ESTUDIO DE SOLUCIONES DE INFRAESTRUCTURA DE NUBE PRIVADA PARA PEQUEÑAS EMPRESAS

Francisco Javier Couñago Magariños

Grado en ingeniería Informática

Área: Administración de redes y Sistemas Operativos

Tutor: Joaquin Lopez Sanchez-Montañes

14/06/2023

FICHA DEL TRABAJO FINAL

Título del trabajo:	*ESTUDIO DE SOLUCIONES DE INFRAESTRUCTURA DE NUBE PRIVADA PARA PEQUEÑAS EMPRESAS*
Nombre del autor:	*Francisco Javier Couñago Magariño*
Nombre del consultor/a:	*Joaquin Lopez Sanchez-Montañes*
Nombre del PRA:	*David Bañeres Besora,* *Montse Serra Vizern*
Fecha de entrega (mm/aaaa):	06/2023
Titulación:	*Grado de Ingeniería informática*
Área del Trabajo Final:	*Administración de redes y sistemas operativos*
Idioma del trabajo:	*Español*
Palabras clave	*Nube privada, PYME, infraestructura, CPD*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados y conclusiones del trabajo.*

Este documento tiene como finalidad encontrar una solución que cubra las necesidades de aquellas empresas de dimensiones pequeñas que no están preparadas para introducir los nuevos modelos basados en sistemas de nube pública. Empresas que, por lo tanto, carecen de las ventajas que estos sistemas pueden aportar al desarrollo de su actividad.

Contextualizándose en el ámbito de las PYME e incluso de las micro PYME, este documento va a desarrollar una serie de alternativas que permitan a dichas empresas implantar nubes privadas adaptadas a sus necesidades tanto tecnológicas como financieras.

Teniendo en cuenta esto, se ha optado por crear cuatro niveles tecnológicos diferentes basados en una mayor o menor complejidad del sistema a implementar. Así pues, partiendo del Nivel 0, o básico, la complejidad tecnológica se va incrementando hasta llegar al Nivel 4, siendo éste el nivel más costoso de implementar no sólo tecnológica sino también financieramente.

Como resultado del desarrollo de los diferentes niveles se obtiene un catálogo progresivo de soluciones que las pequeñas empresas pueden escoger para paliar sus carencias tecnológicas y optar a los beneficios que la nube ofrece.

En conclusión, este documento ofrece una visión tecnológica de la implantación de la nube privada que al estar diseñada de manera incremental permite al usuario decidir en base a sus necesidades actuales e incluso sentar las bases para aumentar en un futuro, en caso de necesidad, las propiedades del sistema escogido.

Abstract (in English, 250 words or less):

The purpose of this document is to find a solution meeting the needs of the small companies which are not prepared to introduce new models based on public cloud systems. Companies that, consequently, lack the advantages that these systems can bring to the development of their activity.

Contextualizing in the field of SMEs and even micro-SMEs, this document will develop a series of alternatives allowing those companies to implement private clouds adapted to their technological and financial needs.

Taking this into account, it has been decided to create four different technological levels based on the greater or lesser complexity of the system implementation. Thus, starting from Level 0, basic, the technological complexity increases until reaching Level 4, being this the most expensive to implement, not only technologically but also financially level.

In conclusion, this document offers a technological view of the implementation of the private cloud which, being designed incrementally, allows the user to take a decision based on their current needs and even to lay the foundations for a future increase of the properties of the chosen system if it was necessary.

Contenido

1. Introducción

1.1 Contexto y justificación del Trabajo

En el tejido empresarial actual de nuestro entorno hay muchas empresas, sobre todo de dimensiones pequeñas (micro PYME[1] e incluso PYME) que no están preparadas para su inmersión en los nuevos modelos basados en sistemas de nube pública.

Se explicará a lo largo del presente trabajo de fin de grado (en adelante, TFG) diversas soluciones que puedan dar cabida a una disponibilidad y garantías de seguridad que cumplan los acuerdos de nivel de servicio[1] (en adelante, ANS) requeridos por este modelo de empresas.

La idea es partir de un modelo básico con el menor coste posible, que permita una correcta gestión de copias de seguridad en entornos virtualizados[1], y escalar hacía mayores compromisos de ANS, lo que va a implicar un mayor coste.

Al final del proyecto se obtendrá un catálogo de soluciones donde, a partir de unos ANS determinados, se podrá optar por una infraestructura en local (*on premise*) para que cada empresa pueda escoger la solución que más le convenga, y escalar al siguiente nivel a medida que se necesite.

1.2 Objetivos del Trabajo

El objetivo principal es conseguir un catálogo de soluciones de implantación de nubes privadas para pequeñas empresas que permita, partiendo de la solución básica, ir adaptando sus necesidades tecnológicas a un grado de disponibilidad lo más óptimo y ajustado posible en costes teniendo en cuenta las características de su negocio.

A lo largo de este proyecto se van a determinar diferentes modelos de infraestructura predefinidos que crecerán en disponibilidad, tiempos de recuperación, seguridad, etc. Cada uno de estos modelos puede considerarse un objetivo parcial, que puede ser aplicado al negocio que se desee. Estos objetivos parciales a su vez, podrán ir subdivididos en unidades determinadas, que pueden ser independientes, de tal forma que la empresa pueda seleccionar los puntos que más le interese implantar.

Se definirán como objetivos parciales:

- Nivel 0: sistema básico virtualizado con software de negocio.
- Nivel 1: acceso remoto seguro y seguridad perimetral.
- Nivel 2: mejorando las copias de seguridad.

[1] Véase glosario

- Nivel 3: aumentando la disponibilidad
- Nivel 4: medidas de seguridad físicas. Mini CPD[2]

En todos estos niveles se pretende ofrecer soluciones de distinta índole, en las cuales la empresa pueda obtener todos los elementos para generar presupuestos a través de sus proveedores habituales. En cada nivel se darán opciones de posibles configuraciones. Por lo general, no se especificará una cuantía de inversión monetaria, puesto que, el criterio a tener en cuenta es a mayor disponibilidad, mayor precio.

Con las soluciones y niveles estimados la empresa podrá libremente escoger que es lo que quiere abarcar y con ello, consultar en el mercado y determinar, de manera actualizada, el orden de magnitud del posible presupuesto.

1.3 Enfoque y método seguido

El desarrollo de este proyecto se ha llevado a cabo mediante una metodología de refinamiento en espiral, partiendo de unas secciones básicas y perfeccionándolas a lo largo del tiempo.

Aunque la definición de las tareas del proyecto y la planificación es relativamente estricta, con principio y final estipulado, ello no impide que necesariamente en cada tarea o grupo de tareas se aplique una metodología de refinamiento sucesivo, por lo que se han incluido tareas de repaso para acometer las mejoras pertinentes.

En cuanto a la metodología empleada para la investigación, se ha utilizado la experiencia propia de más de veinte años en el sector de sistemas y comunicaciones, diseñando diversos tipos de soluciones entre las que no pueden faltar los sistemas de virtualización, desde pequeños proyectos como los que aquí se atañen hasta otros más grandes con servidores diversificados en varios centros de procesos de datos. También se han comentado ciertos aspectos con otros expertos del sector y se ha realizado una investigación bibliográfica complementaria, basada mayoritariamente en recursos digitales.

1.4 Planificación del Trabajo

Para la planificación del trabajo se ha utilizado la estructura propia del TFG que marca sus fases de desarrollo y el tiempo disponible, basado en la disponibilidad de días (calendario) y horas de las que se pueda disponer en dichos días. A partir de estos datos se ha realizado la planificación mostrada a continuación y que conforma la planificación base del proyecto.

[2] Véase glosario

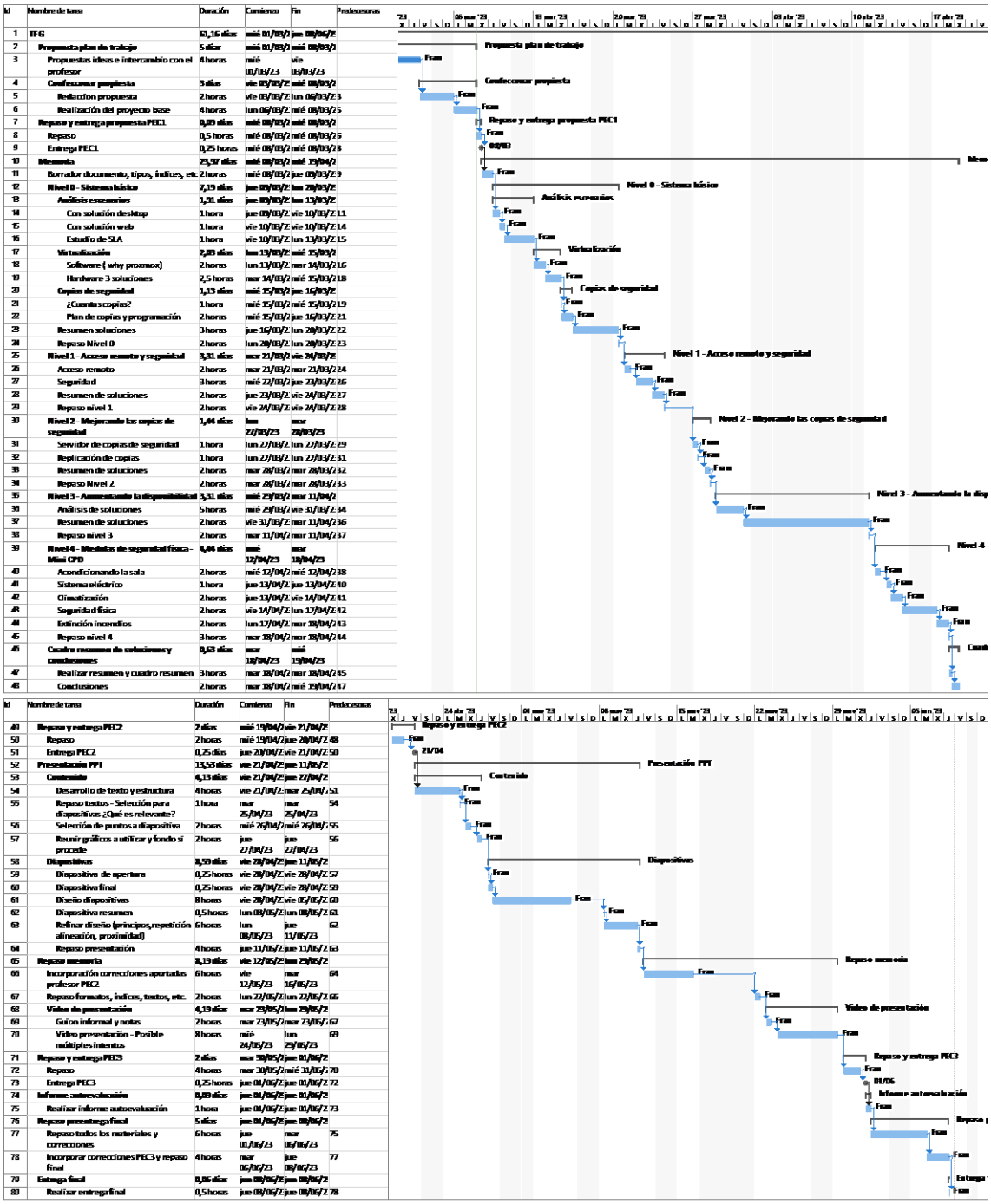

Ilustración *1*: Diagrama de planificación. Fuente: Propia

1.5 Breve sumario de soluciones

Al final de este TFG se dispondrá de un modelo de distintas soluciones que permitirá a las pequeñas empresas tener su propia nube privada con el nivel de disponibilidad que necesiten. Las soluciones abarcan desde el sistema virtualizado más básico con un simple equipo virtual y un sistema de gestión empresarial, hasta un sistema que podría cumplir una clasificación Tier[3] II en base a la norma TIA 942 [1], aplicando todas las

[3] Véase glosario

medidas de redundancia podría llegarse a un Tier III.

1.6 Breve descripción de los otros capítulos de la memoria

Este TFG está estructurado en cinco capítulos principales, uno para cada nivel de evolución de la infraestructura

- Nivel 0: se compondrá de un sistema básico de virtualización del software empresarial con copias de seguridad en local y disponibilidad basada en un solo equipo con restauración de copias en caso de desastre.

- Nivel 1: abarca el acceso remoto a la solución y aseguramiento del acceso tanto desde el exterior como hacía este.

- Nivel 2: añade una solución basada en servidor de copias y replicación de estas hacía ubicaciones remotas.

- Nivel 3: analiza soluciones de redundancia que permiten aumentar la disponibilidad del sistema tanto de forma local, como de forma remota.

- Nivel 4: describe la parte de aseguramiento físico de las instalaciones, permitiendo alcanzar como mínimo un nivel Tier II de la norma TIA-942.

2. Nivel 0: Sistema básico

2.1 Análisis de escenarios

En el mundo de las pequeñas y medianas empresas (PYME), en especial de las no tecnológicas, desde pequeños autónomos hasta empresas de varios cientos de trabajadores, las soluciones informáticas suelen estar formadas por un programa de gestión empresarial tipo ERP[4], alguna herramienta CRM[4] y a veces, otras herramientas de gestión específica.

Se abordará la posibilidad de trasladar todos estos elementos a una nube privada[4] en un entorno virtualizado. La realidad es que los métodos de migración son siempre los mismos independientemente del software, pudiendo tener una o varias máquinas virtuales según las necesidades.

Este caso se centrará en escenarios con una sola máquina virtual, pues la extrapolación a varías maquinas no supone mayor complejidad añadida.

Debe tenerse en cuenta que en muchas pequeñas industrias se trabajan con aplicaciones con necesidades de hardware específicas, por ejemplo aplicaciones CAD[4]. Las soluciones que se abordarán se refieren más a la parte de gestión que a la de producción, estas soluciones podrían aplicarse también a estas otras herramientas, pero no pueden abordarse a través de un planteamiento genérico debido a sus necesidades de hardware y parametrización específicas (por ejemplo, tarjetas gráficas dedicadas).

Existen básicamente dos enfoques en el mundo del software de gestión empresarial: aplicaciones basadas en escritorio y aplicaciones basadas en web.

A la hora de llevar ambas soluciones a un entorno virtualizado debe tenerse en cuenta las peculiaridades de cada una, de esta forma, una herramienta vía web normalmente utiliza un navegador web con un cliente compatible con la solución, sin embargo, una solución basada en escritorio requiere un cliente de escritorio remoto y permitir que el equipo donde esté la solución permita varias sesiones de escritorio remoto simultáneas. Los sistemas de acceso remoto se estudiarán en la sección 3.1 Acceso remoto.

Acuerdos de nivel de servicio

En cualquier solución se debe tener muy claro cuáles son los acuerdos de nivel de servicio (ANS) que vienen determinados por los requerimientos de disponibilidad de la empresa, entre otros factores.

[4] Véase glosario

Lo más importante para determinar los ANS es la sinceridad a la hora de saber cuál es la necesidad de disponibilidad real. Sirva como ejemplo:

Un pequeño taller de aluminio que fabrica ventanas para particulares se puede permitir el riesgo de tener una caída de servicio de uno o varios días, que afecte al departamento administrativo ya que no afecta a su actividad principal. Sin embargo, una pequeña agencia de paquetería que trabaja bajo demanda todo el día no puede permitirse una caída de servicio de un día porque afectaría directamente a su negocio (actividad empresarial principal).

Hay que tener en cuenta cuál es el ANS tácito de la empresa con sus clientes ya que éste determinará fácilmente cuál es el tiempo de disponibilidad que debe ofrecer nuestro sistema.

2.2 Virtualización del entorno

Software de virtualización

Inicialmente se debe asumir que el presupuesto de informática de las pequeñas empresas suele ser limitado, por eso se presentará sólo en una herramienta bajo licencia GNU *Affero General Public License*[5], que permita cubrir las necesidades de cualquier empresa. Así pues, se ha escogido Proxmox Virtual Enviroment (Proxmox VE) [2]. Aunque lo recomendable es adquirir una suscripción que permita el acceso al repositorio *Enterprise*[6], a través de la experiencia de los últimos años en pequeñas empresas, se ha contrastado que el repositorio de no suscripción es perfectamente estable para su uso en entornos empresariales que no tengan unas necesidades de acuerdos de nivel de servicio (ANS) críticos.

Los productos de Proxmox cubren todas las necesidades que pueda tener una pequeña empresa para su sistema de virtualización. Es una herramienta que tiene limitaciones y, si la empresa crece mucho, se podría llegar a necesitar otro producto más avanzada, pero esto mismo es lo que lo hace ideal para una herramienta del público objeto de este TFG, es decir, pequeñas empresas con potencial de crecimiento o no.

Los procesos de virtualización de servidores físicos a Proxmox están perfectamente documentados en su sitio web[7] [3]. Ambos procedimientos vía imagen de disco o vía la herramienta VMware Converter se han utilizado con éxito.

[5] GNU Affero General Public License - GNU Project - Free Software Foundation - https://www.gnu.org/licenses/agpl-3.0.en.html
[6] Véase Package Repositories en [8]
[7] Migration of servers to Proxmox VE - Proxmox VE : https://pve.proxmox.com/wiki/Migration_of_servers_to_Proxmox_VE

Hardware

Debe tenerse en cuenta que el hardware es un punto crítico de fallo[8] (o punto único de fallo, SPOF, del íngles *single point of failure*) a la hora de calcular la disponibilidad del sistema. Teniendo en cuenta que en este nivel 0 se aborda del equipamiento básico con un solo servidor de virtualización, se pueden ofrecer tres modelos de hardware de mayor a menor coste económico y de mayor a menor disponibilidad:

1) Hardware con elementos más propensos a fallos redundados, equipo con dos fuentes de alimentación y discos en RAID[8] 1 o 5, a ser posible con *hot spare*[¡Error! Marcador no definido.] con soporte *in situ* ligado a un ANS que garantice la correcta resolución del problema en un tiempo determinado.

2) Hardware con elementos más propensos a fallos redundados o sólo con algunos (por ejemplo, RAID, pero no fuentes de alimentación) sin soporte *in situ* ni ANS.

3) Hardware sin elementos redundados

Un detalle importante para abaratar costos es la obligatoriedad de utilizar ciertos componentes por parte del contrato de mantenimiento del equipo. Por ejemplo, en un equipo con mantenimiento de fabricante *in situ* se obligada a utilizar componentes estándar del fabricante, pero en equipos sin mantenimiento de este se puede, por ejemplo, comprar discos empresariales SSD sin ser los del fabricante del equipo, estos discos funcionan igual en el equipo y son mucho más económicos, aunque no es una práctica recomendada por parte del fabricante.

Otra opción para conseguir un buen equipo de un fabricante reconocido es hacerlo en el mercado de segunda mano. Hay varios proveedores que venden equipos de este tipo retirados de empresas a las que se les quedaron pequeños, pero que sobrepasan los requisitos necesarios en cuanto a prestaciones para muchas PYME. Invirtiendo en discos SSD, muchos de estos equipos pueden proporcionar años de servicio.

Dimensionamiento del hardware

En cuanto al dimensionamiento del hardware, puede ser bastante complejo dependiendo del tipo de aplicación. En el caso de aplicaciones web estos requisitos vienen marcados por el propio fabricante de la solución y son sencillos de determinar. Para aplicaciones de escritorio, puede ser un poco más complejo, pero aun así pueden determinarse sin mucha dificultad. En cualquier caso, si el uso del equipo es como el de escritorio remoto ofimático se pueden usar las reglas de dimensionamiento para uso medio propuestas por Microsoft

[8] Véase glosario

en las directrices de ajustes para Azure [4].

