CPDs, Riesgos y Virtualización

Bloque IV. Tema 11

Gestión de Sistemas e Informática

Curso 2017 - 18

Juan José Aguado Gil

17 Enero 2018

1. Planificación Física de un CPD

1.1. Energía y Refrigeración en un CPD

- Las siguientes técnicas permiten ahorro de energía en un CPD:
  - Consolidación de servicios.
- Las siguientes técnicas NO permiten ahorro de energía en un CPD:
  - Utilización de sistemas UPS de carga menor.
  - Uso de discos en RAID 5.
  - Instalación de sistemas de climatización muy redundantes.
- Para medir la eficiencia energética de un CPD se utiliza la medida **PUE (Power Usage Effectiveness)** que se define como la potencia total consumida por el CPD por la potencia consumida en el equipamiento TI (servidores, equipos de comunicaciones, almacenamiento y otros).
- Según ASHRAE (Sociedad Americana de Ingenieros de Calefacción, Refrigeración y Aire Acondicionado) en su publicación Standard 90.4-2016 Energy Standard for Data Centers recomienda que la temperatura de operación de un CPD sea de **18-27 grados**.
- El concepto de Green CPD está muy avanzado y se está convirtiendo en un referente. Una de las técnicas utilizadas es el **Free Cooling**. Consiste en utilizar las bajas temperaturas del aire exterior para la climatización.

1.2. Medidas de Seguridad en un CPD

1.2.1. Medidas de Seguridad

A la hora de planificar un Centro de Tratamiento de la Información, dentro de las medidas de seguridad se aplican una serie de salvaguardas:

- Técnicas.
- Organizativas.
- Físicas.
- De política de personal.

1.2.2. Seguridad Física

Los centros de proceso de datos o datacenters deben cumplir una serie de características de seguridad física; las siguientes son buenas políticas de seguridad:

- Debe disponer de puertas de acceso grandes.
- Debe evitar tener ventanas.
- Dispondrá de un sistema de refrigeración.
- Todos los cables tendidos bajo el suelo deberían ser LSZH (Low Smoke Zero Halogen) para prevenir incendios.
- Debería contar con dos acometidas eléctricas independientes.
- Debería ubicarse sobre un aparcamiento o estacionamiento de coches.
- Los extintores manuales contra el fuego deben ser de dióxido de carbono u otros gases con agentes de extinción. No debe haber componentes químicos de extinción por polvo seco en el área de ordenadores.

1.2.3. Clases de Fuego

Clasificación del Fuego según su origen:

- **Clase A**: incendios provocados por materiales orgánicos solidos como el papel, madera, cartón, tela, etc.
- **Clase B**: fuegos alimentados por líquidos y gases inflamables y materiales que arden fácilmente, por ejemplo: gasolina, diésel, bunker, parafina, cera, plásticos, gas natural, hidrógeno, propano, butano, etc.

- **Clase C**: incendios alimentados por equipos eléctricos energizados. Por ejemplo: computadoras, servidores, maquinaria industrial, herramientas eléctricas, hornos eléctricos y microondas etc.
- **Clase D**: fuegos alimentados por ciertos tipos de metales, como el sodio, potasio, polvo de aluminio, básicamente metales alcalinos y alcalinotérreos. Reaccionan violentamente al contacto con agua.

1.3. Metodología MAGERIT

A la hora de planificar la configuración de los equipos de un centro de tratamiento de la información, según un enfoque basado en el riesgo, de acuerdo con la metodología MAGERIT, la tarea de valoración de salvaguardias se encuadra en el proceso de **Análisis de riesgos**.

Además, MAGERIT es la metodología elaborada por el Consejo Superior de Administración Electrónica que se debe emplear para el estudio previo de análisis y gestión de riesgos que se realiza en la planificación de las copias de seguridad.

