Davante

Diseño de un CPD

Actividad 13

Título del índice

Propuesta de diseño del CPD de DataSur Solutions.

1. Importancia de tener nuestro propio CPD

En los últimos meses, la base de usuarios de los servicios de la compañía ha crecido de forma considerable. Esto está siendo al mismo tiempo una oportunidad de negocio y un problema, ya que no poseemos la infraestructura adecuada para mantener los servicios en línea y en un rendimiento apropiados.

Es más que evidente que el ordenador de la oficina con un *post-it* pegado que dice “NO APAGAR”, por muy potente que sea para una estación de trabajo, no da abasto para toda la carga de trabajo que le estamos dando; por lo que va siendo hora de actualizar la infraestructura de los servicios que proveemos. Además, han surgido dos alternativas posibles para el futuro cercano de nuestra infraestructura: Montar nuestro propio centro de procesamiento de datos o contratar la infraestructura en la nube de otra compañía más grande, como podría ser Amazon o Microsoft.

1.1. Necesidades actuales

Primero, analizaremos las necesidades reales de nuestros servicios actuales.

1.1.1. Potencia de procesamiento

Tenemos más servicios y usuarios de los que puede procesar nuestro servidor actual. Eso es un hecho, el equipo que tenemos funciona para cargas de trabajo bajas, pero no está diseñado para procesar tanta información al mismo tiempo ni para funcionar al máximo rendimiento de forma continuada. Necesitamos hardware especializado para servidores que tenga mayor ancho de banda de red, hilos de procesamiento en paralelo, y más memoria RAM.

1.1.2. Almacenamiento y fiabilidad

En cuanto a almacenamiento, tenemos más problemas además de la limitada capacidad de nuestros discos duros: necesitamos evitar a toda costa la pérdida de datos de los usuarios incluso frente a accidentes o desastres naturales. Esto significa que necesitamos un sistema para replicar datos y mantenerlos seguros que, simplemente, no es posible tener con un sólo equipo en la oficina.

1.1.3. Disponibilidad

Como he mencionado antes, el servidor actual no está preparado para estar encendido 24/7 a pleno rendimiento y se nota. Ya se ha apagado en más de una ocasión por sobrecalentamientos, errores de memoria, e incluso actualizaciones de Windows automáticas defectuosas. Debemos tener un sistema más resiliente que podamos tener disponible sin preocuparnos de caídas y errores.

1.1.4. Escalabilidad

Al igual que nos acaba de suceder, tenemos que tener en cuenta en el sistema nuevo la posibilidad de escalar nuestros servicios e infraestructura con mayor facilidad en el futuro sin tener que reestructurar todo desde cero. Esto significa servidores más modulares, control de carga, y hacer uso de bases de datos distribuidas. El objetivo sería poder, en caso de hacer falta, comprar un nuevo equipo y echarlo a andar en el menor tiempo posible.

1.1.5. Seguridad y cumplimiento de normativas

Ya hace tiempo que pasamos del punto en el que tenemos tantos usuarios que se nos puede caer el pelo si no cumplimos con los requisitos de seguridad y privacidad obligatorios en España. No contar con estas medidas de seguridad es un problema grave que tenemos que resolver cuanto antes.

2. Diseño global del CPD

Una vez repasadas las necesidades de la empresa en el punto anterior, creo que lo idóneo sería crear un CPD pequeño pero escalable. Para esto, nos vendría bien ubicarlo en un polígono industrial cercano en el que podamos contar con una nave pequeña. De esta forma, podemos contratar servicios de luz e internet para empresas a menudo disponibles sólo en estas zonas, como fibra de 10Gb de ancho de banda y fuentes de energía redundantes. Además, sería buena idea tener generadores de energía alternativos para poder usarlos en caso de apagones en la zona.

La cercanía a las oficinas agilizará el trabajo de los operarios de los servidores e incluso, si estuviéramos suficientemente cerca, nos podría permitir tener conexión directa mediante un radioenlace o fibra óptica entre la oficina y el CPD, garantizando nuestro acceso incluso frente a errores relacionados con los proveedores de internet. Normalmente tendríamos que tener en cuenta más factores sobre la región, pero en el caso de Málaga contamos con un clima suave

la mayor parte del año y no es una zona con mucha actividad sísmica ni tormentas, lo que nos permite mantener todo en la ciudad con mínimas complicaciones.

