y se ha optado por realizar una estimación realista, en base a productos similares y mi experiencia.

Este diseño se basa en recomendaciones, normativas y buenas prácticas, pero según mi experiencia cada organización o institución son diferentes. Por este motivo, no se puede asegurar que este diseño sea válido para todos los escenarios posibles, el cambio en los requisitos descritos a lo largo del trabajo, conllevaría a la revisión íntegra del mismo para evaluar y analizar qué consecuencias surgen con los nuevos requisitos.

Una posible futura línea de investigación es la implantación automatizada de servicios PaaS y SaaS en el Centro de Datos de Alto Rendimiento que proporciona un Cloud privado. En la actualidad, los Cloud compiten por tener un catálogo de servicios lo más completo y eficiente posible, esto es lo que les distingue que un cliente se subscriba a un Cloud o a otro. Estos servicios se implantan haciendo uso de un API que proporciona el proveedor Cloud, esta API publica a su vez todos los servicios que dispone dicho Cloud.

Capítulo 10 Bibliografía de referencias

[2.1] *V.V.A.A. (septiembre 2020) Data center [reportaje en línea] Wikipedia [Fecha de consulta: 10 de octubre de 2020]. <https://en.wikipedia.org/wiki/Data_center>*

[2.2] *Angel Eulises Ortiz (julio 2020) Historia de los data centers o centros de datos, resumen, evolución y cronología [reportaje en línea] Pcweb.info [Fecha de consulta: 10 de octubre de 2020]. <https://pcweb.info/historia-de-los-data-centers-o-centros-de-datos-resumen-evolucion-y-cronologia/>*

[2.2] *V.V.A.A. (agosto 2020) Cloud computing [reportaje en línea] Wikipedia [Fecha de consulta: 10 de octubre de 2020]. <https://en.wikipedia.org/wiki/Cloud_computing>*

[2.3] *Unknow (sin fecha) Elementos de un CPD – Servicio y Mantenimiento [reportaje en línea] Cormat [Fecha de consulta: 14 de octubre de 2020]. <https://www.cormat.es/index.php/servicios-que-prestamos-para-cpd/89-centro-de-proceso-de-datos-cpd/125-elementos-de-un-cpd-servicio-y-mantenimiento>*

[2.4] *Unknow (sin fecha) Suelos técnicos CPD y salas de servidores [reportaje en línea] Polygroup [Fecha de consulta: 14 de octubre de 2020]. <https://accessfloorpolygroup.com/es/suelo-tecnico-cpd/>*

[2.5] *Unknow (septiembre 2010) Proyecto de centro de proceso de datos hospital 12 de octubre [documento en línea] Comunidad de Madrid [Fecha de consulta: 14 de octubre de 2020]. <http://www.madrid.org/cs/Satellite?blobcol=urldata&blobheader=application/pdf&blobheadername1=Content-Disposition&blobheadervalue1=filename=Proyecto+CPD-203592.pdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1271827309716&ssbinary=true>*

[2.6] *V.V.A.A. (agosto 2020) Uninterruptible power supply [reportaje en línea] Wikipedia [Fecha de consulta: 12 de octubre de 2020]. <https://en.wikipedia.org/wiki/Uninterruptible_power_supply>*

[2.7] *V.V.A.A. (octubre 2020) Grupo electrógeno [reportaje en línea] Wikipedia [Fecha de consulta: 13 de octubre de 2020]. <https://es.wikipedia.org/wiki/Grupo_electr%C3%B3geno>*

[2.8] *Unknow (julio 2020) Tendencias en la climatización de Centros de Datos [reportaje en línea] Clysema [Fecha de consulta: 18 de octubre de 2020]. <https://clysema.com/tendencias-climatizacion-centros-de-datos/>*

[2.9] *Unknow (julio 2020) Impacto de pasillos calientes y fríos en la eficiencia y temperatura del centro de datos [documento en línea] Schneider Electric [Fecha de consulta: 18 de octubre de 2020]. <https://download.schneider-electric.com/files?p_Doc_Ref=SPD_DBOY-7EDLE8_ES>*

[2.10] *Jesús Costas Santos. (julio 2011) Seguridad y Alta Disponibilidad. [libro físico] RA-MA [Fecha de consulta: 25 de octubre de 2020].*

[2.11] *V.V.A.A. (octubre 2020) 19-inch rack [reportaje en línea] Wikipedia [Fecha de consulta: 15 de octubre de 2020]. <https://en.wikipedia.org/wiki/19-inch_rack#Overview_and_history>*

[2.12] *V.V.A.A. (octubre 2020) Patch panel [reportaje en línea] Wikipedia [Fecha de consulta: 16 de octubre de 2020]. < https://en.wikipedia.org/wiki/Patch_panel>*

[2.13] *V.V.A.A. (septiembre 2020) Ethernet [reportaje en línea] Wikipedia [Fecha de consulta: 16 de octubre de 2020]. <https://es.wikipedia.org/wiki/Ethernet>*

[2.14] *V.V.A.A. (septiembre 2020) Fibra óptica [reportaje en línea] Wikipedia [Fecha de consulta: 21 de octubre de 2020]. <https://es.wikipedia.org/wiki/Fibra_%C3%B3ptica>*

[2.15] *V.V.A.A. (septiembre 2020) Firewall [reportaje en línea] Wikipedia [Fecha de consulta: 23 de octubre de 2020]. <https://en.wikipedia.org/wiki/Firewall_(computing)>*

[2.16] *V.V.A.A. (septiembre 2020) Router [reportaje en línea] Wikipedia [Fecha de consulta: 23 de octubre de 2020]. <https://en.wikipedia.org/wiki/Router_(computing)>*

[2.17] *V.V.A.A. (junio 2020) Network Switch [reportaje en línea] Wikipedia [Fecha de consulta: 23 de octubre de 2020]. <https://en.wikipedia.org/wiki/Network_switch>*

[2.18] *V.V.A.A. (junio 2020) Server (computing) [reportaje en línea] Wikipedia [Fecha de consulta: 23 de octubre de 2020]. <https://en.wikipedia.org/wiki/Server_(computing)>*

[2.19] *V.V.A.A. (septiembre 2020) Red de área de almacenamiento [reportaje en línea] Wikipedia [Fecha de consulta: 22 de octubre de 2020]. <https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_de_almacenamiento>*

[3.1] *V.V.A.A. (agosto 2020) Software [reportaje en línea] Wikipedia [Fecha de consulta: 19 de octubre de 2020]. <https://es.wikipedia.org/wiki/Software>*

[3.2] *Unknow (sin fecha) Virtualización [reportaje en línea] VMware [Fecha de consulta: 10 de octubre de 2020]. <https://www.vmware.com/es/solutions/virtualization.html>*

[3.3] *V.V.A.A. (octubre 2020) VMware ESXi [reportaje en línea] Wikipedia [Fecha de consulta: 10 de octubre de 2020]. <https://es.wikipedia.org/wiki/VMware_ESXi>*

[3.4] *V.V.A.A. (octubre 2020) Software-defined networking [reportaje en línea] Wikipedia [Fecha de consulta: 10 de octubre de 2020]. <https://en.wikipedia.org/wiki/Software-defined_networking>*