Con estas recomendaciones, realmente se tendrán las necesidades de hardware de nuestras máquinas virtuales que se trasladaran a nivel físico y se les añadirá, en la medida de lo posible, un 20% adicional para reserva, de los cuales una pequeña parte consumirá el propio Proxmox VE.

Recomendaciones

Tras larga experiencia durante años de entorno ofimático y virtualización lo que se concluye es que, en la mayoría de los casos la capacidad de proceso siempre permanece holgada y lo que suele estar más ajustado es la capacidad de memoria RAM, por eso se recomienda no ajustar este parámetro sino dimensionarlo con holgura o incluso sobredimensionarlo si es posible.

En la medida de lo posible se utilizarán siempre discos SSD[9], y si es viable económicamente de la gama empresarial.

Máquinas virtuales

A la hora de dimensionar el hardware de las máquinas virtuales, además de seguir, si las hubiese, las mejores prácticas recomendadas en la Wiki de Proxmox para el sistema operativo que se va a utilizar, se recomienda también lo siguiente:

- Si los discos son SSD, activar la emulación de disco SSD en la máquina.
- En equipos multiprocesador (con varios sockets), si es posible no sobrepasar el número de vCPU[10] que quepan en un sólo procesador y activar NUMA[10]. El número de vCPU corresponde con el número máximo de subprocesos del procesador, de todas formas, en la pestaña de *Summary* de nuestro host nos lo muestra.

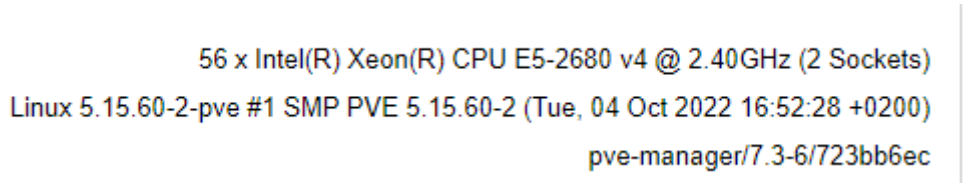

Ilustración 2: Captura del hardware de procesador de una PYME. Fuente: propia

Con la activación de NUMA, proxmox intentará siempre mantener las vCPU de las máquinas en un mismo procesador físico. Para optener el numero de vCPU

[9] Véase glosario
[10] Véase glosario

máximas disponibles, basta con dividir el número de procesadores que nos sale en la pantalla de summary entre el número de sockets, por ejemplo, en el caso de la Ilustración 2 serían 28 vCPU (56 procesadores / 2 sockets).

- Instalar los drivers VirtIO[10] y el QEMU[10] Gest Agent

2.3 Copias de seguridad

Proxmox VE viene con una sencilla herramienta que permite gestionar las copias y guardarlas en un almacenamiento, interno o externo, o en un servidor de copias Proxmox Backup Server. El proceso de copias está perfectamente documentado en la documentación del producto[11].

Conviene tener en cuenta que, las máquinas virtuales con sistema operativo deben tener correctamente instalado el agente QEMU-guest-agent para que la copia se realice de la forma más consistente posible, ya que éste es el encargado de informar al sistema operativo que "congele" (*freeze*) el sistema de ficheros (en caso de sistemas Windows a través de los servicios *Volume Shadow Copy* (VSS)

En caso de que la disponibilidad del servicio nos permita parar la máquina virtual para realizar la copia se recomienda el modo de copia *Stop* que proporciona la copia de seguridad más consistente.

¿Cuántas copias?

La respuesta a cuántas copias viene determinada básicamente por tres parámetros:

- Copias en base a regulación legal aplicable: estas son relativas al número de copias que se deben mantener para cumplir con la legislación vigente en caso de auditorías o inspecciones. Por ejemplo, en el caso del tratamiento de datos personales se deben tener un mínimo de una semana de copias [5]. El código de comercio en su artículo 30 establece 6 años [6], para algunos documentos. La ley general tributaria establece un plazo de prescripción de 4 años (art.66 LGT) siempre y cuando no haya intervenciones por parte de la administración (art.68) [7].

- Copias en base a información que se esté dispuesto a perder en caso de un incidente grave o desastre. Esto marca sobre todo el período de tiempo de copia ya que, no es lo mismo volver a introducir los datos de un día de trabajo que de una semana. Hay que tener en cuenta que se está hablando de un incidente que obligue a recuperar del sistema de copias de Proxmox, lo cual no impide tener por ejemplo otras copias a nivel de aplicación por otros medios.

[11] Backup and Restore - Proxmox VE de [8]: https://pve.proxmox.com/wiki/Backup_and_Restore

- Copias para poder seguir la trazabilidad de algún proceso, sino se dispone de otro medio, por ejemplo, la evolución de histórico de documentos en caso de, por ejemplo, no tener un sistema de gestor documental que nos permita realizarla.

Una solución que normalmente abarca todas las medidas legales es la de copias anuales de los últimos 6 años, copias mensuales del último año, copias semanales del último mes y copias diarias de los últimos 7 a 14 días.

En el caso de las copias de larga conservación, la recomendación es llevarlas a un soporte que permita almacenarlas a más largo plazo de costo inferior, tipo cinta LTO[12] o similar.

2.4 Resumen de soluciones

En este nivel 0, además de realizar una breve disertación sobre como determinar algunos parámetros de nuestro sistema, se ha seleccionado una sola solución de virtualización con tres posibles escenarios *hardware*:

Hardware con elementos redundados y soporte *in situ* según ANS	
Disponibilidad	ALTA: vendrá determinada por el nivel de ANS para el hardware
Solución de compromiso	No se contempla
Hardware con elementos redundados sin soporte *in situ*	
Disponibilidad	MEDIA: vendrá determinada por el tiempo que tardemos en conseguir los repuestos y reemplazaros en caso de parada del sistema por fallo de elementos no redundados.
Solución de compromiso	Trasladar las máquinas virtuales a un nuevo Proxmox en otro equipo, bien desde el mismo disco si es accesible o bien mediante restauración de copias.
Hardware sin elementos redundados	
Disponibilidad	MEDIA-BAJA: determinada por el tiempo que se tarde en conseguir cualquier elemento hardware del sistema que falle.
Solución de compromiso	Trasladar las máquinas virtuales a un nuevo Proxmox en otro equipo, bien desde el mismo disco si es accesible o bien mediante restauración de copias.

[12] Véase glosario

3. Nivel 1: Acceso remoto seguro y seguridad

3.1 Acceso remoto

Una vez que se dispone del sistema virtualizado, se debe plantear como acceder a él para poder trabajar, como se vio anteriormente, existen dos vertientes principales: soluciones basadas en escritorio remoto (con o sin publicación de aplicaciones) y soluciones basadas en Web.

Solución de escritorio remoto

Dado que la mayoría de estos escritorios funciona en sistemas Windows existen tres posibilidades según las necesidades de la empresa. Estas posibilidades, de mayor a menor coste financiero son:

1) Soluciones basadas en Citrix con servicios de escritorio remoto de Microsoft Windows. Esta solución es la más escalable y personalizable.

2) Soluciones basadas en servicios de escritorio remoto de Microsoft. Es una solución bastante escalable, pero no tan personalizable como la anterior, tiene unos costos inferiores ya que la solución Citrix es una capa adicional que funciona sobre los servidores de Microsoft y por lo tanto requiere el licenciamiento de ambas soluciones.

3) Soluciones basadas en sistemas operativos Windows de Microsoft, pero con un software de terceros, como puede ser el Thinstuff XP/VS terminal Server, que además soporta sistemas operativos sin ser de la gama de servidor, por ejemplo, podría instalarse el software en un Windows 1X y usar esta solución para acceso remoto de los usuarios.

Las soluciones de Citrix y de Escritorio Remoto de MS permiten la publicación de aplicaciones sin la publicación del escritorio completo. En el segmento PYME que se aborda, no siempre son requeridas, pero es una funcionalidad para tener en cuenta. Ambas soluciones también permiten la publicación, tanto de aplicaciones como de escritorios vía portal web.

De cualquier manera, cada solución tiene sus pros y sus contras y siempre se puede ir migrando de la más baja a la superior si las necesidades van aumentando.

En cualquier caso, aquellas empresas que sólo necesiten un acceso a la vez a un escritorio y no usuarios simultáneos, pueden utilizar los servicios de escritorio remoto que vienen con cualquier sistema operativo actual de Microsoft. Otra opción es utilizar un software de control remoto del equipo tipo TeamViewer o Anydesk. Si se utiliza

TeamViewer o Anydesk se recomienda su uso con licencia y autenticación de doble factor[13], a ser posible con verificación en dos pasos[13].

Cada entorno empresarial es particular y específico por lo que los casos complejos no pueden ser abarcados a través de esta guía, sino que requerirán un análisis especializado realizado por profesionales del sector.

Solución de aplicación basada en web

En este caso la solución se simplifica bastante ya que, normalmente no hay que tener un licenciamiento adicional para el software, simplemente hay que verificar que el licenciamiento de éste para que el entorno de virtualización no exceda lo licenciado y cumpla los requisitos del fabricante.

Realmente en el segmento que se está tratando no suele haber limitaciones, pero hay productos que licencian por número de *sockets* de CPU[13], *cores*[13], etc. y al virtualizarse requieren licenciamiento de todas las CPU físicas del equipo físico. Esto último puede ser un problema ya que puede encarecer la licencia; en este caso siempre se puede hablar con el fabricante para ver si tienen otro modelo de licenciamiento, por ejemplo, vía CPU virtual (vCPU)

Consideraciones de dirección de acceso

Para acceder al sistema desde el exterior por VPN[13], RDP[13], HTTP[13], etc. se necesita conocer la dirección de acceso. En sistemas de bajo costo como a los que nos referimos suelen existir líneas de conexión a internet sin IP[13] fija y por lo tanto no se puede acceder por dirección, al cambiar ésta a lo largo del tiempo.

Lo ideal es utilizar un nombre de DNS[14] asociado a la IP asignada en cada momento.

La mejor solución es disponer de un nombre de dominio propio gestionado a través de un proveedor que permita realizar una actualización DNS de un registro DNS (por ejemplo Pontevedra.migorganizacion.com) que apunte a la ubicación del servidor. En este caso se debería establecer el TTL[14] al mínimo posible para que, en caso de que se produzca un cambio de IP el tiempo de indisponibilidad sea el mínimo. Cada proveedor implementa uno o varios sistemas para poder actualizar el registro DNS, el más sencillo de implantar es el de hacer una petición HTTP/S a una URL[14] y la DNS se actualiza a la IP de la que recibe la petición. Otros implementan un pequeño programa para actualizar la DNS u otros métodos.

[13] Véase glosario
[14] Véase glosario

En cualquier caso, lo que debe tenerse en cuenta es que una de las máquinas virtuales debe encargarse de esta pequeña tarea, por ejemplo, con una tarea programada cada dos minutos o el tiempo que permita el proveedor.

En caso de no disponer de un nombre de dominio propio o no querer utilizarlo siempre se puede recurrir a uno de los múltiples proveedores que ofrecen este servicio de forma gratuita con limitaciones o sin estas limitaciones pagando una pequeña cuota. Estos proveedores se pueden encontrar fácilmente realizando una búsqueda en la web usando la expresión “Dynamic DNS providers”.

Debido a que muchos proveedores todavía utilizan IPv4[14] es posible que el proveedor de servicios esté haciendo una traducción de direcciones de red a nivel de operador CG-NAT[14] (del inglés *Carrier Grade Network Address Translation*) y en este caso no se podría llegar al servidor desde Internet, habría que llamar al proveedor de servicios y solicitarle que excluyese del CG-NAT la conexión, para poder tener una IP alcanzable desde Internet.

Consideraciones de seguridad

A menos que sea necesario dar algún acceso público desde Internet a alguna de las máquinas virtuales (por ejemplo, acceso web a clientes) se recomienda que el acceso a los servidores desde Internet se realice a través de VPN, a ser posible VPN con autenticación de doble factor y con verificación en dos pasos.

En el equipo de firewall deben limitarse los accesos desde el exterior, incluso a través de la VPN a lo estrictamente necesario, evitar reglas de tipo “Permitir todo de la VPN a la red local” y usar en su lugar reglas parecidas a “Permitir el acceso de VPN al puerto RDP” e incluso, si el equipo lo permite, “Permitir el acceso del usuarioX de VPN al puerto RDP con el tipo de tráfico correspondiente al protocolo RDP” (aquí se restringe usuario puerto y tipo de tráfico). Por supuesto, se tiene que usar un firewall que sea capaz de identificar no sólo la capa de red sino también la capa de protocolo de aplicación.

3.2 Seguridad a nivel de red

Una vez se ha llegado a este punto, se debe analizar en profundidad el tema de la seguridad a nivel de red. El tener toda la información en un entorno virtual, no sólo no simplifica el tema de copias de seguridad a nivel de equipo completo, sino también el aseguramiento de los accesos de red.

Los parámetros para aplicar son siempre los mismos, tanto en una solución por medio de un solo host virtual como en varios.

Lo primero es segmentar bien la red, en cualquier sistema mínimo se va a tener un interfaz

físico para comunicarse con el exterior, o varios en caso de soluciones complejas. En Proxmox se puede segmentar fácilmente la red utilizando varios interfaces *bridge* que pueden contener o no interfaces físicos que permiten comunicación con el exterior.

En segundo lugar, se definen las zonas a proteger, que pueden considerarse las siguientes:

1) Zona externa, equipo perimetral. Separa la red del exterior (Internet).
   En el caso de empresas pequeñas, se recomienda invertir suficientemente en seguridad y poner un equipo de seguridad de una marca reconocida, a ser posible virtualizado dentro del propio Proxmox, lo que normalmente va a encarecer la solución. Este equipo, encargado de realizar las funciones de seguridad externa, también suele ser un buen equipo para la separación de zonas de red interna en capa 3.

2) Zona interna. Es la zona de la red interna y lo ideal sería separarla de la red de servidores, dando el acceso que corresponda a cada cual. Puede hacerse con el propio firewall de Proxmox, con el equipo de seguridad de la zona externa, si lo permite o con otro equipo, si se requiere, por ejemplo, por temas de rendimiento, ya que encarece la solución.

3) Zona de equipos dentro del mismo interfaz Bridge de Proxmox, en este caso podemos usar el propio firewall interno de Proxmox para aislar unos equipos de otros si fuese necesario.

En cualquier caso, se recomienda que el equipo de seguridad cumpla como mínimo los siguientes requisitos:

- Soporte VPN que permita acceder de forma segura nuestra red
- Soporte NAT[15] / PAT[15]
- Cortafuegos o *firewall* , a ser posible a nivel de aplicación y no sólo a nivel de puerto y/o protocolo.
- Sistema de detección de intrusos[15], antivirus, filtrado de contenidos e inspección SSL[15].
- Actualización automática de bases de datos de antivirus, amenazas, etc.

La mayoría de estos requerimientos pueden llevarse a cabo mediante soluciones de código abierto y/o gratuitas, pero requieren un mantenimiento más complicado y no se

[15] Véase glosario

recomiendan para una PYME, a menos que cuente con su propio personal informático o un mantenimiento de seguridad apropiado.

Actualmente, teniendo en cuenta que los problemas de ciberseguridad constituyen una realidad patente, se recomienda tener un buen equipo de seguridad perimetral, con contrato de mantenimiento y gestionado por profesionales.

En caso de no tener ningún conocimiento o no querer invertir mucho se pude optar por una de las muchas soluciones que ofrecen los propios proveedores de servicio de Internet, que suelen ser más limitadas en cuanto a flexibilidad, pero muy sencillas de utilizar.

Soluciones de seguridad para el entorno

Una vez vistas las opciones de conexión remotas y las posibilidades de donde instalar los equipos, se van a a definir 3 soluciones con distintos órdenes de magnitud:

Orden de magnitud 1

Servidor Proxmox con un firewall virtual FW, montado en un equipo básico con un único interfaz de red conectado a través de un conmutador que conecta la red local con el equipo del proveedor de servicios

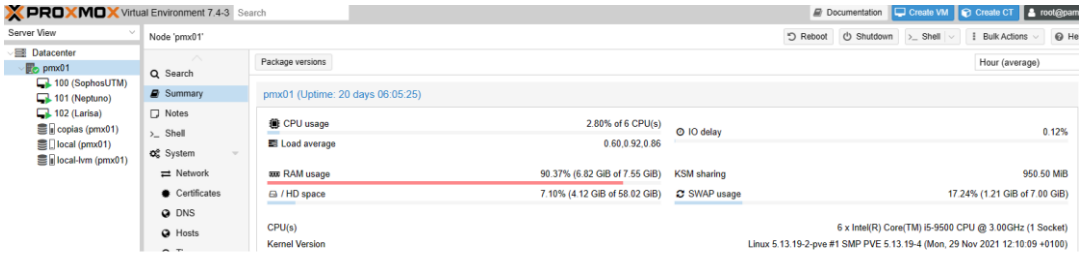

Ilustración 3: Ejemplo de Proxmox de orden de magnitud 1. Fuente: Propia.

En este caso se tiene un esquema de red con la siguiente forma:

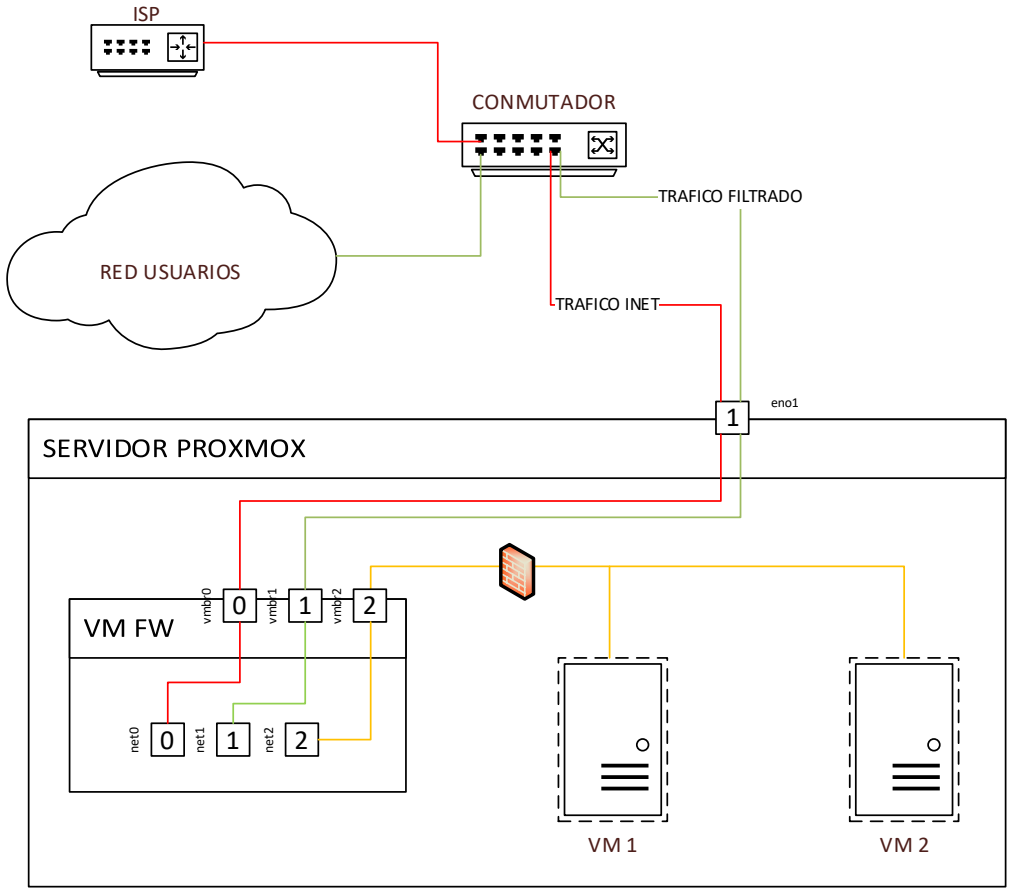

Ilustración 4: Esquema de red de orden de magnitud 1. Fuente: Propia

En este caso, aunque a nivel de firewall existen tres zonas separadas, esta solución no es ideal ya que un usuario interno con conocimientos avanzados puede llegar a hacer pasar el tráfico de su equipo directamente a Internet sin pasar por el firewall de la empresa, aunque para llegar a los servidores virtualizados deberá siempre pasar por el firewall. Hay que tener en cuenta que este tipo de inseguridad también conlleva la posibilidad de suplantar el enrutador del proveedor de servicio permitiendo hacer un “Man in the Midle” con solo tener acceso a un equipo de la red local.