La nave tendrá que estar climatizada y aislada térmicamente para poder mantener los servidores a una temperatura correcta y evitar errores. También sería recomendable que los equipos hagan uso de refrigeración líquida en los casos que sea posible, aunque sea más caro, ya que es la forma más efectiva de refrigerar equipos de alto rendimiento como los servidores que vamos a instalar. Estos sistemas deberían estar integrados a un servidor mediante dispositivos IoT para poder monitorizar en remoto el estado ambiental de la nave y recibir alertas en caso de haber problemas como subidas o bajadas de temperatura excesivas.

En cuanto al interior de la nave, se deberá construir con el fin en mente desde el principio. Esto significa materiales resistentes a cambios de temperatura, evitando materiales inflamables como plástico o madera, aislar correctamente las salas frente a temperatura, ruido, o electricidad, y mantener todo lo relacionado con la fontanería alejado de los ordenadores. Las salas de servidores tienen que ser amplias y tener buena ventilación, y debemos de disponer de vías para mover cableado entre una sala y otra.

3. Organización

Los sistemas informáticos de la empresa se pueden dividir en tres áreas, principalmente: Área de explotación, área de sistemas, y área de administración.

3.1. Área de Explotación

Este área englobaría la parte más grande de los sistemas, ya que incluye todos los servidores relacionados con los servicios destinados a usuarios finales, bases de datos, almacenamiento, y copias de seguridad. En esta área tendremos los siguientes tipos de equipos:

- Servidores web.

Estos serán equipos enfocados a una mayor capacidad de procesamiento. Los servidores serán equipos “esclavos” en un sistema de gestión de carga administrado por un servidor “maestro”, que tendremos a su vez replicado para poder realizar mantenimiento o levantarlo en emergencias con tiempos de caída mínimos en el servicio. Este tipo de sistemas normalmente utilizan software como Kubernetes o Proxmox para virtualización y gestión de carga de los servicios. Con este tipo de diseño, tenemos muchas ventajas, como una gran fiabilidad y un sistema completamente escalable.

- Bases de datos.

Estos servidores formarían parte de un sistema de bases de datos distribuido que funciona de forma parecida a los servidores anteriores, con un servidor principal que gestiona servidores secundarios que aportan su capacidad de almacenamiento y procesamiento al resto de la red.

- Almacenamiento de datos.

Este último tipo de servidor actuaría como un NAS, proveyendo puntos de montaje para los servidores web. Montar estos equipos a parte ayuda a distribuir la carga de trabajo horizontalmente y automatizar tareas de mantenimiento, como las copias de seguridad, sin entorpecer la operación de los servidores principales.

3.2. Área de Sistemas

Esta sería el área de mantenimiento de los sistemas físicos, es decir, todo lo relacionado con que los equipos estén en un estado correcto de funcionamiento. Como mencioné en el punto 2, deberíamos de monitorizar varios aspectos de los sistemas y automatizar algunas tareas de control como el control de la temperatura y humedad de la sala. Además, será necesario comprobar regularmente el estado de las instalaciones, incluyendo cableado y desgaste de los equipos.

3.3. Área de Administración

Las funciones de este área son aquellas relacionadas con el soporte a usuarios y administración de incidencias. Dado que esta parte está centrada mayormente en la atención directa a los usuarios por parte de nuestros compañeros de la oficina, no hay mucho que automatizar y escalar salvo ampliar la oficina y la plantilla, así que no hay necesidad de modificar el flujo de trabajo actual de los departamentos involucrados en estas tareas.

4. Seguridad

Como mencioné en el punto 1.1.5, hay que aumentar las medidas de seguridad de los servidores de la compañía para cumplir los estándares requeridos. Dado que nuestras medidas de seguridad actuales son casi nulas, vamos a tener que instalar y contratar todo desde cero.

Lo primero que hará falta será instalar un sistema de control de acceso con llaves electrónicas. Con ellas, podremos comprobar la identidad de la persona que intenta acceder a las instalaciones y si posee los permisos necesarios para ello. Esto tendría que ir acompañado

de cámaras conectadas a un sistema de vigilancia para tener más formas de verificar la identidad de la persona en el proceso. Además, los vídeos grabados por estas cámaras de vigilancia podrían escanearse con software de análisis como Kerberos, que nos permitiría recibir alertas en caso de detectar personas donde no debería haber nadie, por ejemplo.