[3.5] *RedaccionMCP (marzo 2016) Virtualización de almacenamiento, una opción que aporta grandes ventajas [reportaje en línea] MCPRO [Fecha de consulta: 15 de octubre de 2020]. <https://www.muycomputerpro.com/2016/03/17/virtualizacion-almacenamiento-fujitsu#:~:text=La%20virtualizaci%C3%B3n%20de%20almacenamiento%20se,desde%20una%20%C3%BAnica%20consola%20central>*

[3.6] *Unknow (sin fecha) El centro de datos definido por software [reportaje en línea] VMware [Fecha de consulta: 17 de octubre de 2020]. <https://www.vmware.com/es/solutions/software-defined-datacenter.html>*

[3.7] *Unknow (sin fecha) CONTENEDORES EN GOOGLE [reportaje en línea] Google Cloud [Fecha de consulta: 27 de octubre de 2020]. <https://cloud.google.com/containers>*

[3.8] *Unknow (sin fecha) ¿Qué es Kubernetes? [reportaje en línea] Kubernetes [Fecha de consulta: 30 de octubre de 2020]. <https://kubernetes.io/es/docs/concepts/overview/what-is-kubernetes/>*

[3.9] *Unknow (sin fecha) Conceptos [reportaje en línea] Kubernetes [Fecha de consulta: 30 de octubre de 2020]. <https://kubernetes.io/es/docs/concepts/>*

[3.10] *V.V.A.A (septiembre 2020) Computación en la nube [reportaje en línea] Wikipedia [Fecha de consulta: 10 de octubre de 2020]. <https://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube>*

[4.1] *V.V.A.A (agosto 2020) IEEE 802.3 [reportaje en línea] Wikipedia [Fecha de consulta: 30 de octubre de 2020]. <https://es.wikipedia.org/wiki/IEEE_802.3>*

[4.2] *Unknow (noviembre 2017) Data Center [reportaje en línea] EvaluandoCloud.com [Fecha de consulta: 30 de octubre de 2020]. <https://evaluandocloud.com/data-center/#:~:text=Los%20Centros%20de%20datos%20o,Telecomunicaciones>*

[4.3] *V.V.A.A (mayo 2020) TIA-942 [reportaje en línea] Wikipedia [Fecha de consulta: 30 de octubre de 2020]. <https://en.wikipedia.org/wiki/TIA-942>*

[5.1] *V.V.A.A. (julio 2020) COBIT [reportaje en línea] Wikipedia [Fecha de consulta: 29 de octubre de 2020]. <https://en.wikipedia.org/wiki/COBIT>*

[5.2] *Unknown (diciembre 2013) A Comparison of COBIT, ITIL, ISO 27002 and NIST [reportaje en línea] An Objective look [Fecha de consulta: 30 de octubre de 2020]. <http://agnosticationater.blogspot.com/2013/12/a-comparison-of-cobit-itil-iso-27002.html>*

[5.3] *V.V.A.A. (agosto 2020) ITIL [reportaje en línea] Wikipedia [Fecha de consulta: 30 de octubre de 2020]. <https://en.wikipedia.org/wiki/ITIL>*

[5.4] *Arauzo Sánchez, Mario (octubre 2013) ¿Cuáles son las 5 etapas del servicio en la gestión TI según ITIL 2011? [reportaje en línea] Doit Smart [Fecha de consulta: 30 de octubre de 2020]. <https://www.doitsmart.es/2013/10/cuales-son-las-5-etapas-del-servicio-en-la-gestion-ti-segun-itil-r/>*

[5.5] *V.V.A.A. (febrero 2020) Committee of Sponsoring Organizations of the Treadway Commission [reportaje en línea] Wikipedia [Fecha de consulta: 30 de octubre de 2020]. < <https://en.wikipedia.org/wiki/Committee_of_Sponsoring_Organizations_of_the_Treadway_Commission >*

[5.6] *Council of Sponsoring Organizations of the Treadway Commission (Unknow) Are you getting value out of your risk program? [reportaje en línea] Deloitte [Fecha de consulta: 30 de octubre de 2020]. <https://www2.deloitte.com/us/en/pages/risk/articles/flip-side-coso-erm.html>*

[5.7] *Richard J. Anderson y Mark L. Frigo (enero 2020) Creating and Protecting Value: Understanding and Implementing Enterprise Risk Management [documento en línea] Committee of Sponsoring Organizations of the Treadway Commission (COSO) [Fecha de consulta: 30 de octubre de 2020]. <https://www.coso.org/Documents/COSO-ERM-Creating-and-Protecting-Value.pdf>*

[5.8] *V.V.A.A. (septiembre 2020) DevOps [reportaje en línea] Wikipedia [Fecha de consulta: 30 de octubre de 2020]. <https://es.wikipedia.org/wiki/DevOps>*

[7.1] *Unknow (abril 2005) TIA-942 [documento en línea] Telecommunications Industry Association [Fecha de consulta: 1 de octubre de 2020]. <https://kupdf.net/download/tia-942-espa-ntilde-ol_58ac573d6454a7ab7bb1e905_pdf>*

[7.2] *Unknow (noviembre 2007) ISO/IEC 27001:2005 [documento en línea] AENOR [Fecha de consulta: 2 de octubre de 2020]. <https://www.ombuds.es/documentos/200711-cambio-norma-UNE-ISO-27001.pdf>*

[7.3] *Unknow (enero 2010) Esquema Nacional de Seguridad [documento en línea] BOE [Fecha de consulta: 1 de octubre de 2020]. <https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330>*

[7.4] *Unknow (septiembre 2020) Reglamento general de protección de datos [reportaje en línea] Web Oficial de la Unión Europea [Fecha de consulta: 4 de octubre de 2020]. <https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm>*

[7.5] *Unknow (sin fecha) VMware Cloud Foundation Documentation [reportaje en línea] VMware [Fecha de consulta: 7 de octubre de 2020]. <https://docs.vmware.com/en/VMware-Cloud-Foundation/index.html>*

[7.6] *V.V.A.A. (septiembre 2020) Sistema de alarma [reportaje en línea] Wikipedia [Fecha de consulta: 3 de noviembre de 2020]. <https://es.wikipedia.org/wiki/Sistema_de_alarma>*

[7.7] *V.V.A.A. (octubre 2020) Circuito cerrado de televisión [reportaje en línea] Wikipedia [Fecha de consulta: 3 de noviembre de 2020]. <https://es.wikipedia.org/wiki/Circuito_cerrado_de_televisi%C3%B3n>*

[7.8] *V.V.A.A. (julio 2019) Sistema de monitorización [reportaje en línea] Wikipedia [Fecha de consulta: 3 de noviembre de 2020]. <https://es.wikipedia.org/wiki/Sistema_de_monitorizaci%C3%B3n>*

[7.9] *V.V.A.A. (noviembre 2020) Cable de Categoría 7 [reportaje en línea] Wikipedia [Fecha de consulta: 6 de noviembre de 2020]. <https://es.wikipedia.org/wiki/Cable_de_Categor%C3%ADa_7>*

[7.10] *Unknow (sin fecha) Cable/latiguillo/jumper de fibra óptica LC UPC a LC UPC 1m OM4 50/125 dúplex multimodo PVC 2.0mm [reportaje en línea] FS.com [Fecha de consulta: 7 de noviembre de 2020]. <https://www.fs.com/es/products/40180.html>*

