



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Diseño de un Centro de Procesamiento de Datos Modular para Edge Computing

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Pablo Rojo Mínguez

DIRECTORES: Fernando Suárez Lorenzo

Francisco J. Rodríguez Martínez

CURSO ACADÉMICO: 2023-2024

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Diseño de un Centro de Procesamiento de Datos Modular para Edge Computing

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de la Información

UniversidadeVigo

RESUMEN

El Centro de Procesamiento de Datos [1] es aquella instalación diseñada para albergar equipos informáticos y de telecomunicaciones, permitiendo el procesamiento, almacenamiento y gestión de uno de los activos más valiosos de cualquier organización, la información. La mayoría de las organizaciones son conscientes del valor que posee la información para el negocio y por eso es imperativa la necesidad de una instalación que garantice la disponibilidad y la seguridad.

La necesidad de las organizaciones de almacenar, procesar y salvaguardar la información es innegable. Desde la toma de decisiones hasta la protección de datos y la continuidad del negocio, la información es un recurso esencial en la era digital. Las organizaciones que no priorizan la gestión de la información corren el riesgo de quedar rezagadas y enfrentar serias consecuencias. Por lo tanto, invertir en tecnología y prácticas sólidas de gestión de datos se ha convertido en un imperativo en el mundo empresarial actual.

Históricamente, el diseño de una instalación así atendía a criterios de disponibilidad, rendimiento y seguridad que, en muchos casos, llevan a un sobredimensionamiento de las infraestructuras, lo que provocaba un uso ineficiente de recursos.

Sin embargo, hoy en día, el enfoque principal es el de la eficiencia energética y el aprovechamiento espacial, ya que una instalación eficiente reduce el consumo energético y las emisiones de dióxido de carbono al medio ambiente, así como el subsiguiente ahorro de costes.

En el contexto actual, la información se ha vuelto más móvil que nunca. Los avances tecnológicos han permitido a las organizaciones acceder a datos desde cualquier lugar, lo que ha aumentado la flexibilidad y la productividad. Sin embargo, esta movilidad también plantea desafíos en términos de seguridad y privacidad. Es esencial contar con políticas y tecnologías que protejan la información en tránsito.

La pérdida de datos críticos debido a un fallo técnico o un desastre natural puede ser devastadora. Por lo tanto, las organizaciones implementan estrategias de respaldo y recuperación de datos para garantizar la disponibilidad continua de la información.

Este Trabajo de Fin de Máster se centrará en el diseño de un Centro de Procesamiento de Datos Modular y escalable, alojado en un contenedor y ubicado en las inmediaciones de la organización, teniendo en cuenta las necesidades de disponibilidad, rendimiento y seguridad.

Se abordará estableciendo una base teórica TIC para poner en conocimiento características necesarias en cuanto a los servicios empresariales y la provisión de estos, para más adelante exponer aquellas características y las normativas a las que están sujetas y los elementos que forman parte de un proyecto de este tipo.

PALABRAS CLAVE

“Centro de Procesamiento de Datos”, “Contenedor”, “*Edge Computing*”, “Soberanía del Dato”, “Modular”, “Sistema”, “Servicio”, “Virtualización”.

AGRADECIMIENTOS

A mi mujer, Vicen, por animarme a cursar este Máster y apoyarme en los momentos que más cuestan.

A mi tutor, Fernando, por responder siempre a mis dudas y ayudarme a enfocar cuando las ideas se dispersaban.

A mis compañeros de este Máster, de todos he aprendido algo que me llevo para el futuro.

CONTENIDO

Contenido	1
Índice de Figuras	4
Índice de Tablas.....	5
1 Introducción y objetivos	6
1.1 Motivación del siguiente Trabajo de Fin de Máster	6
1.2 Objetivos del TFM	6
1.3 Estructura de la memoria	7
2 Conceptos básicos a tratar	8
2.1 Introducción de conceptos	8
2.2 Sistemas: La base de los servicios	8
2.3 Servicios: Una definición propia.....	9
2.4 ¿Qué servicios se pueden proporcionar?.....	9
2.5 Modelos de provisión de servicios.....	10
2.5.1 Modelo On Premise	10
2.5.2 Modelo en la nube o CLOUD.....	10
2.5.3 Modelos de servicio	12
2.5.4 Virtualización	14
2.5.5 Virtualización de CPU	15
2.5.6 Virtualización de Almacenamiento	16
2.5.7 Virtualización de Red	17
2.5.8 Virtualización de Escritorios y Aplicaciones	18
3 Estado del arte	20
3.1 Evolución de los CPD	20
3.1.1 Orígenes: Los Mainframe eran el CPD	20
3.1.2 La computación paralela y la computación distribuida	20
3.1.3 Explosión de los 90: Clústers y Grid Computing	21
3.1.4 El presente y futuro de los CPD	22
3.2 Ventajas en inconvenientes del modelo On Premise	23
3.3 Características necesarias a asumir en un CPD	24
3.3.1 Disponibilidad.....	24
3.3.2 Fiabilidad	27
3.3.3 Eficiencia	28
3.4 Construcción de Centros de Datos tradicionales.....	29

4 Desarrollo del TFM	31
4.1 Introducción al Edge Computing y la Soberanía del Dato.....	31
4.1.1 Edge Computing	31
4.1.2 Soberanía del dato.....	32
4.2 Características físicas de un Centro de Procesamiento de Datos Modular	32
4.2.1 Contenerización	32
4.2.2 Características propias de los Contenedores para albergar un CPD.....	33
4.2.3 Suelo técnico.....	35
4.2.4 Sistema de alimentación eléctrica.....	36
4.2.5 Sistema de Alimentación Ininterrumpida (SAI)	36
4.2.6 Sistema de climatización	37
4.2.7 Sistema de protección contra incendios: Detección y Extinción.....	40
4.2.8 Posibles disposiciones del equipamiento	41
4.3 Transporte de los contenedores	42
4.3.1 Construcción en la ubicación final	42
4.3.2 Fabricación o ensamblado y transporte posterior	42
4.4 Equipamiento TI, arquitectura de un CPD	44
4.4.1 Racks.....	44
4.4.2 Servidores de cómputo	44
4.4.3 Dispositivos de Almacenamiento	46
4.4.4 Dispositivos de Backup	47
4.4.5 Dispositivos de seguridad: Firewalls, SIEM, IDS e IPS [29]	47
4.4.6 Dispositivos de comunicaciones para usuarios.....	49
4.4.7 Componentes de Comunicaciones	49
4.5 Ejemplos de racks para los servicios que se pueden cubrir en un despliegue	51
4.5.1 Racks para servicios de Computación y Almacenamiento	51
4.5.2 Racks para Servicios de Seguridad y Comunicaciones	52
4.5.3 Racks de electrónica de red y comunicaciones.....	53
4.5.4 Conclusión sobre el equipamiento	53
4.6 Toma de requisitos para un despliegue	54
4.6.1 Ejemplo: Servicio de virtualización de escritorio de usuario	58
4.7 Buenas prácticas del proyecto	60
5 Análisis de riesgos.....	62
5.1 Identificación de activos	62
5.2 Valoración de activos.....	63
5.3 Identificación y valoración de amenazas	64

5.4 Relación entre los activos y las amenazas	65
5.5 Obtención del riesgo	65
6 Breve conclusión	66
7 Futuras líneas de trabajo	67
7.1 Diseño de un grupo electrógeno auxiliar contenerizado	67
7.2 Toma de requisitos mediante Inteligencia Artificial	67
7.3 Diseño de un proyecto de CPD Modular desplegable para el Ejército	67
8 Bibliografía.....	68
Anexo I: Acrónimos Utilizados.....	71

ÍNDICE DE FIGURAS

Figura 2-1 - Modelos de servicio	12
Figura 2-2 - Hipervisor Nativo (imagen propia)	15
Figura 2-3 - Hipervisor Hospedado (imagen propia)	16
Figura 2-4 - Virtualización de almacenamiento	17
Figura 2-5 - Virtualización de red	18
Figura 2-6 - Virtualización de escritorios y aplicaciones	19
Figura 3-1 - ENIAC y TRADIC (Wikimedia Commons)	20
Figura 3-2 - Un clúster de tipo <i>Beowulf</i> [7] (https://www.climatemodeling.org/)	21
Figura 3-3 - Dos ejemplos de Centros de Datos de Microsoft (Microsoft News).....	23
Figura 3-4 - Causas de las paradas de servicio.....	24
Figura 3-5 - Consumos en un CPD	28
Figura 3-6 - Construcción del CPD de Interxion (Fuente: Interxion)	30
Figura 4-1 - Contenedor Seco 20 Pies Figura 4-2 - Contenedor Seco 40 Pies	33
Figura 4-3 - Estructura modular prefabricada (Fuente: Area Data Paraguay S.A.)	34
Figura 4-4 - Certificación LRQA	34
Figura 4-5 - Placa de suelo técnico con soporte	35
Figura 4-6 - Configuración en pasillo frío/pasillo caliente	38
Figura 4-7 - Panelado de separación frío/caliente (Fuente: Area Data Paraguay S.A.)	38
Figura 4-8 - Detalle del panelado superior (Fuente: Area Data Paraguay S.A.).....	39
Figura 4-9 - Planta del contenedor	39
Figura 4-10 - Alzado lateral de un rack.....	40
Figura 4-11 - CPDM de 20 pies con 5 racks y área de trabajo2 (Fuente: Area Data Paraguay S.A.)	41
Figura 4-12 - CPDM de 8 racks y 10,2m (Fuente: Area Data Paraguay S.A.)	41
Figura 4-13 - Muestra de un CPDM completo (Fuente: Area Data Paraguay S.A.).....	41
Figura 4-14 - Transporte por carretera	42
Figura 4-15 - Transporte aéreo	43
Figura 4-16 - Servidor de montaje en rack HPe DL380 G10.....	45
Figura 4-17 - Chasis HP Synergy	45
Figura 4-18 - Sistema de almacenamiento Dell PowerStore 1200T y Bandejas de discos.....	46
Figura 4-19 - Sistema de backup Dell PowerProtect DD6900.....	47
Figura 4-20 - Firewall Fortigate FG2600	48
Figura 4-21 - Appliance Cisco para comunicaciones corporativas	49
Figura 4-22 - Switch TOR Ethernet	49
Figura 4-23 - Switch TOR con SFP para Ethernet o FC	50

Figura 4-24 - Patch Panel	50
Figura 4-25 - Switch Director Brocade X6-8	50
Figura 4-26 - Ejemplos de rack de cómputo (izqda.) y almacenamiento (dcha.).....	51
Figura 4-27 - Ejemplo de rack de comunicaciones y seguridad.....	52
Figura 4-28 - Ejemplo de rack de electrónica de red.....	53
Figura 4-29 - Ejemplo de parte del formulario de solicitud de requisitos.....	59

ÍNDICE DE TABLAS

Tabla 3-1 - Niveles o TIER de disponibilidad (Fuente: TIA-942).....	26
Tabla 4-1 - Características físicas Contenedor Seco	33
Tabla 5-1 - Inventario de activos.....	62
Tabla 5-2 – Guía de valoración de activos según las dimensiones de seguridad	63
Tabla 5-3 - Valor de activos	63
Tabla 5-4- Amenazas.....	64
Tabla 5-5 - Valoración de Amenazas	64
Tabla 5-6 - Relación entre los activos y las amenazas que los afectan	65
Tabla 5-7 - Análisis de riesgos	65
Tabla 5-8 - Valoración de riesgos	65

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Motivación del siguiente Trabajo de Fin de Máster

A través del desarrollo del Máster que he cursado, he tomado contacto con conceptos y tecnologías que quedaban fuera de mi alcance en mi día a día profesional.

Este Trabajo de Fin de Máster (en adelante TFM) busca plasmar en la práctica esos conocimientos adquiridos.

Realizar un trabajo sobre un Centro de Procesamiento de Datos Modular puede proporcionar una comprensión más profunda de cómo funcionan estos sistemas y cómo pueden mejorar la eficiencia y rentabilidad de las organizaciones que los adquieren o implementan. Además, puede ser una oportunidad para explorar nuevas tecnologías y tendencias en el campo de la gestión de datos.

¿Es posible que un Centro de Procesamiento de Datos Modular pueda ser una alternativa real al despliegue tradicional o a una solución en la nube? Con este TFM intentaré responder a esa pregunta con rigor, precisión y profundidad.

1.2 Objetivos del TFM

El objetivo principal del trabajo es realizar un estudio de necesidades de una organización, en cuanto a los servicios que se deben proveer para su correcto funcionamiento, los sistemas que darán soporte a dichos servicios y cuáles son las necesidades que llevan a la implantación de un CPDM en sus propias instalaciones. Este CPDM contendrá toda la infraestructura necesaria para el desarrollo de todas las necesidades operativas de la organización.

Para ello desarrollaré los siguientes puntos:

1. Expondré unas bases de conocimiento teórico para apoyar el desarrollo.
2. Realizaré un repaso sobre las tendencias, tanto pasadas como actuales y futuras en el desarrollo de los Centros de Procesamiento.
3. Efectuaré el estudio de características físicas y de despliegue de la solución, como pueden ser las capacidades de climatización, suministro eléctrico o extinción de incendios.
4. Ejecutaré un ejemplo de estudio de alcance y necesidades desde el punto de vista de la organización.
5. Propondré un diseño de la infraestructura necesaria para un servicio concreto, que debe estar contenida en el CPDM, contando con las tecnologías disponibles hasta el momento, tanto de fuentes abiertas como propietarias.
6. Realizaré un pequeño resumen de un análisis de riesgos sobre este tipo de infraestructuras.
7. Mostraré mis conclusiones de este trabajo.

Desde el punto de vista del Máster que he cursado, el objetivo es poner en práctica conceptos aprendidos a lo largo del curso, como gestión de riesgos, seguridad TIC y gestión de proyectos.

1.3 Estructura de la memoria

La estructura de esta memoria se establece en los siguientes capítulos y su contenido:

Capítulo 1: Introducción y objetivos

Se trata del presente capítulo. De una manera introductoria, describe cuál ha sido la motivación para realizar este trabajo y qué objetivos se han trazado de alcanzar. Se describe la organización de la memoria y los criterios para ordenar las referencias y formatos.

Capítulo 2: Conceptos básicos a tratar.

Una breve introducción a los sistemas, los servicios y los modelos de provisión de éstos. El objetivo es establecer una base teórica a través de la cual se pongan en contexto las necesidades.

Capítulo 3: Estado del arte

Comienza definiendo las funciones de un Centro de Proceso de Datos, se establecerán unas bases mínimas de conocimiento, para posteriormente centrarse en el estado de desarrollo de este tipo de infraestructuras y la necesidad de abordar esta implementación desde el punto de vista modular.

Capítulo 4: Desarrollo del TFM

En este capítulo se dividirá en dos fases. Una primera que supone el punto de vista de la prestación del servicio, estudio de requisitos planteados y la posterior contratación y adquisición de la infraestructura y una fase posterior que es una composición de estudio, práctica y decisiones que se han asumido como ejemplo práctico. Se muestra el proceso de instalación de los distintos componentes para obtener el producto final.

Capítulo 5: Análisis de Riesgos

Se realizará un pequeño desarrollo sobre un posible análisis de riesgos, aplicando teorías que se han estudiado durante el curso con la metodología MAGERIT. Se trata de explicar, a modo de muestra, lo que implica realizar este tipo de estudios, como analizar los activos, amenazas y riesgos.

2 CONCEPTOS BÁSICOS A TRATAR

2.1 Introducción de conceptos

En este capítulo, se quiere establecer unas pequeñas bases para que sea más sencillo ubicar todos los conceptos que desarrollaré después.

La informática, según la RAE [2], es el “Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores”.

La presencia de la informática en las organizaciones ha sufrido severos cambios desde que a principios de los años 40 se estableciera el uso de los primeros *Mainframes* hasta la irrupción de la nube o las actuales tendencias como Inteligencia Artificial.

En todo este período, la informática ha desempeñado un papel crucial, facilitando la resolución de tareas complejas desgranándolas en tareas más sencillas y proporcionando una interfaz de introducción y salida de datos para los usuarios. Todo esto lleva a dos definiciones muy importantes, los *sistemas* y los *servicios*.

2.2 Sistemas: La base de los servicios

Los sistemas son la infraestructura subyacente que proporciona la funcionalidad necesaria para que un servicio logre su cometido. Son componentes hardware (específico o estándar), software u otros sistemas, interconectados entre ellos, que trabajan juntos para lograr un objetivo común.

Los sistemas informáticos tienen varias partes importantes:

- **Entrada:** Esta es la forma en que el sistema recibe información de su entorno. Esto puede ser a través de dispositivos como teclados, ratones, dispositivos industriales u otros sistemas que permitan ingresar datos.
- **Procesamiento:** Una vez que el sistema tiene los datos, los procesa. Es como el cerebro del sistema. Utiliza un componente llamado procesador, que realiza cálculos matemáticos y toma decisiones lógicas con la información que ha recibido.
- **Salida:** Después de procesar los datos, el sistema debe mostrar los resultados de alguna manera. Esto se hace a través de dispositivos de salida, como impresoras para imprimir documentos, monitores para mostrar imágenes, altavoces para reproducir sonidos e incluso conexiones con otros sistemas que leen dichos datos.
- **Almacenamiento:** Los datos que el sistema ha procesado se guardan para su uso futuro. Esto se hace en dispositivos de almacenamiento, como discos duros o unidades de estado sólido, que actúan como memoria a largo plazo.
- **Control:** Para que todo funcione de manera ordenada, el sistema informático está bajo el control de un sistema operativo. Este software administra tanto el hardware como el software para que todo funcione sin problemas.

Los sistemas cumplen con varias características:

- Proporcionan una **interfaz** amigable para el usuario.
- **Facilitan**, como se ha explicado anteriormente, la automatización de tareas y procesos.
- Deben proporcionar **seguridad** en el tratamiento de la información, protegerse de ataques, intrusiones y alteración o robo de datos.

- Tienen que ser **fiables**, es decir que funcionen correctamente de forma constante.
- En lo posible, deben ser **escalables** o capaces de crecer y adaptarse a las necesidades cambiantes.

Los sistemas informáticos pueden clasificarse por:

- **Volumen de procesamiento:** dependiendo de la capacidad que tienen para procesar y gestionar los datos.
- **Utilización:** es decir, el uso que se le da al sistema informático, ya sea para cumplir tareas con criterio reducido o para manejar un mayor número de variables.
- **Función:** según si es diseñado para cumplir propósitos puntuales dentro de una serie de trabajos. Podría estar programado para dar sugerencias en la toma de decisiones o para tomar una decisión propia a partir de datos recolectados.
- **Agrupamiento:** según sean sistemas aislados o formen parte de redes de equipos interconectados en clúster, redes privadas, locales, amplias, etcétera.

Una vez que se ha establecido la base de qué son los sistemas informáticos, se pasará a nombrar los *servicios*, es decir, para qué sirve un sistema informático en el mundo real.

2.3 Servicios: Una definición propia

A lo largo de todo el tiempo en el que la informática se ha hecho un hueco (se podría decir que imprescindible) en las organizaciones, se ha utilizado para cubrir multitud de necesidades que surgían como resultado del desarrollo de las actividades, como pueden ser comunicación entre personas, análisis o tratamiento de datos, control de maquinaria, etcétera.

Todas estas necesidades dan lugar al nacimiento de los **servicios**.

¿Y qué entendemos cómo servicio? Según el que escribe y siempre en el plano TIC, se definiría como **“un conjunto formado por: sistemas, los recursos para que funcionen éstos y el resultado que ofrecen al usuario”**.

2.4 ¿Qué servicios se pueden proporcionar?