Los problemas de seguridad física de causas naturales, como incendios o desastres naturales, se tratarán en los planes de contingencia del punto 5.2.

Un asunto que también debería tratarse es la formación en ciberseguridad de los empleados de la compañía y es que, además del equipo técnico, el resto de la plantilla carece de conocimiento o experiencia relacionada con la seguridad informática. Esto podría presentar un problema en forma de decenas de puertas traseras, ya que cualquier empleado que caiga víctima de un ciber-delincuente es una potencial brecha de seguridad a nuestra infraestructura. Uno de los ataques más típicos y en los que la gente sigue cayendo serían los ataques de phishing por correo, para los que hay docenas de cursos de prevención que podríamos contratar para todo el personal.

También será necesario comprobar rutinariamente el correcto funcionamiento de los servicios de backups y restauración, así como otros sistemas de seguridad como unidades de alimentación ininterrumpidas, generadores de energía, extintores, etc.

Sería también recomendable pasar una ISO de seguridad o la ENS a la empresa para verificar que cumplimos con todas las normativas necesarias de seguridad y tratamiento de datos de los usuarios. En realidad, esto es lo más importante del apartado de seguridad, ya que estas normativas incluyen todo lo anteriormente mencionado y más.

5. Fallos

Pese a todo el trabajo previo, es imposible evitar los errores por completo, no importa el sistema que estemos utilizando. Lo que sí podemos hacer es minimizar las probabilidades de que surjan y tener planes de acción para cuando suceda.

5.1. Planes de prevención

Serían los planes que ejecutamos durante la instalación y de forma rutinaria con el fin de reducir al mínimo las posibilidades de tener problemas. Estos serían algunos de los posibles problemas y sus respectivos planes de contingencia:

Amenaza	Medidas preventivas
Cualquiera que dañe equipos	- Copias de seguridad en una ubicación externa.
Inundaciones	- Mantener racks al menos 30cm sobre el nivel del suelo. - Instalación de sensores de agua en un falso suelo. - Instalación de bombas de achique.
Terremotos	- Anclar todos los equipos al suelo y paredes. - Evitar la instalación de equipos pesados en las partes superiores de los racks.
Tormentas eléctricas	- Instalación de pararrayos. - Descargadores de sobretensión. - Conectar correctamente todos los equipos electrónicos a tierra.
Averías de suministro eléctrico	- Sistemas de alimentación redundantes. - SAI en línea con bypass automático y una autonomía de al menos 15min en todos los sistemas críticos. - Grupo electrógeno con arranque automático.
Averías de suministro de red	- Instalaciones redundantes de red. - Sistemas de respaldo con fibra o radio-enlace a la oficina.
Incendios	- Evitar el uso de materiales o líquidos inflamables. - Instalación de extintores por todo el recinto.
Malware	- Segmentación de red. - Uso de antivirus activo. - Conceder los privilegios mínimos necesarios a usuarios y programas.

	- Uso obligatorio de 2FA y gestores de contraseñas cifrados. - Copias de seguridad en frío fuera de línea regulares.
Errores de software crítico	- Planes de reversión de cambios. - Utilizar versiones LTS donde sea posible en producción.
Fallos de configuración	- Usar sistemas de configuraciones declarativas (como ansible, docker, o nix). - Copias de seguridad de las configuraciones antes de modificarlas.

5.2. Planes de contingencia

Por último, pero no menos importante, veremos algunos planes de contingencia para solucionar errores que ya han sucedido:

Incidente	Medidas de contingencia
General	- Restaurar las copias de seguridad de los equipos afectados.
Inundaciones	- Cortar la luz si se supera un límite de altura. - Trasladar equipos a una zona segura.
Terremoto	- Comprobar el estado de los equipos. - Verificar integridad de discos duros.
Incendio	- Usar sistemas de extinción. - Evacuar personal si escala el incendio.
Caída de suministro eléctrico	- Apagar servidores no esenciales para aprovechar la batería de los SAI y grupos electrógenos. - Realizar un apagado controlado si no

	se puede alargar más la autonomía.