[7.11] *Unknow (septiembre 2016) Familia de almacenamiento vmax all flash [documento en línea] DELL-EMC [Fecha de consulta: 25 de octubre de 2020]. <https://www.delltechnologies.com/es-mx/collaterals/unauth/white-papers/products/storage/h14920-intro-to-vmax-af-storage.pdf>*

[7.12] *Unknow (abril 2014) Campus - Resumen de diseño [documento en línea] Cisco [Fecha de consulta: 27 de octubre de 2020]. <https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf>*

[7.13] *V.V.A.A. (noviembre 2020) Zona desmilitarizada (informática) [reportaje en línea] Wikipedia [Fecha de consulta: 6 de noviembre de 2020]. <https://es.wikipedia.org/wiki/Zona_desmilitarizada_(inform%C3%A1tica)>*

[7.14] *V.V.A.A. (noviembre 2020) Servidor blade (informática) [reportaje en línea] Wikipedia [Fecha de consulta: 16 de noviembre de 2020]. <https://es.wikipedia.org/wiki/Servidor_blade>*

[7.15] *V.V.A.A. (noviembre 2020) Hyper-converged infrastructure (informática) [reportaje en línea] Wikipedia [Fecha de consulta: 16 de noviembre de 2020]. <https://en.wikipedia.org/wiki/Hyper-converged_infrastructure>*

[7.16] *V.V.A.A. (noviembre 2020) Red de área de almacenamiento [reportaje en línea] Wikipedia [Fecha de consulta: 13 de noviembre de 2020]. <https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_de_almacenamiento>*

[7.17] *Unknow (sin fecha) Ficha VMWARE CLOUD FOUNDATION [documento en línea] VMware [Fecha de consulta: 1 de noviembre de 2020]. <https://www.vmware.com/content/dam/digitalmarketing/vmware/es/pdf/whitepaper/products/vmware-cloud-foundation-datasheet.pdf>*

[7.18] *Unknow (sin fecha) Documentación de VMware vSphere [reportaje en línea] VMware [Fecha de consulta: 12 de octubre de 2020]. <https://docs.vmware.com/es/VMware-vSphere/index.html>*

[7.19] *Unknow (sin fecha) Documentación de VMware NSX-T Data Center [reportaje en línea] VMware [Fecha de consulta: 12 de octubre de 2020]. <https://docs.vmware.com/es/VMware-NSX-T-Data-Center/index.html>*

[7.20] *Unknow (sin fecha) Documentación de VMware vRealize Automation [reportaje en línea] VMware [Fecha de consulta: 12 de octubre de 2020]. <https://docs.vmware.com/es/vRealize-Automation/index.html>*

[7.21] *Unknow (sin fecha) ¿Qué es un clúster de Tanzu Kubernetes? [reportaje en línea] VMware [Fecha de consulta: 15 de octubre de 2020]. <https://docs.vmware.com/es/VMware-vSphere/7.0/vmware-vsphere-with-tanzu/GUID-DC22EA6A-E086-4CFE-A7DA-2654891F5A12.html>*

[7.22] *Unknow (sin fecha) VMware HCX Documentation [reportaje en línea] VMware [Fecha de consulta: 15 de octubre de 2020]. <https://docs.vmware.com/en/VMware-HCX/index.html>*

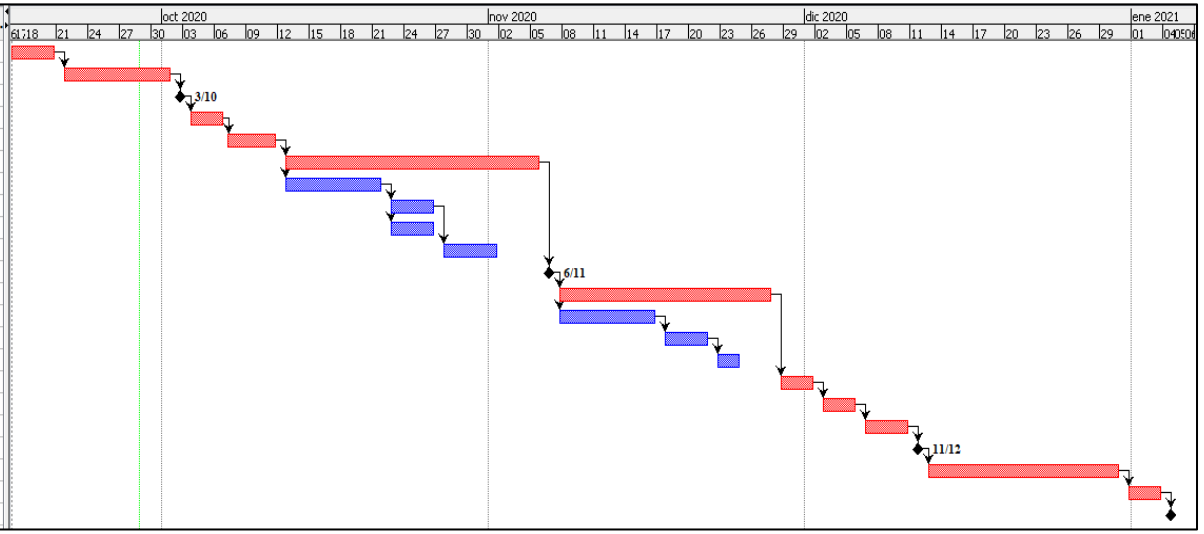
[7.23] *Dídac López, Ferran Martí (febrero 2014) Gestión funcional de servicios SI/TI [libro físico] Material docente de la UOC [Fecha de consulta: 22 de octubre de 2020].*

[7.24] *Unknow (sin fecha) Bimodal [reportaje en línea] Gartner [Fecha de consulta: 22 de noviembre de 2020]. <https://www.gartner.com/en/information-technology/glossary/bimodal>*