Los servicios necesarios para el funcionamiento de una organización, que provean de todas las capacidades necesarias para la operativa en diferentes ámbitos, son muy numerosos, un breve desglose, que posteriormente ayudaría a la toma de requisitos, puede ser:

- Servicios de propósito general:
 - Computación (servidores, almacenamiento)
 - Bases de Datos
 - Copias de seguridad
- Servicios de software desarrollado específicamente para la ejecución de la actividad:
 - Software Gestor de Relaciones de Clientes (CRM - *Customer Relationship Manager*)
 - Software de Sistema de Planificación de Recursos Empresariales (ERP - *Enterprise Resource Planning*)
 - Otro software específico
- Servicios de comunicaciones:
 - Electrónica de red (switches, balanceadores)
 - Correo electrónico
 - VoIP [3]

- Servicios de Seguridad:
 - Firewalls
 - IDS - Detección de intrusiones (*Intrusion Detection System*)
 - IPS - Prevención de Intrusiones (*Intrusion Prevention System*)
 - Proxies
 - Gestores centralizados de antivirus

Disponer de infraestructura para dotar de estos servicios es la necesidad que se ha querido cubrir con la elaboración de este TFM.

2.5 Modelos de provisión de servicios

En este punto se definirán las formas de provisión y ventajas e inconvenientes de cada modelo.

Existen dos modelos de provisión de la infraestructura necesaria, *On Premise* (*in situ – en las propias instalaciones*) y *Cloud*, que se pueden incluso combinar entre ellas, dependiendo de quién sea el responsable de gestionar la infraestructura con respecto al usuario que la demanda.

2.5.1 Modelo On Premise

Este modelo de prestación de servicio podríamos llamarlo “tradicional”, en el que la organización dispone, bien sea en propiedad, bien sea con un acuerdo de cesión y renovación periódica, de todo el equipamiento en sus instalaciones.

Como es el objetivo de este TFM el desarrollo de un CPD de estas características para la ubicación en las instalaciones de la propia organización, se detallarán de manera breve las características más destacadas.

Una de las características principales del entorno *on premise* es que se necesita comprar la licencia y montar la infraestructura alrededor del software. Por lo que antes de empezar a operar, ya se tienen unos gastos iniciales obligatorios como; servidores, routers, cableados, localización correctamente acondicionada, sistema de seguridad y gasto en personal para realizar la puesta en marcha.

Los costes de la instalación *on premise* no acaban aquí, una vez está toda la instalación montada, esta necesita de mantenimiento constante que todo el equipo anterior necesita; suministro eléctrico y personal para mantenimiento correctivo, preventivo y monitorización de la instalación por si fuera necesario ampliarla.

Al tener toda la infraestructura dentro de la empresa, la instalación *on premise* ofrece un **mayor grado de seguridad física** de la información dado que la empresa sabe en todo momento dónde se encuentra su información y es responsable de tomar todas las medidas necesarias para su protección. Aun así, es un arma de doble filo debido a que una mala manipulación por parte del personal puede acarrear graves daños a la información de la organización.

El **análisis de riesgos** es un punto que trataremos dentro del desarrollo del TFM.

2.5.2 Modelo en la nube o CLOUD

Este es un modelo que se encuentra en auge en la actualidad.

En términos sencillos, *Cloud Computing* permite “alquilar” tecnologías de la información, en lugar de adquirirlas. Este modelo nos permite evitar grandes inversiones en bases de datos, software y hardware, las organizaciones usuarias deciden acceder a su capacidad de computación a través de Internet y pagar según el uso que hagan de esa capacidad.

Este modelo proporciona la velocidad, escalabilidad y flexibilidad que permite que los negocios se desarrollen e innoven, no teniendo que incurrir en costes de infraestructura.

Una definición más completa y formal expuesta por el NIST¹:

“Modelo que permite el acceso ubicuo, práctico y bajo demanda, a través de la red, a un *pool* común de recursos configurables de computación (redes, servidores, almacenamiento, aplicaciones, servicios, etc.) que pueden ser rápidamente puestos a disposición del usuario sin necesidad de una gran complejidad en la gestión por el proveedor del servicio.”

Podemos hablar de tipos de nube, que dependen de la compartición de la infraestructura por parte de las organizaciones usuarias y podemos hablar de:

Nube pública

En una nube pública, toda la infraestructura informática está ubicada en las instalaciones del proveedor de servicios en la nube, que presta estos servicios al cliente a través de Internet. Los clientes no tienen que mantener sus propios recursos informáticos y pueden agregar rápidamente más usuarios o potencia informática según sea necesario. En este modelo, diversos inquilinos comparten la infraestructura informática del proveedor de la nube.

Nube privada

La nube privada es de uso exclusivo de una organización. Se puede alojar en la ubicación de la organización o en el Centro de Datos del proveedor de la nube. La nube privada proporciona un nivel más alto de seguridad y control. Podemos decir que este modelo es una pequeña introducción al desarrollo de este TFM.

Nube híbrida

Como su nombre indica, una nube híbrida es una combinación de nubes públicas y privadas. En general, los clientes de nubes híbridas alojan sus aplicaciones críticas en sus propios servidores para mayor seguridad y control y las aplicaciones secundarias se almacenan en el entorno de un proveedor de nube.

Comunitaria

Es una variante modificada o híbrida de la nube privada, que permite que distintas organizaciones de una comunidad concreta, como sector bancario, investigación o universidades, puedan compartir programas y cuestiones comunes para trabajar de manera colaborativa en una misma plataforma con infraestructuras y recursos compartidos.

Multinube

Multinube hace referencia a varias nubes públicas diferentes que se están implementando y, aunque se pueda dar el caso, no tiene por qué incluir una nube privada.

La nube híbrida describe la combinación de dos o más tipos distintos de infraestructura: combina una nube privada, un Centro de Datos en las instalaciones, o ambos con al menos una nube pública.

A la hora del tipo de servicio que se proporciona, hablamos de tres modelos básicos:

¹ NIST: Instituto Nacional de Normas y Tecnología es la agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos encargada de promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología.

2.5.3 Modelos de servicio

Este es un extracto de los modelos de servicio más habituales atendiendo al nivel de gestión de la infraestructura:

IAAS (Infrastructure as a Service – Infraestructura como servicio)

Este es el servicio más básico dentro de Cloud Computing y consiste en proporcionar una infraestructura de computación, que supone procesamiento, almacenamiento y recursos de red.

Ofrece la posibilidad, sobre dicha infraestructura, de desplegar aplicaciones y manejar recursos, todo ello gracias a la *virtualización*.

Nos permite abstraernos de las limitaciones que impone el hardware físico.

El cliente despliega sus Sistemas Operativos y aplicaciones en los recursos que Cloud Computing expone y es el responsable de administrar y actualizarlos Sistemas Operativos y aplicaciones.

PAAS (Platform as a Service – Plataforma como Servicio)

Plataforma virtualizada que incluye SO, aplicaciones específicas (por ejemplo, motores de bases de datos) y herramientas de desarrollo.

Permite al usuario desplegar sus propias aplicaciones usando las librerías y herramientas que el proveedor del servicio pone a su disposición.

El desarrollador tiene el control del despliegue de sus aplicaciones y la posibilidad de configurar el entorno de ejecución.

PaaS ofrece servicio de integración con Bases de Datos, servidores web, mecanismos de seguridad, almacenamiento, copias de seguridad y control de versión entre otros.

SAAS (Software as a Service – Software como servicio)

En este modelo el proveedor instala y publica aplicaciones que serán utilizadas por los usuarios de la nube a través de clientes ligeros (normalmente cliente web o aplicaciones para dispositivos móviles).

El usuario ni tiene acceso ni gestiona la infraestructura donde se ejecutan las aplicaciones.

Esto permite al cliente olvidarse de toda la gestión de actualización, tanto del software base como de las aplicaciones, siendo responsabilidad del proveedor.

Aplicaciones que se ajusten a este modelo son CRM, ERP o soluciones de BackOffice.

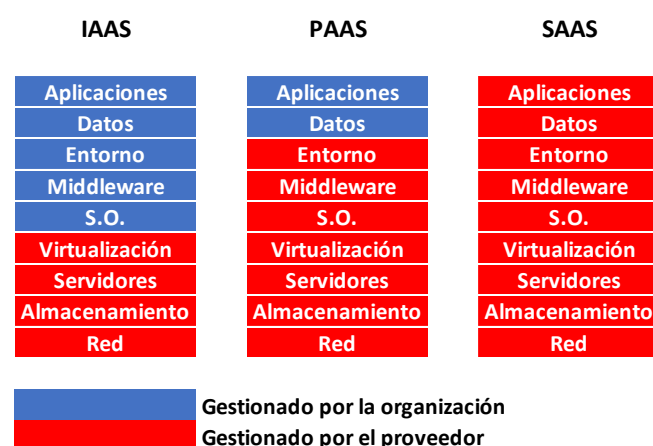


Figura 2-1 - Modelos de servicio

De la misma manera, existen diferentes *modelos de negocio* sobre estos servicios, que también se pueden contratar a la hora de disponer de infraestructura en la nube, que han ido surgiendo como necesidad en las diferentes implementaciones y se han visto demandadas, un breve resumen de los modelos de negocio sería:

BaaS/DRaaS – Backup as a Service/Disaster recovery as a Service

Servicio en pago por uso que permite a empresas externalizar en un proveedor el proceso de copias de seguridad incluyendo los repositorios necesarios para las copias, el software de backup, servicios de comprobación, administración y restauración y réplica remota segura de sus copias de seguridad a ubicaciones alternativas y/o nube para garantizar la disponibilidad y cumplimiento legal.

BPaaS - Business Process as a Service

Las soluciones BPaaS y SaaS a menudo se confunden entre sí; sin embargo, existe una clara diferencia entre ellos:

BPaaS es un proceso de negocio como servicio. Está basado en la nube y se puede utilizar para automatizar tareas repetitivas, aumentar la eficiencia y mejorar la experiencia del cliente.

BPaaS es un concepto más amplio que SaaS. Se puede usar para subcontratar procesos comerciales de todo tipo, no solo software; por ejemplo, se puede usar para optimizar la experiencia del cliente o mejorar la productividad dentro de una organización.

El concepto se basa en proporcionar interacciones e integraciones entre, por ejemplo, aplicaciones “legacy” del cliente con otras aplicaciones proporcionadas por proveedores que disponen de su servicio como PaaS.

SecaaS - Security as a Service

Modelo de computación en la nube que ofrece servicios de seguridad administrados a través de Internet.

Si los usuarios se pueden conectar desde cualquier punto, no tiene sentido que la seguridad esté fijada en el centro de datos.

La provisión de servicios en Cloud tiene unas *ventajas*:

- Reducción de coste con respecto a la adquisición de hardware en propiedad.
- Aumento de la flexibilidad de servicio, ya que actualmente se dispone de la posibilidad (dependiendo del proveedor) de adquirir una capacidad de cómputo o almacenamiento inicial, acorde a las necesidades de servicio, para posteriormente aumentar bajo demanda dichas capacidades de manera independiente.
- Disponibilidad de los datos, ya que el acceso se puede realizar desde virtualmente cualquier dispositivo con acceso a Internet.
- Capacidades de seguridad, dependiendo del modelo de servicio que se elija:
 - De las instalaciones: Limitación contractual de acceso a las infraestructuras. Si se trata de una nube privada, se debería disponer de una ubicación no compartida con otros clientes.
 - De los datos: Una buena gestión del contrato supone un mantenimiento tanto de hardware como de software para mantener versiones actualizadas y menos vulnerables a ataques.

Como *inconvenientes*, podemos destacar:

- Menor grado de control por parte de la organización cliente (menor capacidad de influir directamente en el rendimiento de aplicaciones o infraestructuras y pérdida de control directo sobre datos).

- Mayor movilidad de datos y menor transparencia para el cliente sobre la localización de servidores y/o sobre subcontratistas.
- Uso intensivo de recursos compartidos, lo que acrecienta determinados riesgos relacionados con el aislamiento lógico y jurídico de la información.

La intensidad de estos factores varía según el modelo de servicio o de implantación que se adopte y de la arquitectura de servicio específica, así como el perfil del cliente (dimensión, presión regulatoria, aversión al riesgo), existiendo perfiles de cliente que otorgan mayor peso a las ventajas del modelo cloud relativizando la evaluación de riesgos.

El cliente, por ejemplo, queda también expuesto a posibles incidencias en el marco jurídico que afecten al proveedor, el despliegue de los servicios de computación en la nube puede provocar riesgos para la protección de datos de carácter personal derivados de la falta de control sobre ellos o la insuficiente información sobre su tratamiento.

2.5.4 Virtualización

El objetivo de este TFM es proporcionar el estudio de capacidades y necesidades para el desarrollo de un CPD Modular para Edge Computing, es decir, lo más cerca posible de donde están siendo generados los datos. La **virtualización** permite a las organizaciones ofrecer servicios empresariales de forma más eficiente, flexible y segura.

No es un concepto precisamente moderno, si no que aparece con los primeros *mainframes*.

Cuando una organización adquiría uno de estos equipos, los desarrollos eran increíblemente costosos y exigían personal experto. Si aparecía una nueva versión del hardware, era impensable migrar todos esos desarrollos entre versiones, por lo que los fabricantes crearon los primeros espacios “virtualizados”, que permitían la ejecución en modo de compatibilidad de los programas antiguos en equipos hardware más modernos.

Un ejemplo de esto fueron las Jails de FreeBSD, LPAR y WPAR de IBM para los sistemas AIX o los espacios en Oracle en máquinas Solaris.

La virtualización se puede definir, según el que escribe, como **“la creación de una capa de abstracción de los recursos hardware, que posibilita ejecutar diferentes instancias de programas o sistemas operativos independientemente de la arquitectura subyacente”**.

Algunos conceptos básicos de la virtualización:

- Máquina virtual (MV): Es una representación virtual de un servidor físico. Cada VM tiene su propio sistema operativo, aplicaciones y datos.
- Hypervisor: Es el software que controla el acceso de las máquinas virtuales a los recursos de la CPU. El hipervisor divide la CPU física en varias particiones, cada una de las cuales se asigna a una máquina virtual. Se ampliará el concepto en el punto siguiente.
- Aislamiento: Las máquinas virtuales están aisladas entre sí, lo que significa que no pueden acceder a los recursos de las demás máquinas virtuales.
- Portabilidad: Las máquinas virtuales se pueden mover de un servidor a otro sin necesidad de realizar cambios en el software.

Como ventajas principales, favorece la eficiencia en el uso de recursos y facilita la gestión, tanto de éstos como de la infraestructura desplegada, gracias a la existencia de los *hipervisores*, capa de administración entre el hardware y la virtualización.

Existen diferentes tipos de virtualización (véase el artículo “Virtualización” de IBM [4]), dependiendo de qué capa queramos abstraer, pero nos centraremos en los siguientes.

2.5.5 Virtualización de CPU

La virtualización de CPU es una tecnología que permite que una sola CPU física se divida en varias CPU virtuales. Esto permite que varias máquinas virtuales se ejecuten en una sola máquina física.

La virtualización de CPU se basa en un componente llamado hipervisor. El hipervisor es un software que controla el acceso de las máquinas virtuales a los recursos de la CPU. El hipervisor divide la CPU física en varias particiones, cada una de las cuales se asigna a una máquina virtual.

Existen dos tipos de hipervisor, según dónde se encuentren alojados con respecto al hardware:

Tipo-1: – Nativo:

También conocidos como hipervisores «bare-metal», se encuentran entre los sistemas operativos invitados y el hardware, es decir, se ejecutan directamente en el hardware de la computadora host. El hipervisor tipo 1 interactúa con la memoria y la CPU del host haciéndola transparente al sistema invitado. El acceso directo lo convierte en una opción eficiente, además de aumentar la seguridad, ya que no hay nada entre la CPU y sí mismo que pueda ponerse en juego. Se necesita una máquina separada para administrar el hardware del host y diferentes máquinas virtuales.

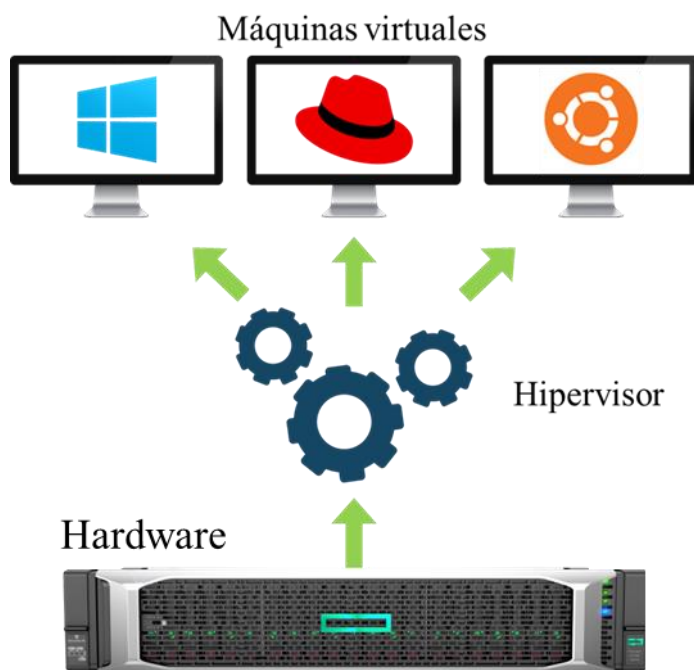


Figura 2-2 - Hipervisor Nativo (imagen propia)

Tipo-2: – Hospedado:

Este tipo de hipervisor funciona como otro software. Necesita ser alojado o instalado. Difiere con los hipervisores nativos en el rendimiento. El hipervisor tipo 2 proporciona una mejor conexión entre el sistema operativo host y la máquina virtual invitada, lo que permite a los usuarios entrar o salir según sea necesario y les permite acceder a las carpetas y archivos del sistema operativo host desde la máquina virtual. Existe un riesgo potencial de seguridad porque el SO huésped puede ser manipulado si el SO host se ve comprometido.

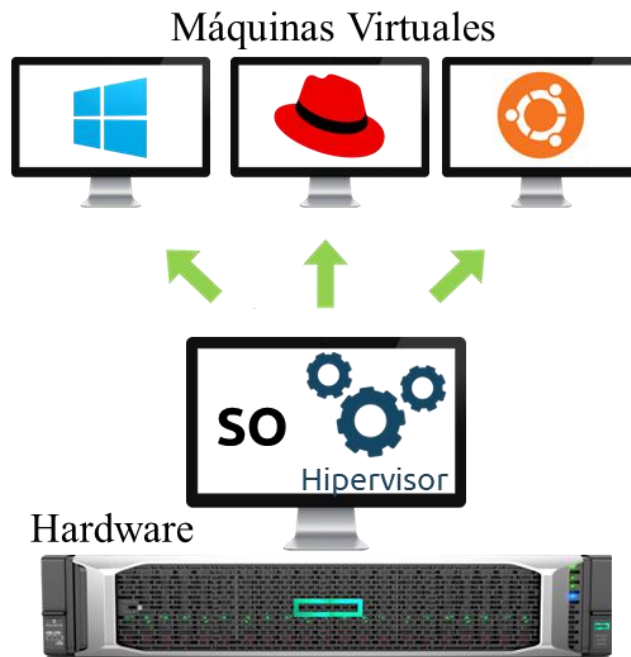


Figura 2-3 - Hipervisor Hospedado (imagen propia)

Las máquinas virtuales se ejecutan de forma independiente entre sí y no son conscientes de que están compartiendo la misma CPU física. Esto permite que cada máquina se ejecute como si tuviera su propia CPU física.

La virtualización de CPU tiene varias ventajas, entre las que se incluyen:

- **Eficiencia:** La virtualización de CPU permite que se ejecuten más VM en una sola máquina física. Esto puede ayudar a las empresas a ahorrar dinero en hardware.
- **Flexibilidad:** La virtualización de CPU permite que las empresas cambien el tamaño de sus VM según sea necesario. Esto puede ayudar a las empresas a adaptarse a los cambios en la demanda.
- **Seguridad:** La virtualización de CPU puede ayudar a mejorar la seguridad de los datos. Esto se debe a que las VM se pueden aislar entre sí, lo que dificulta que un ataque afecte a todas las VM.

La virtualización de CPU es una tecnología importante que se utiliza en una amplia gama de aplicaciones, desde centros de datos hasta entornos de TI empresariales.

2.5.6 Virtualización de Almacenamiento

La virtualización de almacenamiento es una tecnología clave en el campo de la gestión de datos y el almacenamiento de información. Consiste en abstraer y separar la capa de almacenamiento físico de los recursos de almacenamiento disponibles, creando una capa de virtualización que gestiona y asigna estos recursos de manera más eficiente y flexible.