1.4. Categorías CPDs

El estándar **ANSI/TIA-942** describe distintos niveles en relación a ciertos requisitos de seguridad en los CPD referentes a los sistemas de telecomunicaciones, arquitectura y estructura, sistemas eléctricos y sistemas mecánicos. Existen 4 niveles:

1. **Tier 1 (Basic)**: instalación que no tiene redundadas sus componentes vitales (climatización, suministro eléctrico). Este nivel garantiza un porcentaje de disponibilidad del 99.671, lo que en la práctica supondría que podríamos estar sin servicio durante 28.82 horas en un año. En este caso se dispone de climatización y una adecuada distribución de líneas de alimentación. No es necesario que disponga de suelo técnico, SAI o grupo electrógeno. El fallo o mantenimiento del servicio causa la detención del mismo.
2. **Tier 2 (Redundant Components)**: este nivel proporciona un porcentaje de disponibilidad del 99.741, que en la práctica supone 22.68 horas sin servicio anuales. Todos los componentes están redundados (duplicados). Se dispone de suelo técnico, SAI y grupos electrógeno, pero únicamente tiene una acometida de alimentación. El mantenimiento no requiere detención del servicio siempre que no implique la acometida eléctrica.
3. **Tier 3 (Concurrently Maintainable)**: en este nivel disponemos de un porcentaje de disponibilidad del 99.982, lo que supone 1:57 horas sin servicio anuales. Además de tener todos los elementos anteriormente citados, también se dispone de más de una línea de distribución de alimentación, aunque únicamente una de ellas está activa. Por tanto cualquier mantenimiento no implica la detención del servicio.
4. **Tier 4 (Fault Tolerant)**: es el nivel más exigente, con un nivel de disponibilidad del 99.995 %, siendo en la practica 52.56 minutos anuales. Además de todo lo citado en

el anterior TIER, se dispone de múltiples líneas de alimentación activas y ambas con componentes redundados para cada línea. Lo que supone permite una tolerancia a fallos sin detención del servicio.

2. Vulnerabilidad, Riesgo y Protección

2.1. Backup y Recuperación

2.1.1. Métodos de Backups

- **Backup Completo**: incluye todos los archivos y pone en cada uno una marca que indica que se ha hecho una copia de seguridad del mismo.
- **Backup Incremental**: sólo copia los archivos creados o modificados desde la última copia de seguridad completa o incremental, marcando los archivos como copiados. Para restaurar necesita de la última copia de seguridad completa y de todas las incrementales.
- **Backup Diferencial**: incluye todos los archivos creados o modificados desde la última copia de seguridad completa, sin marcarlos individualmente como copiados. Para restaurar necesita de la última copia de seguridad completa y de la última diferencial.

2.2. Recuperación de Desastres

Disaster Recovery-as-a-Service is a hot topic in cloud, and in business, right now. And, for good reason. The technology that powers disaster recovery has never been more efficient, affordable and capable than it is today.

- **Recovery Point Objective (RPO)**: refers to the point in time **in the past** to which you will recover.
- **Recovery Time Objective (RTO)**: refers to the point in time **in the future** at which you will be up and running again.

The recovery point objective (RPO) and the recovery time objective (RTO) are two very specific parameters that are closely associated with recovery. The RTO is how long you can basically go without a specific application. This is often associated with your maximum allowable or maximum tolerable outage.

La fuente principal para calcular los tiempos estimados de recuperación de actividades (RTO) es el **Análisis de impacto en el negocio**.

3. Virtualización de Plataforma y Recursos

3.1. Virtualización Open Source

- Tecnologías de virtualización que son open source:

  - Kernel-based Virtual Machine (KVM).
  - Xen.
  - OpenVZ.
  - Virtuozzo para Linux se basa en OpenVZ, que está disponible bajo la licencia pública general de GNU.
- Tecnología de virtualización que NO es open source:
  - VMWare vSphere.

3.2. Hipervisor

A hypervisor or virtual machine monitor (VMM) is computer software, firmware or hardware that creates and runs virtual machines. A computer on which a hypervisor runs one or more virtual machines is called a host machine, and each virtual machine is called a guest machine. The hypervisor presents the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems. Multiple instances of a variety of operating systems may share the virtualized hardware resources: for example, Linux, Windows, and macOS instances can all run on a single physical x86 machine. This contrasts with operating-system-level virtualization, where all instances (usually called containers) must share a single kernel, though the guest operating systems can differ in user space, such as different Linux distributions with the same kernel.

The term hypervisor is a variant of supervisor, a traditional term for the kernel of an operating system: the hypervisor is the supervisor of the supervisor, with hyper used as a stronger variant of super.