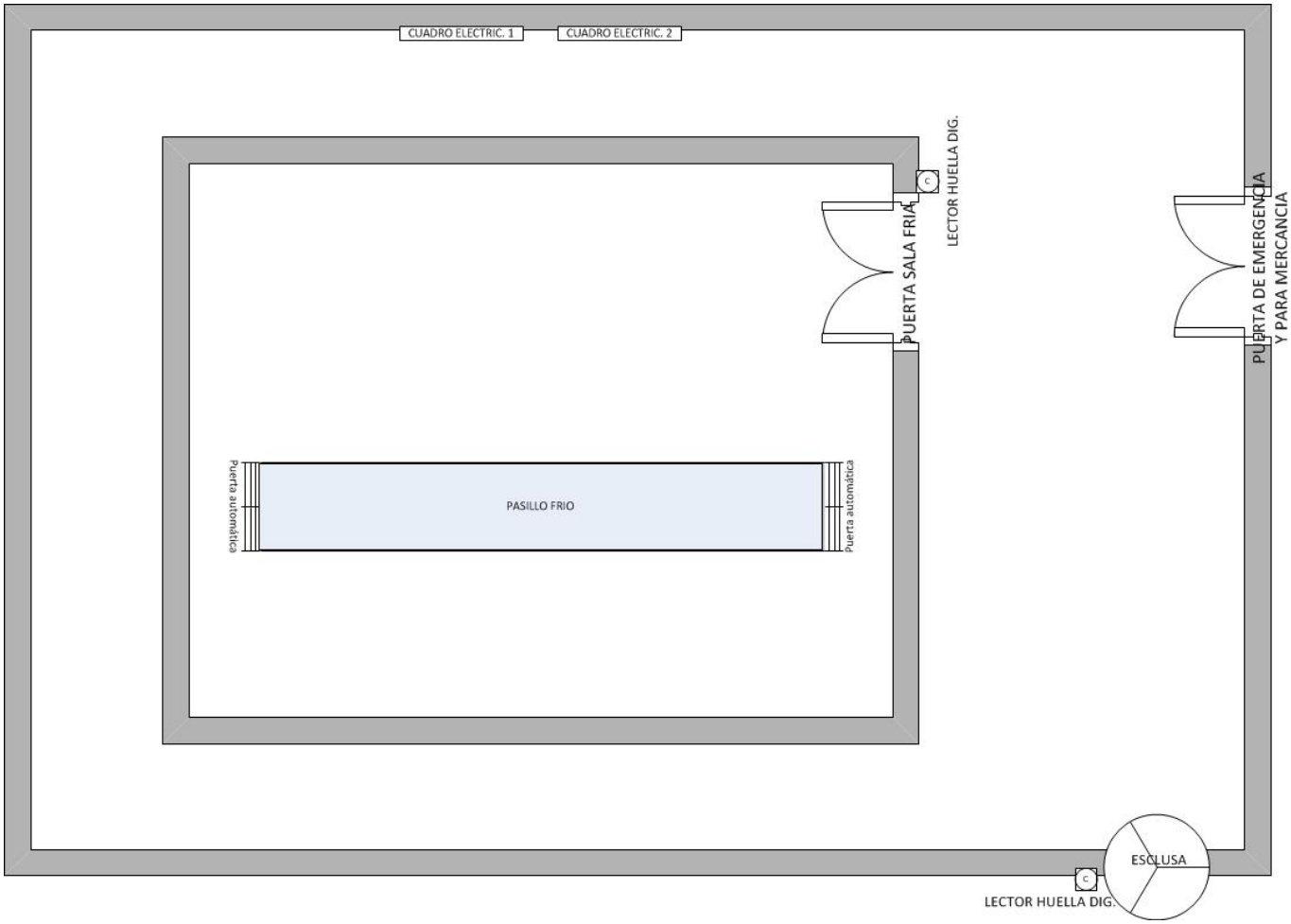
Capítulo 11 ANEXOS

11.1 ANEXO I: Planificación del proyecto con diagrama de Gantt

	Nombre	Durac...	Inicio	Terminado	Pre.
1	Inicio TFG	5 days	16/09/20 18:00	20/09/20 22:00	
2	Desarrollo del Plan de Trabajo	11 days	21/09/20 18:00	1/10/20 22:00	1
3	Entrega PEC1: Plan de Trabajo	1 day	2/10/20 18:00	2/10/20 22:00	2
4	Análisis y estudio de tecnologías, soluciones y equipamiento para un Centro de Datos	4 days	3/10/20 18:00	6/10/20 22:00	3
5	Definición de requrimientos y alcance del proyecto	6 days	7/10/20 8:00	11/10/20 22:00	4
6	Definir y documentar la FASE de Diseño	25 days	12/10/20 18:00	5/11/20 22:00	5
7	Buscar el equipamiento identificado con sus caracteristicas y necesidades	10 days	12/10/20 18:00	21/10/20 22:00	5
8	Buscar documentación técnica de VMware vCloud Foundation	5 days	22/10/20 18:00	26/10/20 22:00	7
9	Buscar ejemplos de implantaciones de VMware vCloud Foundation	5 days	22/10/20 18:00	26/10/20 22:00	7
10	Definir Analisis de riesgos y cambios	6 days	27/10/20 18:00	1/11/20 22:00	8
11	Entrega PEC2: FASE de Diseño	1 day	6/11/20 18:00	6/11/20 22:00	6
12	Definir y documentar la FASE de Implantación	21 days	7/11/20 18:00	27/11/20 22:00	11
13	Proponer la instalación y puesta marcha del equipamiento	10 days	7/11/20 18:00	16/11/20 22:00	11
14	Definir la organización del equipo de trabajo	5 days	17/11/20 18:00	21/11/20 22:00	13
15	Esquema de red del Centro de Datos	3 days	22/11/20 18:00	24/11/20 22:00	14
16	Definir Marco de trabajo	4 days	28/11/20 18:00	1/12/20 22:00	12
17	Ejecución de un presupuesto económico	4 days	2/12/20 18:00	5/12/20 22:00	16
18	Conclusiones, bibliografía y ANEXOS	5 days	6/12/20 18:00	10/12/20 22:00	17
19	Entrega PEC3: Proyecto completado 95%	1 day	11/12/20 18:00	11/12/20 22:00	18
20	Desarrllo de la Presentación del proyecto	19 days	12/12/20 18:00	30/12/20 22:00	19
21	Revision y Entrega TFG y Presentación	4 days	31/12/20 18:00	3/01/21 22:00	20
22	Fin TFG	7 days	4/01/21 18:00	10/01/21 22:00	21