Con respecto a la conexión a internet, se ofrecen dos posibilidades.

1) La mejor opción, es poner el equipo del proveedor de servicios en modo monopuesto (o *bridge*) de tal forma que el interfaz net0 del ordenador de la empresa FW sea el encargado de recibir la IP del proveedor y de esta forma toda la comunicación con el equipo se realice en capa 2

2) La configuración 1 no siempre es posible, en este caso, para poder asegurar que nadie de la red interna se salta el firewall se deberían establecer dos

direccionamientos distintos uno para la LAN[16] y otro para las comunicaciones entre el equipo FW y el equipo del proveedor de servicios, de esta forma los equipos de la LAN no se pueden comunicar directamente en nivel 3 con el equipo del proveedor.

Como nivel de seguridad adicional, para evitar que un usuario pueda saltarse el firewall, si el enrutador del proveedor lo soporta, se puede filtrar para que sólo admita tráfico del equipo FW, esto podemos hacerlo bien a través de MAC[16](posiblemente no lo soporte) o bien poniendo la IP de nuestro interfaz net0 del equipo FW.

Esta solución es la más básica y económica ya que no es necesario tener equipos de red que soporten VLAN[16] y el servidor sólo tiene un único interfaz de red, lo cual permite que incluso un equipo de usuario con características hardware suficientes pueda usarse de servidor Proxmox.

Orden de magnitud 2

Servidor Proxmox con al menos dos interfaces de red conectado uno a nuestro proveedor de servicio y el otro a nuestra red local.

En este caso el esquema de una posible solución sería el siguiente:

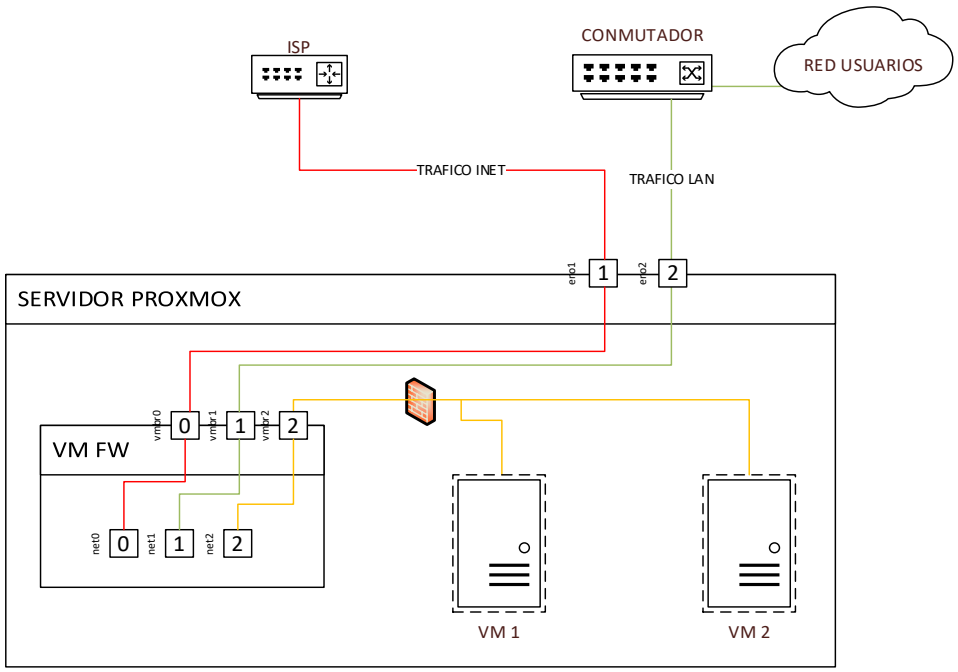

Ilustración 5:Esquema de red de orden de magnitud 2. Fuente: Propia

[16] Véase glosario

Esta configuración es mucho más sencilla de realizar y manejar porque además de tener cada zona separada en el firewall a través de un interfaz, se tienen los elementos externos separados entre sí, de tal forma que es imposible la comunicación sin que esta se realice a través del firewall, incluso en capa 2.

Así pues, esta solución ofrece una mayor seguridad que la de orden de magnitud 1. De hecho, esta es una configuración que ofrece mucha seguridad sin entrar en complejidades de filtrar por direcciones MAC en el enrutador del proveedor y sin tener que comprar equipos que tengan soporte VLAN.

Sin embargo, tanto la solución de orden de complejidad 1 como ésta, ofrecen un problema de crecimiento para aumentar el número de servidores físicos de manera segura.

Ambas soluciones permitirían crear interfaces de tipo bridge para segmentar distintas redes de servidores dentro del servidor, pudiendo segmentar de esta forma diferentes grupos de servidores si fuese necesario, independientemente de poder definir firewall entre ellas. Por ejemplo, en el esquema siguiente habría dos redes de servidores, cada uno con su interfaz de capa 3 en el firewall y con su firewall a nivel de Proxmox dentro de la propia red.

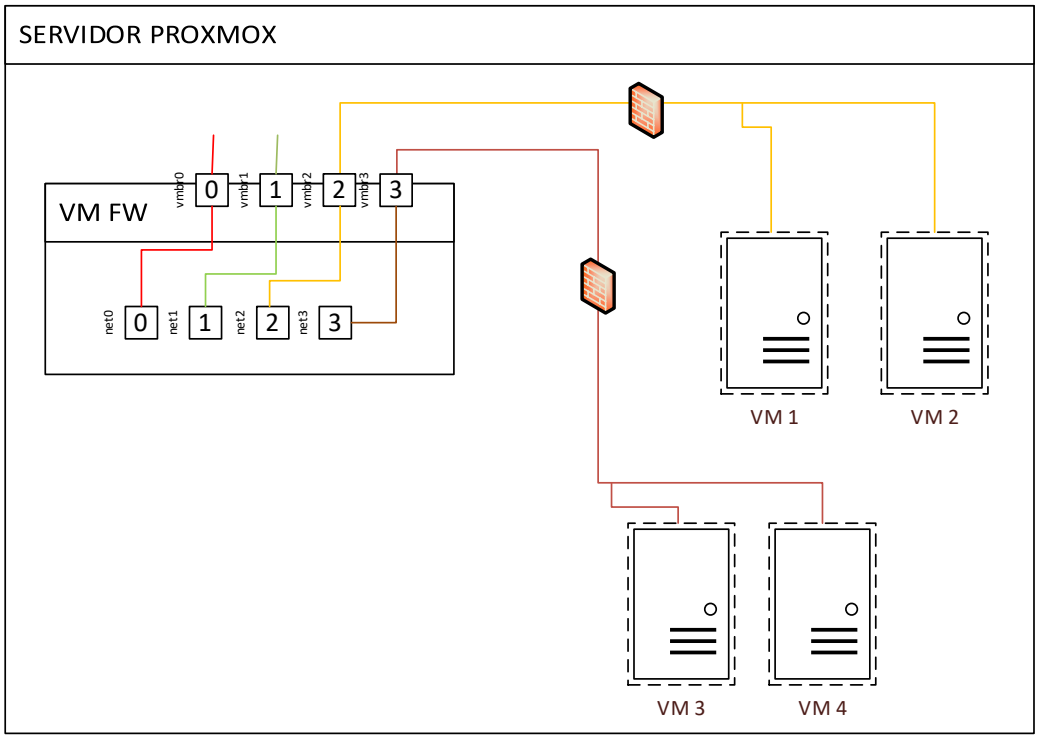

Ilustración 6: Ejemplo de servidor con varías redes de servidores virtuales. Fuente: propia

Orden de magnitud 3

Esta es una solución que permite un crecimiento mucho mayor que las anteriores y una

mayor segmentación en redes incluso a través de varios servidores físicos.

Para esta solución se debe disponer de equipos de red que soporten configuraciones de VLAN, dado que Proxmox soporta VLAN en su interfaz bridge, se pueden definir estos con soporte para VLAN y, de esta forma gestionar la VLAN que se asigna a cada servidor virtual a través de su propio interfaz.

En este caso se va a utilizar un esquema basado en una solución con un equipo Fortigate virtual (Fortigae VM64-KVM) y un switch de red DLINK DGS 3130, aunque serviría igualmente cualquier firewall y cualquier switch con soporte de VLAN.

Es una solución básica por lo tanto se utilizará solo las siguientes VLAN:

NOMBRE VLAN	ID	DESCRIPCIÓN
PROVEEDORES	3	Interconexión con equipos de proveedores
USUARIOS	30	Equipos de usuarios
SRV_VM1	201	Servidores virtuales Grupo 1
SRV_VM2	202	Servidores virtuales Grupo 2
SRV	100	Servidores físicos

Para esta solución el esquema de la red quedaría de la siguiente forma:

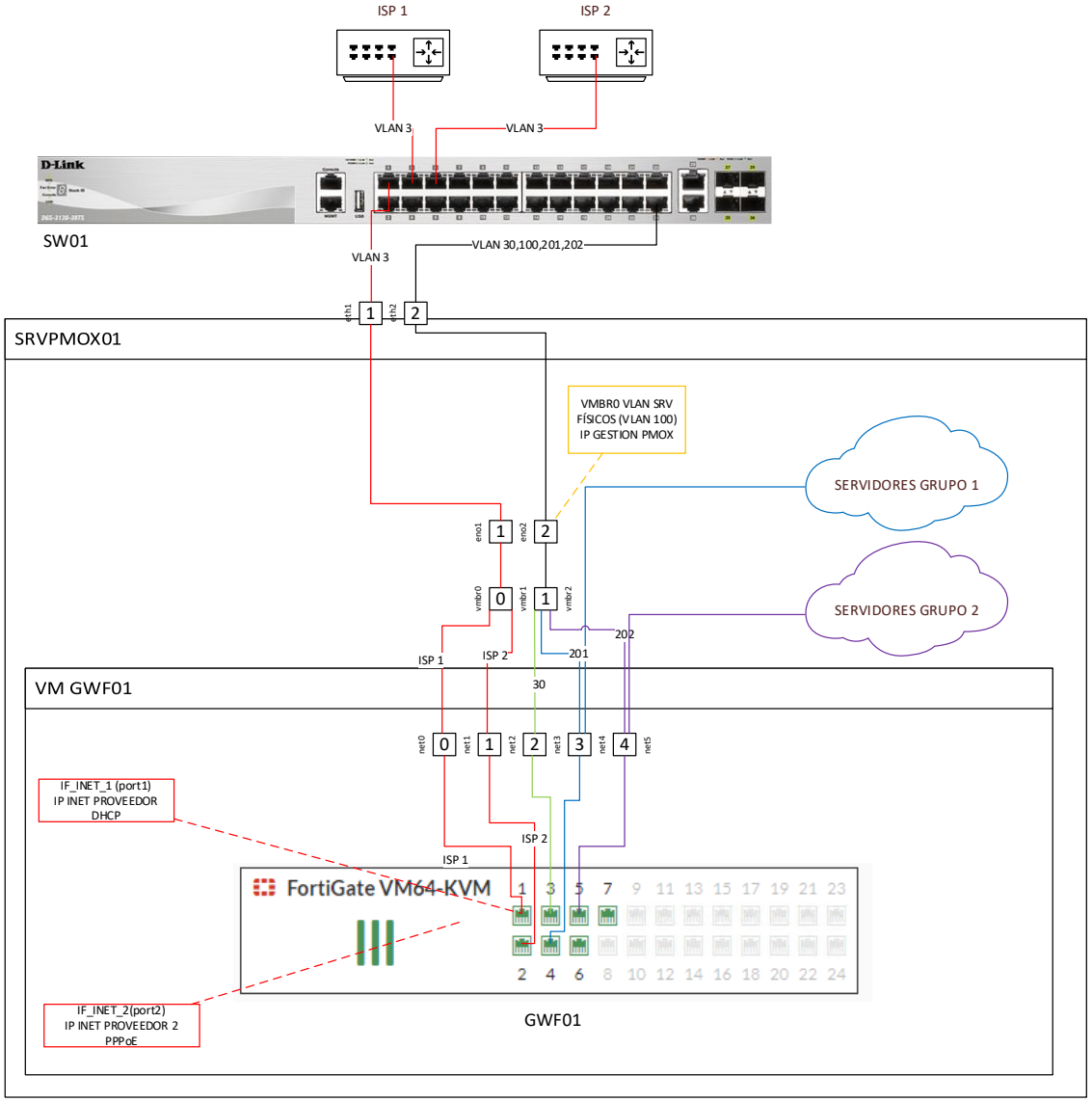

Ilustración 7: Orden de magnitud 3. Fuente: Propia

Se han puesto a modo de ejemplo dos proveedores de internet con dos modos de conexión distintos uno por DHCP[17] y el otro por PPPoE[17] (hay que recordar que ambas son líneas estándar de comercios, sin ninguna configuración especial, lo más económico).

Esta solución se ha diseñado sólo con dos interfaces de red ethernet pero teniendo un Conmutador que lo soporte podrían hacerse interfaces agrupados de distintos interfaces ethernet formando un *bonding*[18] y podría asociarse este al interfaz bridge, para obtener un mejor rendimiento. En PYME que ya requieren una infraestructura con VLAN y varios grupos de servidores es posible que sea una característica necesaria para aprovechar para obtener un mejor rendimiento o mayor disponibilidad (para mayor información sobre

[17] Véase glosario
[18] Véase glosario

este tipo de configuraciones véase [8] en la entrada “Network Configuration“).

El motivo por el cual se separa la VLAN de Internet en una troncal diferente a la del resto de VLAN se debe a la posible versatilidad a futuro y funcionalidad, por ejemplo, se puede separar físicamente esos equipos a futuro en un switch de capa dos independiente o conectados a una solución de alta disponibilidad (HA) facilitada por el proveedor.

En general si se está justo de interfaces se pude usar una VLAN que puede incluirse en un enlace troncal, pero la recomendación, basada en la experiencia, para este tipo de instalaciones es dejarla separada.

3.3 Resumen de soluciones

En este nivel 1, se han determinado las posibilidades de conexión dependiendo de la modalidad de aplicación web o de escritorio.

Método de conexión WEB
En este caso la conexión se realiza simplemente dando acceso a los puertos que utilice la aplicación desde el exterior
Métodos de conexón a aplicación de escritorio (de más versátil, compleja y cara a más barata y simple)
Acceso remoto mediante Citrix
Acceso remoto mediante servicios de escritorio remoto de Microsoft
Acceso remoto mediante ThinStuff XP/VPS

Por otra parte, se han analizado soluciones de seguridad de red y se han mostrado tres soluciones con distintos alcances.

Orden de magnitud 1
Solución basada en un solo equipo con una sola tarjeta de RED, sin VLAN y firewall virtualizado. Es una solución valida, pero bastante limitada de cara a que el tráfico del proveedor de servicio se conecta a través del mismo conmutador de red que la red local, lo cual la hace vulnerable a ciertos ataques.
Orden de magnitud 2

Solución basada en un solo equipo con al menos dos tarjetas de red, sin VLAN y *firewall* virtualizado. En este caso es una buena solución para muchas PYME que además es más segura que la anterior al tener el tráfico de Internet totalmente separado de la red local lo que permite mayor seguridad. No es escalable a un sistema *cluster*[19] manteniendo la seguridad.
Orden de magnitud 3
Solución basada en un equipo con dos o más interfaces de red, VLAN y *firewall* virtualizado. Es la solución es la más versátil y escalable, permite su migración a un sistema *cluster.*

[19] Véase glosario

4. Nivel 2: Mejorando las copias de seguridad

4.1 Servidor de copias de seguridad

Cuando anteriormente se abordó el tema de las copias de seguridad siempre se refería a copias de seguridad completas de las máquinas virtuales. Este método de copias es bueno, pero tiene una serie de deficiencias, especialmente en lo que se refiere al tiempo de realizar la copia de seguridad y al espacio que estas ocupan.

Para mejorar estos dos parámetros fundamentales, lo ideal es instalar un servidor de copias del propio fabricante Proxmox, Proxmox Backup Server [9] (en adelante PBS).

PBS ofrece una solución que soporta deduplicación[19], copias incrementales[19], además de añadir compresión y cifrado, así como otras características que mejoran la seguridad e integridad de datos.

Es un servidor muy sencillo de instalar siguiendo las instrucciones y toda la gestión se puede realizar por web.

El fabricante recomienda que se instale en un servidor físico independiente o incluso en el mismo servidor que el Proxmox VE. En base a la experiencia, una PYME podría utilizar una máquina virtual con el PBS dentro del mismo servidor de virtualización Proxmox. Aunque no es una práctica recomendada funciona perfectamente, para un volumen pequeño de máquinas virtuales.

Se dispone de 3 posibles montajes de servidor PBS que, de peor a mejor solución, son:

1) Servidor PBS en una máquina virtual.

2) Servidor PBS en la misma máquina que el servidor Proxmox VE.

3) Servidor PBS en una máquina independiente.

En los casos 1 y 2 debe tenerse en cuenta que el servidor de backup está consumiendo recursos del propio servidor que realiza la virtualización de servidores, por lo tanto, es recomendable que tanto las copias como las tareas de mantenimiento del PBS se realicen una ventana de horas de bajo uso de los equipos virtuales.

Del mismo modo, es altamente recomendable para los casos 1 y 2 que se realicen las copias en soportes de almacenamiento distintos a los que se utilizan para las máquinas virtuales, ya que ante el fallo de uno de esos soportes seguiremos teniendo las copias en otros. Sería incluso recomendable que estos soportes fuesen en algún tipo de sistema

totalmente independiente que pueda montarse por iSCSI[20] o similar.

En la mayoría de las pequeñas PYME que sólo tengan uno o dos servidores virtualizados un simple PBS virtualizado con almacenamiento independiente, será más que suficiente.

La ventaja de un PBS virtualizado es la misma que la del resto de máquinas virtuales, se puede hacer una copia del PBS (sin el almacenamiento de copias) en un soporte distinto al del PBS y de esta forma restaurarla fácilmente.

4.2 Replicación de copias

El PBS tiene una característica que permite de forma sencilla replicar los datos de un servidor PBS a otro.

Un servidor PBS puede conectarse a varios servidores remotos y a través de procesos de sincronización guardar copias de las copias de cada servidor.

Como el nivel de permisos es bastante granular y las copias además pueden cifrarse, en un ambiente de colaboración entre varias pequeñas empresas, estas podrían unirse para tener un PBS en algún sitio y guardar de forma remota copias de cada uno.