3.2.1. Tipos de Hipervisor

There are two types of hypervisors:

- **Type-1, native or bare-metal hypervisors**: these hypervisors run directly on the host's hardware to control the hardware and to manage guest operating systems. For this reason, they are sometimes called bare metal hypervisors. The first hypervisors, which IBM developed in the 1960s, were native hypervisors. These included the test software SIMMON and the CP/CMS operating system (the predecessor of IBM's z/VM). Modern equivalents include **Xen**, Oracle VM Server for SPARC, Oracle VM Server for x86, **Microsoft Hyper-V** and **VMware ESX/ESXi**.
- **Type-2 or hosted hypervisors**: These hypervisors run on a conventional operating system (OS) just as other computer programs do. A guest operating system runs as a process on the host. Type-2 hypervisors abstract guest operating systems from the host operating system. VMware Workstation, **VMware Player**, **VirtualBox**, Parallels Desktop for Mac and QEMU are examples of type-2 hypervisors.

The distinction between these two types is not necessarily clear. Linux's Kernel-based Virtual Machine (KVM) and FreeBSD's bhyve are kernel modules that effectively convert the host operating system to a type-1 hypervisor. At the same time, since Linux distributions and FreeBSD are still general-purpose operating systems, with other applications competing for VM resources, KVM and bhyve can also be categorized as type-2 hypervisors

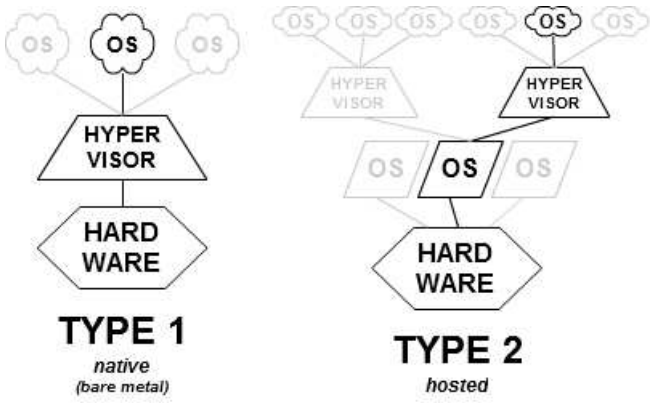

Figura 1: Tipos de Hipervisor.

3.3. Escritorio Remoto

- Solución de Escritorio Remoto que se distribuye bajo licencia propietaria:
  - DameWare Mini Remote Comntrol.
- Soluciones de Escritorio Remoto que NO se distribuyen bajo licencia propietaria:
  - Vinagre.
  - TightVNC.
  - Rdesktop.

3.4. Cloud Computing

- Modelos de infraestructura de Cloud Computing definidos por el **NIST** (National Institute of Standards and Technology):
  - Privado.
  - Público.
  - Comunitario.
- Modelos de servicio de Cloud Computing definido por el NIST:

- **SaaS (Software como servicio)**: las másquinas virtuales para albergar el software que se demande, con el sistema operativo que se requiera.
- **PaaS (Plataforma como servicio)**: el cliente contrata toda la plataforma y servicios para implementar su solución.
- **IaaS (Infraestructura como servicio)**: el cliente contrata todos los recursos que necesite: servidores, almacenamiento, redes. Todos los recursos son gestionados por el proveedor.

4. Preguntas de Exámenes

1. (GSI.PI.2016.B4.06). **Según ASHRAE (Sociedad Americana de Ingenieros de Calefacción, Refrigeración y Aire Acondicionado) en su publicación Standard 90.4-2016 Energy Standard for Data Centers recomienda que la temperatura de operación de un CPD sea de:**

   a) 20-25 grados.

   b) 20-26 grados.

   c) 18-20 grados.

   d) 18-27 grados.

2. (GSI.PI.2016.B4.30). **¿Cuál de las siguientes técnicas permite ahorro de energía en un CPD?:**

   a) Utilización de sistemas UPS de carga menor.

   b) Consolidación de servicios.

   c) Uso de discos en RAID 5.

   d) Instalación de sistemas de climatización muy redundantes.

3. (GSI.PI.2016.B4.31, GSI.LI.2016.B4.26). **¿Qué porcentaje de disponibilidad garantizada tiene un Data Center de categoría Tier 2?:**

   a) 99.895

   b) 99.671

   c) 99.741

   d) 99.982

4. (GSI.PI.2016.B4.Reserva.02). **Tecnología de virtualización que NO es open source:**

   a) VMWare vSphere.

   b) Kernel-based Virtual Machine (KVM).

   c) Xen.

   d) OpenVZ.