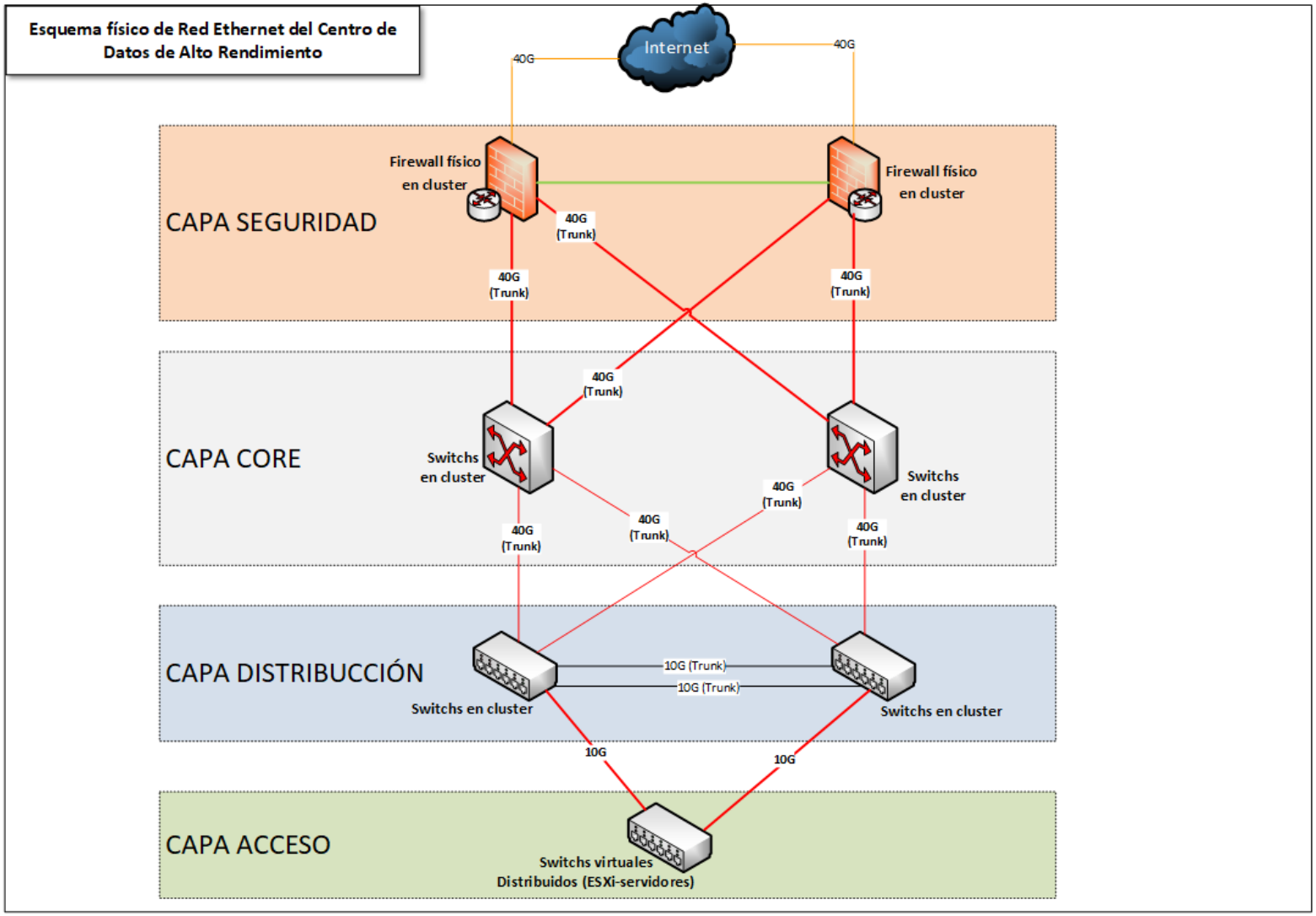


11.2 ANEXO II: Plano de obra civil del CPD

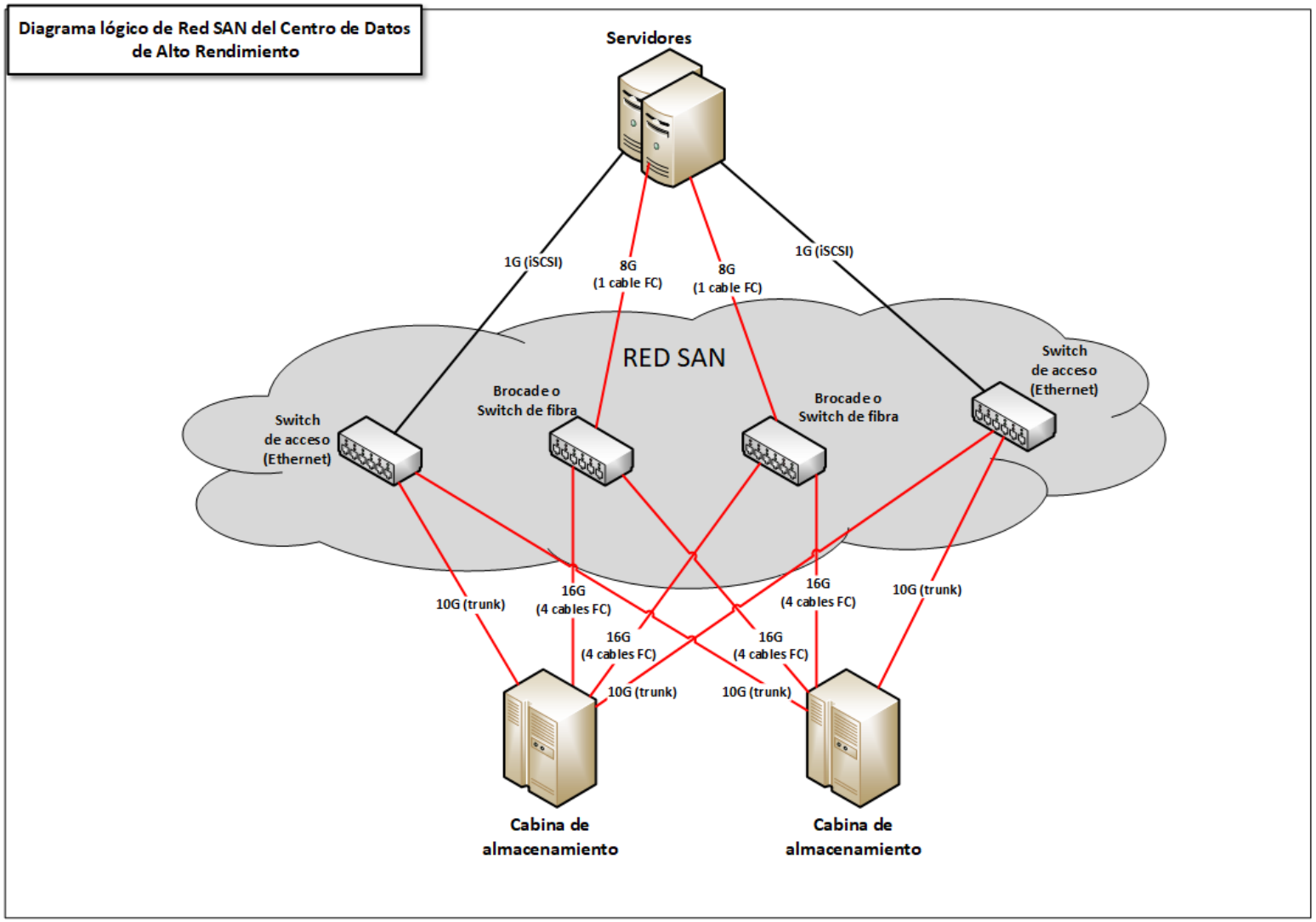


*Total de superficie 82 m2

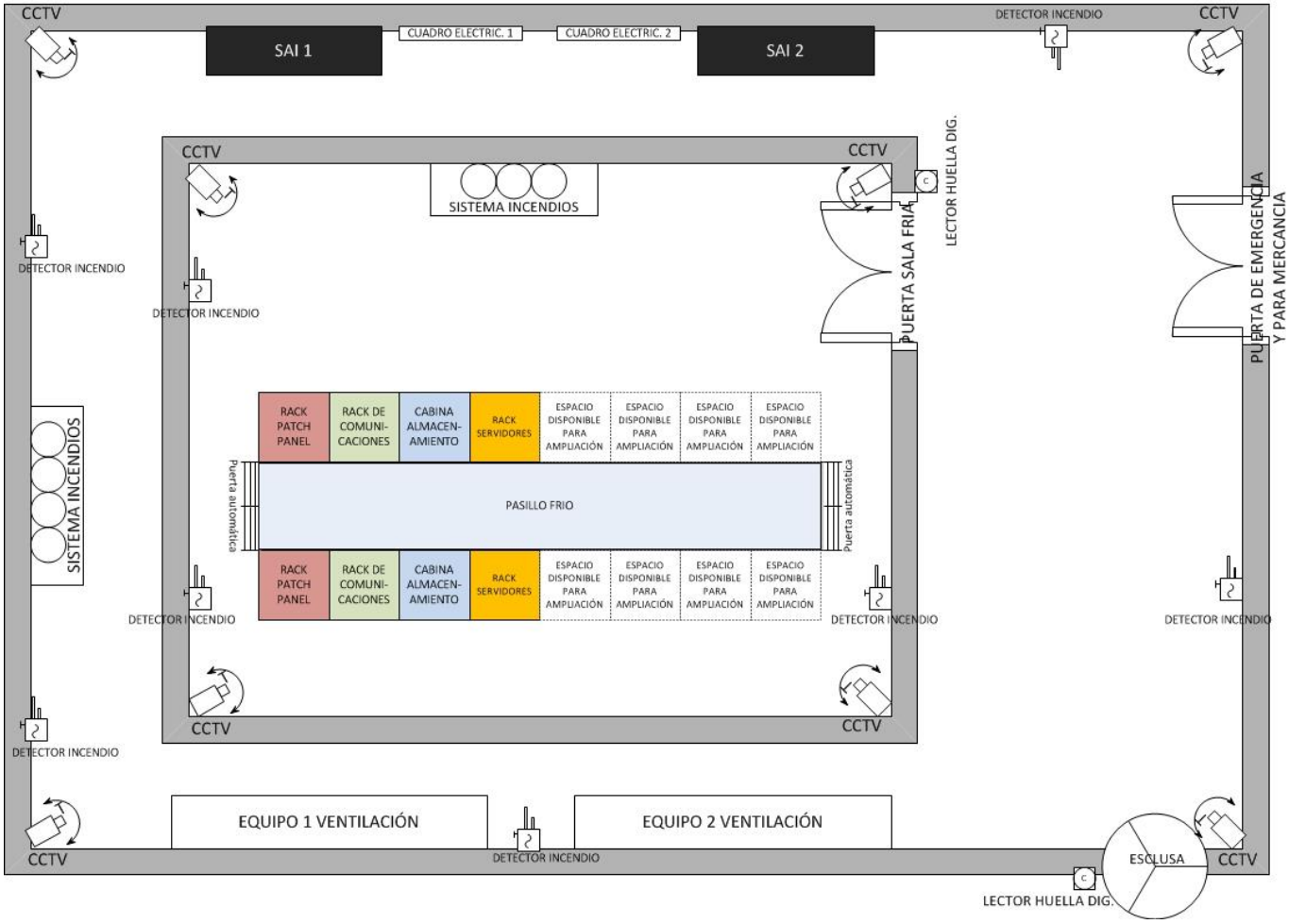
11.3 ANEXO III: Esquema físico de red Ethernet