En lugar de depender de hardware de almacenamiento específico, la virtualización de almacenamiento permite que múltiples dispositivos de almacenamiento físico se agrupen en un único conjunto de recursos virtualizados. Esto facilita la gestión y asignación de almacenamiento, ya que los administradores pueden asignar y redimensionar recursos de manera dinámica sin preocuparse por la ubicación física de los datos.

Aporta varios beneficios:

- Mejora la utilización de los recursos de almacenamiento, evitando la asignación excesiva de espacio.
- Facilita la migración de datos, ya que los datos pueden moverse entre dispositivos físicos sin interrupciones.
- Aumenta la disponibilidad y la escalabilidad, ya que los recursos pueden ser fácilmente ampliados según las necesidades.

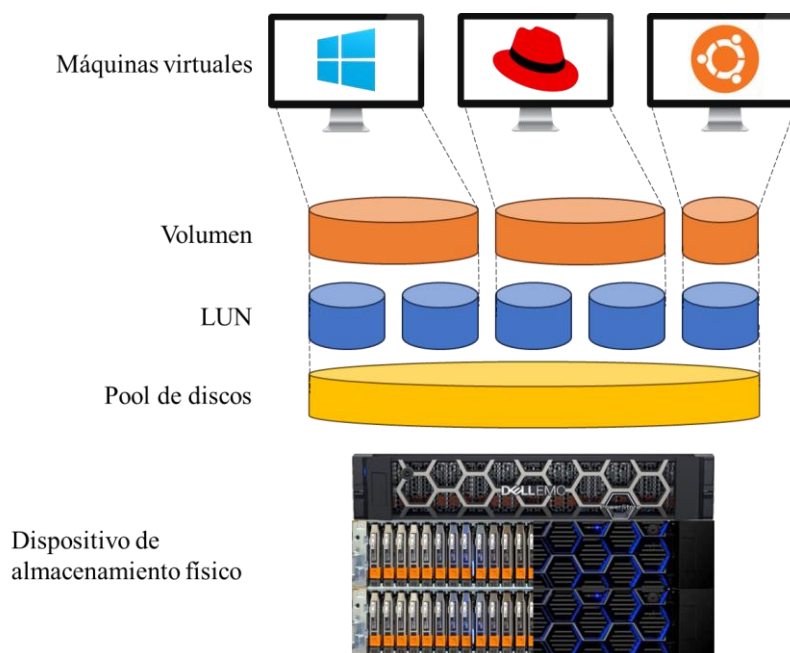


Figura 2-4 - Virtualización de almacenamiento

2.5.7 Virtualización de Red

La virtualización de red es una tecnología que permite que los recursos de red físicos se presenten como un único espacio de red lógico. Esto permite a las empresas gestionar de forma centralizada los recursos de red, lo que puede mejorar la eficiencia y la flexibilidad.

La virtualización de red se basa en un componente llamado conmutador virtual. El conmutador virtual es un software que controla el acceso a los recursos de red físicos. El conmutador virtual divide la red física en varios segmentos, cada uno de los cuales se asigna a una VM.

Las VM se pueden acceder a los segmentos de red como si fueran redes físicas. Esto permite que las VM se comuniquen entre sí como si estuvieran en la misma red.

La virtualización de red también facilita la movilidad de recursos, ya que las máquinas virtuales pueden cambiar de servidor físico conservando sus configuraciones de red. Esto es fundamental en la computación en la nube y la administración de centros de datos, donde la escalabilidad y la flexibilidad son esenciales.

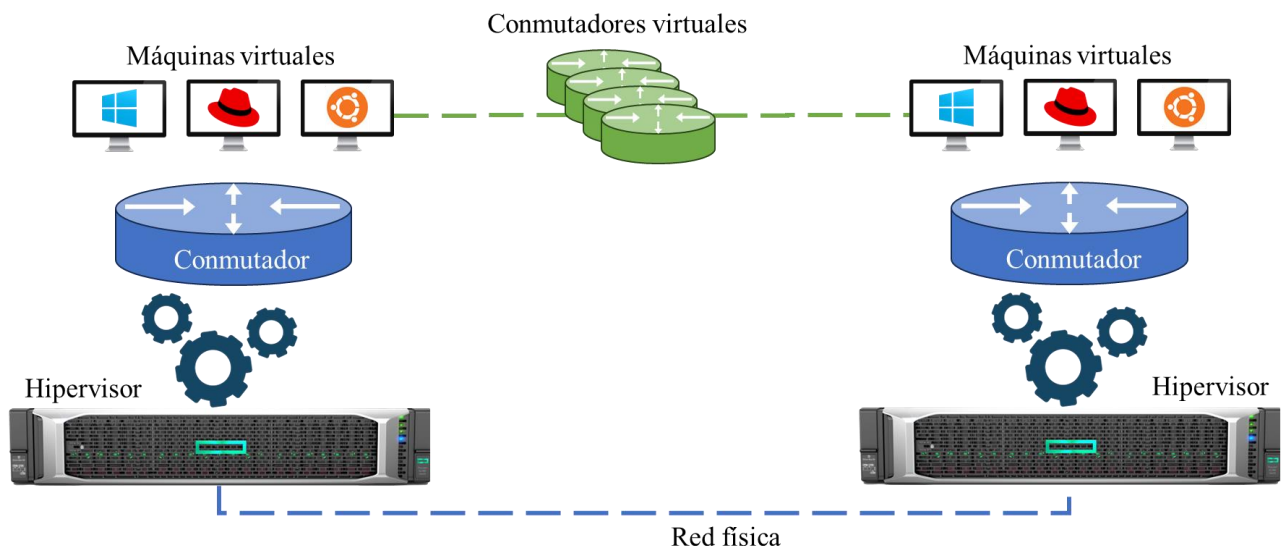


Figura 2-5 - Virtualización de red

2.5.8 Virtualización de Escritorios y Aplicaciones

La virtualización de escritorios, también conocida como VDI (*Virtual Desktop Infrastructure*), es una tecnología que cambia la forma en que los usuarios acceden y utilizan sus computadoras de trabajo. En lugar de contar con una computadora física dedicada, los escritorios se ejecutan en servidores virtuales y se entregan a través de la red a dispositivos cliente como computadoras, clientes ligeros, tabletas o incluso teléfonos móviles.

Esta tecnología ofrece numerosos beneficios:

- En primer lugar, proporciona una mayor **flexibilidad**, ya que los usuarios pueden acceder a sus escritorios desde cualquier lugar con conexión a Internet. Esto es especialmente útil para empresas con trabajadores remotos o en movilidad.
- Facilita la **administración y el soporte** de escritorios, ya que los administradores pueden gestionar y actualizar imágenes de escritorios de manera centralizada.
- Mejora la **seguridad**, ya que los datos y las aplicaciones se almacenan en servidores centralizados, lo que reduce el riesgo de pérdida de datos en dispositivos cliente.
- Además, ofrece **aislamiento** de aplicaciones, lo que significa que problemas en una aplicación no afectan a otras en el mismo escritorio virtual.

Algunos ejemplos específicos de cómo se utiliza la virtualización de escritorios son:

- **Aprovisionamiento de escritorios:** La virtualización de escritorios se puede utilizar para aprovisionar escritorios de forma rápida y sencilla. Esto puede ser útil para empresas que necesitan escalar rápidamente su capacidad de escritorio.
- **Migración de escritorios:** La virtualización de escritorios se puede utilizar para migrar escritorios de un sistema a otro. Esto puede ser útil para empresas que necesitan actualizar su infraestructura de escritorio.
- **Protección de escritorios:** La virtualización de escritorios se puede utilizar para proteger los escritorios mediante la creación de copias de seguridad y la recuperación ante desastres.

La virtualización de aplicaciones tiene un funcionamiento similar a la de escritorios, con la diferencia de que la aplicación se ejecuta sobre un escritorio virtual y se le presenta al usuario en modo “pantalla completa” para simular la ejecución en su propio equipo cliente.

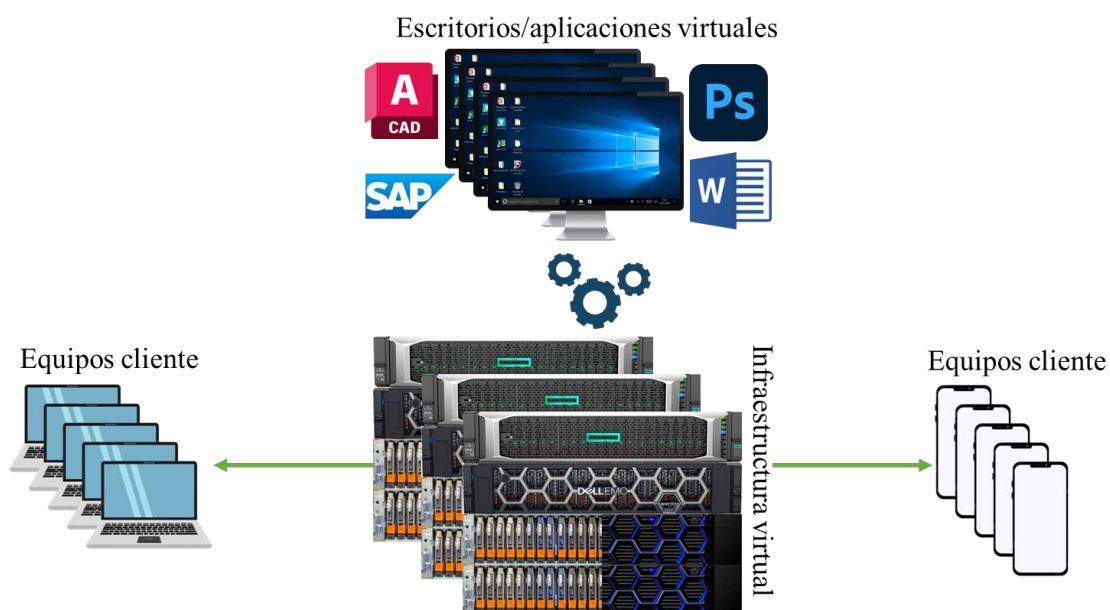


Figura 2-6 - Virtualización de escritorios y aplicaciones

3 ESTADO DEL ARTE

3.1 Evolución de los CPD

Los centros de procesamiento de datos (CPD) han evolucionado significativamente desde sus inicios. A continuación, se revisará esta evolución por épocas e hitos más destacados.

3.1.1 Orígenes: Los Mainframe eran el CPD

En las décadas entre 1940 y 1960, se construían en torno a los equipos *mainframe* y eran utilizados por grandes corporaciones y entidades gubernamentales para tareas como la gestión de nóminas, el mantenimiento de registros y el procesamiento de transacciones.

En esta época los CPD estaban contruidos en torno a estas máquinas, que suponían el núcleo de negocio y parte esencial. Se trataba de arquitecturas eminentemente monolíticas, es decir, que no eran parte de una red si no que disponían de toda la lógica de computación, base de datos y visualización en el mismo equipo.

Superordenadores como ENIAC (1946) [5] supondrían el primer Centro de Datos, esta supercomputadora usaba la tecnología de válvulas de vacío, ocupaba un espacio de más de 150 m² y era muy compleja de operar y mantener. Unos años después en 1954 llegó TRADIC [6] dando un salto en la computación por la introducción de los transistores.



Figura 3-1 - ENIAC y TRADIC (Wikimedia Commons)

3.1.2 La computación paralela y la computación distribuida

El avance de la microelectrónica en las décadas de 1970 y 1980 propició la miniaturización y mayor accesibilidad a las computadoras, dando paso a la creación de CPD de tamaño medio, aptos para organizaciones más pequeñas. En contraste con sus predecesores, estos CPD requerían menos personal para su operación y mantenimiento.

Ambos paradigmas surgidos en la década de los 80 y son fundamentales para el desarrollo de la informática moderna.

La *computación paralela* es el uso de múltiples unidades de procesamiento para resolver un problema. Las unidades de procesamiento pueden ser procesadores, núcleos de procesador, hilos o vectores. La computación paralela se utiliza para acelerar el tiempo de ejecución de las aplicaciones.

La *computación distribuida* consiste en el uso de múltiples computadores para resolver un problema. Los equipos pueden estar conectados a una red local o a Internet. La computación distribuida se utiliza

para aplicaciones que requieren una gran cantidad de potencia de procesamiento, como el modelado científico, la inteligencia artificial y el aprendizaje automático.

La computación paralela y distribuida tienen muchas ventajas sobre la computación secuencial, que es el uso de una sola unidad de procesamiento para resolver un problema. Las ventajas de la computación paralela y distribuida incluyen:

- Incremento de la velocidad de ejecución
- Mejora del rendimiento
- Mayor capacidad de cálculo
- Reducción de los costes

3.1.3 Explosión de los 90: Clústers y Grid Computing

En la década de los años 90 surgen los primeros grupos de computadoras, conocidos como *clústeres* [6]. Un clúster consiste en la interconexión de varias computadoras a través de una red de alta velocidad, de manera que operen como una unidad única. Esto tiene como propósito mejorar el rendimiento, la eficiencia y la disponibilidad, a la vez que resulta más asequible que utilizar computadoras individuales.

Los componentes hardware de un clúster son elementales, similares a los de una PC convencional. Pueden ejecutar distintos sistemas operativos y están equipados con adaptadores Ethernet estándar. No incluyen ninguna pieza de hardware personalizada y su reproducción es sencilla.



Figura 3-2 - Un clúster de tipo Beowulf [7] (<https://www.climate modeling.org/>)

Esto posibilitó la creación de CPD de tamaño medio, ideales para organizaciones pequeñas.

Comparados con los CPD iniciales, estos requerían menos personal para operar y mantener. El equipo en estos CPD estaba compuesto principalmente por técnicos y operadores.

El siguiente paso en la evolución fue el *Grid Computing* (o computación en malla), que hacía uso de las comunicaciones sobre Internet para trabajar en un determinado problema. Utilizaba todos los recursos de varios ordenadores para funcionar como un supercomputador.

La cima del *grid computing* fue en los años 90. Su principal uso era una única aplicación que requería una gran cantidad de fuentes dedicadas.

La explosión de la demanda de servicios informáticos a raíz del desarrollo de Internet y la World Wide Web en las décadas de 1990 y 2000 dio pie a la necesidad de los CPD de gran tamaño. Estos centros se erigen en zonas apartadas con electricidad económica y amplio espacio.

Asimismo, se hizo necesario el contar con estrictas medidas de seguridad para salvaguardar datos y hardware. Los CPD de gran tamaño se convirtieron en el soporte vital de organizaciones, instituciones gubernamentales y personas, gestionando transacciones financieras, redes de telecomunicaciones y almacenando información de clientes.

En estos años comienza la externalización de los centros de datos con el *Housing* y *Hosting* para compañías que no podían asumir el coste de todo un Centro de Datos e 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.

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.

3.1.4 El presente y futuro de los CPD

Los CPD seguirán siendo una pieza fundamental en la economía moderna a medida que la tecnología evolucione. Actualmente, gracias al surgimiento de normativas (que se expondrán más adelante) es posible cumplir con unas necesidades de alimentación, climatización, rendimiento y fiabilidad muy altas en instalaciones complejas.

Se espera que se descentralicen y distribuyan aún más, almacenando y procesando datos de diversas fuentes, como teléfonos inteligentes, tabletas y dispositivos “vestibles”.

El futuro de los CPD está marcado por una serie de tendencias, incluyendo:

- **Creciente Volumen de Datos:** El incremento exponencial en la generación y almacenamiento de datos en los CPD resulta de la proliferación de tecnologías digitales como el Internet de las Cosas (*IoT*), la Inteligencia Artificial (*IA*) y el Aprendizaje Automático (*Machine Learning*).
- **Demanda de Eficiencia Energética:** Los CPD consumen gran cantidad de energía, planteando desafíos ambientales. En respuesta, los gestores de CPD buscan tecnologías más eficientes que reduzcan el consumo energético.
- **Imperativo de la Seguridad:** La naturaleza confidencial de los datos almacenados en los CPD los convierte en objetivos atractivos para ciberataques. Los responsables de los CPD trabajan en fortalecer la seguridad mediante medidas físicas y cibernéticas.

El futuro de los CPD está lleno de oportunidades. Los operadores que sean capaces de adaptarse a las nuevas tendencias y desafíos tendrán un papel importante en el desarrollo de la economía digital.

En este sentido, algunos ejemplos concretos de la evolución de los CPD en el futuro son:

- **Mayor descentralización:** Históricamente, los CPD se concentraban en unos pocos emplazamientos. Sin embargo, la demanda creciente de servicios de nube ha propiciado la creación de CPD más pequeños y distribuidos, que se encuentran en proximidad con los usuarios.
- **Mayor eficiencia:** Los CPD están implementando soluciones como la refrigeración al aire libre, CPD sumergidos [8] y la energía solar para mitigar su huella energética.
- **Refuerzo de la seguridad:** Los CPD están adoptando la Inteligencia Artificial, el Aprendizaje Automático y otras tecnologías avanzadas para identificar y prevenir ciberataques.



Figura 3-3 - Dos ejemplos de Centros de Datos de Microsoft (Microsoft News)

3.2 Ventajas en inconvenientes del modelo On Premise

En general, un modelo que sitúa en la propia organización toda la infraestructura, podemos decir que tendrá los siguientes inconvenientes:

- **Coste inicial elevado:** El costo inicial de adquirir, instalar y mantener un CPD on premise puede ser elevado.
- **Complicaciones de gestión:** La gestión de un CPD on premise puede ser compleja y requiere un equipo de expertos en TI o bien de personal contratado.
- **Dependencia de la infraestructura local:** Los CPD on premise dependen de la infraestructura local, como la electricidad, la refrigeración y la seguridad. Si hay problemas con la infraestructura local, puede afectar al funcionamiento del CPD.
- **Limitaciones de escalabilidad:** Los CPD on premise pueden ser difíciles de escalar, ya que se necesita adquirir más hardware y software, de ahí la necesidad de un buen estudio de requisitos.
- **Problemas de seguridad:** Los CPD on premise son un objetivo atractivo para los ciberdelincuentes, ya que almacenan una gran cantidad de datos confidenciales.

Ahora bien, esta solución dispone de ciertas ventajas en contraposición al punto anterior, que debemos tener en cuenta:

- **Mayor control:** Un CPD on premise ofrece un mayor control sobre los sistemas informáticos y redes de comunicaciones de la organización. Esto incluye el control de la infraestructura, el software y los datos.
- **Mayor seguridad:** Los CPD on premise pueden ofrecer un mayor nivel de seguridad que los CPD en la nube. Esto se debe a que los CPD on premise se sitúan en una ubicación física que puede estar mejor protegida, bien por acceso físico o bien contra ciberataques si es una instalación aislada.
- **Latencia Reducida:** Las latencias de red tienden a ser más bajas en comparación con las opciones basadas en la nube. Esto es especialmente crítico para aplicaciones en tiempo real y procesos sensibles a la latencia.
- **Cumplimiento Normativo:** Algunas industrias tienen regulaciones estrictas sobre dónde y cómo se almacenan los datos. Un CPD en las instalaciones puede ayudar a cumplir con los requisitos normativos al mantener los datos bajo control directo.
- **Mayor disponibilidad:** Los CPD on premise pueden ofrecer una mayor disponibilidad que los CPD en la nube. Esto se debe a que los CPD on premise no están sujetos a las mismas interrupciones que los ubicados en la sede de un proveedor, como las interrupciones del servicio o las caídas de red.

- **Mayor personalización:** Los CPD on premise pueden ser personalizados para satisfacer las necesidades específicas de una organización. Esto incluye la elección de la infraestructura, el software y los datos.
- **Coste Predecibles a Largo Plazo:** Aunque la inversión inicial puede ser mayor, un CPD en las instalaciones puede ofrecer costos más predecibles a lo largo del tiempo, ya que no está sujeto a tarifas de uso o almacenamiento asociadas con los servicios en la nube.

3.3 Características necesarias a asumir en un CPD

En este epígrafe desarrollaremos aquellas características teóricas esenciales que debe cumplir un CPD, basándonos en los estudios y normativa adecuada.

Disponibilidad, fiabilidad y eficiencia.