Debe tenerse en cuenta que guardar copias en un sitio remoto es la mayor garantía de cara a un gran desastre como un incendio, inundación o similar que pudiese destruir completamente el hardware.

4.3 Resumen de soluciones

Se han analizado escenarios de copias de seguridad basadas en Proxmox Backup Server que mejoran el sistema de copias de Proxmox VE.

Sistema PBS en local en máquina virtual local
Permite tener el sistema de copias en el mismo servidor del entorno de virtualización Afecta al rendimiento de la máquina Es una solución ideal para pequeñas PYME que además permite una fácil recuperación del PBS en caso de fallo del servidor físico
Sistema PBS en local en el mismo servidor Proxmox
Permite tener el sistema de copias en el mismo servidor del entorno de virtualización

[20] Véase glosario

Afecta al rendimiento de la máquina En caso de fallo del servidor físico no tenemos una copia del PBS.
Sistema PBS montado en su propio servidor
Es la solución recomendada en caso de tener un sistema de virtualización con varias máquinas virtuales o muy ajustado en rendimiento.
Sistema PBS en local con sistema PBS en otra ubicación
Añade a cualquiera de las anteriores un nivel de seguridad adicional al tener una copia guardad en un sitio remoto. Incrementa el coste, pero permite la continuidad de negocio en caso de gran desastre, que afecte al PBS local, mediante restauración de copias.

5. Nivel 3: Aumentando la disponibilidad

5.1. Análisis de soluciones

Cada solución puede tener unas determinadas condiciones particulares que permitan aumentar su disponibilidad, por ejemplo, las aplicaciones de escritorio pueden ser tipo cliente servidor y por lo tanto se podría montar algún tipo de *cluster* en la parte del servidor para aumentar esta, lo mismo podría aplicarse a las aplicaciones web. Esta disponibilidad de la "capa de aplicación" no es objeto del presente documento ya que es específica de cada solución.

Estas soluciones se centrarán en las capas que aumentan la disponibilidad del sistema de virtualización y, por ende, de las máquinas virtuales que contiene, en concreto cabe mencionar:

- Redundancia de hardware: básicamente aquí se recuerda lo que se trató en el Nivel 0, comprando hardware con elementos redundados que puedan fallar y usando discos en algún nivel de RAID con redundancia (1,5, etc.) y a ser posible con un disco *hotspare* aumentamos la disponibilidad a nivel del hardware del propio servidor.

- Redundancia a nivel de red local

- Redundancia a nivel de conexión a Internet

- Redundancia a nivel de servidor completo mediante *cluster* de servidores Proxmox VE

- Garantías de suministro eléctrico, climatización y otras medidas de seguridad física y redundancia.

En la redundancia a nivel hardware no se entrará en mucho más detalle de lo ya explicado hasta el momento, sin embargo, las otras requieren una explicación más pormenorizada.

En cuanto a las medidas de seguridad física, suministro eléctrico etc. se abordarán en el apartado 1. Introducción6. Nivel 4: Medidas de seguridad físicas.

Redundancia a nivel de red local

Siempre se debe tener en cuenta que cualquier elemento electrónico puede fallar, esto incluye la electrónica de red. Es, por lo tanto, sumamente importante que si se quiere garantizar la disponibilidad de un sistema se garantice que ante el fallo de un conmutador de red el sistema siga funcionando.

Una solución bastante sencilla para esto es duplicar elementos de conexión, por lo tanto, se puede poner un segundo conmutador y otra tarjeta de red adicional para cada conexión. Después se debe configurar un interfaz *bonding* para cada una de las conexiones según lo que soporte nuestro conmutador, o como se desee, el cómo realizar estas configuraciones está perfectamente explicado en la wiki de Proxmox [8] en la página de “Network Configuration”.

Partiendo del modelo más complejo definido en la sección anterior ahora la solución quedaría de la siguiente forma:

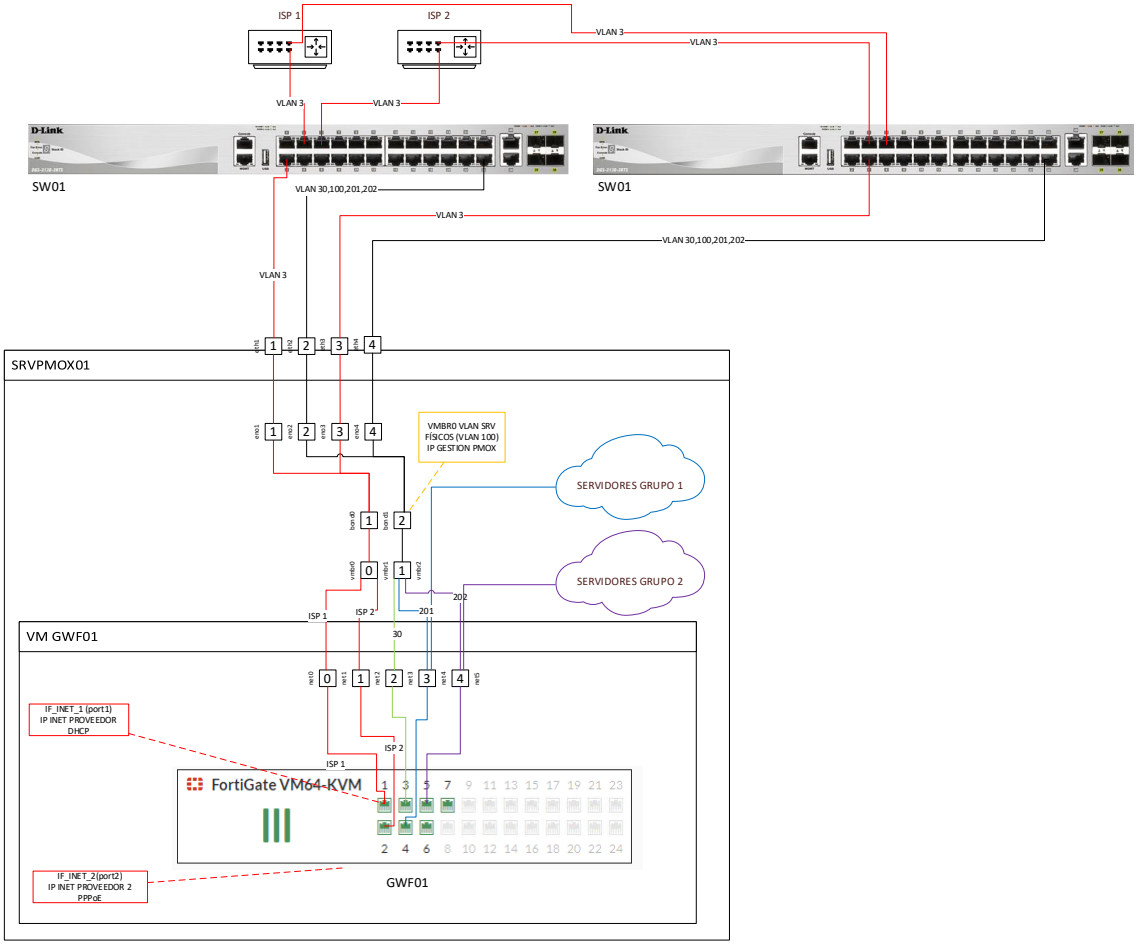

Ilustración 8: Redundancia a nivel de red local e Internet. Fuente: propia

Como se puede observar hay un interfaz *bonding* que forma parte del bridge con una conexión a cada conmutador para todas las interfaces *bridge* del proxmox. Se sigue manteniendo el esquema con dos enrutadores de proveedor (ISP1 e ISP2) que se explicará a continuación.

Redundancia a nivel de conexión a Internet

Para el tipo de solución que se está barajando, normalmente se dispone de líneas de conexión económicas de empresa. En este caso el equipo encargado de realizar el

enrutado (en el esquema el GWF01) debe soportar el poder manejar el enrutado por una u otra línea dependiendo de varias circunstancias, como mínimo lo suyo es un enrutado basado en disponibilidad por una o por otra, aunque generalmente este tipo de equipos soporta muchas más opciones, como podría ser utilizar las dos conexiones a la vez mediante balanceo o utilizar cada conexión para unas determinadas funciones, siempre permitiendo utilizar de respaldo la otra conexión.

Debe tenerse en cuenta que, si se va a utilizar ambas conexiones a la vez, se deben crear dos entradas DNS dinámicas una para cada una y conectarse a la que corresponda para cada servicio. La opción más sencilla es, si son VM distintas, poner el cliente que realiza la actualización DNS en la máquina que presta el servicio (Véase Consideraciones de dirección de acceso).

El esquema de conexión con redundancia de dos proveedores es el mostrado en la Ilustración 8: Redundancia a nivel de red local e Internet.

Esta solución puede mejorarse (con más coste) de la siguiente forma:

- Montando una solución en alta disponibilidad con un mismo proveedor con dos tipos de acceso distintos compartiendo direccionamiento.

- Como solución muy cara y que pocas PYME necesitan, se puede plantear el disponer de direccionamiento IP propio y un sistema autónomo[21] que permita enrutar el tráfico de forma dinámica según necesidades por varios proveedores.

Redundancia a nivel de servidor

Tener más de un servidor permite disponer de un hardware completo en caso de fallo.

Servidor preinstalado

La solución más simple es tener un servidor preinstalado que n permita una rápida recuperación de las copias.

Este servidor se puede tener apagado en algún sitio, por ejemplo, una estantería, con un Proxmox VE instalado y usarlo en caso de avería, restaurando las copias. Esta sería la solución más simple de redundancia a nivel de servidor, pero también quizás la más lenta a la hora de recuperar el servicio y la que más desperdicia los recursos al tener el servidor apagado.

[21] Véase glosario

Cluster Proxmox sin almacenamiento compartido

Disponer de un segundo servidor permite crear un *cluster* Proxmox, de tal forma que se pueda aprovechar los recursos de esta máquina de forma paralela, distribuyendo las distintas máquinas virtuales entre ambos servidores.

En caso de fallo total de uno de los servidores se puede pasar todas las máquinas virtuales al otro servidor restaurando las últimas copias de seguridad.

Si el equipo no fallase totalmente, sino que estuviese en un estado degradado pero funcional, por ejemplo, ante un fallo de disco en un RAID, se puede, por seguridad o mejore rendimiento, mover las máquinas virtuales sin apagarlas al otro equipo, en esta operación puede producirse en algún pequeño corte del orden de milisegundos.

Hay que tener en cuenta que, en este escenario se tienen dos equipos con su propio almacenamiento cada uno independiente, y proxmox desde el entorno web, en el momento de la realización de este documento, sólo permite migrar las máquinas cuando estén encendidas o cuando el almacenamiento del servidor destino tenga el mismo nombre en caso de máquinas apagadas (desde la línea de comandos podría hacerse con la herramienta *qm* mediante el comando *qm migrate*).

Para realizar una migración online Proxmox VE creará un NBB [10] temporal que le permitirá realizar la copia de datos sin apagar el equipo. Teniendo en cuenta esto es muy importante y una práctica recomendada tener un interfaz de red dedicado a la comunicación entre miembros del *cluster*, sin embargo, en entornos de bajo coste, este interfaz puede compartirse con el de gestión o incluso con el del bridge principal por el que se da servicio, aunque no es la solución ideal.

Cluster Proxmox con almacenamiento compartido

A pesar de que la solución mencionada es perfectamente válida, en caso de que se quiera aumentar mucho más la disponibilidad, lo recomendable es tener un almacenamiento compartido para que permita una migración mucho más rápida o recuperación en caso de fallo.

Evidentemente una solución con almacenamiento compartido incrementa los costes, en este caso se recomienda utilizar una premisa de proporcionalidad, es decir, no se necesita un sistema de almacenamiento de miles de euros para tener unas pocas máquinas virtuales con un rendimiento para necesidades ofimáticas.

Muchas NAS[22] de bajo coste soportan NFS[22] o iSCSI con un rendimiento suficiente para unas pocas máquinas virtuales.

Cluster Proxmox con alta disponibilidad

Un *cluster* con alta disponibilidad es la mejor solución, sin dudas, pero como mínimo requerirá 3 servidores, este permitirá establecer reglas de HA para las distintas VM, para que, por ejemplo, en caso de fallo de un servidor, automáticamente las máquinas virtuales que se determinen empiecen a ejecutarse en otro nodo.

Esta solución incrementa bastante los costos y hay que tener muy claro si el negocio lo necesita o no, porque la tecnología es importante casi en cualquier negocio, pero la disponibilidad de la información no tiene las mismas necesidades. En el caso de un cluster proxmox se podría conseguir una disponibilidad con HA de 99.999%[23].

Si realmente por necesidades del número de máquinas virtuales hay que ir a esta escala, no habría lugar a dudas a que es la mejor solución, pero pocas pequeñas empresas necesitan esta solución.

Básicamente es como una solución con almacenamiento compartido de 2 nodos, pero con tres, aunque en este caso podría ser también una solución interesante que los nodos diesen este almacenamiento con Ceph.

Esta solución de más de tres nodos no es objeto de este documento ya que, con estas necesidades, es posible que haya que estudiar la solución para el caso específico. Una solución con Ceph por ejemplo es viable en unos casos, pero en otros es mejor una SAN, algunas máquinas pueden tener una afinidad a unos nodos específicos, etc.

En cualquier caso, está solución podría ser un caso de estudio específico para otro TFG.

Consideraciones sobre los cluster proxmox

Se debe tener en cuenta que las soluciones de *cluster* pueden plantearse de dos maneras, redundancia a través de cada servidor con la infraestructura o redundancia total de ambos servidores con el resto de la infraestructura.

Pensando en las comunicaciones con el resto de la infraestructura y se tendrá, como mínimo:

- Comunicación con Internet

[22] Véase glosario
[23] Véase la página High Availability - Proxmox VE de [8]

- Comunicación con la LAN

- Comunicación entre los nodos del *cluster* (Corosync).

- Comunicación con el almacenamiento compartido

Aunque, como ya vimos, muchos de estas funciones se pueden compartir entre interfaces de conexión, lo ideal es dejar cada una de estas conexiones para una función específica, lo cual permite separar también las redes (a nivel físico) y da una mayor versatilidad a la solución. Por ejemplo, si el día de mañana se dispone de un sistema HA de proveedor en la conexión a Internet con su propio switch sólo hay que cambiar, en este ejemplo, el cable de las bocas que van a la VLAN 3 al nuevo switch, en este caso, al igual que en el caso de la red de almacenamiento.

Se determina, como mínimo de 3 o 4 (con almacenamiento compartido) interfaces de comunicaciones distintos, que si se desea que cada host sea totalmente redundante con respecto a la electrónica de comunicaciones se convertirían en 6 u 8, sin embargo, el tener dos nodos, permitiría a lo mejor tener simplemente 3 o 4 interfaces en cada equipo.

Para el caso de no redundancia total, ante el fallo de algún componente de comunicaciones externo tendríamos dos soluciones:

- Con almacenamiento compartido, bastaría con levantar manualmente las máquinas en el otro host

- Sin almacenamiento compartido, en el caso de dos nodos, lo ideal es tener los interfaces de Corosync conectados mediante un cable cruzado, de esta forma se podrían migrar las máquinas del nodo incomunicado al otro, a pesar de no tener comunicaciones en uno de ellos.

A la red se debería añadir además dos VLAN una para Corosync y la otra para almacenamiento. Por temas de rendimiento, muchas veces la red de almacenamiento se separa en electrónica distinta, pero en el tipo de infraestructura que se están analizando, inicialmente puede ir en los mismos conmutadores, si se quisiese independizar simplemente habría que poner los equipos nuevos correspondientes y conectar los cables, la solución seguiría siendo factible.

Las VLAN quedarían como siguen:

NOMBRE VLAN	ID	DESCRIPCIÓN
PROVEEDORES	3	Interconexión con equipos de

		proveedores
USUARIOS	30	Equipos de usuarios
SRV_VM1	201	Servidores virtuales Grupo 1
SRV_VM2	202	Servidores virtuales Grupo 2
SRV	100	Servidores físicos
COROSYNC	50	Comunicación servidores (Corosync)
ALMACENAMIENTO	250	Red de almacenamiento

Esquemas de Proxmox cluster con y sin redundancia total de electrónica de red

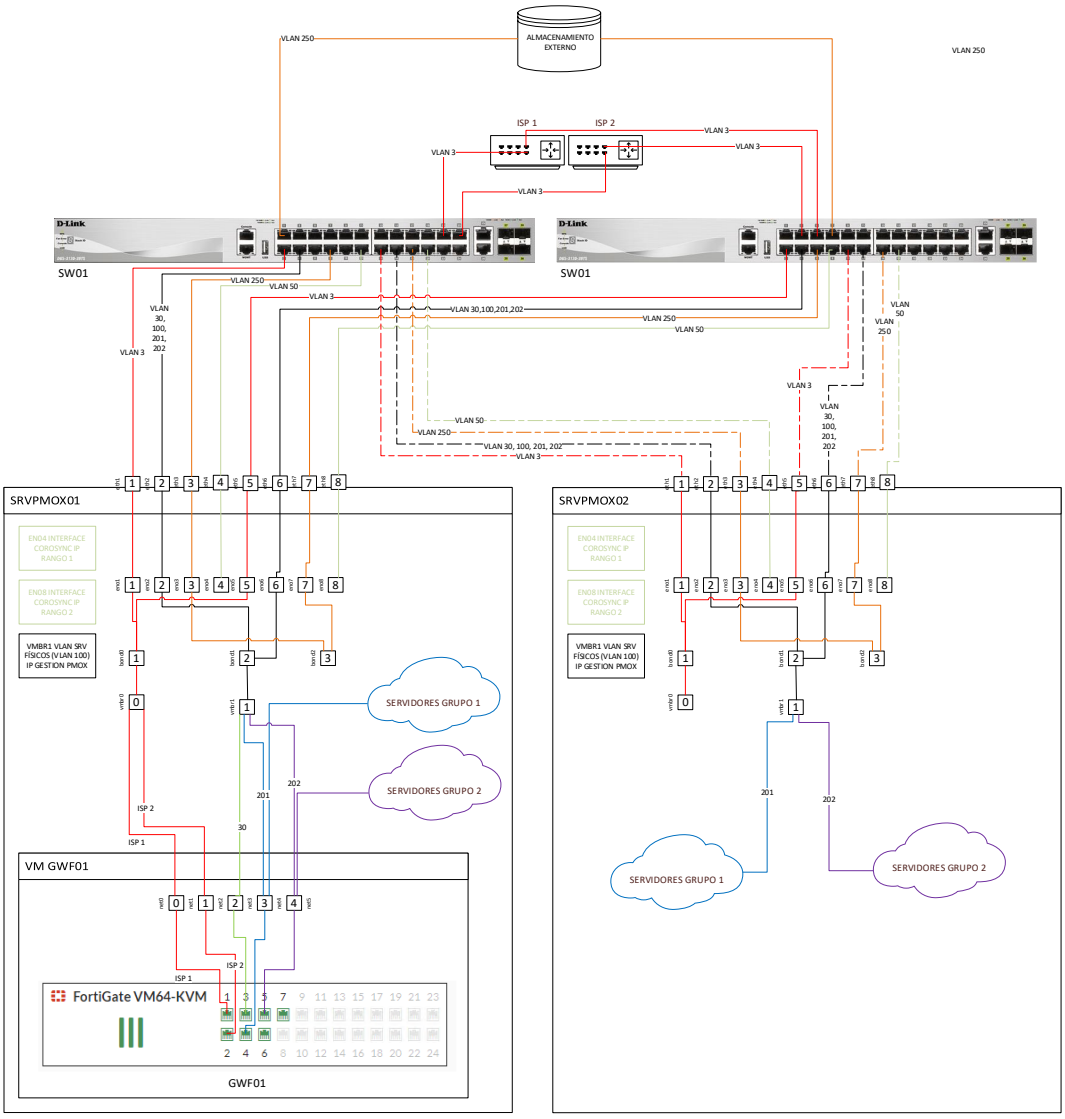

Ilustración 9: Cluster proxmox con redundancia de conexión a red por host. Fuente: propia

En el esquema cabe destacar que se han definido dos redes corosync distintas una por

interfaz en vez de hacer un interfaz bond. El corosync ya se encarga de gestionar por cuál de ellas irá según la prioridad definida, incluso se puede poner con una prioridad más baja el interfaz de gestión para usar como un último recurso.