11.4 ANEXO IV: Esquema de red SAN

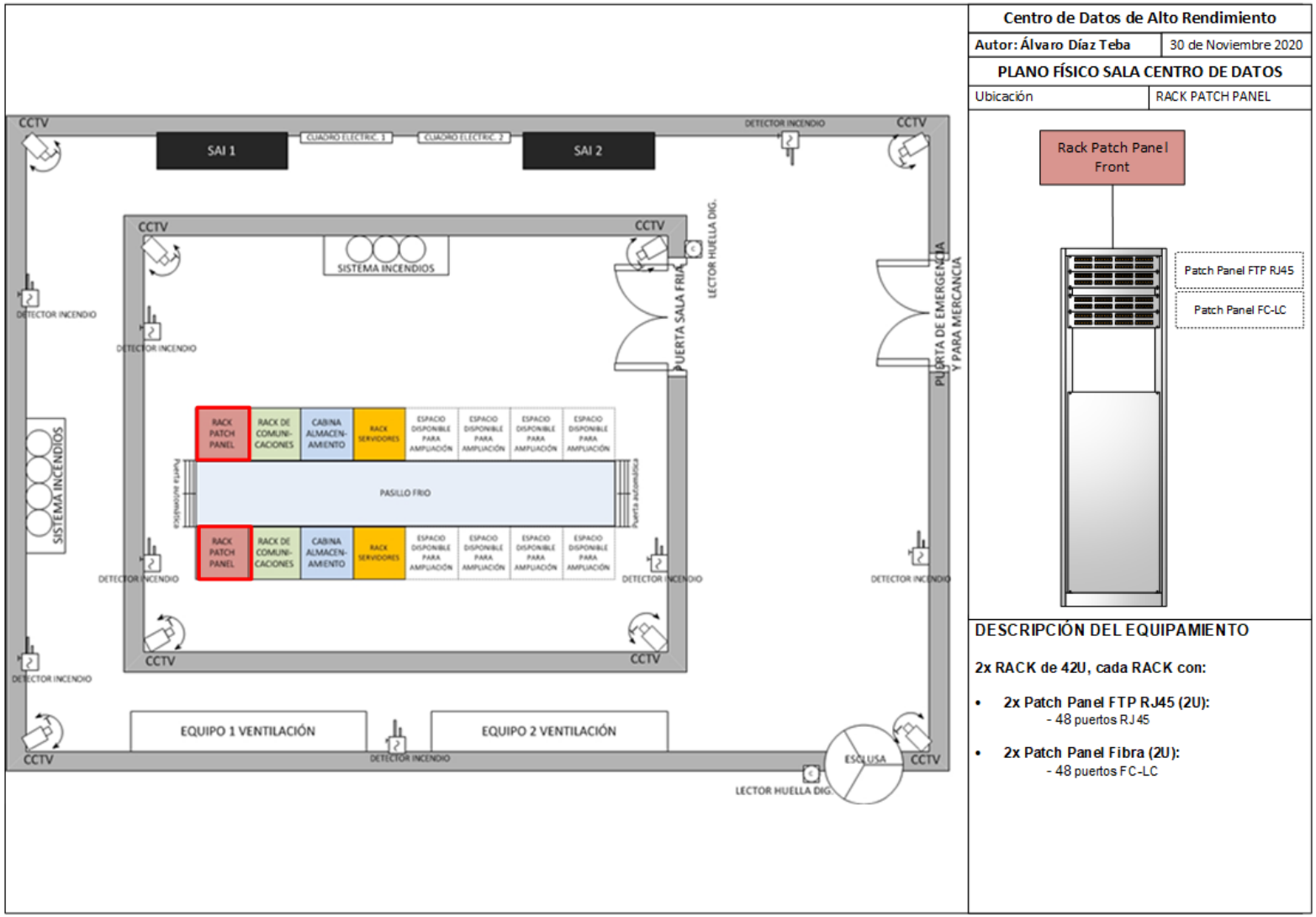


11.5 ANEXO V: Plano de la Sala del Centro de Datos.