3.3.1 Disponibilidad

En un estudio [9] realizado por Emerson Network Power² en 2011, basándose en las respuestas proporcionadas por 41 empresas de distintos sectores (financiero, telecomunicaciones, sanidad, gobierno...) se estima que el coste medio por minuto de la caída de un CPD es de alrededor de 6.000\$, basados en la pérdida o corrupción de datos, pérdida de productividad, daños en el equipamiento, repercusiones legales, repercusiones en la reputación de la compañía, y un largo etcétera.



Figura 3-4 - Causas de las paradas de servicio

Como se muestra en la Figura 3-4, la mayoría de las causas de las paradas de servicio del CPD fueron fallos en las infraestructuras de alimentación y refrigeración. Sin embargo, otro gran porcentaje se corresponde a los errores humanos, por lo que es imprescindible promover los buenos hábitos en el CPD.

² Emerson Network Power es una empresa líder global en soluciones de redes de comunicaciones, CPDs, servicios de salud e instalaciones industriales. Web: www.emerson.com

La disponibilidad se mide como un porcentaje de tiempo que el CPD se encuentra proporcionando servicio. Encontramos varias normativas [10] [11] [12] [13] [14] internacionalmente aceptadas de cara a la medición de esta característica:

- Uptime Institute Tiers (I-IV)
- EN 50600 Availability classes (1-4)
- TIA 942-C Ratings (1-4)
- 10 Syska Hennessy Criticality Levels
- ANSI/BICSI Classes (F0-F4)

Como norma mundialmente aceptada, utilizaremos la ANSI/TIA 942-C, aprobada inicialmente en 2005 por ANSI/TIA (*American National Standards Institute –Telecommunications Industry Association*), clasifica a este tipo de centros en varios grupos, llamados TIER (Tabla 3-1), indicando así su nivel de fiabilidad en función del nivel de disponibilidad

Concebido como una guía para los diseñadores e instaladores de CPD, el estándar TIA-942 proporciona una serie de recomendaciones y directrices para la instalación de sus infraestructuras.

Al diseñar los centros de datos conforme a la norma, se obtienen ventajas fundamentales, como son:

- Nomenclatura estándar.
- Funcionamiento a prueba de fallos.
- Aumento de la protección frente a agentes externos.
- Fiabilidad a largo plazo, mayores capacidades de expansión y escalabilidad.

De acuerdo con el estándar TIA-942, la infraestructura de soporte de un CPD estará compuesta por cuatro subsistemas:

- Telecomunicaciones: Cableado de armarios y horizontal, accesos redundantes, cuarto de entrada, área de distribución, backbone, elementos activos y alimentación redundantes, patch panels y latiguillos, documentación.
- Arquitectura: Selección de ubicación, tipo de construcción, protección ignífuga y requerimientos NFPA 75(Sistemas de protección contra el fuego para información), barreras de vapor, techos y pisos, áreas de oficina, salas de UPS y baterías, salade generador, control de acceso, CCTV, NOC (Network Operations Center – Centro Operativo de Redes).
- Sistema eléctrico: Número de accesos, puntos de fallo, cargas críticas, redundancia de UPS y topología de UPS, puesta a tierra, EPO (Emergency Power Off- sistemas de corte de emergencia) baterías, monitorización, generadores, sistemas de transferencia.
- Sistema mecánico: Climatización, presión positiva, tuberías y drenajes, CRACs (Computer Room Air Conditioners) y condensadores, control de HVAC (High Ventilating Air Conditioning), detección de incendios y sprinklers, extinción por agente limpio (NFPA 2001), detección por aspiración (ASD), detección de líquidos.

Los servicios a proporcionar se pueden clasificar dependiendo su criticidad en baja, media, alta y crítica.

- **Un servicio de criticidad baja** es aquel servicio suplementario que no afecta a la actividad del negocio. Son necesarios para la prestación de otros servicios, pero su caída no afecta a estos. Un ejemplo de estos servicios son los servicios de repositorio software o control de versiones. La caída de esos servicios impacta en la actualización de otros servicios o desarrollos, pero nunca sobre la actividad de negocio, porque los servicios continúan funcionando con las versiones de software anteriores.
- **Un servicio de criticidad media** es aquel servicio que impacta en el negocio, pero que no produce pérdidas económicas significativas. Por ejemplo, un servicio de gestión de nóminas consistente en un portal en el que cada empleado sea capaz de descargar su nómina sería un

servicio de criticidad media, puesto que, ante la caída a finales de mes, el departamento de RRHH debería subir las nóminas de cada empleado al portal.

- **Un servicio de criticidad alta** es aquel servicio que impacta en el negocio, con una repercusión en los ingresos del mismo. El servicio de correo electrónico hoy en día es un ejemplo de servicio de criticidad alta, puesto que todas las empresas se comunican a través de este.
- **Un servicio crítico** es aquel servicio que hace que el negocio funcione y cuya parada puede suponer la parada del negocio. En una plataforma de tele operación, por ejemplo, el servicio telefónico es crítico, puesto que, si este se encuentra indisponible, ningún empleado podría trabajar.

Estos niveles los podemos ver en la siguiente tabla:

TIER	% Disponibilidad	% Parada	Tiempo anual de parada
TIER I	99,67%	0,33%	28,82 horas
TIER II	99,74%	0,25%	22,68 horas
TIER III	99,982 %	0,02%	1,57 horas
TIER IV	100,00%	0,01%	52,56 minutos

Tabla 3-1 - Niveles o TIER de disponibilidad (Fuente: TIA-942)

TIER I- Nivel 1 (Básico)

- Disponibilidad del 99,671 %.
- Sensible a las interrupciones, planificadas o no.
- Un solo paso de corriente y distribución de aire acondicionado, sin componentes redundantes.
- Sin exigencias de piso elevado.
- Generador independiente.
- Plazo de implementación: 3 meses.
- Tiempo de inactividad anual: 28,82 horas.
- Debe cerrarse completamente para realizar mantenimiento preventivo.

TIER II- Nivel II (Componentes redundantes)

- Disponibilidad del 99,741 %.
- Menor sensibilidad a las interrupciones.
- Un solo paso de corriente y distribución de aire acondicionado, con un componente redundante.
- Incluye piso elevado, UPS y generador.
- Plazo de implementación: 3 meses.
- Tiempo de inactividad anual: 22,68 horas.
- Plazo de implementación: 3 a 6 meses.
- El mantenimiento de la alimentación y otras partes de la infraestructura requieren de un cierre de procesamiento.

TIER III- Nivel III (Mantenimiento concurrente)

- Disponibilidad 99,982 %.
- Interrupciones planificadas sin interrupción de funcionamiento, pero posibilidad de problemas en las no previstas.

- Múltiples accesos de energía y refrigeración, por un solo encaminamiento activo. Incluye componentes redundantes (N+1).
- Plazo de implementación: 15 a 20 meses.
- Tiempo de inactividad anual: 1,6 horas.

TIER IV- Nivel IV (Tolerante a errores)

- 99,995 % de disponibilidad.
- Interrupciones planificadas sin interrupción de funcionamiento de los datos críticos. Posibilidad de sostener un caso de imprevisto sin daños críticos.
- Múltiples pasos de corriente y rutas de enfriamiento. Incluye componentes redundantes (2(N+1)).
- Plazo de implementación: 15 a 20 meses.
- Tiempo de inactividad anual: < 57 minutos.

Este TFM versa sobre un CPD Modular, es decir, encapsulado dentro de un contenedor. En su implementación consideraremos el equivalente a **TIER III** conforme a la norma anteriormente citada.

3.3.2 Fiabilidad

Además de la disponibilidad, existen ciertos parámetros que miden la fiabilidad del sistema. De acuerdo con, dichos parámetros son:

MTTF, Tiempo medio hasta el fallo

El MTTF (*Mean Time To Failure*) es el tiempo que pasa desde que un componente se pone en marcha hasta que sucede su primer fallo.

MTBF, Tiempo medio entre fallos

El MTBF (*Mean Time Between Failures*) representa el tiempo de funcionamiento correcto del componente entre dos fallos consecutivos.

Es importante saber que la redundancia de un componente no aumenta el MTBF, aunque sí aumenta al MTBF del conjunto de componentes.

MTTR, Tiempo medio de reparación

El MTTR (*Mean Time To Repair*) representa el tiempo que estará el componente fuera de servicio a causa de reparaciones.

Disponibilidad

La disponibilidad “A” viene definida por la siguiente fórmula:

$$A = \left(1 - \frac{MTTR}{MTBF}\right) \times 100$$

Si un sistema experimenta N fallos a lo largo de su vida, estará $N \times MTTF$ horas operativo y $N \times MTTR$ horas en reparación. La disponibilidad media será:

$$A = \frac{N \times MTTF}{N \times MTTF + N \times MTTR} = \frac{MTTF}{MTTF + MTTR}$$

3.3.3 Eficiencia

Las dos magnitudes más extendidas para medir la eficiencia energética del CPD son las siguientes:

- **Power Usage Effectiveness (PUE):** Fue creado por los miembros del Green Grid³. Consiste en dividir la potencia total suministrada al CPD entre la potencia que consume el equipamiento IT. La máxima eficiencia es 1.
- **Data Center Infrastructure Efficiency (DCIE):** Es el recíproco del PUE y se expresa como un porcentaje, que mejora a medida que se acerca al 100%.

Asociada a la eficiencia energética está la huella de carbono. La huella de carbono es la cantidad de gases de efecto invernadero generada por el CPD.

Al igual que en otros sectores, debido en parte al encarecimiento de la energía y también a la cada vez mayor conciencia ecológica, reportar la huella de carbono está siendo cada vez más habitual. En los CPD se consume mucha electricidad y se genera mucha energía térmica que se desperdicia. El uso de CPD supone un consumo del 1% de la energía a nivel mundial y las TIC suponen ya el 2% de las emisiones globales de gases de efecto invernadero a la atmósfera [15].

En los últimos años, el coste de los servidores ha seguido una tendencia descendente y prácticamente se ha visto superado por el coste de la electricidad que consumen. La distribución de consumo energético en un CPD la podemos ver en la siguiente imagen:

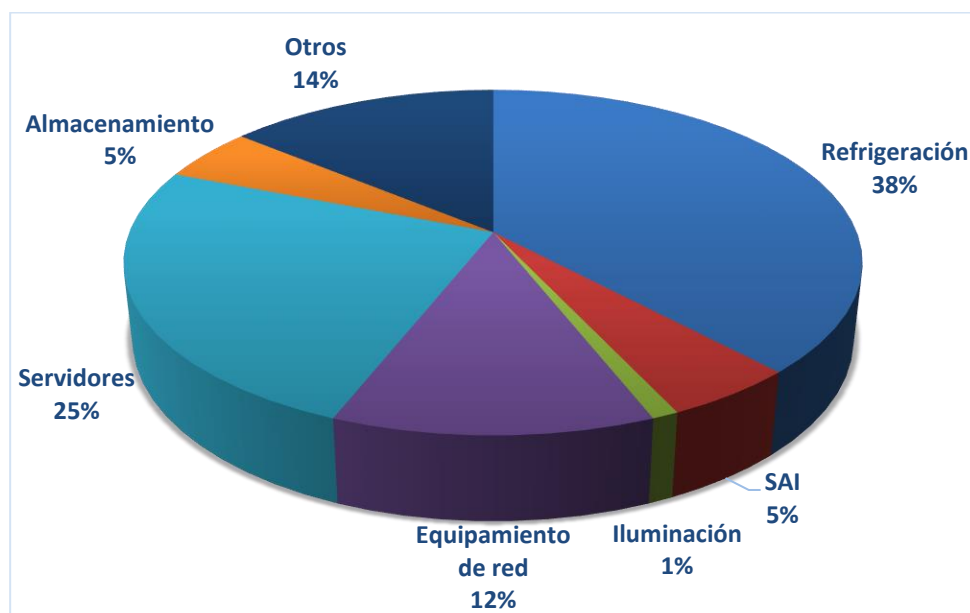


Figura 3-5 - Consumos en un CPD

En lo que respecta a la refrigeración, es importante señalar que cualquier dispositivo eléctrico genera calor como subproducto de su funcionamiento, y es fundamental disiparlo para evitar que la temperatura interna alcance niveles no deseables.

La cantidad de energía transmitida a través de las líneas de datos por los equipos TIC es mínima. En consecuencia, la totalidad de la energía suministrada por la red eléctrica, en forma de corriente alterna,

³ Green Grid: Organización miembro afiliada del Information Technology Industry Council (ITI). Trabaja a nivel mundial para crear herramientas, brindar experiencia técnica y abogar por la optimización de la eficiencia energética. <https://www.thegreengrid.org/>

se transforma principalmente en calor. En este sentido, la energía térmica en vatios (W) que generan los equipos equivale a su consumo energético en vatios.

La energía térmica global generada por un sistema es el resultado de la suma de las contribuciones térmicas de cada uno de sus componentes. El sistema completo incluye los dispositivos TIC, así como otros elementos como sistemas de alimentación ininterrumpida (SAIs), unidades de climatización, sistemas de iluminación y la presencia de personal.

En cuanto a las unidades de climatización, es importante mencionar que estas generan una cantidad significativa de calor, el cual es dirigido hacia el exterior del entorno del CPD. Aunque este calor no impacta directamente en la carga térmica interna del Centro de Datos, sí tiene efectos negativos en la eficiencia del sistema de climatización. Por lo tanto, este factor es tenido en cuenta al determinar las dimensiones adecuadas para el sistema de aire acondicionado.

3.4 Construcción de Centros de Datos tradicionales

Como he introducido en anteriores epígrafes, el desarrollo de este TFM versa sobre un CPD implantado dentro de un contenedor, que se tratará exhaustivamente en el [capítulo 4](#). No obstante, se explicarán de manera resumida algunos conceptos de la metodología de construcción tradicional con obra civil en el desarrollo de centros 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.

Los fundamentos básicos a la hora de acometer el proyecto de obra civil de un Centro de Datos difieren de los de una construcción orientada a otros servicios principalmente a la hora elegir materiales y distribución de los elementos. Tal y como he tratado en el punto 3.1, a través de los años se han ido cambiando los requerimientos a la hora del diseño de los Centros de Datos, que anteriormente eran ubicaciones genéricas dentro de las dependencias de una organización para pasar a ser ubicaciones exclusivas orientadas a proporcionar las mejores condiciones posibles para todo el equipamiento.

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 [12], 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.



Figura 3-6 - Construcción del CPD de Interxion (Fuente: Interxion)

4 DESARROLLO DEL TFM

4.1 Introducción al Edge Computing y la Soberanía del Dato

Estos son dos conceptos íntimamente ligados con esta tipología de proyectos, por la ubicación de los datos y la autoridad que se desea tener sobre ellos.

4.1.1 Edge Computing

El Edge Computing o Computación Frontera es un concepto vertiente de la computación distribuida, que consiste en el almacenamiento, tratamiento y análisis de los datos lo más cerca posible de donde éstos se generan.

Lleva las aplicaciones empresariales más cerca de los datos, como los dispositivos *IoT* o los servidores locales. Esto tiene varias ventajas, como la reducción de la latencia, la posibilidad de realizar análisis en tiempo real, una mejor seguridad de los datos y una mayor eficiencia de costes.

Este concepto es muy amplio ya que puede ser aplicado en muchos campos como, por ejemplo:

- **Vehículos autónomos:** Los vehículos autónomos utilizan el Edge Computing para procesar datos de sensores en tiempo real, como cámaras, radares y LIDAR. Esto les permite tomar decisiones de conducción seguras y eficientes.
- **Realidad virtual y realidad aumentada:** Puede mejorar la experiencia de usuario de las aplicaciones de realidad virtual y realidad aumentada al reducir la latencia y la necesidad de ancho de banda.
- **Internet de las cosas (IoT):** Es ideal para aplicaciones IoT, ya que permite procesar datos de sensores y dispositivos en tiempo real.
- **Ciberseguridad:** Puede ayudar a mejorar la seguridad de las redes al procesar datos de seguridad en los bordes de la red sin necesidad de salir a la nube.
- **Monitorización y procesamiento industrial:** Almacenar y analizar datos de sensores industriales en tiempo real. Esto puede optimizar procesos y mejorar la eficiencia.
- **Gestión de la energía:** Recopilar y analizar datos de consumo de energía en tiempo real para que las empresas puedan reducir sus costes.
- **Atención médica:** Un uso más vanguardista, análisis de datos médicos en tiempo real para ayudar a los médicos a tomar decisiones de tratamiento más rápidas y precisas.
- **Comercio minorista:** Se pueden realizar análisis de datos de clientes en tiempo real. Esto puede ayudar a las empresas a mejorar la experiencia de compra.
- **Fabricación:** El Edge Computing ofrece la posibilidad de recolectar y analizar datos de producción en tiempo real de manera efectiva para optimizar los procesos y mejorar la calidad de los productos.
- **Logística:** Se pueden examinar datos de transporte en tiempo real, para mejorar la eficiencia de las cadenas de suministro.

En el caso de este TFM, el Edge Computing supone ese acercamiento del procesamiento de los datos al lugar de producción, ya que el CPD Modular se ubica en las instalaciones de la organización y evita que estos datos tengan que transmitirse fuera de la organización, con lo que esto conlleva a efectos de seguridad, latencia y disponibilidad.

Un concepto importante que se quiere abordar con este proyecto es la de soberanía del dato.

4.1.2 Soberanía del dato

En la era digital, la soberanía de los datos se refiere al concepto de que un país o entidad tiene control y jurisdicción sobre los datos generados y almacenados en su territorio. Esto implica que los datos son gestionados y protegidos de acuerdo con las leyes y regulaciones locales.

Es un tema de creciente importancia debido a la naturaleza global de Internet y la ubicuidad de los servicios en la nube. A medida que las organizaciones almacenan datos en servidores ubicados en diferentes países, surgen cuestiones sobre quién tiene el control sobre esos datos y qué leyes se aplican. Esto tiene implicaciones tanto en la privacidad como en la seguridad de la información.

Varios países han promulgado leyes y regulaciones que respaldan la soberanía de los datos. Por ejemplo, la Unión Europea implementó el Reglamento General de Protección de Datos (GDPR) [16], que establece normas estrictas sobre el manejo de datos personales y requiere que las empresas que operan en la UE almacenen datos de ciudadanos de la UE dentro de la región, a menos que haya acuerdos específicos de transferencia de datos.

La soberanía de los datos también se ha convertido en una preocupación en el ámbito de la seguridad nacional. Algunos países consideran que ciertos datos críticos, como los relacionados con la infraestructura crítica o la defensa, deben mantenerse dentro de sus fronteras para garantizar su seguridad.

En resumen, la Soberanía del Dato es un concepto que aborda quién tiene control sobre la información en un mundo digital interconectado. A medida que las regulaciones y las preocupaciones sobre la privacidad y la seguridad de los datos continúan evolucionando, la soberanía de los datos seguirá siendo un tema de debate y acción en el ámbito global.

Por este motivo se considera que la “salida” a la nube no siempre es la mejor solución para almacenar y tratar los datos, debido a las posibles implicaciones o necesidades, todavía en un momento delicado y previo que supone regulación constante.

4.2 Características físicas de un Centro de Procesamiento de Datos Modular

En un proyecto de Edge Computing se pueden proveer multitud de servicios tal y como se ha explicado en el punto anterior. Este TFM versa sobre la provisión de un contenedor en el cual se instala la infraestructura necesaria para ese almacenamiento, análisis y tratamiento de los datos, de la misma manera que se proveen por un CPD tradicional en una “habitación” acondicionada (punto 3.4), que son:

- Computación
- Almacenamiento
- Seguridad
- Comunicaciones

En los siguientes puntos se tratarán las características principales que debe cumplir la estructura que contiene el CPD.

4.2.1 Contenerización

Los Contenedores Secos son el tipo de contenedor más usado en el mundo: un 90% de mercancías enviadas por transporte marítimo se cargan en este tipo de contenedores [17]. El uso de contenedores secos, apto para transporte marítimo y transporte terrestre, permite optimizar las operaciones portuarias, ya que sus dimensiones favorecen apilarlos y manipularlos con grúas u otro tipo de maquinaria.

Los contenedores de carga seca de 20 pies y 40 pies están fabricados con aluminio o acero y al ser completamente cerrados y herméticos son adecuados para todo tipo de mercancía, ya que no requieren

de sistemas de ventilación o refrigeración. Los contenedores de aluminio permiten mayor capacidad de peso de mercancía, mientras que los de acero disponen de una capacidad cúbica interna ligeramente superior.