El interfaz bond3 se utiliza para las conexiones a la red de almacenamiento, es decir para definir los *storages* que luego serán utilizados en las máquinas virtuales.

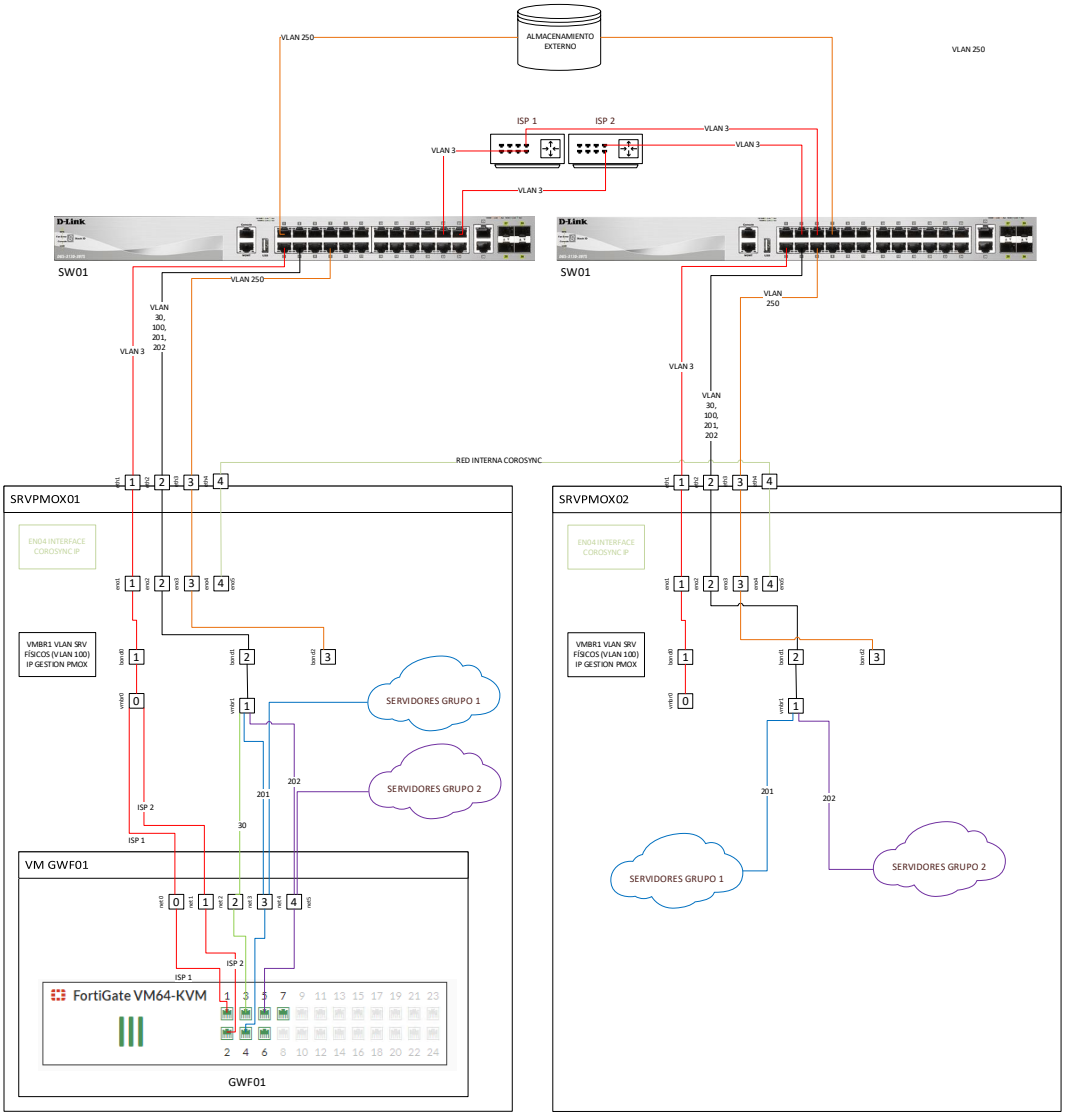

Ilustración 10: Cluster proxmox sin redundancia de conexión a red por host. Fuente: propia

En este caso los dos servidores se conectarán a través de un cable cruzado en sus interfaces Corosync, garantizando de este modo que, aunque uno de los conmutadores falle, los hosts podrán comunicarse directamente.

5.2 Resumen de soluciones

Redundancia a nivel de red local

- Duplicar electrónica de red de interconexión entre los distintos elementos y el servidor - Requiere al menos dos tarjetas ethernet en cada equipo, pero lo ideal es poder separar como mínimo ciertos tráficos a nivel físico, por lo tanto se determina entre cuatro y ocho interfaces de red.
Redundancia a nivel de conexión a Internet
- La solución más económica es tener dos líneas de dos proveedores independientes - Nuestro firewall debe soportar la gestión de varias conexiones.
Redundancia a nivel de servidor

- Servidor Proxmox VE preinstalado y restauración de copias
- *Cluster* Proxmox VE formado por dos servidores
  o Sin almacenamiento compartido
  o Con almacenamiento compartido
- *Cluster* Proxmox VE formado por más de dos servidores (requiere análisis específico)

6. Nivel 4: Medidas de seguridad físicas

En este apartado se analizarán aquellas medidas que deben llevarse a cabo para el acondicionamiento de un pequeño centro de proceso de datos (en adelante CPD), la mayoría de estas medidas están basadas en las recomendaciones de la Asociación Americana de Industria y Telecomunicaciones (TIA), publicadas por el American National Standard Institute en su norma ANSI-TIA-942 aprobado en 2005.

Esta norma establece que la infraestructura de soporte de un centro de proceso de datos estará compuesta por cuatro subsistemas:

- Sistema eléctrico: accesos, puntos de fallo, cargas críticas, redundancia y tipos de SAI, puesta a tierra, sistemas de corte de emergencia (EPO), baterías, monitorización, generadores, sistemas de transferencia.

- Telecomunicaciones: cableado de armarios y horizontal, accesos redundantes, cuarto de entrada, área de distribución, red troncal, elementos activos y alimentación redundantes, paneles de parcheo 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 SAI y baterías, sala de generador, control de acceso, CCTV, NOC (Network Operations Center – Centro operativo).

- Sistema mecánico: climatización, presión positiva, tuberías y drenajes, CRAC (del inglés, *computer room air conditioning*) y condensadores, detección de incendios, extinción por agente limpio, detección por aspiración (ASD, del inglés, *aspirating smoke detector*), detección de líquidos.

El grado de disponibilidad se determina en base a cuatro niveles denominados Tier, cuanto mayor es el Tier mayor es la disponibilidad [11]:

- Tier I – CPD Básico: un centro de datos de nivel I es susceptible a las interrupciones de la actividad planificada y no planificada. Tiene distribución de energía y climatización, pero puede tener o no un piso elevado, un SAI o un generador eléctrico. Si dispone de SAI o grupos electrógenos, son sistemas mono módulo y tienen muchos puntos únicos de fallo. La infraestructura debe cerrarse por completo una vez al año para la realización de trabajos de mantenimiento preventivo y reparación. Las situaciones urgentes pueden requerir más paradas frecuentes. Errores de funcionamiento o espontáneos de los componentes de la infraestructura provocarán una interrupción en el CPD.
  Disponibilidad: 99,671%

- Tier II – CPD Con componentes redundantes: es menos susceptible a las interrupciones por actividad planificada o no planificada que un CPD básico. Tiene su propio piso elevado, SAI y generador pero su diseño es *Need plus One* (N+1), es decir un solo paso de corriente y aire acondicionado con un componente redundante. El mantenimiento de esta ruta crítica de electricidad u otras partes de la infraestructura no redundada conllevarán una interrupción del servicio del CPD.
  Disponibilidad del 99,741%

- Tier III – CPD concurrentemente mantenible: permite cualquier actividad planificada en la infraestructura si interrumpir la actividad de los servidores de ninguna manera. Las actividades previstas incluyen medidas preventivas u de mantenimiento programable, reparación y reemplazo de componentes, realización de pruebas en sistemas o subsistemas. Para sitios grandes, fuera del alcance de este TFG, que utilizan sistemas de refrigeración con agua, supone tener dos juegos de tuberías independientes. En general el sistema debe tener suficiente capacidad de distribución para disponible para transportar la carga de una ruta, mientras se realiza el mantenimiento, por otra. Actividades no planificadas tales como fallos de funcionamiento o espontáneos en los componentes de la infraestructura de la instalación aún podrían causar una interrupción del CPD. Los CPD con Tier III suelen diseñarse para poder ser actualizados a Tier IV cuando el caso de negocio del cliente justifique la inversión adicional.
  Disponibilidad 99,982%.

- Tier IV – CPD tolerante a fallos: soporta cualquier actividad planificada sin interrupción y puede soportar al menos un fallo o evento no planificado en el peor de los casos sin afectar al CPD. Requiere rutas de distribución activas simultáneamente. Eléctricamente significa dos sistemas UPS separados en los que cada uno tiene redundancia N+1. Debido a los códigos de seguridad eléctrica y contra incendios, aún podría haber tiempo de inactividad debido a alarmas por incendio o interacciones con personas que supongan un apagado de emergencia (EPO). El nivel IV requiere que todos los servidores o equipos de la infraestructura de procesamiento de datos tenga doble fuente de alimentación.
  Disponibilidad 99,995 %

Aunque aplicando todas las soluciones aquí propuestas en su solución más completa se podría conseguir un Tier III,

En caso de necesitar una instalación con un nivel Tier garantizado, para pequeñas empresas con baja densidad de servidores, del orden inferior a decenas, suele ser más económico un alojamiento en un CPD de terceros ya acondicionado con un nivel Tier ya

certificado.

Tanto la TIA-942 como las subsiguientes actualizaciones especifican requisitos que no se trataran aquí, incluso modificaciones, referentes a tipos de cableado, conectores, etc. Por ejemplo, la TIA-942 (A) sólo permite la utilización de cables de fibra multimodo OM3 y OM4 y suprime la limitación de 100m de longitud en cableados horizontales, para fibra óptica, dejando este concepto de longitud máxima determinado por las especificaciones del fabricante.

6.1 Acondicionando la sala

En la norma TIA-942 se definen distintos tipos de espacios y separaciones entre ellos que en una pequeña instalación serían difíciles de mantener, por lo tanto, se va a a definir la sala como un espacio diáfano de dimensiones suficientes para albergar el equipamiento, lo que en la TIA-942 viene definido como *computer room.*

Ubicación

En la medida de lo posible, para la ubicación del pequeño CPD:

- Debe seleccionarse un espacio que tenga las menores restricciones de expansión posibles, por ejemplo, lejos de ascensores, muros de carga, paredes exteriores u otras estructuras físicas que no puedan ser eliminadas en un futuro en caso de necesidad. En muchos casos el pequeño CPD se construye dentro de una sala más amplia que permite futuros expansiones.

- Debe ser accesible para que se pueda entregar el equipamiento necesario, por ejemplo, si se va a meter una máquina de aire acondicionado grande o un armario rack que quepa por la puerta y los pasillos de acceso para no tener que desmontarlos.

- No debe tener ventanas exteriores ya que aumentan la carga de calor y reducen la seguridad.

- Debe estar lejos de fuentes de interferencia electromagnética como transformadores eléctricos, motores, etc.

Consideraciones generales de la sala

El tamaño de la sala debe ser proporcional al equipamiento que se va a introducir en ella, incluyendo los posibles proyectos futuros conocidos.

En la sala podrán coexistir el equipamiento informático y equipamiento de índole eléctrica como cuadros de distribución, equipos de control o SAI de hasta 100kVA, excepto las baterías con líquido en su interior (de tipo ácido).

Cualquier otro equipamiento que no tenga que ver con la infraestructura del CPD no debe instalarse dentro del mismo o atravesarlo, por ejemplo, no debe haber una tubería atravesando el techo del CPD, aunque quede por debajo del suelo elevado.

La norma dice que la altura del CPD debería tener un mínimo de 2.6 metros, pero en este caso se puede adaptar para que quepa el equipamiento encima del suelo sobreelevado, si se considera invertir en él y una distancia mínima de unos 460 mm a cualquier elemento situado en el techo.

El suelo, las paredes y el techo deben estar sellados y construidos con un material que minimice el polvo con acabados de color blanco para mejorar la iluminación. El suelo debe tener propiedades antiestáticas, idealmente según la norma IEC 61000-4-2.

A pesar de que todas estas características se pueden realizar de obra, actualmente existen en el mercado paneles autoportantes que proporcionan todas estas características.

Debe haber unas condiciones de luz suficiente para poder trabajar adecuadamente tanto en el plano horizontal como vertical.

El suelo debe soportar el peso de los distintos elementos del CPD sin ceder.

Solución de acondicionamiento físico

Una posible solución que satisface muchos de los requerimientos de la TIA y considerada como una solución adecuada para un CPD pequeño sería la siguiente.

Descripción de la obra civil

El espacio se acondicionará con un sistema de cerramiento con protección sobre el fuego, el agua, protección térmica, física, eléctrica y medioambiental, protección electromagnética y protección contra intrusión.

Este cerramiento se podrá realizar (y se recomienda) mediante un sistema de paneles autoportantes tipo sándwich construidos con materiales ignífugos (RF mínimo 60, recomendado 120) y aislantes para soportar altas temperaturas y aislar de forma estanca el recinto.

En caso de que la sala esté en una ubicación que pueda verse afectada por inundaciones se recomienda una impermeabilización perimetral previa incluyendo el forjado interior y un sistema de detección de inundación.

De acuerdo con la norma TIA-942, se instalará un suelo técnico sobre elevado que permita la circulación del aire de refrigeración y los tendidos de cableado necesarios. El suelo por ejemplo podría ser de baldosas de 600x600 mm totalmente encapsuladas en chapa de acero galvanizado con núcleo aglomerado de alta densidad y pedestales graduables.

Los paneles proporcionan un sellado hermético permitiendo que el espacio entre los dos suelos (el de panel y el técnico) actúe como una cámara plena de aire facilitando el reparto de cargas. La altura será de 30 cm con objeto de que el aire acondicionado pueda fluir adecuadamente, en caso de que sea de tipo *plenum.* En este caso también deberá incluir rejillas de refrigeración adecuadas, como las de aluminio anodizado de alta resistencia con mecanismo de apertura y cierre manual para el ajuste exacto del caudal de aire.

El suelo técnico soportará una carga de 1.200 Kg/m^2.

La puerta de acceso debe tener una resistencia al fuego mínimo de 60 minutos y una altura libre de paso adecuada de unos 2,2 metros de altura. Las cerraduras de la pueta deben de ser de seguridad, resistentes al fuego, con barra antipánico interior, cierre mediate electro cerradura integrado y sistema de cierre automático no motorizado.

Los pasamuros practicados en el recinto modular deberán ser sistemas aislantes resistentes al fuego y al agua, de sellado de paso de cables. Y deben tener la posibilidad de módulos con diámetro practicable en función del grosor de cables de energía y datos con marcos de acero.

Se encajarán en la estructura de la pared a través de marco y contramarco específico de acero galvanizado. El sellado total se realizará mediante módulos de dimensiones y cableado adaptables y unidad de compresión.

Se instalará un sistema de canalizaciones aéreas (por encima de los armarios rack), para la conducción del cableado estructurado, de esta forma se acometerá por la parte superior de los mismos. De esta forma, al no requerir el tendido de cableado estructurado dentro del hueco de debajo del suelo técnico, por donde si serán conducidos los eléctricos que son poco voluminosos, no se corre el riesgo de impedir la libre circulación de aire frío procedente de las máquinas de aire acondicionado y servirá para crear conducciones de flujo de aire.

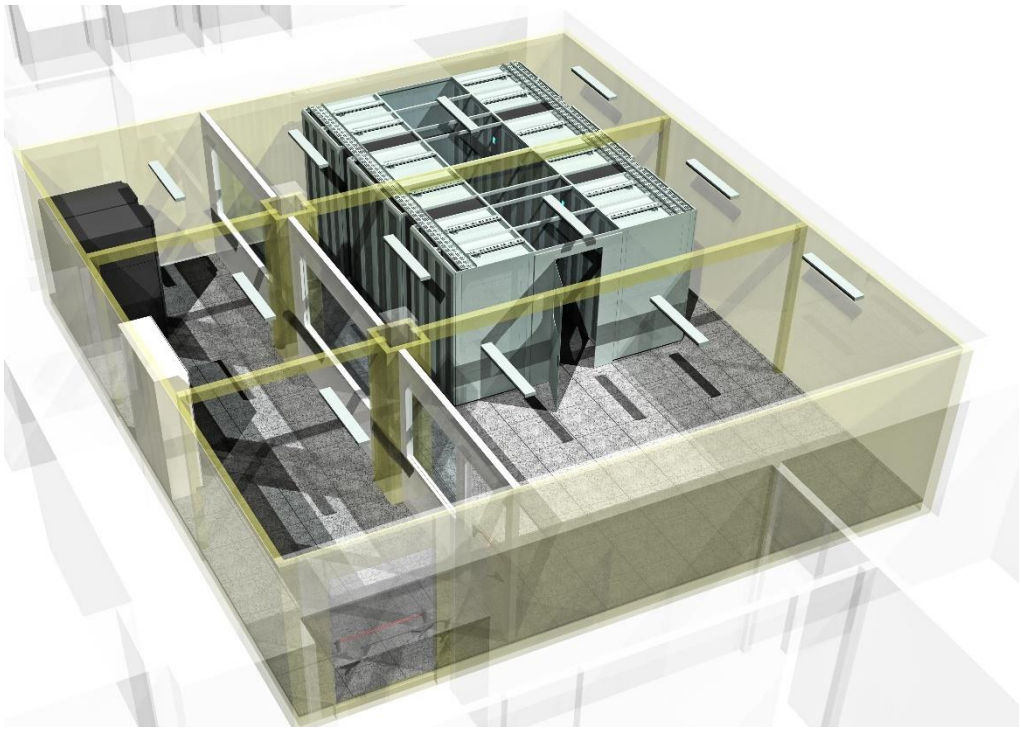

Ilustración 11: Infografía de un CPD con sala técnica previa. Fuente: propia, infografía de documentación de proyecto real.

Adaptación de la solución a las características de mini CPD

Esta solución supone una inversión bastante alta de cara al acondicionamiento de una sala de CPD y por ello es conveniente comentar las circunstancias de aquellas PYME cuya infraestructura cabe en uno o dos armarios de rack.