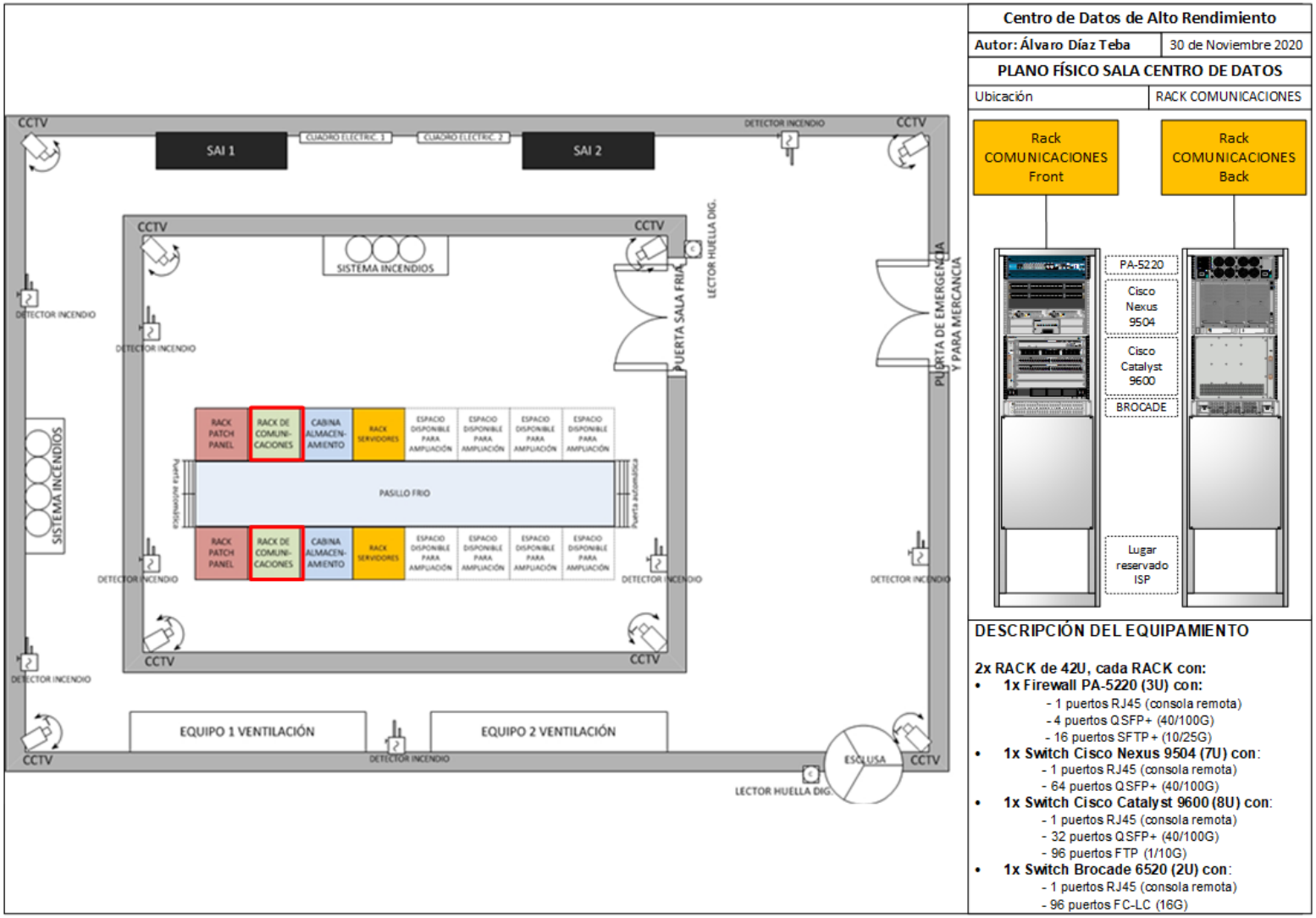


*Total de superficie 82 m2

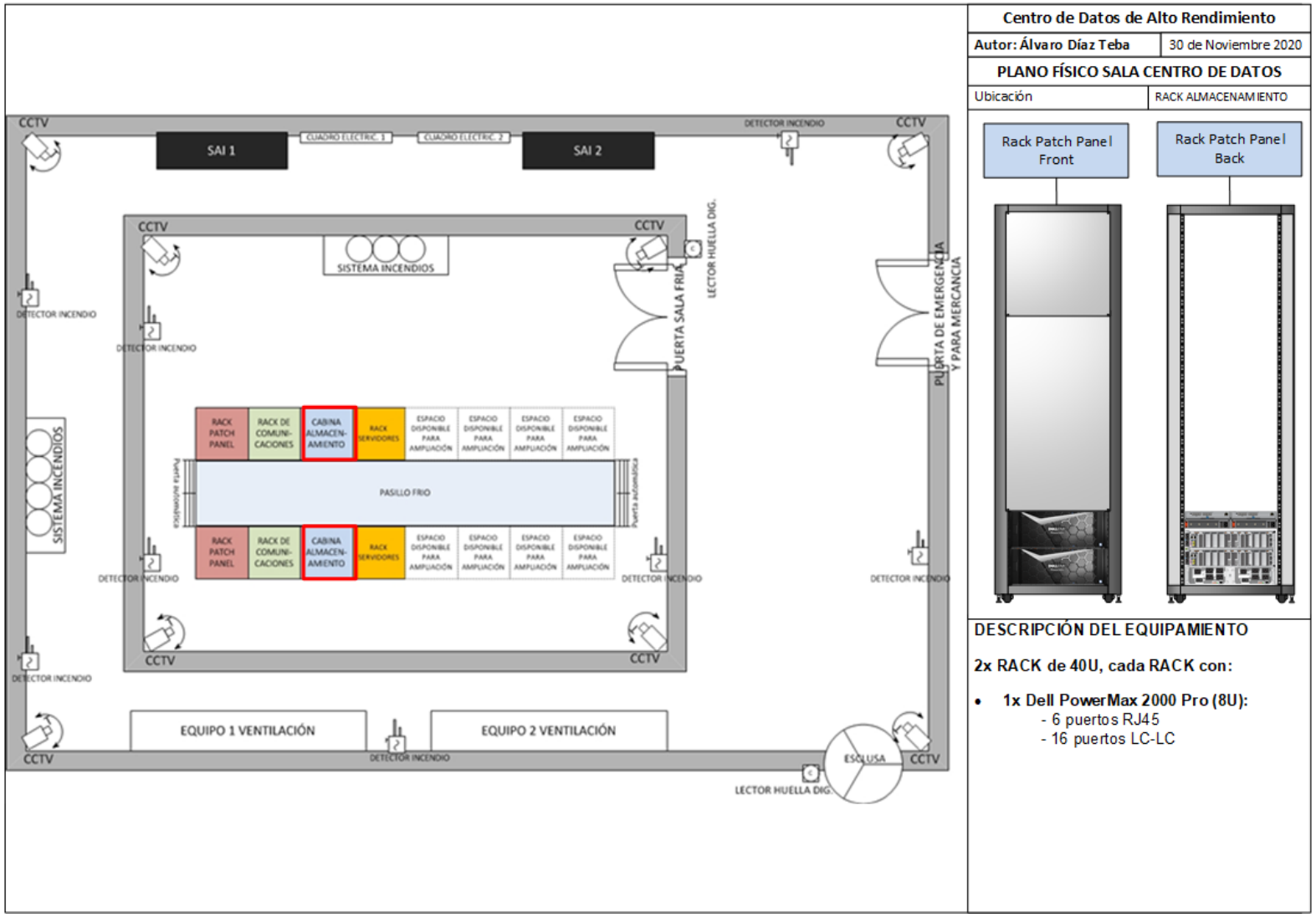
11.6 ANEXO VI: RACK DE PATCH PANEL.