Las dimensiones específicas y capacidad del contenedor seco pueden variar dependiendo del fabricante y del propietario del contenedor. Las especificaciones que se indican a continuación son, sin embargo, las más representativas.



Figura 4-1 - Contenedor Seco 20 Pies



Figura 4-2 - Contenedor Seco 40 Pies

En la siguiente tabla se muestran las medidas más habituales para los contenedores, aunque existen muchos modelos, estos son los más utilizados:

Medidas y capacidad Contenedor Seco 20 pies			
Peso Tara 2.300 kg	Capacidad de carga 25.000 kg	Capacidad cúbica 33,2 m ³	Longitud interna 5,9 m
Ancho interno 2,35 m	Altura interna 2,39 m	Ancho Apertura Puertas 2,34 m	Altura Apertura Puertas 2,28 m

Medidas y capacidad Contenedor Seco 40 pies			
Peso Tara 3.750 kg	Capacidad de Carga 27.600 kg	Capacidad Cúbica 67,7 m ³	Longitud Interna 12,03 m
Ancho Interno 2,35 m	Altura Interna 2,39 m	Ancho Apertura Puertas 2,34 m	Altura Apertura Puertas 2,28 m

Tabla 4-1 - Características físicas Contenedor Seco

No obstante, se rigen por la norma ISO 668:2020 [18] [19]

4.2.2 Características propias de los Contenedores para albergar un CPD

A la hora de albergar un CPD, estos contenedores deben cumplir con ciertas características concretas que los diferencian de un contenedor, por ejemplo, para transporte de mercancías.

Entre estas características podemos encontrar:

- **Resistencia:** Los contenedores secos están diseñados para soportar las condiciones de transporte, pero también deben ser resistentes a los elementos y a las vibraciones. Esto es importante para proteger los equipos y sistemas del CPD de daños.

- **Aislamiento:** Los contenedores secos deben estar bien aislados para evitar cambios bruscos de temperatura y humedad. Esto es importante para garantizar el funcionamiento correcto de los equipos y sistemas del CPD.
- **Ventilación y climatización:** Los contenedores secos deben tener una ventilación adecuada para evitar el sobrecalentamiento de los equipos.
- **Protección contra incendios:** Los contenedores secos deben estar equipados con sistemas de protección contra incendios para evitar la propagación de un incendio.

Además de estas características, los contenedores secos que albergan un CPD pueden incorporar otros elementos opcionales para mejorar su funcionalidad, como:

- **Sistemas de climatización:** Los sistemas de climatización pueden ayudar a mantener las condiciones ambientales óptimas para el funcionamiento del CPD.
- **Sistemas de alimentación ininterrumpida (SAI):** Los SAI pueden proporcionar energía al CPD en caso de un corte de luz.
- **Sistemas de seguridad:** Los sistemas de seguridad pueden ayudar a proteger el CPD de intrusiones y robos.

En determinadas ocasiones es preferible realizar una estructura modular prefabricada y panelada adaptada a las necesidades de la organización, lo que permite mejorar las dimensiones estándar a unas personalizadas, pero por contra no permitiría el transporte de estos contenedores mediante los medios de transporte habituales por diferencias con las estructuras estandarizadas (remolques de camión, bodega de carga aérea, etc.), salvo que cumpla con certificación Lloyd's International LRQA⁴.



Figura 4-3 - Estructura modular prefabricada (Fuente: Area Data Paraguay S.A.)



Figura 4-4 - Certificación LRQA

⁴ Lloyd's Register Quality Assurance (LRQA) es el proveedor líder de servicios de auditoría independiente, incluyendo la certificación, validación, verificación y formación, con el reconocimiento de más de 50 organismos de acreditación.

Una vez que tenemos el contenedor, será necesario adaptar sus características internas para albergar de manera adecuada todo el equipamiento.

4.2.3 Suelo técnico

Se le conoce también como falso suelo. Está compuesto de baldosas de medida estándar de 60x60 cm. apoyadas sobre pedestales de acero ajustables en altura, consiguiendo un falso suelo firme sobre la solera existente. Bajo el suelo técnico se crea una cámara (plenum) que consiste en un espacio libre, antiguamente para el alojamiento de cableado, empleado en el circuito de refrigeración de la sala. Al ser los paneles idénticos se facilita el intercambio de los mismos, garantizando tanto la accesibilidad como la flexibilidad.

Se rige por la norma UNE-EN 12825:2002 [20]

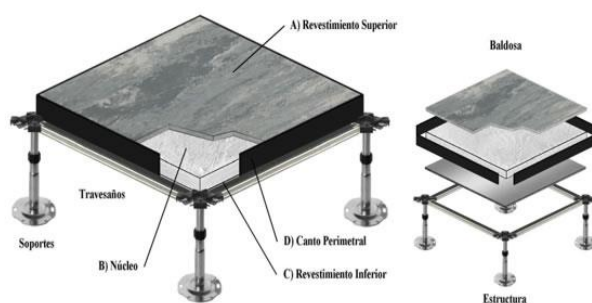


Figura 4-5 - Placa de suelo técnico con soporte

Estructura

La estructura está formada por dos partes, cabeza y base. Es regulable en altura. Sobre la cabeza se apoyan los travesaños, que sujetarán la baldosa. Existen diferentes tipos de estructuras, y sus parámetros más importantes son:

- Altura mínima
- Altura máxima
- Carga máxima axial sin deformación

Suelen ser de aluminio o acero.

Baldosas

Las baldosas son de un tamaño estándar de 60x60 cm. y 4 cm. de grosor.

Están constituidas por un núcleo central, recubierto superior e inferiormente por distintos materiales, y rematado por una protección perimetral de PVC de 2 mm de espesor. Los tableros pueden ser aglomerados de madera y otros materiales lignocelulósicos, de cemento o de anhidrita. Los recubrimientos pueden ser de PVC, Linóleoum, tarimas, corchos, estratificados, ...

Marcado y Etiquetado

En la norma UNE-EN 12825 se indica la información que debe acompañar en los documentos comerciales:

- La marca registrada o la marca de identificación del fabricante.
- Número y año de esta norma.
- Año y mes del marcado.

Las siguientes características que le sean aplicables:

- Reacción al fuego
- Reacción al fuego
- Capacidad de carga y flecha
- Grado de tolerancia
- Coeficiente de seguridad
- Conductividad electrostática
- Aislamiento a ruido de impacto
- Aislamiento a ruido aéreo
- Conductividad térmica
- Resistencia al pelado
- Protección contra la corrosión
- Riesgo de electrocución
- Impacto de cuerpos duros
- Impacto de cuerpos blandos

4.2.4 Sistema de alimentación eléctrica

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, 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 pérdida 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 el etiquetado correspondiente en cada diferencial del cuadro y a cada toma de los racks.

Este sistema se implanta por la comercializadora de la red eléctrica y por la empresa constructora implantadora del CPDM. La comercializadora lleva las acometidas desde la estación eléctrica más cercana hasta las tomas principales de energía eléctrica de la organización y la empresa implantadora conecta las acometidas que van desde las tomas generales hasta las tomas principales del CPDM.

Todos elementos usados en esta instalación como los cables, conectores, cuadros de energía, etc. cumplen normativas nacionales e internacionales [12] 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.

4.2.5 Sistema de Alimentación Ininterrumpida (SAI)

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 principales problemas que puede producirse en el suministro eléctrico [21]:

- Corte de electricidad
- Sobretensión
- Picos de tensión
- Bajada de tensión
- Baja y alta tensión continuada
- Ruidos o interferencias radioeléctricas o electromagnéticas en la línea
- Variaciones de frecuencia
- Micro cortes y conmutaciones
- 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, para activar los grupos de respaldo o en caso de emergencia apagado de las máquinas.

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.

4.2.6 Sistema de climatización

Los centros de datos generan mucho calor debido al funcionamiento de los equipos informáticos, lo que puede afectar negativamente al rendimiento y vida útil de los equipos, así como suponer un riesgo de incendio.

La normativa ASHRAE [22] (American Society of Heating Refrigeration and Air conditioning Engineers) recomienda que la temperatura de un centro de datos esté entre 18 y 27 grados centígrados, y la humedad relativa sea inferior al 60%. Si la humedad es demasiado alta, se puede condensar agua en los equipos, lo que puede provocar cortocircuitos.

Existen tres tipos principales de sistemas de refrigeración para centros de datos:

- Refrigeración por aire: Es el sistema más sencillo y económico. Consiste en bombear aire frío a través de los equipos informáticos.
- Refrigeración por agua: Es más eficiente que la refrigeración por aire. Consiste en bombear agua fría a través de tuberías que están en contacto con los equipos informáticos.
- Refrigeración por inmersión: Es el sistema más eficiente. Consiste en sumergir los equipos informáticos en un fluido dieléctrico que no conduce la electricidad, pero sí es capaz de llevarse el calor.

Para reducir el consumo de energía, los sistemas de refrigeración suelen utilizar una configuración de pasillo frío y pasillo caliente. En esta configuración, el aire frío se bombea al pasillo frío, donde se encuentran los equipos. El aire caliente se expulsa al pasillo caliente.

El aislamiento de pasillo frío es una técnica que ayuda a separar el pasillo frío del pasillo caliente. Esto puede ayudar a reducir el consumo de energía en un 30%.

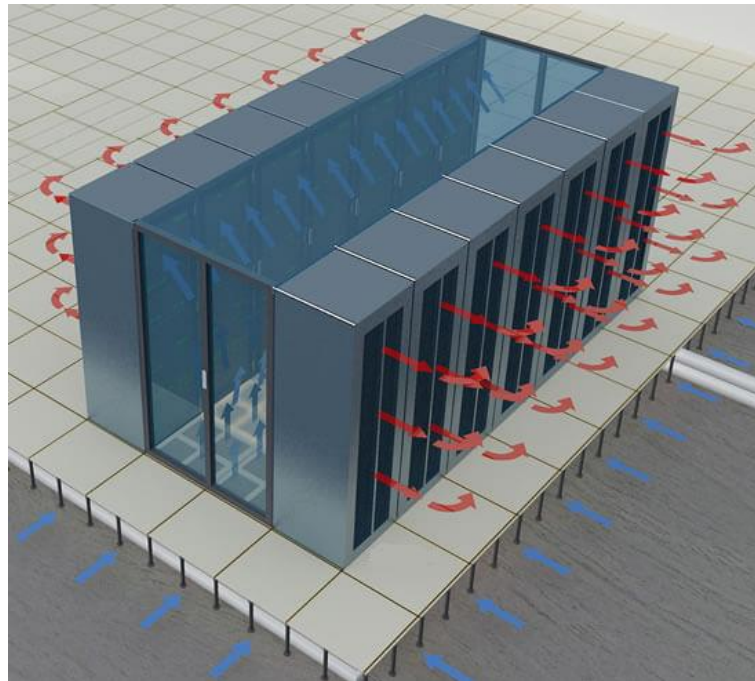


Figura 4-6 - Configuración en pasillo frío/pasillo caliente

En un CPD Modular la configuración se puede realizar con una o dos filas de racks, aunque como se ha comentado antes (punto 4.2.2), es posible adaptar las dimensiones interiores a diferentes necesidades del cliente, que posiblemente no quiera desplazar con medios homologados la estructura. De manera opcional, se puede realizar un panelado en la parte superior de los racks para separar los pasillos.

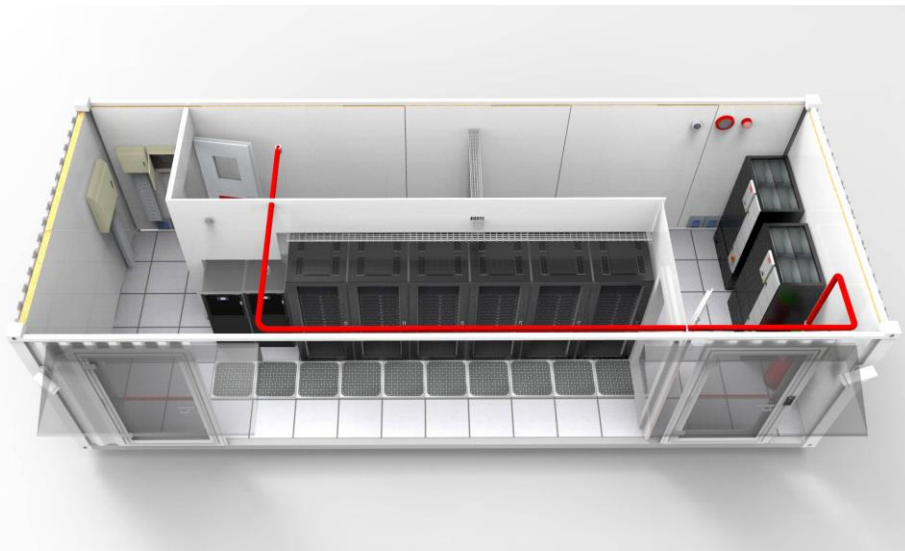


Figura 4-7 - Panelado de separación frío/caliente (Fuente: Area Data Paraguay S.A.)



Figura 4-8 - Detalle del panelado superior (Fuente: Area Data Paraguay S.A.)

El exceso de calor en un centro de datos puede causar los siguientes problemas:

- Rendimiento reducido: El equipamiento TI tiene un menor rendimiento cuando está expuesto a altas temperaturas.
- Acortamiento de la vida útil: El calor puede dañar los componentes de los equipos, lo que reduce su vida útil.
- Riesgo de incendio: El calor puede provocar que los materiales inflamables se incendien.

Por eso, es importante diseñar un sistema de refrigeración que mantenga una temperatura y humedad óptimas en los centros de datos.

La capacidad de refrigeración depende del número de racks, equipos que se instalen dentro de cada rack y de la potencia instalada, usualmente 4,5KW por rack.

En las siguientes imágenes se puede apreciar la circulación del flujo de aire dentro de un contenedor adaptado (en este caso de 20 pies, el diseño de 40 pies es similar. Se reflejan disposiciones habituales del equipamiento).

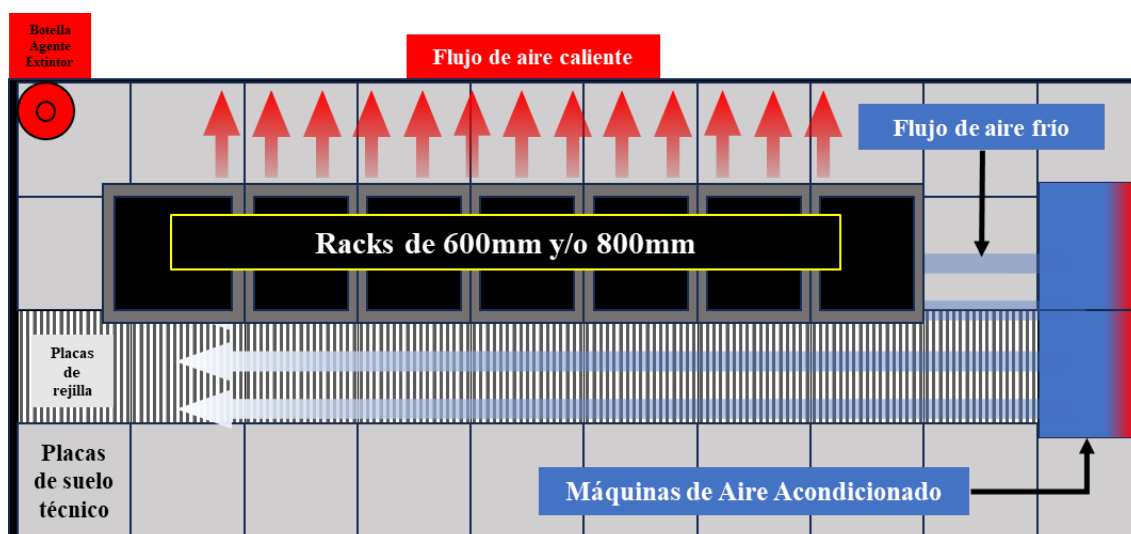


Figura 4-9 - Planta del contenedor

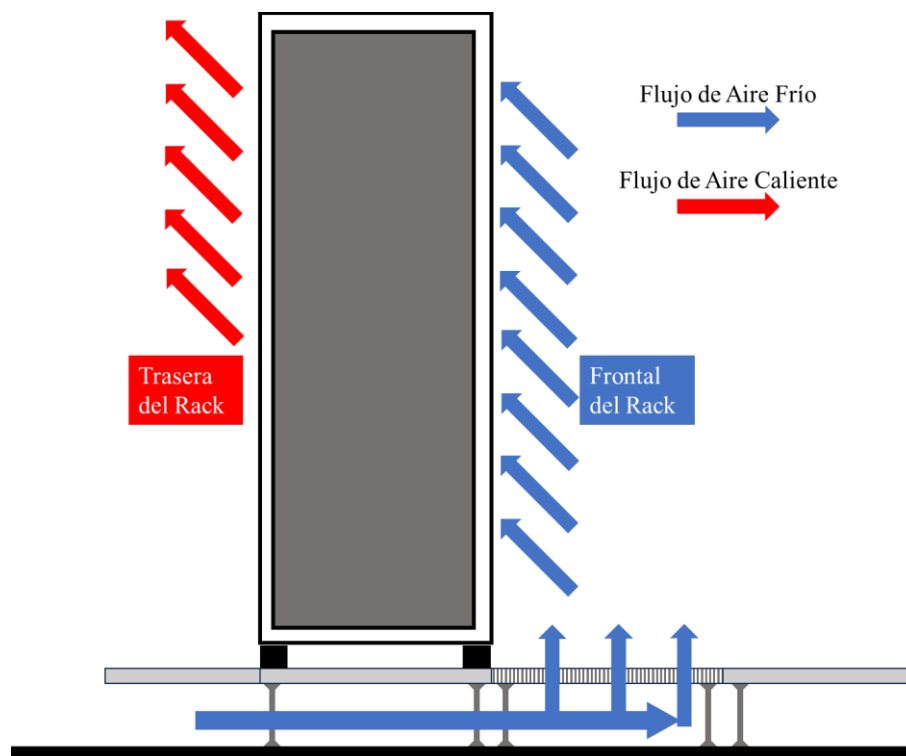


Figura 4-10 - Alzado lateral de un rack

4.2.7 Sistema de protección contra incendios: Detección y Extinción

La mayoría de los fuegos empiezan fuera del CPD. Sin embargo, y pese a que estructuralmente el CPD debe estar preparado para resistir la amenaza de un fuego exterior, también debe existir un sistema de detección y extinción de incendios en el interior de la sala, por si se propagase desde el exterior al interior o por si se originase en el interior.

El sistema de detección de incendios permite la localización de un incendio y activa la alarma correspondiente. La central de incendios puede estar programada para realizar determinadas acciones automáticamente.

Los componentes principales del sistema de detección de incendios son [23]:

- Detectores.
- Pulsadores manuales.
- Central de señalización.
- Líneas.
- Sistemas auxiliares: alarma general, teléfono, accionamiento de los sistemas de extinción, etc.

La extinción por gas tiene una serie de ventajas frente a la extinción por agua:

- No dejan residuos.
- No conducen la electricidad.
- Evitan los daños producidos por el agua.
- Rápida actuación en el foco del incendio.
- La actividad se reinicia rápidamente tras la descarga.
- La inundación total permite que el agente extintor llegue incluso a las zonas menos accesibles.

4.2.8 Posibles disposiciones del equipamiento

Gracias al formato modular, el equipamiento puede ubicarse posibilitando que se habiliten zonas diferenciadas de trabajo o enfocadas a distintos cometidos:



Figura 4-11 - CPDM de 20 pies con 5 racks y área de trabajo2 (Fuente: Area Data Paraguay S.A.)



Figura 4-12 - CPDM de 8 racks y 10,2m (Fuente: Area Data Paraguay S.A.)