En unas dimensiones tan pequeñas sería ideal poder realizar toda la obra propuesta, pero hay cosa de las que se puede prescindir:

- Falsos suelo: para uno o dos armarios se puede buscar una solución que no lo requiera, por ejemplo, canalizar las acometidas eléctricas mediane tubo corrugado a la vista o canaleta, según se determine en la obra y acometerlas directamente al armario por la parte inferior

- Bandejas para cableado: en el caso de un armario o dos, puede llevarse el cableado como en el caso anterior a través de tubo corrugado, canaleta o similar, es importante que el cableado eléctrico y el de datos se acometan por conducciones diferentes.

- Protección RF (resistencia al fuego): puede realizarse de obra, por ejemplo, con paneles RF de pladur que abaratan el coste. En este caso téngase en cuenta que los niveles de protección RF del pladur no son acumulables, es decir, si se ponen dos planchas con protección 60 contiguas no se va a conseguir una plancha de

protección 120 [12].

En resumen, para uno o dos armarios podemos evitar costes en la obra civil, pero asegurando siempre que el mini CPD se encuentre protegido contra las causas externas, especialmente el fuego y en caso de ser zona inundable, las inundaciones.

En el caso de ser zona sísmica se sobreentiende que las obras realizadas en la zona cumplirán la normativa vigente.

En cualquier caso, tener bien protegido el CPD no exime de tener copias en una ubicación remota que proteja ante un incidente grave o desastre.

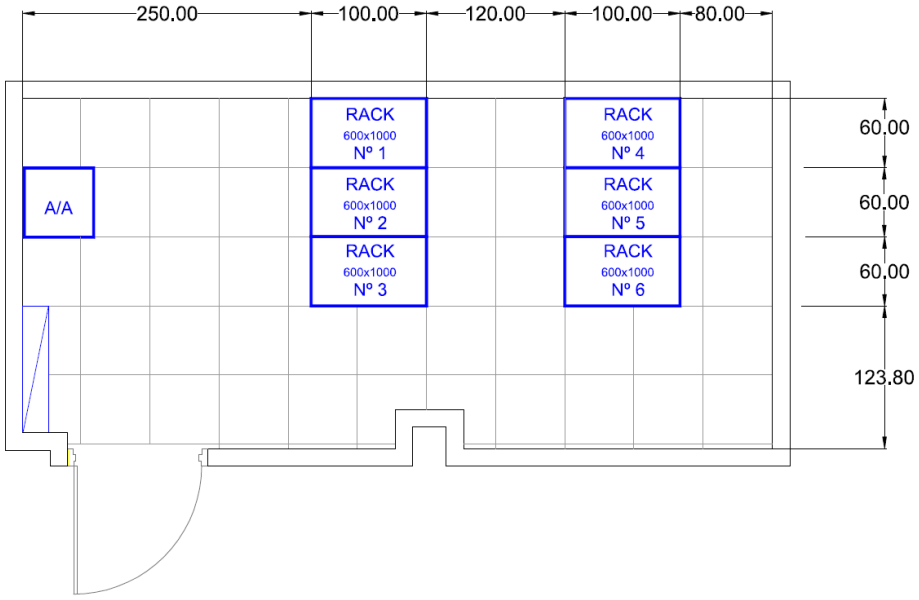

Ilustración 12: distribución de planta de un pequeño CPD con seis armarios rack. Fuente: propia de proyectos.

6.2 Sistema eléctrico

Toda la instalación dispondrá de corriente eléctrica alterna distribuida mediante cuadros eléctricos redundantes), con sistemas de alimentación ininterrumpida (SAI) independientes y de última generación, y con un grupo electrógeno ubicado en un lugar seguro que entre en funcionamiento en caso de fallo de la compañía suministradora de energía.

El CPD contará con los elementos necesarios para funcionar autónomamente en caso de producirse un fallo de suministro eléctrico con una autonomía mínima de 24 horas para el grupo electrógeno y de 10 minutos para el caso de los SAI tiempo que debe ser más que suficiente para el arranque del generador.

En principio en esta solución no se estima necesario que el edificio tenga una segunda

acometida de otra compañía, ni de otra subestación ni de otro transformador; por todo esto, para conseguir una mayor redundancia a la hora de garantizar el suministro eléctrico continuado al equipamiento del CPD, se incluirá en la solución:

- un grupo electrógeno que deberá soportar el 130% de la carga estimada para el CPD. Este tipo de generadores suele instalarse con carrocería acústica, para minimizar el ruido que este pueda producir, con una autonomía de mínimo 24 horas.

- 2 SAI redundantes con alimentaciones independientes entre sí, provenientes de distintos embarrados, garantizando así el suministro eléctrico incluso teniendo en consideración los fallos por elementos pasivos (bornas de conexión, pletinas de cobre, etc.).

El cuadro general del CPD estará dividido en dos partes, una de red normal (red sucia) y otra de SAI (red limpia), y a su vez tendrá dos embarrados para garantizar que cada una de las fuentes de alimentación de los equipos sea conectada a un embarrado distinto. Se dispondrá de doble acometida desde el cuadro de distribución del CPD hasta cada uno de los armarios rack, procediendo cada una de un embarrado distinto.

El cuadro eléctrico general del CPD tendrá un sistema automático de conmutación red-grupo.

En general, el sistema eléctrico deberá cumplir las especificaciones del Reglamento Electrónico de Baja Tensión (REBT) actual en el momento de la construcción.

A modo esquemático el cuadro de distribución general del CPD contendrá las siguientes salidas:

- Alumbrado normal y de emergencia.

- SAI (primario y redundante, configuración 2N).

- Sistema de control de accesos.

- Sistema de detección y extinción de incendios.

- Sistema de control de instalaciones.

- Sistemas de CCTV y CCAA.

- Sistema de climatización (redundante, configuración 2N).

- Reservas.

Así mismo tendrá dos embarrados para entrada/salida de SAI. Desde el embarrado de salida de SAI se alimentarán las siguientes salidas:

- Racks y equipos CPD (al menos una salida por embarrado para cada armario).
- Sistema de detección y extinción de incendios.
- Sistemas de CCTV y CCAA.
- Reservas.

En la entrada de los cuadros red/grupo y SAI, se instalaran descargadores, con el fin de evitar sobretensiones del Tipo II, garantizando así la protección ante cualquier pico de sobretensión, que pudiese venir por la red o grupo. En los embarrados críticos (SAI) se instalarán protectores de sobretensiones, diferenciales superinmunizados, analizador de red eléctrica, señales de estado y defecto de cada interruptor, etc. Esto permitirá tener controlado en todo momento tanto la instalación eléctrica como los posibles fallos que se pudiesen producir en ella.

Del cuadro general de CPD se suministra fuerza a través de interruptores generales a las vías de distribución. La distribución de corriente para las máquinas o armarios rack del CPD se canalizarán bajo el falso suelo siempre con redundancia de caminos físicos y por canalizaciones independientes y homologadas de acuerdo con IEC 439-1.

Se hará una distribución homogénea de fuerza en toda la sala y redundante, ya que de cada SAI llegará una línea a cada rack por caminos físicos diferentes y con sus correspondientes protecciones magnetotérmicas y diferenciales.

Con el fin de hacer frente al posible fallo de suministro eléctrico de la compañía, se instalará un grupo electrógeno, cuyo mando y control se realizará a través de un cuadro de mando automático por fallo de red. Este mando será capaz de detectar el fallo de red mediante un detector de tensión el cual, en caso de bajada del suministro de red de los límites establecidos, dará las órdenes correspondientes de arranque y transferencia de cargas de Red a Grupo y la supervisión del correcto funcionamiento del grupo electrógeno durante su servicio.

Una vez restablecido el suministro eléctrico de la compañía y comprobado que es un retorno estable, el control automático dará las órdenes de conmutación de Grupo a Red e iniciará el procedimiento de detención del grupo electrógeno.

El cuadro automático dispondrá de alarmas de fallo, a ser posible integrables en algún sistema de monitorización remota mediante algún tipo de protocolo estándar.

El sistema de alimentación ininterrumpida (SAI) tendrá redundancia 2N y deberá ser

ampliable en caliente. Por tanto, funcionarán en paralelo de forma redundante con el fin de conseguir un sistema de suministro eléctrico sin punto simple de fallo, y con suficiente capacidad individual de las unidades de SAI para que cualquiera de ellas pueda realizar el mantenimiento del suministro eléctrico. Esto implica que se podrán realizar las tareas de mantenimiento sin paso por cero.

Se recomienda una solución de SAI ampliables en caliente mediante adición de módulos de potencia, consiguiendo una reserva para la previsión del crecimiento futuro.

Si se quiere optimizar el espacio, es recomendable que la solución de SAI sea integrada en su propio armario con las baterías integradas en el mismo. Hay soluciones de varios fabricantes que ya contemplan esta integración y ofrecen su solución en armario con ampliaciones con armarios adicionales si fuese necesario, cada una tiene unas capacidades de potencia y ampliación que deben determinarse para cada proyecto en concreto según las necesidades.

Es recomendable que el equipo SAI emplee alguna técnica que evite el deterioro de las baterías. También es recomendable que el equipo pueda gestionable de forma remota vía IP y con protocolos de alarma y seguridad integrables con algún protocolo estándar en un sistema de monitorización.

La instalación deberá disponer de un sistema de *by-pass* manual con el cual se pueda desconectar la carga del SAI pudiendo ésta ser alimentada directamente de la red de entrada y al mismo tiempo, aislar completamente el SAI que se desee. Es altamente recomendable que estos seccionadores estén rotulados de manera inequívoca y que exista un esquema visible con los pasos a seguir para la realización de la maniobra *by-pass.*

También se recomienda que el equipo SAI tenga un mecanismo de *by-pass* automático en caso de detectadas como sobrecargas, sobretemperatura u otros problemas de funcionamiento.

Para garantizar la seguridad de personas y equipos ante posibles fugas de corriente y garantizar el disparo del diferencial, será necesario instalar un mallado de tierras equipotencial. Además, se evitarán bucles de corriente que podrían provocar fallos de comunicación y otros problemas.

La Red de Tierras contará con las siguientes características:

- Malla realizada mediante cable de cobre desnudo de 25 mm².
- Cable en forma de retícula de 2 m x 2 m.
- Uniones con los pedestales de soporte del falso suelo mediante bridas

conductivas.

- Conexión a la tierra eléctrica del edificio (cuadro eléctrico) mediante cable aislante.

- Cumplimiento de la normativa EN 50310 para sistema de tierras y equipotencialidad en CPD

En cuanto al diseño e instalación de los elementos del sistema de alumbrado se realizará teniendo en cuenta las siguientes características principales:

- La iluminación del CPD tendrá unos niveles aproximados de 500LUX en el plano de trabajo y 300LUX en el plano vertical medida a un metro del falso suelo en pasillo entre racks.

- Las luminarias estarán dotadas de rejilla anti deslumbramiento y reflector longitudinal para cada tubo fluorescente de led, con el fin de tener un ahorro energético.

- El encendido y apagado se realizará mediante detectores volumétricos de presencia, obteniendo así un mayor ahorro energético.

- En caso de ser un CPD que lo requiera, se realizará la sectorización de zonas, con el fin de mejorar la eficiencia y ahorro de energía.

- Los equipos contarán con Certificado CE de baja radiación electromagnética.

- Resistencia al impacto 20J o superior.

- Grado IP 50 o superior.

- Las vías de evacuación de emergencia serán iluminadas con equipos autónomos de iluminación de emergencia distribuidos por la sala, así como encima de las puertas para indicar las vías de emergencia, incluyendo rótulos indicadores.

- El sistema de iluminación de emergencia se llevará a cabo con lámparas fluorescentes de 18W, con una autonomía mínima de 60 minutos. Las baterías utilizadas serán recargables y libres de mantenimiento. Se realizará la distribución para acometer una iluminación de 30 Lux como mínimo

Adaptación de la solución a las características de mini CPD

En el caso de un pequeño CPD de uno o pocos armarios no tiene sentido realizar esta solución tan compleja a menos que la disponibilidad lo requiera.

El objetivo mínimo es mantener el sistema operativo el máximo tiempo posible con los menores cortes del servicio, pero todo el sistema puede abaratarse de acuerdo con los ANS necesarios.

Lo que es totalmente imprescindible es que los equipos tengan al menos un sistema SAI en línea que pueda comunicarse con los servidores para realizar un apagado ordenado. En cualquier caso, el SAI debe disponer de autonomía suficiente para permitir el apagado ordenado de los equipos de nuestro mini-CPD en caso de falta de suministro eléctrico.

Siempre sería necesario la instalación de un cuadro eléctrico independiente, aunque sólo sea con un embarrado para las entradas y salidas de corriente desde y hacia el SAI.

El grupo electrógeno no es estrictamente necesario, pero al igual que el resto de la solución, su necesidad va a depender de los SLA específicos de la solución a implantar.

En la ilustración siguiente se muestra un diagrama unifilar típico, sin redundancia de SAI, para un mini CPD de 5 armarios.

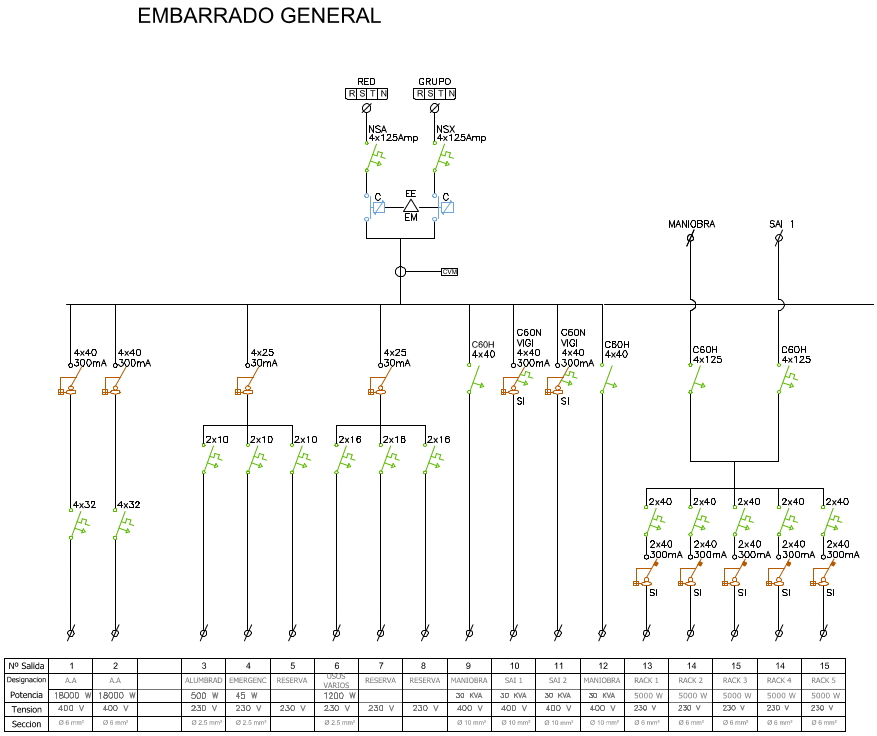

Ilustración 13: Diagrama unifilar 5 armarios. Fuente: propia de proyectos.

6.3 Climatización

El equipamiento que se instala en los CPD suele tener necesidades de climatización muy elevadas debido a la gran cantidad de calor que desprende.

El sistema de climatización es un factor importante para garantizar la disponibilidad y durabilidad del equipamiento. Para dimensionar el equipamiento, es importante tener en cuenta los datos de las temperaturas exteriores y exteriores para este tipo de proyecto. Para ello se pueden utilizar los datos que aparecen en la Guía técnica Condiciones climáticas exteriores de proyecto del IDEA [13] o los de la UNE 100001.

Las condiciones exteriores de funcionamiento pueden establecerse en una temperatura de bulbo seco de 22ºC y una humedad relativa del 50%

Las características del sistema de climatización deberán ser:

- Instalación de climatización independiente de la del resto del edificio.
- Funcionamiento 24 horas al día, 365 días al año.
- Estricto control de temperatura de la sala (22º C +/- 1ºC).
- Filtración de partículas según EU4.
- Funcionamiento en configuración 2N paralelo redundante, de forma que la climatización de la sala esté garantizada en sus condiciones de máxima ocupación y utilización dejando siempre un equipo en estado de reserva para cubrir posibles paradas por avería o mantenimiento de los equipos. La rotación de los equipos se producirá de forma automática, entrando el de reserva cuando le corresponde o cuando se averíe uno de los equipos en funcionamiento.

Solución de climatización

En la solución se propone un sistema de climatización realizado a través de sistema *plenum* por el falso suelo, de manera que se optimice al máximo la eficiencia energética.

En el método de refrigeración con equipos de impulsión inferior a falso suelo la máquina de aire acondicionado aspira el aire caliente por su parte superior. Este aire es tratado y se impulsa por la parte inferior del equipo al suelo interior del suelo técnico, donde se creará una sobrepresión y a través de las rejillas de suelo estratégicamente colocadas (con regulación manual de caudal), el aire frío llegará directamente a cada uno de los racks que se refrigerará de abajo a arriba y de delante hacia atrás (el equipamiento para montaje en rack suele utilizar entrada de aire delantera con expulsión trasera).

Estará compuesto por máquinas de control estricto específicas para salas informáticas y control micro procesado de temperatura y humedad del tipo servicio total, capaz de producir frío y humectar o des humectar de forma automática, dentro de unos márgenes de ± 1º C y ± 5% HR para valores de funcionamiento previstos de 22ºC y 50% HR.

Las unidades de refrigeración que compondrán el sistema serán dedicadas en exclusiva a la sala CPD. Por lo tanto, no compartirán el frío generado con ningún otro sistema.

Las máquinas de aire que se instalarán estarán equipadas con un sistema de filtros con una eficiencia mayor del 90% sobre partículas de 1 micrón.

Las unidades de climatización estarán diseñadas para un funcionamiento continuo de 24 h/día y 365 días/año y su potencia frigorífica para una temperatura de bulbo seco interior adecuada. El sistema será capaz de mantener las características de la sala o de los equipos para las variaciones de temperatura ambiente medias registradas en el momento de acometer la obra del pequeño CPD.

Se instalará una configuración 2N, redundante que, en el caso de avería de una de las máquinas permita seguir funcionando al sistema con el 100% de la potencia frigorífica necesaria.

Se instalarán sondas de temperatura y humedad relativa para registrar los parámetros dentro de la sala, los cuales darán constancia de las anomalías en el sistema de climatización.

Se implementará un sistema de aislamiento de pasillo que puede mejorar el funcionamiento de la refrigeración del CPD, teniendo en cuenta que este debe tener una configuración de pasillo frío/pasillo caliente. El aislamiento de pasillo frío separa constantemente las áreas frías y las calientes si necesidad de realizar cambios estructurales en el CPD.

Un sistema de este tipo, si está bien realizado, podría suponer un ahorro de costes de hasta un 25% [14].

Un método convencional de refrigeración hace circular el aire frío desde la sala de los equipos de aire acondicionado de precisión (CRAC) a través del falso suelo. Las unidades de CRAC se colocan alejadas de las filas de rack, alrededor del perímetro del CPD.

Configurar los racks en pasillo caliente/pasillo frío es una de las mejores formas de refrigerar que se pueden implementar para mejorar la eficiencia de los centros de datos con suelo técnico.

Sin embargo, el aire caliente se puede mezclar con el aire frío en la parte superior de los racks y al final de los pasillos fríos. En algunos casos, la temperatura resultante del aire mezclado puede ser inaceptablemente alta en la parte superior de los servidores y al final de los pasillos. La mezcla del aire caliente y frío se puede agravar por un equilibrio inadecuado entre la demanda total de aire frío de los racks y del aire total suministrado desde las rejillas del pasillo. El aumento de la circulación de aire en los pasillos fríos puede

ayudar a reparar condiciones desequilibradas, pero esto aumentará el consumo de energía, haciendo que sea una solución menos eficiente.