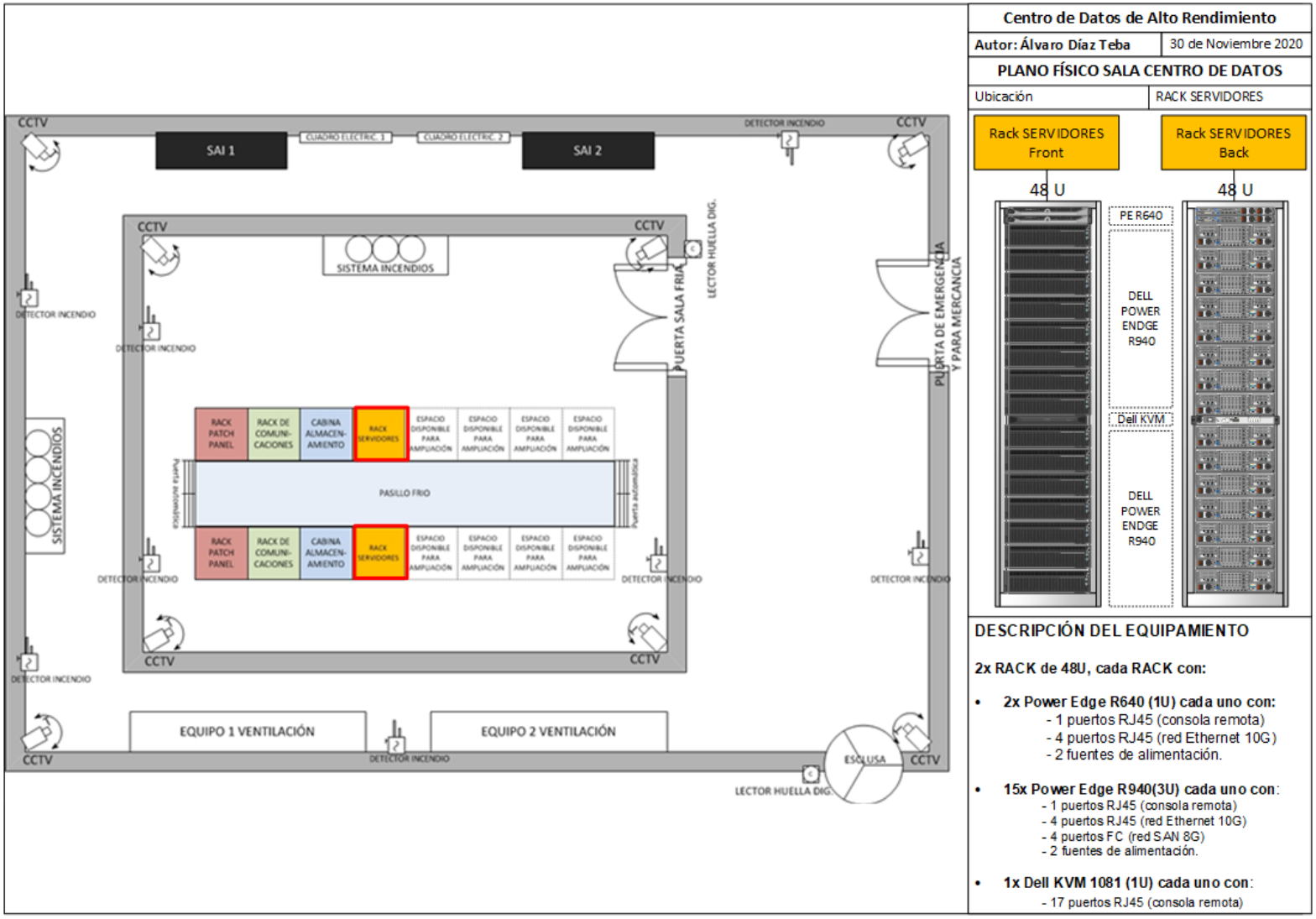
11.7 ANEXO VII: RACK DE EQUIPOS DE COMUNICACIONES.



11.8 ANEXO VIII: RACK DE EQUIPOS DE ALMACENAMIENTO.



11.9 ANEXO IX: RACK SERVIDORES FÍSICOS.



11.10 ANEXO X: Diagrama de Gantt de la FASE de Implantación.

	Nombre	Duración	Inicio	Terminado	Pre
1	Inicio	0 days	1/01/21 19:00	1/01/21 19:00	
2	FASE I	90 days	1/01/21 19:00	1/04/21 19:00	1
3	Kickoff del proyecto	1 day	1/01/21 19:00	2/01/21 19:00	1
4	Instalacion SAIs	15 days	2/01/21 19:00	17/01/21 19:00	3
5	Instalacion de los grupos de ventilación y clima	30 days	17/01/21 19:00	16/02/21 19:00	4
6	Sistema de protección contra incendios	60 days	2/01/21 19:00	3/03/21 19:00	3
7	Sistema CCTV	7 days	17/01/21 19:00	24/01/21 19:00	4
8	Sistema de monitorización	20 days	3/03/21 19:00	23/03/21 19:00	6
9	Instalacion de los Rack	3 days	17/01/21 19:00	20/01/21 19:00	4
10	Instalacion de los Pacth Panel	2 days	20/01/21 19:00	22/01/21 19:00	9
11	Instalacion de los equipos de comunicaciones	25 days	3/03/21 19:00	28/03/21 19:00	6
12	Instalacion de las cabinas de almacenamiento	20 days	3/03/21 19:00	23/03/21 19:00	6
13	Instalacion de los servidores físicos	27 days	3/03/21 19:00	30/03/21 19:00	6
14	Fin FASE I	1 day?	30/03/21 19:00	31/03/21 19:00	13
15	FASE II	15 days	1/04/21 19:00	16/04/21 19:00	2
16	Instalacion de VMware Cloud Foundation (VCF)	10 days	31/03/21 19:00	10/04/21 19:00	14
17	Comprobaciones y pruebas sobre la VCF	4 days	10/04/21 19:00	14/04/21 19:00	16
18	Fin FASE II	1 day?	14/04/21 19:00	15/04/21 19:00	17
19	FASE III	60 days	16/04/21 19:00	15/06/21 19:00	15
20	Creación de nuevos workload domains en VCF	10 days	15/04/21 19:00	25/04/21 19:00	18
21	Despliegue de Tanzu	5 days	25/04/21 19:00	30/04/21 19:00	20
22	Cargar contenido en el portal de autoprovisionamiento	30 days	30/04/21 19:00	30/05/21 19:00	21
23	Pruebas sobre el portal de autoprovisionamiento	14 days	30/05/21 19:00	13/06/21 19:00	22
24	Fin FASE III	1 day?	13/06/21 19:00	14/06/21 19:00	23
25	FASE IV	15 days	15/06/21 19:00	30/06/21 19:00	19
26	Certificación SAIs	2 days	14/06/21 19:00	16/06/21 19:00	24
27	Cerficación grupos de ventilación y clima	1 day	16/06/21 19:00	17/06/21 19:00	26
28	Certificación equipos de comunicaciones	2 days	17/06/21 19:00	19/06/21 19:00	27
29	Certificación cabinas de almacenamiento	1 day	19/06/21 19:00	20/06/21 19:00	28
30	Certificación de los equipos de cómputo	3 days	20/06/21 19:00	23/06/21 19:00	29
31	Certficiación integral del Centro de Datos	5 days	23/06/21 19:00	28/06/21 19:00	30
32	Fin Fase IV	1 day?	28/06/21 19:00	29/06/21 19:00	31
33	FIN	1 day?	30/06/21 19:00	1/07/21 19:00	25