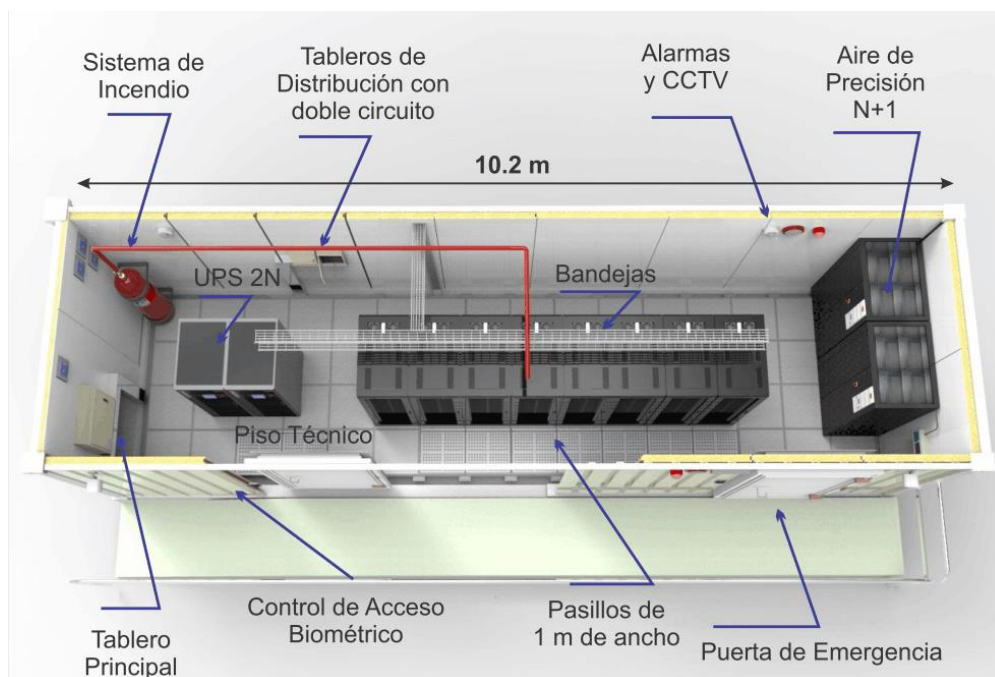


Figura 4-13 - Muestra de un CPDM completo (Fuente: Area Data Paraguay S.A.)

4.3 Transporte de los contenedores

Para el traslado del equipamiento a la ubicación final, pueden darse dos situaciones:

4.3.1 Construcción en la ubicación final

En este caso, toda la estructura puede realizarse en la ubicación en la que vaya a dar servicio, como se ha mostrado antes (punto 4.2.2), se puede realizar una estructura modular prefabricada para posteriormente realizar el panelado y montar el equipamiento en su interior.

Esta solución es viable, por ejemplo, si la instalación no se puede trasladar completa a su ubicación final, por encontrarse dentro de otro edificio (recordemos que la implantación modular también tiene que ver con la eficiencia energética).

4.3.2 Fabricación o ensamblado y transporte posterior

En esta situación, es importante recalcar alguna de las normativas que se han mencionado anteriormente, como por ejemplo la Certificación LRQA o la norma ISO 668:2020. Gracias a estas normativas se establecen los tamaños que se pueden transportar en medios de locomoción estandarizados.

La ventaja de este modelo es que no es necesario ocupar un espacio para el ensamblado de las piezas que conforman en CPDM, así como poder llevarse de una ubicación a otra en el caso, por ejemplo, de cambio de ubicación de una sede de una organización.



Figura 4-14 - Transporte por carretera



Figura 4-15 - Transporte aéreo

4.4 Equipamiento TI, arquitectura de un CPD

Es este subapartado se definirán aquellos componentes TI que forman parte de una instalación modular.

4.4.1 Racks

Los racks [24] de equipamiento TI son del tipo estándar 19" y 600mm u 800mm, ya que pueden estar dedicados a computación o comunicaciones, según la norma UNE 20539-2:1996 [25]. 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.

Hay una multitud de racks para servidores especializados, incluidos racks para servidores insonorizados, con aire acondicionado, con clasificación NEMA [26], con clasificación sísmica, de marco abierto, estrechos e incluso en miniatura de 19 pulgadas para aplicaciones más pequeñas.

Los racks deben estar unidos unos a otros, atornillados al suelo o utilizar un dispositivo anti inclinación por motivos de seguridad. En caso de extraer parcialmente una pieza de equipamiento de 19" de un rack para su mantenimiento, el rack puede llegar a tener mucho peso en la parte superior, hacerse inestable (si no tiene el peso equilibrado desde abajo) y crear un riesgo para la seguridad. La forma más barata de lograr estabilidad es la fijación.

Los dispositivos anti inclinación se instalan en la parte delantera del rack y constan de un juego de patas del que se puede tirar hacia fuera cuando se realiza el mantenimiento de los componentes del rack, ampliando la superficie de la base del rack. La seguridad física puede ser necesaria también en una zona de alta actividad sísmica; los racks deben ser suficientemente estables para soportar posibles terremotos

Los accesorios comunes de los racks de TI son:

- Gestión de los cables
- Gestión del flujo de aire
- Estantes y brazos o carriles de soporte
- Anclaje
- Puertas perforadas individuales
- Paneles laterales
- Raíles de servidores
- Brackets para gestión de cables/PDU
- Paneles superiores

4.4.2 Servidores de cómputo

El servidor de montaje en rack, como su propio nombre indica, está diseñado para ser ubicado en un bastidor mediante un sistema de anclaje y de liberación de cables o extensión de estos para su mantenimiento, lo que supone un ahorro de espacio frente al formato tipo torre, prácticamente en desuso en aplicaciones en los centros de datos. Este formato dota de escalabilidad a la solución. Su principal problema radica en la dificultad que existe para refrigerarlos.

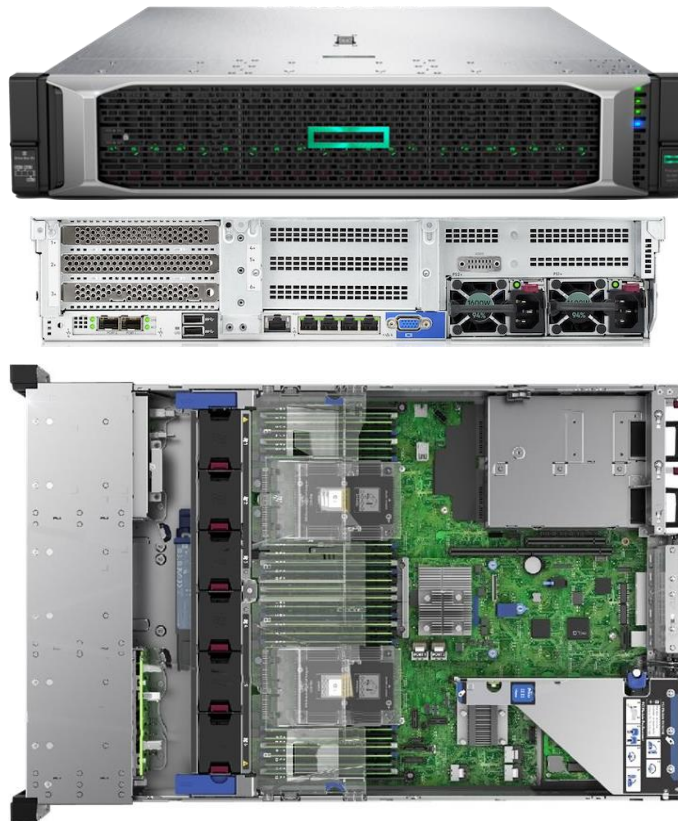


Figura 4-16 - Servidor de montaje en rack HPe DL380 G10

Con la virtualización aparecen los servidores tipo blade. Se trata de un servidor modular diseñado para minimizar el uso de espacio físico. Un chasis contiene múltiples servidores blade, además de mecanismos de ventilación, comunicaciones y alimentación. Es una solución altamente escalable. Sin embargo, requiere de mecanismos de refrigeración adicionales y mayor energía que los otros formatos, lo que incrementa su coste a largo plazo.



Figura 4-17 - Chasis HP Synergy

4.4.3 Dispositivos de Almacenamiento

Los Centro de Datos necesitan 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 de almacenamiento [27] de varios dispositivos conectados tipo SAN [28] o unidades NAS individuales, generalmente con tecnología iSCSI. Estos dispositivos deben cumplir con diferentes objetivos:

- **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.
- **Alta disponibilidad y resistencia:** Con una arquitectura confiable que no tiene puntos únicos de fallo y tiene una disponibilidad comprobada.
- **Compresión:** 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 la máxima eficiencia en el sistema.
- **Escalabilidad**
 - La red SAN puede comprender miles de dispositivos de almacenamiento SAN y servidores host que se pueden escalar para satisfacer las necesidades empresariales en evolución. Las organizaciones pueden agregar nuevos hosts y dispositivos de almacenamiento para desarrollar la SAN cuando aumentan las necesidades de capacidad.
 - Los sistemas NAS permiten a las organizaciones escalar la capacidad de almacenamiento sin reemplazar ni actualizar los servidores existentes ni apagar la red. El almacenamiento se puede aumentar fácilmente agregando otro dispositivo NAS, otro disco duro o un disco duro con mayor capacidad

Estos equipamientos pueden o bien disponer de racks propios proporcionados por los fabricantes o bien colocarse en los racks estándar que se instalen en el CPD para que sea un diseño más uniforme.

Normalmente están compuestos por un servidor de procesamiento o *Service Processor* y una o varias bandejas de discos o *Disk Array Enclosures*.



Figura 4-18 - Sistema de almacenamiento Dell PowerStore 1200T y Bandejas de discos

4.4.4 Dispositivos de Backup

De la misma manera que los dispositivos de almacenamiento proporcionan espacio lógico para los datos, los dispositivos de backup son cruciales para prevenir la pérdida de datos debido a errores humanos, fallos hardware, ciberataques o desastres naturales.

La elección del dispositivo adecuado depende de las necesidades específicas, el volumen de datos a respaldar y la disponibilidad de recursos. Es importante mantener un plan de respaldo actualizado y realizar pruebas periódicas de restauración para asegurar que los datos estén protegidos y sean recuperables en caso de necesidad.

Estos dispositivos pueden ser tanto hardware como software, y existen diversas tecnologías y métodos para llevar a cabo el respaldo de datos.

Dispositivos de Backup Hardware:

- Unidades de Disco Duro Externo: Son discos duros portátiles que se conectan al servidor a través de USB u otras interfaces. Son ideales para copias de seguridad locales y rápidas.
- Cintas Magnéticas: Aunque menos comunes en la actualidad, las cintas magnéticas son una opción económica para el almacenamiento de grandes volúmenes de datos.
- Servidores de backup: Estos dispositivos están diseñados para respaldar múltiples computadoras en una red empresarial. Son escalables y ofrecen una gestión centralizada de las copias de seguridad.
- Servicios de Copia de Seguridad en la Nube: Plataformas como Dropbox, Google Drive y Microsoft OneDrive ofrecen almacenamiento en la nube con funciones de copia de seguridad automática.

Al igual que los dispositivos de almacenamiento, se componen de una unidad de procesamiento y bandejas de discos ampliables para poder crecer en cuanto a capacidad de almacenamiento.



Figura 4-19 - Sistema de backup Dell PowerProtect DD6900

4.4.5 Dispositivos de seguridad: Firewalls, SIEM, IDS e IPS [29]

Su principal función es monitorear y controlar el tráfico de datos que entra y sale de una red. Esto se logra mediante reglas predefinidas que determinan qué tipo de tráfico se permite o bloquea. Se utilizan para proteger sistemas y datos sensibles de amenazas como malware, ataques o intrusiones no autorizadas. Actúan como filtros, inspeccionando cada paquete de datos en busca de posibles amenazas y decisiones en tiempo real sobre si permitir o bloquear su paso.

Cortafuegos

Se pueden clasificar en diferentes categorías, según su ubicación, su función o su tecnología.

Según su **ubicación**, los cortafuegos se pueden dividir en:

- Cortafuegos de red: Son los cortafuegos más comunes y se utilizan para proteger una red interna de una red externa, como Internet.
- Cortafuegos de host: Se instalan en un dispositivo individual para protegerlo de ataques de la red.

- Cortafuegos personal: Se instalan en un ordenador personal para protegerlo de ataques de Internet.

Según su **función**, los cortafuegos se pueden dividir en:

- De filtrado de paquetes: Examinan los paquetes de datos que entran y salen de una red y permiten o bloquean el tráfico según sus reglas.
- De inspección con estado: Además de examinar los paquetes de datos, mantienen un registro del estado de las conexiones entre los dispositivos. Esto les permite detectar y bloquear ataques que utilizan conexiones no autorizadas.
- De aplicaciones web: Se utilizan para proteger las aplicaciones web de ataques específicos, como inyecciones de código, ataques de fuerza bruta y ataques de denegación de servicio.

Según su **tecnología**, los cortafuegos se pueden dividir en:

- Cortafuegos de hardware: Se implementan en un dispositivo físico, como un enrutador o un servidor.
- Cortafuegos de software: Se implementan en un ordenador o en un dispositivo virtual.
- Cortafuegos basados en la nube: Se implementan y administran en la nube.

En el caso de un despliegue industrial o empresarial, los más efectivos son los cortafuegos hardware, por potencia y capacidad de cómputo.

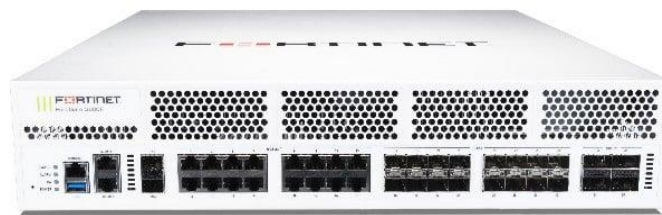


Figura 4-20 - Firewall Fortigate FG2600

SIEM

SIEM (Security Information and Event Management) o sistema de gestión de eventos e información de seguridad: es una solución híbrida centralizada que engloba la gestión de información de seguridad (Security Information Management) y la gestión de eventos (Security Event Manager).

La tecnología SIEM proporciona un análisis en tiempo real de las alertas de seguridad generadas por los distintos dispositivos hardware y software de la red. Recoge los registros de actividad (logs) de los distintos sistemas, los relaciona y detecta eventos de seguridad, es decir, actividades sospechosas o inesperadas que pueden suponer el inicio de un incidente, descartando los resultados anómalos, también conocidos como falsos positivos y generando respuestas acordes en base a los informes y evaluaciones que registra, es decir, es una herramienta en la que se centraliza la información y se integra con otras herramientas de detección de amenazas.

IDS

IDS (Intrusion Detection System) o sistema de detección de intrusiones: es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red, es decir, son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas. Ante cualquier actividad sospechosa, emiten una alerta a los administradores del sistema quienes han de tomar las medidas oportunas. Estos accesos pueden ser ataques esporádicos realizados por usuarios malintencionados o repetidos cada cierto tiempo, lanzados con herramientas automáticas. Estos sistemas sólo detectan los accesos sospechosos emitiendo alertas anticipatorias de posibles intrusiones, pero no tratan de mitigar la intrusión. Su actuación es reactiva.

IPS

IPS (Intrusion Prevention System) o sistema de prevención de intrusiones: es un software que se utiliza para proteger a los sistemas de ataques e intrusiones. Su actuación es preventiva. Estos sistemas llevan a cabo un análisis en tiempo real de las conexiones y los protocolos para determinar si se está produciendo o se va a producir un incidente, identificando ataques según patrones, anomalías o comportamientos sospechosos y permitiendo el control de acceso a la red, implementando políticas que se basan en el contenido del tráfico monitorizado, es decir, el IPS además de lanzar alarmas, puede descartar paquetes y desconectar conexiones.

4.4.6 Dispositivos de comunicaciones para usuarios

Para proporcionar el servicio de las comunicaciones corporativas entre usuarios, se utilizan soluciones integradas de nueva generación, capaces de unificar todos los servicios como telefonía, chat, mensajería, etcétera.

El VoIP, o voz sobre protocolo de internet, es una tecnología que permite realizar llamadas telefónicas a través de la red IP. Es una alternativa al servicio telefónico tradicional, ya que ofrece una serie de ventajas, como la reducción de costes, la flexibilidad y la facilidad de uso.

En el contexto de las comunicaciones corporativas, el VoIP se utiliza cada vez más para mejorar la comunicación interna y externa de las empresas. Permite a los empleados comunicarse de forma más eficiente, ya que no tienen que depender de teléfonos fijos o móviles de ninguna compañía. También permite a las empresas comunicarse con sus clientes y proveedores de forma más económica y flexible.



Figura 4-21 - Appliance Cisco para comunicaciones corporativas

4.4.7 Componentes de Comunicaciones

Estos dispositivos de red proporcionan la conectividad necesaria entre los componentes. Pueden ser para red de tipo Ethernet o de Fibra Óptica según la capacidad y volumen de datos a proporcionar. Los elementos más comunes serían:

- Switches TOR, se despliegan en la parte superior del rack y a él van conectados todos los equipos



Figura 4-22 - Switch TOR Ethernet



Figura 4-23 - Switch TOR con SFP para Ethernet o FC

- Patch panels, que son también conocidos como panel de conexión o bahía de rutas, es una pieza de montaje de hardware con varios puertos para conectar y gestionar los cables LAN o los cables de fibra/cobre entrantes y salientes. Los paneles de conexión pueden ser bastante pequeños, con sólo unos pocos puertos, o muy grandes, con varios centenares de puertos.



Figura 4-24 - Patch Panel

- Switch director, son generalmente conmutadores con características de alta disponibilidad, como componentes redundantes y la capacidad de realizar actualizaciones de hardware y software sin tener que desconectar el dispositivo. Normalmente, los conmutadores de clase director pueden admitir una gran cantidad de puertos y arquitectura Blade.



Figura 4-25 - Switch Director Brocade X6-8

4.5 Ejemplos de racks para los servicios que se pueden cubrir en un despliegue

4.5.1 Racks para servicios de Computación y Almacenamiento

Este servicio le dará a la organización la capacidad de almacenamiento, procesamiento y tratamiento de los datos de que dispongan, así como la posibilidad de despliegue de infraestructura corporativa de propósito general como sería:

- Servicio de autenticación de usuarios
- Servicio de ficheros distribuido
- Servidores de virtualización de escritorios y aplicaciones
- Servicio de licenciamiento de escritorios y aplicaciones
- Servicio de impresión y administración de colas
- Servicio de correo electrónico
- Antivirus corporativo
- MDM para servicio de control de dispositivos móviles
- Servicio de monitorización de los sistemas

Ejemplo de racks para computación y almacenamiento, con servidores de montaje en rack [4.3.2] y cabinas de almacenamiento [4.3.3], así como switches TOR [4.4.6] para conexonado de equipos.

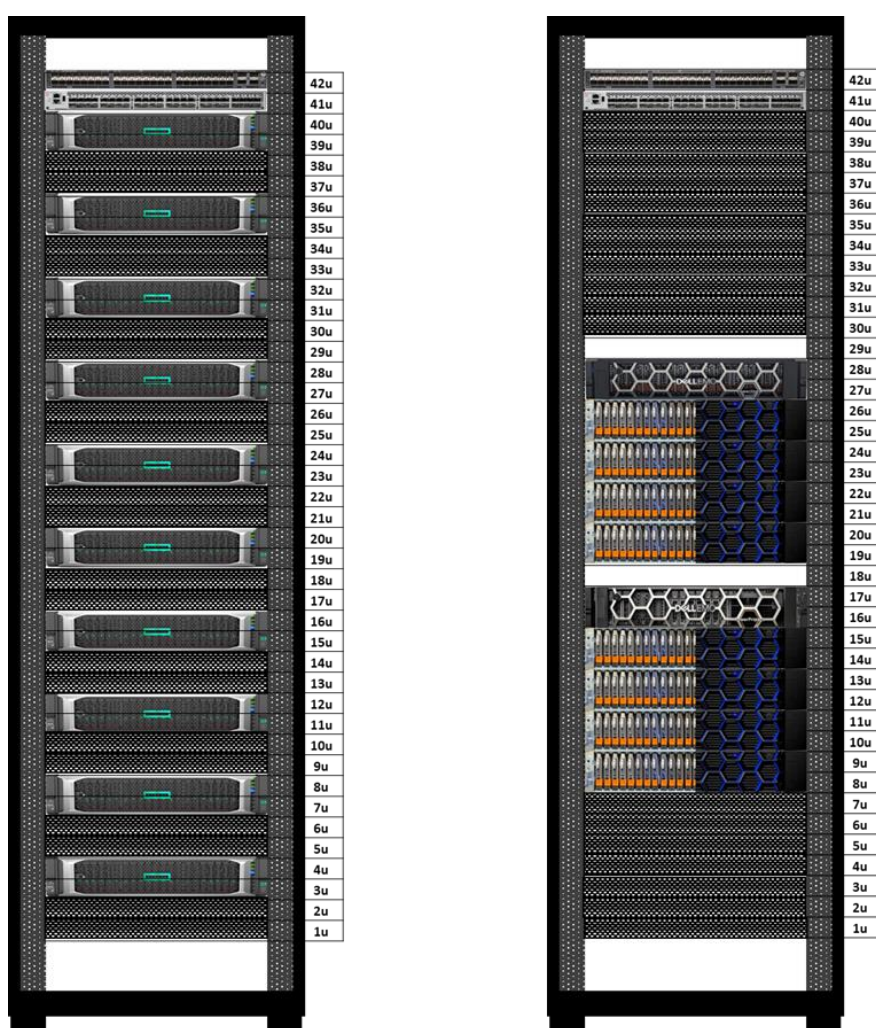


Figura 4-26 - Ejemplos de rack de cómputo (izqda.) y almacenamiento (dcha.)