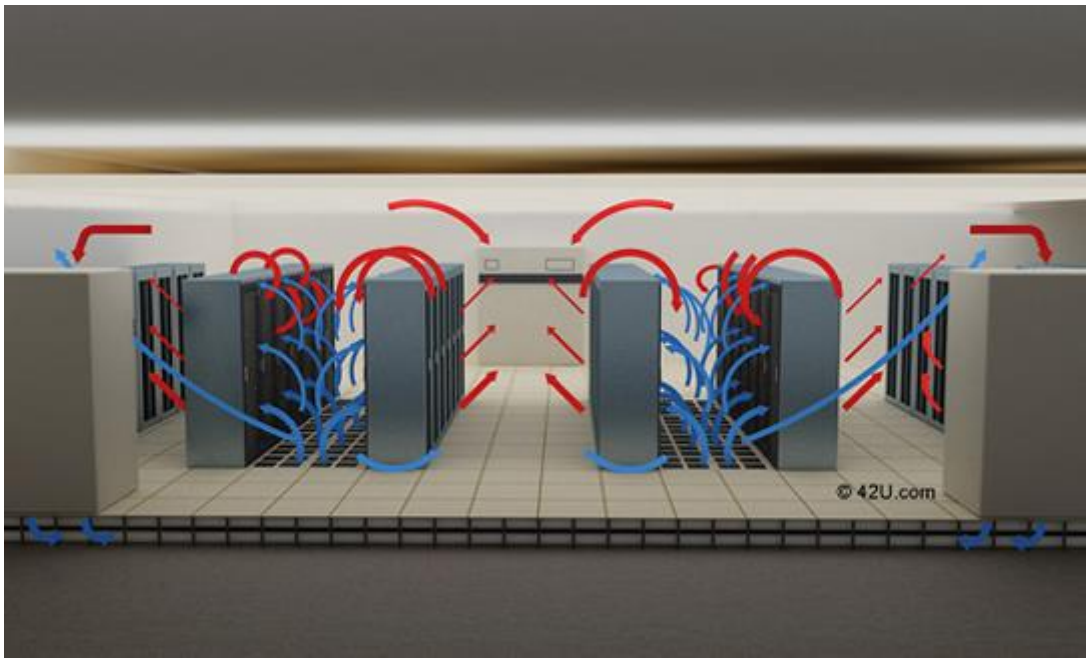

Ilustración 14: Pasillo frío caliente sin aislar. Fuente: Energy Star [15]

Los pasillos aislados trabajan para remediar esta situación. Antes de instalar un pasillo aislado, se deben tomar medidas para mejorar el rendimiento del consumo energético total del sistema de refrigeración.

La mayoría de los equipos fabricados hoy en día están diseñados con una entrada de aire frontal y una salida en la parte posterior. Esto permite que los racks se puedan colocar de forma enfrentada para crear pasillos calientes y pasillos fríos. De esta manera, el aire frío entra a los racks por el pasillo frío y se expulsa hacia al pasillo caliente, lo que permite que los racks puedan estar más cerca unos de otros y dispuestos frente a frente hacia el pasillo frío. elevando la temperatura del aire en este pasillo y haciendo funcionar la unidad CRAC, lo que permite que tenga un rendimiento más eficiente.

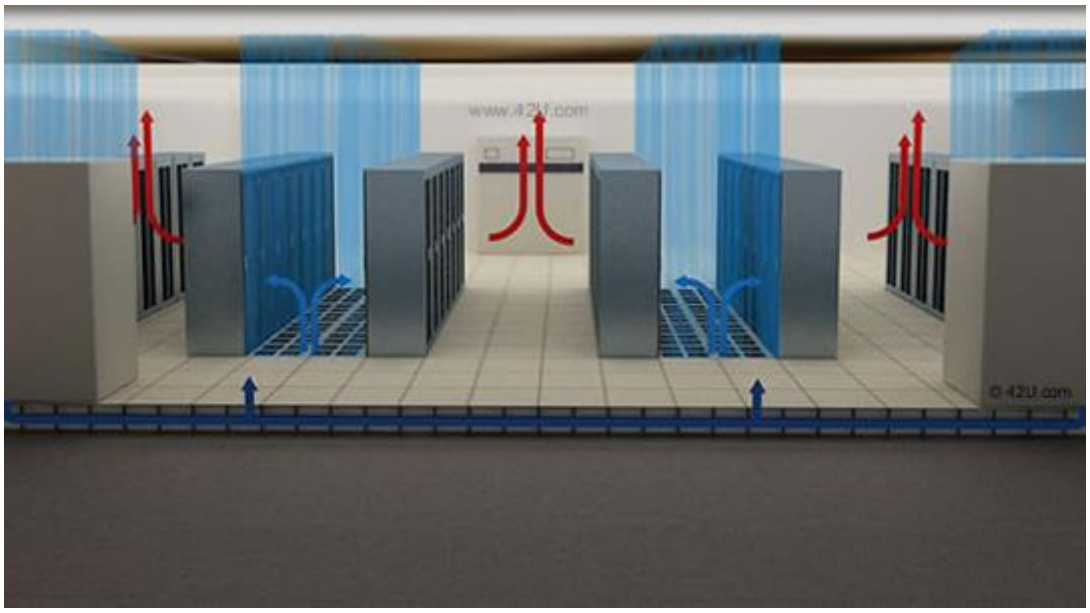

Ilustración 15: Pasillos fríos aislados: Imagen tomada de Energy Star [15]

El aislamiento de pasillo tiene dos ventajas. En primer lugar, aumenta la capacidad de refrigeración y el rendimiento energético de la unidad de refrigeración, asegurándose de que temperatura del aire que vuelve a la unidad de refrigeración sea elevada. En segundo lugar, la separación de aire caliente y frío permite refrigerar mayores cargas de calor por rack.

Si el aire que vuelve a la unidad de refrigeración es más caliente, se aumenta su capacidad para refrigerar el calor generado por el equipo electrónico. Bajo estas condiciones la temperatura del aire frío suministrado estará casi siempre por encima del punto de condensación. Por lo tanto, hay una mínima condensación (enfriamiento latente), lo que supone un ahorro de energía al asignar la mayor parte de la capacidad de refrigeración en disipar el 100% de la carga de calor. El mínimo enfriamiento latente también aumenta el rendimiento energético total debido a que la rehumectación del aire no se realizará tan a menudo.

En la imagen, Ilustración 16: CFD con y sin aislamiento, se observa un ejemplo de temperaturas del aire con CFD (Computacional Fluid Dynamics – Dinámica Computacional de Fluidos) en una sala de racks de alta densidad CRAC refrigerados por el sistema tradicional de falso suelo.

Se muestra una refrigeración aislada y uniforme en los pasillos fríos que utilizan el sistema CAC (del inglés *Cold Aisle Containmnet) en* comparación con la imagen donde no se utiliza este sistema. La temperatura media del aire de vuelta a la unidad CRAC sin CAC

menos elevada que con CAC.

La instalación del sistema de climatización debe realizarse por una empresa especializada del sector,

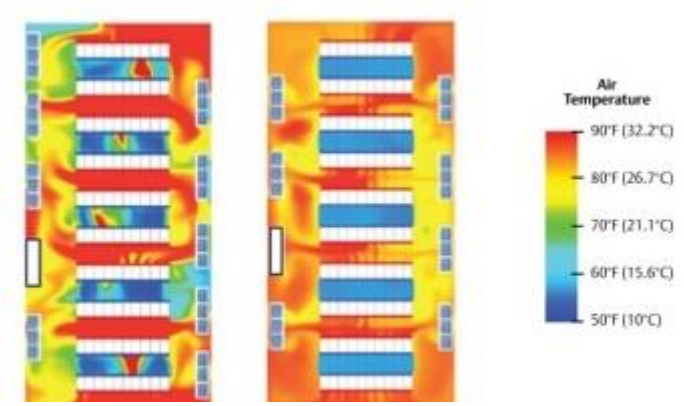

Ilustración 16: CFD con y sin aislamiento. Fuente: Búsqueda imágenes en Bing – Encontrado en Techtarget

En cualquier caso, es recomendable que el sistema de climatización esté supervisado (funcionamiento, temperatura y humedad) por un sistema de gestión automatizado que produzca las alertas correspondientes en caso de problemas y registre las incidencias de funcionamiento diario de los equipos.

Es imprescindible también la realización de revisiones periódicas, según las especificaciones de equipamiento y recomendaciones del fabricante y/o la empresa instaladora.

Adaptación de la solución a las características de mini CPD

En el caso de un mini CPD de uno a tres armarios, no ha lugar a un sistema tan complejo y se podría utilizar un sistema de refrigeración menos complejo, lo ideal es que fuese un sistema de aire específico para salas de CPD, pero, en cualquier caso, siempre es mejor tener una pequeña sala con aire acondicionado independiente, a ser posible con control de humedad, aunque sea un equipo de *split* doméstico que no tener ningún tipo de refrigeración.

Tener una solución 2N en estos casos puede ser complejo y aumentar los considerablemente ya que el calor que emite un solo armario, dependiendo de la ubicación y las condiciones climáticas puede ser disipado de muchas formas durante un período corto de reparación del equipo de refrigeración, por ejemplo, con una máquina de aire acondicionado portátil.

6.4 Seguridad física

Para controlar el acceso al CPD se instalará un sistema de control de accesos conectado a la red de monitorización del CPD y CCTV a través de protocolo TCP/IP para todas las puertas de acceso al CPD (y puertas de división de zonas si existiesen), debiendo haber lectores de control de acceso tanto a la entrada como a la salida. Evidentemente las puertas en dirección de salida podrán accionarse con la barra antipánico sin usar el

sistema de control de accesos, pero esto debe generar una alarma que quede registrada en el sistema.

Una posible solución se puede basar en un sistema de control de acceso con lectores de proximidad de tarjetas. Lo ideal es que al lado de cada lector se habilite un interfono para contactar mediante audio con algún centro de control ante cualquier incidencia.

El circuito cerrado de CCTV puede realizarse a través de cámaras de vigilancia que se grabarán y almacenarán durante el máximo periodo de retención permitido por la legislación vigente en algún tipo de grabador o en un servidor remoto en otro sitio (en la nube). En caso de grabación en servidor remoto las cámaras o el sistema CCTV deberán disponer de un sistema de almacenamiento en local que les permita mantener las grabaciones de imágenes como mínimo el tiempo de falla que se permita en el SLA del contrato de almacenamiento de imágenes en el servido remoto.

Si el edificio ya dispone de un sistema de control de accesos o CCTV adecuado se podrán integrar estos sistemas con los previamente existentes (ampliación).

Adaptación de la solución a las características de mini CPD

En caso de pequeños mini CPD de uno o pocos armarios se puede considerar la siguiente opción para abaratar costes:

- Eliminar el control de acceso en base a un sistema de llave tradicional con registros de acceso. En este caso debe haber un responsable de las llaves que se encargará de llevar un registro de entrada salida y seguir el protocolo oportuno.

En cuanto al CCTV estos CPD podrían vigilarse casi en su totalidad con una cámara, por lo tanto, la recomendación es que al menos se instale una con algún sistema de grabación.

6.5 Extinción de incendios

Sistema de detección de incendios

El sistema de protección contra incendios (PCI) recomendado se basará en un sistema de detección de humo por aspiración [16] que actúa con un principio de detección sencillo y suele estar construido de una forma altamente modular. Se compone básicamente de dos elementos principales: las tuberías de muestreo de aire en la zona controlada y el detector de humo que puede ubicarse en otro lugar. Un extractor integrado en el detector de humo produce una presión negativa en las tuberías de muestreo. Esta presión negativa genera un flujo de aire constante aspirado a través de los puntos de muestreo que se

definan en la instalación, siendo este un sistema de detección precoz.

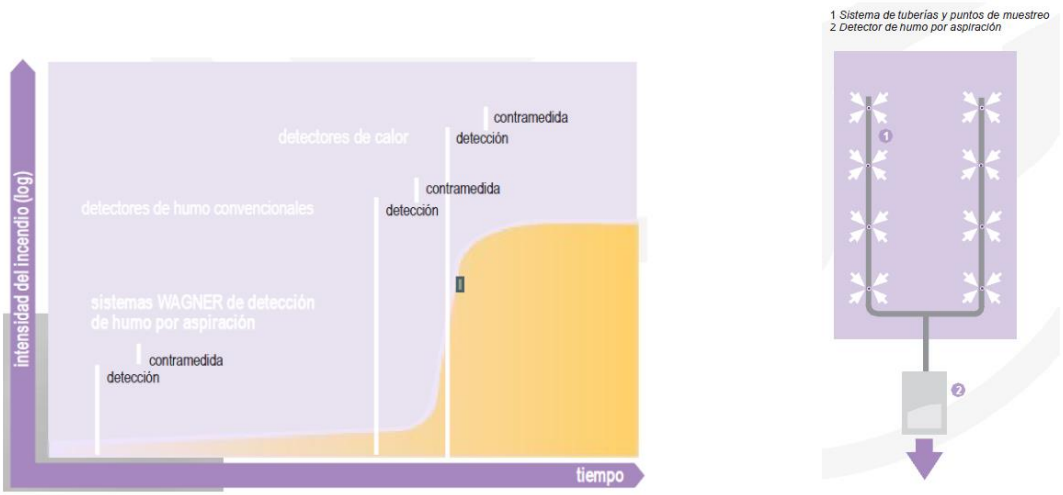

Ilustración 17: Sistema de detección por aspiración. Fuetnte: Gráficos comerciales de una oferta con WAGNER

En la cámara de medida del detector, se analiza la existencia de partículas de humo. Para la eliminación de falsas alarmas, un procesador de señales inteligente analiza los datos medidos y los compara con patrones típicos característicos del fuego.

Estos sistemas de tipo precoz de aspiración tienen por misión detectar lo más rápido posible la existencia de un incendio.

El detector suele disponer de al menos do sensores independientes para mayor seguridad, con dos sensibilidades distintas (típica 0,1 % y 0,5%) de oscurecimiento/m. Los ledes de alta eficacia detectarán fuego en la etapa más temprana posible y medirá confiablemente concentraciones de humo desde las muy bajas a las extremadamente altas. El aire será aspirado hacia dentro a través de una red de tubos de muestreo de aire mediante un aspirador de alta eficiencia. Cada vez que se monitoricen los cambios en el flujo de aire en el tubo, la muestra del aire se hará pasar hacia la cámara de detección a través de filtros de aire de doble etapa. El sistema monitorizará el ambiente y ajustará los umbrales de alarma apropiados (alerta, acción, fuego 1 y fuego 2) durante el proceso de puesta en servicio para permitir la advertencia más temprana posible de una situación potencial de incendio, sin falsas alarmas.

Los sistemas de aspiración de humos disponen del denominado efecto colectivo. Este efecto se produce si en una sala hay varios puntos de extracción de muestras de aire y están expuestos al humo del fuego al mismo tiempo. Por esta razón, la sensibilidad de la respuesta de un sistema de aspiración de humos tiene muchas ventajas.

El poder del efecto colectivo depende del tamaño de la zona controlada y de la altura de una sala. En salas con techos altos puede suponerse un efecto colectivo de hasta un

50%. Esto significa que al menos la mitad de todos los puntos de extracción de muestras de aire, estén normalmente expuestos al humo.

Incluso sin este efecto colectivo, los sistemas de aspiración de humos constituyen ya, sin embargo, una alternativa suficientemente válida a los detectores convencionales. Unas unidades de detección muy desarrolladas permiten una sensibilidad hasta 5.000 veces mayor que la de los detectores convencionales.

Mediante una fuente de luz de gran potencia (HPLS), la sensibilidad de los módulos de detección es hasta 5.000 veces mayor que la de los detectores de humo convencionales y garantiza un comportamiento en respuesta homogéneo ante diferentes tipos de fuego. En comparación con sistemas convencionales de detección de humo por aspiración, el flujo de aire principal no es conducido a un punto de detección, sino a una cámara de medición que está especialmente diseñada para evitar el depósito de partículas de polvo.

El sistema de detección será controlado por un panel de control que deberá presentar la información de incidencias producidas mediante indicaciones luminosas y acústicas.

Sistema de extinción de incendios

El sistema de protección contra incendios deberá dimensionarse de acuerdo con el tamaño del CPD, respetuoso con el medio ambiente y no perjudicial para las personas. Estará diseñado para proteger los bienes internos del CPD en cada disparo.

Existen múltiples soluciones en el mercado, pero una solución sin coste muy elevado se puede realizar con el uso de gas inerte para recintos cerrados FE-13. El FE-13 o trifluorometano es un agente extintor limpio de baja presión, que extingue los incendios principalmente por absorción de calor, su baja toxicidad lo hace el gas más seguro para proteger las áreas donde las personas están presentes. Gracias a su alta presión de vapor a temperatura ambiente (41 bar a 20ºC) el FE-13 no requiere presurización con nitrógeno. El bajo punto de ebullición del FE-13 permite el almacenamiento de los contenedores que se encuentran en zonas remotas, lejos del espacio protegido, así como en otros lugares a temperatura ambiente.

Los principales componentes del sistema son:

- Cilindro(s) de gas.
- Difusores de gas.
- Distribución de canalizaciones para gas.
- Rotulo luminoso de “extinción disparada” o similar.

- Pulsadores de “alarma”, “paro de extinción” y “disparo de extinción”.
- Sirena de alarma.
- Botellas de gas inerte que dispongan de válvulas de disparo automático, electroválvulas y presostato.

Es recomendable que las botellas sean supervisadas por un sistema de pesaje continuo que permita detectar mediante algún tipo de sistema de alarma, las pérdidas de peso, averías de equipo o averías de cualquier otro equipo de control de pesaje conectadas al sistema.

Pulsadores y sirenas

La situación de los pulsadores de alarma irá correctamente señalizada conforme a lo establecido en la normativa aplicable y a lo especificado en la norma UNE 23034 con una distancia máxima de 25m, en pasillos de recorrido horizontal. Su señal será identificada individualmente en la centralita de detección.

Estarán provistos de dispositivos de protección para no activarlos involuntariamente, irán correctamente rotulados y serán de distintos colores.

- Pulsador de bloqueo de extinción. Anula el disparo del sistema de extinción. Color azul.
- Pulsador de disparo de extinción. Provoca el disparo del sistema de extinción. Color amarillo.
- Sirena de alarma

La sirena de alarma se activará al actuar cualquier línea de detección o pulsador, bien de forma manual o a través de la centralita.

La instalación de sirenas de alarma tiene como misión el dar a conocer a los ocupantes de una zona la existencia de un incendio mediante una señal acústica. Estarán situadas de tal forma que sus señales deberían ser perceptibles en todo el recinto con un nivel sonoro de 85 dB_{SPL}.

Extintores manuales

Se instalarán extintores móviles de acuerdo con la normativa vigente. El tipo de extintor vendrá determinado por la clase de fuego a combatir, establecido en la norma UNE EN 23010 y la distancia máxima a un extintor no será superior a 15m.

En una buena solución el sistema PCI deberá integrarse mediante la correspondiente red con los sistemas de seguridad o monitorización restantes, como CCTV o control de

accesos.

Adaptación de la solución a las características de mini CPD

Los sistemas aquí expuestos tienen un coste considerable que es adecuado para una PYME de ciertas dimensiones, pero en el caso de una pequeña PYME con de uno a tres armarios de infraestructura pueden suponer un coste muy elevado. Para estos casos debe contemplarse el principio de una solución económica, aunque no sea óptima, es mejor que ninguna solución. Es por ello por lo que se considera que el mini CPD deberá contemplar los siguientes sistemas de PCI

- Sistema de detección de incendios con alarma sonora, aunque sea un sistema tradicional conectado al sistema del resto del edificio.