5. (GSI.PI.2015.B4.33). **De los siguientes softwares de virtualización, ¿cuál NO corresponde a un Hipervisor de tipo 1 (nativo o bare metal):**

   a) ESXi.

   b) XenServer.

   c) VirtualBox.

d) Hyper-V.

6. (GSI.PI.2014.B4.26). **El estándar ANSI/TIA-942 describe distintos niveles en relación a ciertos requisitos de seguridad en los CPD. ¿Cuál es el nivel (Tier) que se refiere a una instalación que no tiene redundadas sus componentes vitales (climatización, suministro eléctrico)?:**

   a) Tier 0.
   b) Tier 2.
   c) Tier 1.
   d) Tier 3.

7. (GSI.PI.2013.B4.38). **El estándar ANSI/TIA-942 establece distintos niveles en relación a ciertos requisitos de seguridad en los Centros de Proceso de Datos (CPD). ¿Cuál es el nivel más exigente?:**

   a) Tier 5
   b) Tier 4
   c) Tier 3
   d) Tier 0

8. (GSI.PI.2011.B4.31). **Uno de los siguientes NO es un modelo de infraestructura de Cloud Computing definido por el NIST (National Institute of Standards and Technology). Señálalo:**

   a) Privado.
   b) Público.
   c) Comunitario.
   d) Sectorial.

9. (GSI.PI.2011.B4.60, GSI.LI.2011.B4.14). **En un CPD se tiene la siguiente política de backup: los domingos se hace una copia de seguridad completa y a diario una copia de seguridad diferencial. Si se necesita recuperar un backup del martes, ¿qué se debería restaurar?:**

   a) Sólo el backup del martes.
   b) El backup del domingo y el del lunes.
   c) El backup del domingo y el del martes.
   d) El backup del domingo, el del lunes y el del martes.

10. (GSI.PI.2010.B4.05). **¿Cuál de las siguientes soluciones de Escritorio Remoto se distribuye bajo licencia propietaria?:**

a) Vinagre.

b) DameWare Mini Remote Comntrol.

c) TightVNC.

d) Rdesktop.

11. (GSI.PI.2010.B4.15). **¿Cuál de las siguientes NO es una plataforma de virtualización?:**

a) Xen.

b) Alfresco.

c) VMWare.

d) Virtuozzo.

12. (GSI.PI.2010.B4.33). **Se está planificando la configuración de los equipos de un centro de tratamiento de la información, según un enfoque basado en el riesgo. De acuerdo con la metodología MAGERIT, la tarea de valoración de salvaguardias se encuadra en el proceso:**

a) Gestión de riesgos.

b) Análisis de salvaguardias.

c) Análisis de riesgos.

d) Gestión de salvaguardias.

13. (GSI.PI.2010.B4.34). **Los centros de proceso de datos o datacenters deben cumplir una serie de características de seguridad física, ¿cuál de las siguientes NO es una buena política de seguridad?:**

a) Debe disponer de puertas de acceso grandes.

b) Debe estar explícitamente señalizado.

c) Debe evitar tener ventanas.

d) Dispondrá de un sistema de refrigeración.

14. (GSI.PI.2008.B4.38). **A la hora de planificar un Centro de Tratamiento de la Información, dentro de las medidas de seguridad se aplican una serie de salvaguardas. Señale cuáles son:**

a) Solamente técnicas.

b) Técnicas, organizativas y físicas.

c) Técnicas, organizativas, físicas y de política de personal.

d) Técnicas, metodológicas, físicas y organizativas.

15. (GSI.LI.2016.B4.25). **¿Qué medida se utiliza para medir la eficiencia energética de un centro de proceso de datos?:**

    a) BTU (British Thermal Unit).

    b) Estándar TIA 942.

    c) TIER I, II, III, IV.

    d) PUE (Power Usage Effectiveness).

16. (GSI.LI.2015.B4.07). **¿Cuál es la fuente principal para calcular los tiempos estimados de recuperación de actividades (RTO)?:**

    a) Plan de Respuesta ante incidentes.

    b) Pruebas de stress.

    c) Plan de Comunicación de crisis.

    d) Análisis de impacto en el negocio.