4.5.2 Racks para Servicios de Seguridad y Comunicaciones

En el CPD se debe proporcionar la infraestructura necesaria para la seguridad de las comunicaciones, tal y como se ha explicado en el punto 4.4.5, a través de los firewalls se consiguen filtrar los datos y protocolos de comunicación entre equipos.

Este sería un ejemplo de un rack equipado con elementos de seguridad y de comunicaciones para usuarios, con firewalls [4.4.5] y dos appliance Cisco [4.4.6].

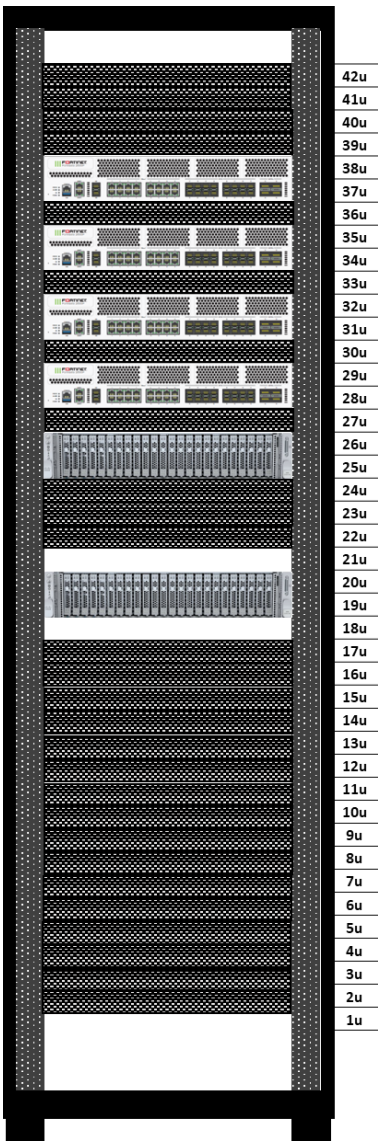


Figura 4-27 - Ejemplo de rack de comunicaciones y seguridad

4.5.3 Racks de electrónica de red y comunicaciones

Los racks de electrónica de red son de diferente tamaño a los que se despliegan para cómputo o almacenamiento que se han mostrado en anteriores puntos, ya que el equipamiento habitualmente es de mayores dimensiones y, además, permite el cableado más accesible.

Este sería un ejemplo de rack de electrónica de red, con patch panels y un switch director de fibra óptica [4.4.7].

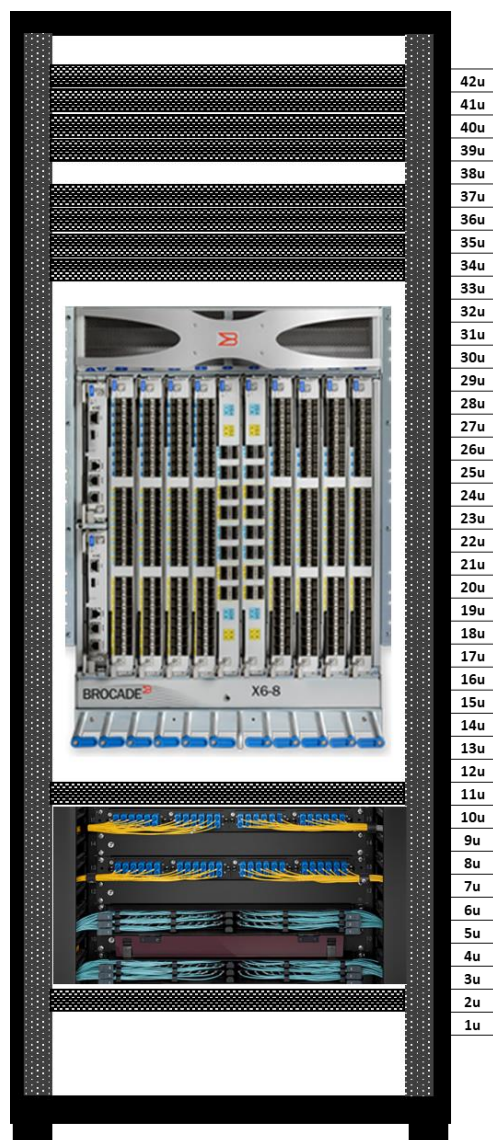


Figura 4-28 - Ejemplo de rack de electrónica de red

4.5.4 Conclusión sobre el equipamiento

Como se puede observar, estos racks deben estar correctamente dimensionados de acuerdo a la capacidad portante del suelo técnico, que en ningún caso se debe superar para evitar accidentes o posibles hundimientos del suelo.

También se debe tener en cuenta que los racks completamente equipados (sin huecos libres) pueden provocar que sea menos eficiente la ventilación, por lo que es muy importante el correcto cálculo de las necesidades.

Este equipamiento debe ser flexible para posibles ampliaciones y crecimiento, así como el espacio en los propios racks.

4.6 Toma de requisitos para un despliegue

La toma de requisitos es, probablemente, la fase más importante antes de la planificación. Una correcta toma de requisitos redundará en una infraestructura bien dimensionada, flexible y escalable.

Las necesidades se deben cubrir para proporcionar correctamente el servicio objetivo del estudio a un número de usuarios, pero es imprescindible que se dimensione pensando en posibles crecimientos, siempre teniendo en cuenta que este despliegue debe ser lo suficientemente flexible para que, ante la necesidad, se pueda ampliar la propia infraestructura dentro del contenedor actual o crecer en número de contenedores.

De manera general al abordar un proyecto, es importante analizar diversos tipos de requisitos para comprender completamente lo que se necesita y planificar adecuadamente. Estos tipos de requisitos incluyen:

- **Requisitos del negocio:** Estos requisitos se centran en los objetivos y problemas que la empresa quiere resolver con el producto. Deben estar basados en una necesidad real del usuario, sea esta conocida o no por él.
- **Requisitos funcionales:** Se relacionan con las funciones específicas que el sistema o producto debe realizar. Definen lo que el sistema debe hacer, como características, procesos y comportamientos.
- **Requisitos no funcionales:** Se centran en aspectos que no están directamente relacionados con las funciones, sino en cómo se deben llevar a cabo esas funciones. Incluyen aspectos como la seguridad, el rendimiento, la escalabilidad, la usabilidad y la disponibilidad.
- **Requisitos técnicos:** Se refieren a la tecnología, herramientas y plataformas que se utilizarán en el proyecto. Esto abarca desde el hardware y el software hasta los estándares tecnológicos y las integraciones necesarias.
- **Requisitos de cumplimiento:** Afectan a las regulaciones, estándares y normativas que el proyecto debe cumplir. Pueden incluir requisitos legales, de seguridad o de calidad.
- **Requisitos de datos:** Se centran en la gestión y el flujo de datos en el proyecto. Incluyen la definición de las fuentes de datos, la estructura de la base de datos, la migración de datos y la privacidad de los datos.
- **Requisitos de rendimiento:** Especifican los niveles de rendimiento que se deben cumplir, como tiempos de respuesta, velocidad, capacidad de carga, etc.
- **Requisitos de seguridad:** Relacionados con la protección de datos, sistemas y usuarios. Incluyen medidas de seguridad, autenticación, autorización y gestión de amenazas.
- **Requisitos de mantenimiento:** Consideran la sostenibilidad y la facilidad de mantenimiento del sistema o producto a largo plazo. Incluyen actualizaciones, parches y soporte continuo.
- **Requisitos de documentación:** Se refieren a la documentación necesaria para el proyecto, como manuales de usuario, guías de instalación y documentación técnica.
- **Requisitos de capacitación:** Especifican necesidades de capacitación para los usuarios finales y el personal relacionado con el proyecto.

Al analizar estos diferentes tipos de requisitos de manera detallada, se puede asegurar que el proyecto esté bien definido y que las expectativas estén claras para todas las partes interesadas. Esto es esencial para la planificación, ejecución y éxito del proyecto.

El diseño y la evaluación de todos los elementos que componen la infraestructura y el servicio del CPD serán la parte principal de la toma de requisitos, que incluyen, como parte más genérica:

- La ubicación y el espacio del CPD, que debe ser seguro, accesible y resistente a posibles desastres naturales o humanos. En este caso necesitaremos una ubicación menos exigente que si de una obra civil se tratara.

- La alimentación eléctrica, que debe ser estable, continua y redundante, con sistemas de respaldo como generadores o baterías. Puede haber doble acometida de dos proveedores para evitar caídas por períodos de mantenimiento.
- La refrigeración, que debe mantener una temperatura y humedad óptimas para evitar el sobrecalentamiento o la condensación de los equipos.
- El software DCIM (Data Center Infrastructure Management), que debe permitir la monitorización y el control de todos los sistemas del CPD, con sensores, alarmas y paneles de gestión.

La parte más importante y específica de la toma de requisitos se centraría en la obtención del cometido (o cometidos) principal de la infraestructura, esto es, qué tipos de servicios se deben cubrir con ella.

Esto lleva a definir de manera muy rigurosa determinados componentes:

- La computación, que debe proporcionar la memoria y la potencia de procesamiento necesarias para ejecutar las aplicaciones, con servidores, sistemas operativos y software.
- El almacenamiento, que debe preservar la integridad y la seguridad de los datos importantes, con discos duros, unidades de cinta o sistemas en la nube.
- La conectividad, que debe garantizar una velocidad y una disponibilidad adecuadas para el tráfico de datos, con cableado estructurado, routers, switches y firewalls.
- El software a desplegar, que incluirá licencias, permisos, instalaciones, paquetes y las actualizaciones y mantenimiento necesarios.

El proceso de toma de requisitos se puede automatizar a través de un formulario o aplicación, para que la organización objetivo del proyecto pueda seleccionar los diferentes servicios que necesite cubrir y esto se traslade a una plantilla estandarizada que provea de las capacidades necesarias a implementar.

Grosso modo, una toma inicial de requisitos mediante web se podría realizar con un formulario de este tipo:

Formulario para solicitud de requisitos para el diseño de un centro de procesamiento de datos	
Información general	
Nombre de la empresa:	
Dirección de la empresa:	
Teléfono de la empresa:	
Correo electrónico de la empresa:	
Requisitos del centro de procesamiento de datos	
Servicio de autenticación de usuarios:	
Tipo de autenticación:	
☐	LDAP
☐	Active Directory (AD)
☐	Security Assertion Markup Language (SAML)

Número de usuarios:

Servicio de ficheros distribuido:

Capacidad de almacenamiento:

Tipo de acceso:

- ☐ Lectura
- ☐ Escritura
- ☐ Modificación

Eliminación

Servidores de virtualización de escritorios y aplicaciones:

Número de escritorios y aplicaciones virtualizados:

Sistema operativo:

Servicio de licenciamiento de escritorios y aplicaciones:

Tipos de licencias:

- ☐ Licencias por usuario
- ☐ Licencias por máquina

Servicio de impresión y administración de colas:

Número de dispositivos de impresión:

Tipo de impresión:

- ☐ Básica
- ☐ Avanzada

Servicio de correo electrónico:

Número de usuarios:

Tipos de servicios de correo electrónico:

- ☐ POP3
- ☐ IMAP
- ☐ Exchange

Antivirus corporativo:

Tipo de protección:

- ☐ Específica para el sistema operativo
- ☐ Específica para el dispositivo

Número de dispositivos a proteger:

MDM para servicio de control de dispositivos móviles:

Número de dispositivos móviles:

Tipo de control:

- ☐ Permisos
- ☐ Restricciones
- ☐ Uso

Servicio de monitorización de los sistemas:

Tipos de sistemas a monitorizar:

- ☐ Servidores
- ☐ Aplicaciones
- ☐ Redes

Datos a recopilar:

- ☐ Estado
- ☐ Rendimiento
- ☐ Seguridad

Servicio de virtualización de escritorios:

Tipos de escritorios a virtualizar:

- ☐ Escritorios de usuario
- ☐ Escritorios de servidor

Infraestructura requerida:

- ☐ Servidores
- ☐ Almacenamiento
- ☐ Red

Servicio de almacenamiento compartido SAN:

Capacidad de almacenamiento:

Tipo de acceso:

- ☐ Lectura
- ☐ Escritura
- ☐ Modificación
- ☐ Eliminación

Servicios comunes de seguridad y comunicaciones:

Tipo de seguridad:

- ☐ Firewall
- ☐ Antivirus
- ☐ Encriptación

Tipo de comunicaciones:

- ☐ Ethernet
- ☐ Fibra óptica
- ☐ Wi-Fi

Información adicional:

Requisitos adicionales:

Un **ejemplo** podría ser el siguiente:

4.6.1 Ejemplo: Servicio de virtualización de escritorio de usuario

Para realizar la toma de requisitos de este servicio, se deben tener en cuenta los siguientes conceptos:

Alcance del servicio, que incluye los siguientes pasos:

1. Definir las necesidades.
2. Excluir expresamente lo innecesario.
3. Proyectar los objetivos.
4. Describir las actividades.
5. Analizar las capacidades.
6. Entender las limitaciones.

Número de usuarios a los cuales se les debe proporcionar el servicio.

Plazo de ejecución en el que debe estar disponible el servicio.

En el caso de este servicio, una buena toma de requisitos debe incluir:

- Qué características debe tener el puesto de trabajo de los empleados, es decir, qué sistema operativo debe ejecutar, con qué cantidad de recursos deben contar y qué herramientas se deben proporcionar.
- Número de usuarios que van a dar uso del servicio, tanto en condiciones normales como en previsión de crecimiento, tanto puntual como prevista según política (por ejemplo, si la plantilla crece un tanto por ciento anualmente).
- Versiones de las herramientas y software disponible, así como política de actualizaciones, licenciamiento etc.
- En qué horario se debe dar disponibilidad y de cuántos 9s [30] debe ser ésta, tanto en horario laboral como fuera de éste.
- Características del sistema como, por ejemplo, qué redundancia deben tener los servidores, switches y otros elementos que lo proporcionen.

Esos puntos a determinar se pueden parametrizar con formularios, para que la propia organización cliente pueda establecer las características que van a conformar la arquitectura definitiva, por ejemplo:

- El servicio se debe proporcionar para 1000 usuarios.
- Se proporcionará usando Citrix DaaS.
- El equipo virtual de escritorio debe disponer de 16GB de RAM, 4 cores y 100GB de disco duro.
- Escritorio: Microsoft Windows 11.
- Ofimática: Microsoft Office 2019.
- Herramienta Corporativa: Microsoft Dynamics 365.
- *Resto de software*
- Disponibilidad del 99% de servicio en horario de 7 a 17h.
- Disponibilidad del 90% fuera de ese horario.

Número de usuario del servicio 10 ————— 5000 2000	
Tecnología de virtualización ☐ Citrix DaaS ☐ Microsoft Azure Desktop ☐ VMWare Horizon	
Características hardware de los escritorios	
Memoria RAM (GB) 4 ————— 64 16	Observaciones: Memoria RAM 4GB: Usualmente para escritorios con operaciones de ofimática y aplicaciones de poca carga 16GB: Recomendado para escritorios con uso intensivo de aplicaciones de cálculo >32GB: Recomendado para diseño profesional, renderizado y edición de video o audio. Cores CPU Un mayor número de núcleos redundará en un rendimiento superior en aplicaciones de alta demanda de procesamiento
Cores CPU 4 ————— 32 8	
Almacenamiento de usuario (GB) 4 ————— 64 256	
Sistema Operativo del escritorio ☐ Microsoft Windows ☐ Linux	

Figura 4-29 - Ejemplo de parte del formulario de solicitud de requisitos

En base a esas características, el proveedor puede diseñar con el hardware tipo (definido en el punto 4.4), la siguiente arquitectura:

- 1 rack de 600mm y 42u para cómputo
- Al menos un rack de 800mm y 42u para comunicaciones
- 10 servidores de montaje en bastidor para servir los escritorios
- 5 servidores más para desplegar la solución Citrix
- Licencias para el software
- Componentes de comunicaciones (switches, firewalls, etc.)
- *Resto de arquitectura*

Una vez realizados estos pasos para todos los servicios y las necesidades, será posible diseñar la solución completa, llevará a un tamaño necesario de contenedor y de despliegue de los elementos dentro de éste.

4.7 Buenas prácticas del proyecto

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 la Biblioteca de Infraestructura de Tecnologías de Información ITIL [31].

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.

El trabajo de un Centro de Datos debe ser seguro y fiable. Se desea que la sala y el equipamiento que se encuentra en ella, operen sin incidencias. Tal y como nos recomienda ITIL, implementando una gestión de cambios pueden evitarse situaciones indeseadas en el servicio. Se trata de un método de planificación, coordinación y comunicación acerca de actividades que se desarrollan en torno a las instalaciones de la organización, aquellas que son imprescindibles para mantener la operación del negocio y el servicio a los clientes.

La idea es que cuando el Centro de Datos se encuentra funcionando adecuadamente, se desea limitar aquellos factores que pueden alterar su funcionamiento y controlar los que son necesarios. Cualquier

acción que pueda cambiar las condiciones en estas salas debe ser previamente comunicada a las personas a las que puede influir. Esto permite planificar la situación que se aproxima y, en caso de ser necesario, solicitar una replanificación de la actividad o incluso una cancelación de la misma.

Las buenas prácticas no sirven de mucho si una vez definidas y comunicas al personal no se realizan revisiones periódicas de su aplicación, por este motivo es recomendable realizar auditorías para valorar la aplicación de las mismas.

5 ANÁLISIS DE RIESGOS

En este capítulo se realizará un análisis de activos, amenazas y posibles riesgos de una implantación de este tipo. Como no se trata de una instalación concreta si no un estudio genérico, no se tomarán medidas de corrección, no se desarrollará un Plan de Tratamiento de Riesgos ni sus controles aplicados, que se pueden obtener según la norma ISO:27001 [32].

5.1 Identificación de activos

En este punto se listan los activos más usuales de los que dispone la una organización con un despliegue de un CPDM.

Para la clasificación de los activos se usará MAGERIT v.3 [33] y se desglosan en:

- [D] Datos / Información
- [SW] Software - Aplicaciones
- [HW] Equipamiento hardware
- [S] Servicio
- [COM] Redes de comunicaciones
- [Media] Soportes de información digital
- [L] Instalaciones

Activos	Tipo	Confidencialidad	Integridad	Disponibilidad	Total	Valor
Datos	Información	10	10	10	30	Muy Alto
Software - Aplicaciones	Información	3	5	3	11	Bajo
Equipamiento Hardware	Información	9	7	8	24	Muy Alto
Servicio	Información	5	1	7	13	Medio
Redes de Comunicaciones	Información	8	9	7	24	Muy Alto
Soportes digitales	Software	6	8	8	22	Alto
Instalaciones	Hardware	2	7	10	19	Alto

Tabla 5-1 - Inventario de activos

5.2 Valoración de activos

Según las principales dimensiones de la seguridad, que son Confidencialidad, Integridad y Disponibilidad, la valoración de los activos sería:

	Confidencialidad	Integridad	Disponibilidad
10-9	Secreta Solo puede acceder a ella por el comité de dirección.	Información de suma importancia desde el punto de vista de la veracidad, coherencia y exactitud para la organización.	La información debe recuperarse inmediatamente.
8-7	Confidencial Solo puede acceder a ella personal asignado a un proyecto concreto.	Información que debe tener alto nivel de exactitud.	Recuperación de la información en un plazo inferior a un día.
6-4	Uso restringido No puede ser divulgada entre las diferentes áreas de la organización.	Información que exige disponer de medidas que garanticen su veracidad.	Recuperación de la información en un plazo inferior a tres días.
3-2	Información de uso interno Solo puede ser divulgada dentro de la organización.	Información restringida en su actualización a cualquier persona de la organización con acceso permitido.	La información debe recuperarse en un tiempo inferior a una semana.
1-0	Información pública Puede ser consultada por personal externo a la organización.	Información cuya modificación no implica ningún riesgo y puede realizarla cualquier persona.	Se puede volver a disponer de la información en un periodo inferior a medio mes.