- Disponer de medios de extinción de incendios, si es posible automático, pero en su defecto extintores manuales próximos que permitan sofocar un fuego en el mini CPD de forma rápida.

Estas dos medidas no tienen un coste muy alto y permitirán la extinción de pequeños incendios localizados dentro del CPD, la protección ante un gran incendio no tiene garantías de supervivencia del equipamiento si el sistema de extinción es manual.

7. Cuadro resumen de soluciones

El presente cuadro resumen, pretende servir de hoja de selección de soluciones para que el usuario pueda determinar el nivel de implementación que desea realizar.

Los distintos elementos incluyen un indicador de calidad (C) entre 1 y 3, siendo 3 la solución que ofrece más disponibilidad, versatilidad y/o funcionalidades, pero también la más cara. Por lo tanto, el indicador C puede ser un buen indicador para seleccionar el tipo de medida a implantar según el presupuesto que se maneje. Algunas soluciones no tienen sentido sin otras y están en el mismo indicador, por ejemplo, el generador está en un indicador 3 y la solución de cuadro eléctrico con conmutación automática también. Las soluciones pueden tomarse de forma independiente según las necesidades, por ejemplo, una empresa por su ubicación puede tener una necesidad de un sistema de aire acondicionado que no falle y sin embargo no necesitar grupo electrógeno.

C	Elemento	Variante
Hardware de servidor		
1	Hardware sin elementos redundados	
2	Hardware con elementos redundados	Sin soporte in situ
3	Hardware con elementos redundados	Con soporte
Acceso remoto y seguridad		
Acceso remoto basado en escritorio o aplicaciones remotos		
1	Acceso remoto mediante ThinStuff XP/VPS	
2	Acceso remoto mediante servicios de escritorio remoto de Microsoft	
3	Acceso remoto mediante Citrix	
Acceso remoto a aplicación web		
1	Acceso remoto mediante acceso directo a puertos de la aplicación	Sin filtrado *firewall*
2	Acceso remoto mediante acceso directo a puertos de la aplicación	Con filtrado *firewall* o acceso por VPN
3	Acceso remoto mediante acceso directo a puertos de la aplicación	Con filtrado de *firewal*l y/o VPN de proveedor reconocido y mantenimiento
Soluciones de arquitectura y seguridad de red		
1	Equipo con un solo interfaz de red y un solo equipo y *firewall* virtual	
2	Equipo con al menos dos interfaces de red, sin VLAN y *firewall* virtualizado	

3	Equipo con dos o más interfaces de red, uso de VLAN y *firewall* virtualizado	
Mejora del sistema de copias de seguridad		
1	Sistema PBS en el mismo servidor que el PVE	En una VM
1	Sistema PBS en el mismo servidor que el PVE	En mismo host
2	Sistema PBS en su propio servidor en la misma ubicación	
3	Sistema PBS en local con otro PBS en una ubicación remota	
Aumento de disponibilidad de la arquitectura de la solución		
2	Redundancia a nivel de red local	
3	Redundancia a nivel de red local + Internet	
1	Redundancia a nivel de servidor preinstalado y restauración de copias	
2	*Cluster* Proxmox VE de dos servidores	Sin almacenamiento compartido
3	*Cluster* Proxmox VE de do s servidores	Con almacenamiento compartido
3	*Cluster* Proxmox VE de 3 o más servidores	
Acondicionamiento de sala de ordenadores (CPD)		
1	Cerramiento con protección sobre el fuego (Incluida puerta)	mínimo 60 minutos
2	Cerramiento con protección sobre el fuego (Incluida puerta)	mínimo 120 minutos
3	Cerramiento RF 7120 mediante paneles y sellado	
1	Medidas en caso de peligro de inundación	Constructivas
2	Medidas en caso de peligro de inundación	Constructivas y de detección proactiva
2	Suelo técnico	
2	Bandejas de cableado y canalizaciones bajo suelo técnico	
1	Sistema alimentado mediante SAI	1 SAI
2	Sistema alimentado mediante SAI	2 SAI
3	Sistema alimentado mediante SAI	2 SAI con capacidad total simultánea
3	Grupo electrógeno	
1	Cuadro eléctrico específico para el CPD	
2	Cuadro eléctrico específico con embarrados independientes	
3	Cuadro eléctrico específico con embarrados independientes y conmutación automática Red-Grupo	
3	Red de toma de tierras	
1	Climatización con equipo estándar no de CPD	
2	Climatización con equipo específico de CPD	Sin redundancia

3	Climatización con equipo específico de CPD	Con redundancia total
3	Cerramiento de pasillos y distribución en pasillos fríos y calientes	
2	Control de accesos	
3	CCTV	
1	Sistema de detección de incendios común del edificio	
3	Sistema de detección de incendios específicos de CPD por sistema de aspiración	
1	Sistema de extinción de incendios basado en extintores	
2	Sistema de extinción de incendios específico para CPD con autodisparo	
3	Sistema de extinción de incendios específico para CPD con autodisparo y monitorización de estado	

8. Conclusiones

En el presente TFG se han presentado diversas soluciones que parten de una solución básica para una pequeña PYME conformada por un simple servidor virtualizado y que le permiten ir creciendo a medida que lo va necesitando.

En general, las soluciones son incrementales, es decir, pueden irse aplicando unas sobre las otras, de un servidor, podemos pasar a dos, de una sala sin acondicionar podemos pasar a un mini CPD, etc.

La descripción de soluciones no está exenta de intervención de terceras partes, puesto que hay determinadas situaciones que requieren de personal experto externo a la solución tecnológica, por ejemplo, la instalación de un sistema de aire acondicionado.

La idea del proyecto es que exista un conocimiento de pasos y medidas a tomar para responsables de empresas con conocimientos informáticos básicos. Y aunque algunas soluciones presentadas puedan requerir un conocimiento más experto, la idea no es que lo implemente una persona sin esos conocimientos, sino que pueda entender que es lo que tiene que solicitar a alguien que sí los tenga.

Ha sido muy difícil o imposible en algunos casos no hablar en términos específicos de las soluciones, aunque se ha intentado minimizar la terminología técnica, hay conceptos, por ejemplo, de obra civil que una persona con conocimientos informáticos necesariamente tendría que conocer, y que podrían explicarse de una forma más comprensible para el usuario medio de esta guía.

Originalmente al empezar este TFG se pensó en incluir presupuestos para las distintas soluciones, pero era tal la granularidad y la dependencia específica que se llegó a la conclusión de que era inviable, por eso en el resumen final se ha incluido el indicador de calidad.

El factor tiempo ha sido muy determinante a la hora de la redacción de este proyecto, aunque se ha podido seguir la planificación del proyecto base, en cuanto a aquellos puntos marcados como hitos, llegando en plazo y forma, en tareas intermedias han existido desplazamientos considerables en el tiempo con retrasos de incluso semana y media. La realidad es que la disponibilidad de tiempo, en caso de personas en cuya vida, además de la parte académica también existen una parte familiar y laboral, la gestión del tiempo es especialmente compleja.

En cualquier caso, haciendo modificaciones en el calendario de recursos del proyecto y modificaciones en tareas intermedias se ha conseguido el cumplimiento de las entregas necesarias.

Este trabajo podría ampliarse de muchas formas, por ejemplo, a partir de este catálogo y centrándose en un sector en concreto, se podrían plantear soluciones cerradas que diesen solución a situaciones específicas.

No se ha entrado en factores específicos, donde se podría entrar, como por ejemplo el cableado de datos, tipos de canalizaciones, etc.

Queda pendiente la inclusión de un sistema de monitorización centralizado desde el que se pudiese realizar la gestión de todos los sistemas, pero esto quedará para un futuro. Hay grandes soluciones en el mercado, como Zabbix por ejemplo que podrían, si nos metemos en la parte técnica abarcar un TFG entero.

9. Glosario

La mayoría de las definiciones aquí reflejadas han sido recogidas literalmente de Wikipedia. En algunos casos se han modificado o redefinido completamente para que fuesen correctas o más inteligibles.

Acuerdos de nivel de servicio, ANS o SLA: Un acuerdo de nivel de servicio (siglas ANS), también conocidas por las siglas SLA (del inglés Service Level Agreement), es un acuerdo escrito negociado entre dos partes donde una de ellas es el cliente y la otra un proveedor de servicios con objeto de fijar el nivel acordado para la calidad de dicho servicio, 1

Autenticación de doble factor: a autenticación de dos factores (A2F), también usada la sigla inglesa 2FA (de two-factor authentication), es un método que confirma que un usuario es quien dice ser combinando dos componentes diferentes de entre; 1) algo que saben; 2) algo que tienen, 11

Bonding: es una tecnología que permite la agregación de múltiples enlaces en un solo enlace virtual, lo que permite obtener tasas de datos más altas y brindar soporte a fallos en caso de fallo de alguno de los enlaces físicos que lo conforman.., 20

CAD: diseño asistido por computadora (o diseño asistido por ordenador, en España) habitualmente conocido como CAD por sus siglas en inglés computer-aided design, es el uso de computadores para ayudar en la creación, modificación, análisis u optimización de un diseño. El software CAD se utiliza para aumentar la productividad del diseñador, mejorar la calidad del diseño, mejorar las comunicaciones a través de la documentación y crear una base de datos para la fabricación., 5

CCTV: El circuito cerrado de televisión (en inglés closed circuit television, CCTV) es una tecnología de videovigilancia diseñada para supervisar una diversidad de ambientes y actividades. Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión, todos sus componentes están enlazados. Además, a diferencia de la televisión convencional, este es un sistema pensado para un número limitado de espectadores., 33

CG-NAT: Carrier-Grade NAT (CGN o CG-NAT) también conocido como NAT masivo o NAT a gran escala (Large-Scale NAT o LSN), es una herramienta de diseño de redes IPv4 donde los extremos de la comunicación, en concreto, las redes residenciales, se configuran con direcciones de red privadas, que se traducen a direcciones públicas mediante equipos de traducción que se interponen dentro de la red del proveedor entre el usuario e Internet. Estos dispositivos permiten compartir conjuntos pequeños de direcciones públicas entre muchos puntos finales. Esto cambia el lugar tradicional donde se hace y se configura la función de NAT desde el equipo de casa del cliente, hacia la red del proveedor de acceso a Internet., 12

Cluster: Un clúster es un conjunto de ordenadores que trabaja en conjunto por lo que pueden ser vistos como uno mismo. En este caso un clúster de servidores Proxmox VE se pude ver como el conjunto de servidores que se utiliza para dar soporte a las máquinas virtuales de la empresa., 21

Copia incremental: Se basa en copiar solamente los datos que han sufrido algún cambio., 21

core: Un core (o núcleo) es cada una de las unidades de procesamiento que conforman un procesador multinúcleo que está integrado en un solo circuito, cada una de las cuales lee y ejecuta instrucciones de programa., 11

CPD: Centro de Proceso de Datos (CPD) (en inglés; data center o data centre) al edificio o sala usada para mantener en él una gran cantidad de equipamiento informático y electrónico, 2

CRM: La gestión o administración de relaciones con el cliente (customer relationship management), más conocida por sus siglas en inglés CRM. En este caso nos referimos al Software para la administración o gestión de la relación con los clientes, es decir los, sistemas informáticos de apoyo a la gestión de las relaciones con los clientes, a la venta y al marketing, 4

Deduplicación: a deduplicación de datos es una técnica especializada de compresión de datos para eliminar copias duplicadas de datos repetidos. Un término relacionado con la deduplicación de datos es la compresión inteligente de datos. Esta técnica se usa para optimizar el almacenamiento de datos en disco y también para reducir la cantidad de información que debe enviarse de un dispositivo a otro a través de redes de comunicación., 21

DHCP: El protocolo de configuración dinámica de host (en español; Dynamic Host URL https Configuration Protocol, también conocido por sus siglas de DHCP), desarrollado a partir de 2002 como extensión de IP, es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP., 19

DNS: El sistema de nombres de dominio (Domain Name System o DNS, por sus siglas en inglés)1 es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombres de dominio asignados a cada uno de los participantes. Su función más importante es «traducir» nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente., 12

ERP: Los sistemas de planificación de recursos empresariales (ERP, por sus siglas en inglés, enterprise resource planning) son los sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía en la producción de bienes o servicios. Un ERP debería ser un sistema especializado que permita la unificación y organización de todas las áreas, es decir, ser un sistema que permita la trazabilidad de todos los procesos y, por lo tanto, dé paso a la planificación y optimización de los recursos., 4

HA: Alta disponibilidad (High availability) es un protocolo de diseño del sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional durante un período de medición dado., 28

Hot spare: unidades preinstaladas que pueden usarse inmediatamente (y casi siempre automáticamente) tras el fallo de un disco del RAID. Esto reduce el tiempo del período de reparación al acortar el tiempo de reconstrucción del RAID., 6

HTTP: El Protocolo de transferencia de hipertexto (en inglés; Hypertext Transfer Protocol, abreviado HTTP) es el protocolo de comunicación que permite las transferencias de información a través de archivos (XML, HTML…) en la World Wide Web., 12

IP: Una dirección IP (del inglés, Internet Protocol) es una etiqueta numérica que identifica de manera lógica y jerárquica a una interfaz —habitualmente un dispositivo— conectada a la red, que utilice el protocolo de internet o que corresponda al nivel de red del modelo TCP/IP., 12

IPv4: Protocolo de Internet versión 4 (en inglés; Internet Protocol version 4, IPv4) es la cuarta versión del Internet Protocol (IP), un protocolo de interconexión de redes basados en Internet, y que fue la primera versión implementada en 1983 para la producción de ARPANET. Usa direcciones de 32 bits, limitadas a 4.294.967.296 direcciones únicas. Por el crecimiento enorme que ha tenido la seguridad electrónica y la automatización, combinado con el hecho de que hay desperdicio de direcciones en muchos casos ya hace varios años se observó que escaseaban las direcciones IPv4., 12

iSCSI: iSCSI (Abreviatura de Internet SCSI) es un estándar que permite el uso del protocolo SCSI sobre redes TCP/IP. iSCSI es un protocolo de la capa de transporte definido en las especificaciones SCSI-3., 22

LAN: Una red de área local o LAN (por las siglas en inglés local rea network) es una red de computadoras que permite la comunicación y el intercambio de datos entre diferentes dispositivos a nivel local, ya que está limitada a distancias cortas., 16

LTO: Linear Tape-Open (LTO) es una tecnología de cinta magnética de almacenamiento de datos, desarrollada originalmente a finales de 1990 como alternativa de estándares abiertos a los formatos de cinta magnética patentada que estaban disponibles en ese momento, 9

NAS: El almacenamiento conectado en red, Network Attached Storage (NAS), es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador/ordenador (servidor) con computadoras personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un sistema operativo optimizado para dar acceso a través de protocolos que permiten el acceso a ficheros en sistemas remotos, 28

NAT: La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT (del inglés Network Address Translation), es un mecanismo utilizado por routers IP para cambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados., 14

VPN: Una red privada virtual (RPV) (en inglés, virtual private network, VPN) es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet., 12

Wiki: (palabra que proviene del hawaiano wiki, 'rápido') alude al nombre que recibe una comunidad virtual, cuyas páginas son editadas directamente desde el navegador, donde los usuarios crean, modifican, corrigen o eliminan contenidos que, habitualmente, comparten., 8

10. Bibliografía

[1] Telecommunications Industry Assosiation, «TIA 942 CERTIFICATIONS & RATINGS,» 2020. [En línea]. Available: https://tiaonline.org/products-and-services/tia942certification/tia-942-certifications-ratings/. [Último acceso: 20 03 2023].

[2] Proxmox Server Solutions GmbH, «Proxmox Virtual Environment,» 2023. [En línea]. Available: https://www.proxmox.com/en/proxmox-ve. [Último acceso: 20 03 2023].

[3] Proxmox Server Solutions GmbH, «Proxmox VE Documentation Index,» 22 03 2023. [En línea]. Available: https://pve.proxmox.com/pve-docs/. [Último acceso: 23 03 2023].

[4] H. Lohr, C. Cooper y y. o. c. d. A. Docs, «Directrices de ajuste de tamaño de máquina virtual del host de sesión,» 03 03 2023. [En línea]. Available: https://learn.microsoft.com/es-es/windows-server/remote/remote-desktop-services/virtual-machine-recs. [Último acceso: 29 03 2023].

[5] S. Parra Sáez, «Copias de seguridad: una obligación legal,» 24 06 2008. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/copias-de-seguridad-una-obligacion-legal. [Último acceso: 27 03 2023].

[6] Ministerio de Gracia y Justicia, «BOE: Real Decreto de 22 de agosto de 1885 por el que se publica el Código de Comercio. Texto Consolidado,» 11 01 1996. [En línea]. Available: https://www.boe.es/buscar/act.php?id=BOE-A-1885-6627&b=20&tn=1&p=19961101. [Último acceso: 27 03 2023].

[7] Jefatura del Estado, «BOE:Ley 58/2003, de 17 de diciembre, General Tributaria. Legislación consolidad,» 24 12 2022. [En línea]. Available: https://www.boe.es/buscar/act.php?id=BOE-A-2003-23186. [Último acceso: 27 03 2023].

[8] Proxmox Server Solutions GmbH, «Proxmox Wiki,» 28 03 2023. [En línea]. Available: https://pve.proxmox.com/wiki/Main_Page. [Último acceso: 11 04 2023].

[9] «Proxmox Backup Server,» 2023. [En línea]. Available: https://www.proxmox.com/en/proxmox-backup-server. [Último acceso: 11 04 2023].

[10] Colaboradores de WikiPedia, «Network block device,» 16 04 2023. [En línea]. Available: https://en.wikipedia.org/wiki/Network_block_device. [Último acceso: 18 04 2023].

[11] Telecommunications Industry Association, *Telecommunications Infrastructure Standard for Data Centers,* S. a. T. Department, Ed., Arlington, VA: TELECOMMUNICATIONS INDUSTRY ASSOCIATION , 2005.

[12] A. Lanchas, «Ensayos de resistencia al fuego en sistemas constructivos de placa de yeso laminado,» [En línea]. Available: http://www.aelaf.es/ensayos-de-resistencia-al-fuego-en-sistemas-constructivos-de-placa-de-yeso-laminado/. [Último acceso: 19 04 2023].

[13] Instituo para la Diversificación y Ahorro de la Energia, «Guia técnica - Condiciones climáticas exteriores de proyecto,» IDAE, Madrid, 2010.

[14] ENERGY STAR - U.S. Environmental Protection Agency y otras organizaciones, «Hot Aisle/Cold Aisle Layout,» [En línea]. Available: https://www.energystar.gov/products/low_carbon_it_campaign/12_ways_save_energy_data_center/hot_aisle_cold_aisle_layout. [Último acceso: 20 04 2023].

[15] ENERGY STAR - U.S. Environmental Protection Agency y otras organizaciones, «Containment/Enclosures,» [En línea]. Available: https://www.energystar.gov/products/low_carbon_it_campaign/12_ways_save_energy_data_center/containment_enclosures. [Último acceso: 20 04 2023].

[16] WAGNER Group GmbH, «Early fire detection with TITANUS® aspirating smoke detectors,» [En línea]. Available: https://www.wagnergroup.com/en/systems/early-fire-detection-with-titanusr-air-sampling-smoke-detectors.html. [Último acceso: 2023 04 2020].