Tabla 5-2 – Guía de valoración de activos según las dimensiones de seguridad

En este caso para cada activo se sumarán las puntuaciones y en función de ello obtendremos un valor para cada activo.

Valor del activo		
Valor acumulado (C+I+A)	Valor cualitativo	Valor cuantitativo
De 0 a 11	Bajo	1
De 12 a 23	Medio	2
De 24 a 30	Alto	3

Tabla 5-3 - Valor de activos

5.3 Identificación y valoración de amenazas

Las amenazas a las que se expone la infraestructura. En función de las vulnerabilidades y condiciones de contorno temporales y particulares de la organización se identifican las posibles amenazas y valora la probabilidad de que estas se produzcan.

Además, se evalúan las consecuencias que, en caso de materializarse, podrían provocar esas amenazas en los activos.

Amenaza	Tipo
Pérdida de suministro eléctrico	Servicios
Fuga de información	Información
Robo de elementos	Hardware
Destrucción de información	Información
Acceso no autorizado a los SI	Información
Código malicioso	Información
Cambio involuntario de datos en un SI	Información
Suplantación de identidad	Personas
Destrucción de medios	Hardware
Fallo de comunicaciones	Servicios
Errores de usuario	Información

Tabla 5-4- Amenazas

Degradación del activo en caso de materialización de la amenaza		
Valor		Descripción
Alto	Degradación del activo $\geq 60\%$	Interrupción de los procesos de negocio
		Robo de información estratégica
		Afecta a más del 50% de los empleados
		Compromiso alto de los niveles SLA
Medio	Degradación de los activos entre 30% - 60%	Caída notable en el rendimiento de los procesos de negocio
		Robo de información confidencial
		Afecta a menos del 50% de los empleados
		Puede comprometer SLAs de clientes
Bajo	Degradación de los activos $< 30\%$	Pérdida de recursos secundarios
		Robo de información interna no publicada
		Afecta a menos del 5% de los empleados
		No compromete de ninguna manera los SLA

Tabla 5-5 - Valoración de Amenazas

5.4 Relación entre los activos y las amenazas

No todos los activos están igualmente expuestos a las amenazas. En la siguiente tabla se muestran estas relaciones:

Relación Activos / Amenazas	Pérdida de suministro eléctrico	Fuga de información	Robo de elementos	Destrucción de información	Acceso no autorizado a los SI	Código malicioso	Cambio involuntario de datos en un SI	Suplantación de identidad	Destrucción de medios	Fallo de comunicaciones	Errores de usuario
Datos	X	X	X	X	X	X	X				X
Software – Aplicaciones			X	X	X	X	X				
Equipamiento Hardware		X	X		X	X	X		X		
Servicio		X	X	X					X	X	
Redes de Comunicaciones	X	X			X	X	X			X	X
Soportes Digitales	X	X	X		X	X	X		X		X
Instalaciones	X								X		X

Tabla 5-6 - Relación entre los activos y las amenazas que los afectan

5.5 Obtención del riesgo

Una vez se disponen de los activos y amenazas más relevantes valorados, se realizará una correlación en la que se mide riesgo que provoca la unión de ambos factores.

El riesgo será por tanto la probabilidad por el impacto aplicado al valor de cada activo o servicio. Para la realización de esta parte se ha utilizado la siguiente tabla como base por cada servicio.

Probabilidad Amenaza	3	3	6	9	6	12	18	9	18	27
	2	2	4	6	4	8	12	6	12	18
	1	1	2	3	2	4	6	3	6	9
Valor del activo		1	2	3	1	2	3	1	2	3
Impacto de la amenaza		1			2			3		

Tabla 5-7 - Análisis de riesgos

Conforme a los datos obtenidos en esta tabla, se deberán realizar unas acciones concretas, que la metodología MAGERIT desglosa en:

Riesgo	Acción a realizar	
1-3	Bajo	Aceptar
4-8	Medio	Transferir
>9	Alto	Mitigar

Tabla 5-8 - Valoración de riesgos

6 BREVE CONCLUSIÓN

Los Centros de Procesamiento de Datos (CPDs) han experimentado una notable evolución en las últimas décadas, adaptándose a las cambiantes necesidades de la tecnología y las empresas. Esta evolución ha pasado por diversas etapas, desde un enfoque más centralizado hasta la actualidad, donde la consolidación y virtualización de sistemas son la norma.

En sus inicios, los CPDs eran estructuras centralizadas que albergaban servidores y equipos de procesamiento de datos en un solo lugar físico. Sin embargo, esta configuración se volvió limitada a medida que la demanda de capacidad y disponibilidad aumentaba. Como resultado, se produjo una transición hacia un enfoque más distribuido, con múltiples centros de datos repartidos geográficamente.

Hoy en día, la tendencia predominante en la gestión de CPDs es la consolidación y virtualización de sistemas. Esto implica la creación de infraestructuras altamente eficientes y escalables, donde la virtualización de servidores y almacenamiento desempeña un papel crucial. Estas tecnologías permiten a las empresas maximizar la utilización de recursos y reducir costes operativos significativamente.

Además de la virtualización, un aspecto crítico en la gestión de CPDs es la infraestructura de soporte. Esto incluye sistemas de refrigeración avanzados para mantener temperaturas óptimas, sistemas de alimentación ininterrumpida (SAIs) para garantizar la continuidad de la energía eléctrica, sistemas de detección y extinción de incendios para la seguridad y sistemas de seguridad y monitorización avanzados.

Un Centro de Procesamiento de Datos bien diseñado es fundamental para cualquier organización en la era digital. No solo garantiza la disponibilidad, continuidad y estabilidad del entorno de Tecnologías de la Información (TI), sino que también mejora la eficiencia operativa y optimiza el retorno de la inversión.

Esto se logra adoptando las mejores prácticas en diseño y gestión de CPD. Estas prácticas permiten a las organizaciones enfrentar los desafíos tecnológicos actuales y futuros de manera más efectiva. Al mantenerse al día con las tendencias tecnológicas emergentes, un CPD puede adaptarse y evolucionar, asegurando que la organización esté preparada para el futuro.

Además, un CPD bien gestionado puede proporcionar a las organizaciones una ventaja competitiva en un mundo cada vez más digitalizado. Al garantizar que los sistemas y servicios críticos estén siempre disponibles y funcionen a su máximo rendimiento, las organizaciones pueden ofrecer un mejor servicio a sus clientes, mejorar su productividad y, en última instancia, impulsar el crecimiento del negocio.

Por lo tanto, invertir en el diseño y gestión de un CPD es una decisión estratégica que puede tener un impacto significativo en el éxito a largo plazo de una organización.

7 FUTURAS LÍNEAS DE TRABAJO

Como posibles ampliaciones a desarrollar para mejorar este TFM, se podría contar con las siguientes líneas de trabajo.

7.1 Diseño de un grupo electrógeno auxiliar contenerizado

Una posible mejora a este TFM sería desarrollar de manera paralela un grupo que pueda proporcionar suministro eléctrico temporal de emergencia para una posible situación de corte por parte del distribuidor, que se ubicase en un punto cercano a la ubicación de este CPDM.

Un grupo electrógeno es un dispositivo compacto y autónomo que genera energía eléctrica. Funciona generalmente con un motor de combustión interna, como gasolina o diésel, que acciona un generador eléctrico. Estos grupos electrógenos son diseñados para ser transportados y utilizados en lugares donde la energía eléctrica no está disponible. Son una fuente confiable de electricidad de respaldo y pueden alimentar equipos y dispositivos esenciales. Su ubicación dentro de una estructura tipo contenedor como las que se han explicado anteriormente facilitaría su transporte y despliegue.

7.2 Toma de requisitos mediante Inteligencia Artificial

Mediante un intérprete tipo chatbot de Inteligencia Artificial, al estilo de los existentes actualmente (ChatGPT⁵, Google Bard⁶, Microsoft Bing AI⁷), se podría realizar una toma previa de requisitos redactada de manera ligera, para que se pudiese realizar un perfilado previo de la arquitectura necesaria.

Posteriormente se puede mejorar la predicción ya ajustando modelos de equipos, datos más concretos u otros datos, integrando la toma de requisitos con algún modelo semántico que nos relacionase necesidades con capacidades propuestas por fabricantes.

El uso de un intérprete de chatbot simplifica la recopilación de información al permitir a los usuarios proporcionar detalles de manera más accesible. Sin embargo, es fundamental que este proceso sea respaldado por un equipo de TI experimentado que pueda analizar los datos recopilados y traducirlos en soluciones técnicas efectivas para el CPD. La colaboración entre el chatbot y expertos es esencial para garantizar que los requisitos se capturen de manera adecuada y se traduzcan en una infraestructura de CPD óptima.

7.3 Diseño de un proyecto de CPD Modular desplegable para el Ejército

El diseño del Centro de Procesamiento de Datos Modular Desplegable para el Ejército busca proporcionar una solución eficiente y adaptable a necesidades operativas. El proyecto se centraría en la creación de una infraestructura tecnológica que pueda transportarse y desplegarse rápidamente en diferentes entornos, garantizando la continuidad de las operaciones.

Se incorporan módulos interconectados que albergan equipos de última generación, asegurando la capacidad de procesamiento, almacenamiento y comunicación necesaria. La seguridad y la resistencia son elementos clave, integrando medidas para proteger la información sensible y resistir condiciones adversas. Además, se contempla la eficiencia energética y la sostenibilidad en el diseño.

La modularidad facilita futuras expansiones y actualizaciones. Este enfoque estratégico busca mejorar la agilidad y capacidad de respuesta del Ejército ante desafíos tecnológicos en zona de despliegue.

⁵ <https://chat.openai.com/>

⁶ <https://bard.google.com/>

⁷ <https://www.bing.com/?/ai>

8 BIBLIOGRAFÍA

- [1] «CPD,» [En línea]. Available: https://es.wikipedia.org/wiki/Centro_de_procesamiento_de_datos. [Último acceso: 17 agosto 2023].
- [2] RAE, «RAE,» [En línea]. Available: <https://www.rae.es/drae2001/inform%C3%A1tica>. [Último acceso: 13 09 2023].
- [3] Wikipedia, «VoIP,» [En línea]. Available: https://es.wikipedia.org/wiki/Voz_sobre_protocolo_de_internet. [Último acceso: 18 8 2023].
- [4] «Virtualización,» [En línea]. Available: <https://www.ibm.com/es-topics/virtualization>. [Último acceso: 18 8 2023].
- [5] Wikipedia, «Wikipedia - ENIAC,» [En línea]. Available: <https://es.wikipedia.org/wiki/ENIAC>. [Último acceso: 29 12 2023].
- [6] «Wikipedia,» [En línea]. Available: <https://en.wikipedia.org/wiki/TRADIC>. [Último acceso: 22 08 2023].
- [7] J. M. Bravo, «uhu,» [En línea]. Available: <http://www.uhu.es/josem.bravo/AD/Tema3.pdf>. [Último acceso: 22 08 2023].
- [8] F. M. Hoffman y W. W. Hargrove, «climatemodeling,» [En línea]. Available: <https://www.climatemodeling.org/~forrest/osdj-2000-11/>. [Último acceso: 22 08 2023].
- [9] J. Roach, «Microsoft News,» [En línea]. Available: <https://news.microsoft.com/es-xl/features/microsoft-descubre-que-los-centros-de-datos-submarinos-son-confiables-practicos-y-utilizan-energia-sustentable/>. [Último acceso: 22 08 2023].
- [10] Vertiv, «UNDERSTANDING THE COST OF DATA CENTER DOWNTIME: An Analysis of the Financial Impact on Infrastructure Vulnerability,» 2011.
- [11] U. Institute, «Uptime Institute - Sistema de clasificación Tier,» [En línea]. Available: <https://es.uptimeinstitute.com/tiers>. [Último acceso: 21 08 2023].
- [12] U. AENOR, «UNE-EN 50600-1:2019,» [En línea]. Available: <https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0062011>. [Último acceso: 21 08 2023].
- [13] TIA, «TIA-942-C,» [En línea]. Available: <https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/>. [Último acceso: 21 08 2023].
- [14] S. H. Group, «Wiley Online Library,» [En línea]. Available: <https://onlinelibrary.wiley.com/doi/pdf/10.1002/9780470089040.app3>. [Último acceso: 21 08 2023].
- [15] BICSI, «bicsi.org,» [En línea]. Available: <https://www.bicsi.org/docs/default-source/publications/002-2019-preview.pdf>; https://www.bicsi.org/docs/default-source/publications/002-2019-methodology.pdf?sfvrsn=5c4f65b5_2. [Último acceso: 21 08 2023].

- [16] E. Press, «Europa Press,» [En línea]. Available: <https://www.europapress.es/ciencia/cambio-climatico/noticia-tic-emiten-mas-gases-efecto-invernadero-aviacion-20210910173106.html>. [Último acceso: 22 08 2023].
- [17] BOE, «BOE.es - REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO,» [En línea]. Available: <https://www.boe.es/doue/2016/119/L00001-00088.pdf>. [Último acceso: 22 10 2023].
- [18] M. y. A. U. MITMA (Ministerio de Transportes, «mitma.gob.es,» [En línea]. Available: https://cdn.mitma.gob.es/portal-web-drupal/OTLE/elementos_otle/Informe_anual_2021.pdf. [Último acceso: 22 08 2023].
- [19] ISO.org, «ISO 668:2020,» [En línea]. Available: <https://www.iso.org/standard/76912.html>. [Último acceso: 09 10 2023].
- [20] ISO.org, «iTeh Standards,» [En línea]. Available: <https://cdn.standards.iteh.ai/samples/76912/7354663676144f8ab1a7b57cb573b0a6/ISO-668-2020.pdf>. [Último acceso: 09 10 2023].
- [21] U. AENOR, «UNE-EN 12825:2002,» [En línea]. Available: <https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0026213>. [Último acceso: 10 09 2023].
- [22] Wikipedia, «Uninterruptible power supply,» [En línea]. Available: https://en.wikipedia.org/wiki/Uninterruptible_power_supply. [Último acceso: 26 09 2023].
- [23] I. Gómez-Cornejo, «ASHREA Español,» [En línea]. Available: <https://spain-ashrae.org/wp-content/uploads/CLIMATIZACI%C3%93N-Y-EFICIENCIA-ENERG%C3%89TICA-EN-LA-INDUSTRIA-CPD.pdf>. [Último acceso: 26 09 2023].
- [24] J. L. V. Muñoz, «insst: NTP 40: Detección de incendios,» [En línea]. Available: https://www.insst.es/documents/94886/326853/ntp_040.pdf/9ba14077-7121-415a-a6e9-d8c9f2a4031c. [Último acceso: 26 09 2023].
- [25] Wikipedia, «19-inch rack,» [En línea]. Available: https://en.wikipedia.org/wiki/19-inch_rack. [Último acceso: 26 09 2023].
- [26] U. AENOR, «UNE 20539-2:1996,» [En línea]. Available: <https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0001343>. [Último acceso: 23 08 2023].
- [27] Rittal, «Rittal: NEMA,» [En línea]. Available: https://www.rittal.com/es-es/content/es/support/technischeswissen/qminformiert/schutzarten/nema/nema_1.jsp. [Último acceso: 26 09 2023].
- [28] VMWare, «Almacenamiento en red,» [En línea]. Available: <https://docs.vmware.com/es/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-E3B77DE4-7525-47D3-B2D7-BC71CCD7992D.html>. [Último acceso: 26 09 2023].
- [29] VMWare, «Red de Almacenamiento (SAN),» [En línea]. Available: <https://www.vmware.com/es/topics/glossary/content/storage-area-network-san.html>. [Último acceso: 26 09 2023].

- [30] INCIBE, «¿Qué son y para qué sirven los SIEM, IDS e IPS?,» [En línea]. Available: <https://www.incibe.es/empresas/blog/son-y-sirven-los-siem-ids-e-ips>. [Último acceso: 22 10 2023].
- [31] Wikipedia, «Alta disponibilidad - Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/Alta_disponibilidad. [Último acceso: 09 11 2023].
- [32] Wikipedia, «ITIL,» [En línea]. Available: https://es.wikipedia.org/wiki/Information_Technology_Infrastructure_Library. [Último acceso: 04 10 2023].
- [33] ISO27001.es, «Norma ISO 27001,» [En línea]. Available: <https://normaiso27001.es/>. [Último acceso: 04 10 2023].
- [34] MINHAP, «Portal de Administración Electrónica,» [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html. [Último acceso: 04 10 2023].
- [35] CCN-CERT, «Guías STIC CCN,» [En línea]. Available: <https://www.ccn-cert.cni.es/es/guias.html>. [Último acceso: 06 11 2023].

ANEXO I: ACRÓNIMOS UTILIZADOS

Aunque se ha tratado de indicar el significado de cada acrónimo utilizado a lo largo de este TFM, se procederá a exponer de manera centralizada todos aquellos que se han usado.

BAAS: Salvaguarda como Servicio - Backup as a Service

BPAAS: Procesos de Negocio como Servicio - Business Process as a Service

Citrix DaaS: Citrix Desktop as a Service – Servicio de despliegue de escritorios virtuales

CPD: Centro de Procesamiento de Datos

CPDM: Centro de Procesamiento de Datos Modular

CPU: Unidad Central de Procesamiento - Central Processing Unit

CRM: Customer Relationship Management - Gestor de Relaciones de Clientes

DCIE: Eficiencia de la Infraestructura del Centro de Datos - Data Center Infrastructure Efficiency

ERP: Enterprise Resource Planning - Software de Sistema de Planificación de Recursos Empresariales

FC: Fibra Óptica - Fiber Channel

IA: Inteligencia Artificial

IAAS: Infraestructura como Servicio - Infrastructure as a Service

IDS: Sistema de Detección de Intrusiones - Intrusion Detection System

IOT: Internet de las Cosas - Internet of Things

IPS: Sistema de Prevención de Intrusiones - Intrusion Prevention System

ISCSI: Interfaz de Sistema para Pequeñas Computadoras - Internet Small Computer System Interface

ISO: International Standards Organization

LIDAR: Detección y Medición por láser - Light Detection and Ranging o Laser Imaging Detection and Ranging

LRQA: Lloyd's Register Quality Assurance

ML: Aprendizaje automatizado - Machine Learning

MTBF: Tiempo Medio entre Fallos - Mean Time Between Failures

MTTF: Tiempo Medio hasta el Fallo - Mean Time To Failure

MTTR: Tiempo Medio de Reparación - Mean Time To Repair

NAS: Almacenamiento Conectado en Red - Network Attached Storage

PAAS: Plataforma como Servicio - Platform as a Service

PUE: Eficiencia de Uso de Potencia - Power Usage Effectiveness

RAE: Real Academia Española

SAAS: Software como Servicio - Software as a Service

SAI: Sistema de Alimentación Ininterrumpida

SAN: Red de Área de Almacenamiento - Storage Area Network

SECAAS: Seguridad como Servicio - Security as a Service

SIEM: Gestor de Eventos y Seguridad - Security Information and Event Management

TOR: Top of Rack

UNE: Una Norma Española

VDI: Infraestructura de Escritorios Virtuales - Virtual Desktop Infrastructure

VoIP: Voz sobre Protocolo IP – Voice over IP

WWW: World Wide Web