17. (GSI.LI.2015.B4.25). **El intervalo o la latencia de tiempo entre la última transacción de datos confirmada antes del error y los datos más recientes recuperados después del error se denomina:**

    a) Objetivo de tiempo de recuperación (RTO)

    b) Objetivo de punto de recuperación (RPO)

    c) Objetivo de nivel de recuperación (RLO)

    d) Objetivo de datos de recuperación (RDO)

18. (GSI.LI.2015.B4.26). **El concepto de Green CPD está muy avanzado y se está convirtiendo en un referente. Una de las técnicas utilizadas es el Free Cooling. ¿En qué consiste?:**

    a) Utilizar software libre en el control de la climatización.

    b) Utilizar temperaturas bajo cero para la climatización.

    c) Se trata del pasillo frío.

    d) Utilizar las bajas temperaturas del aire exterior para la climatización.

19. (GSI.LI.2015.B4.Reserva.01). **Es una herramienta para virtualizar un equipo:**

    a) Jaikoz.

    b) Websphere.

    c) Toad.

    d) VirtualBox.

20. (GSI.LI.2014.B4.12). **¿Cuál de los siguientes NO es un producto de virtualización?:**

    a) Virtual PC.

    b) XEN.

    c) Atheros.

    d) VirtualBox.

21. (GSI.LI.2014.B4.29). **El PUE (Power Usage effectiveness) es una métrica que trata de determinar la eficiencia energética de un Centro de Proceso de Datos, y se define como el resultado de dividir:**

    a) La potencia total consumida por el CPD por la potencia consumida en el equipamiento TI (servidores, equipos de comunicaciones, almacenamiento y otros).

    b) La potencia total consumida por el CPD por la potencia usada en el equipamiento no TI (climatización, distribución eléctrica, iluminación, etc).

    c) La potencia consumida por el equipamiento TI entre la consumida por el equipamiento no TI.

    d) La potencia total consumida por el CPD por la potencia consumida en el equipamiento de cómputo (servidores), excluyendo equipos de comunicaciones y almacenamiento.

22. (GSI.LI.2013.B4.28). **Según la ANSI/TIA-942 el porcentaje de disponibilidad de 99.982 % en un CPD corresponde a:**

    a) TIER I

    b) TIER II

    c) TIER III

    d) TIER IV

23. (GSI.LI.2013.B4.30). **Los fuegos de clase D son los que implican:**

    a) Combustibles sólidos como papel, cartón, madera, plásticos, etc.

    b) Metales y aleaciones: magnesio, sodio, etc.

    c) Combustibles líquidos, por ejemplo: aceite, derivados del petróleo, etc.

    d) Gases: butano, metano, propano, etc.

24. (GSI.LI.2011.B4.46). **Uno de los siguientes NO es un modelo de servicio de Cloud Computing definido por el NIST (National Institute of Standards and Technology). Señálalo:**

    a) NaaS - La red como servicio.

b) SaaS - Software como servicio.

c) PaaS - Plataforma como servicio.

d) IaaS - Infraestructura como servicio.

25. (GSI.LI.2011.B4.Reserva.01). **La infraestructura básica (servidores, software y equipamiento de red) gestionada por un proveedor como un servicio bajo demanda, en el cual se pueden crear entornos para desarrollar, ejecutar o probar aplicaciones, es el concepto de:**

a) IaaS.

b) Hosting.

c) Housing.

d) CPD de respaldo.

26. (GSI.LI.2010.B4.09). **Una copia de seguridad que incluye todos los archivos creados o modificados desde la última copia completa. sin marcarlos individualmente como copiados, es una copia de seguridad:**

a) Acumulativa.

b) Intermedia.

c) Incremental.

d) Diferencial.

27. (GSI.LI.2008.B4.07). **La planificación de las copias de seguridad vendrá derivada de un estudio previo de análisis y gestión de riesgos basado en una metodología. Indicar la metodología elaborada por el Consejo Superior de Administración Electrónica que se debería emplear para este estudio:**

a) SOROLLA

b) MAGERIT

c) NEDAES

d) BADARAL

28. (GSI.LI.2008.B4.31). **A la hora de crear un CPD, señale qué consideración NO debe tener en cuenta:**

a) Todos los cables tendidos bajo el suelo de un CPD deberían ser LSZH.

b) El CPD debería contar con dos acometidas eléctricas independientes.

c) El CPD no debería ubicarse sobre un aparcamiento o estacionamiento de coches.

d) Dentro de un CPD, en el área de ordenadores, debería utilizarse para la extinción de incendios polvo seco.

5. Soluciones

1. D
2. B
3. C
4. A
5. C
6. C
7. B
8. D
9. C
10. B
11. B
12. C
13. B
14. C
15. D
16. D
17. B
18. D
19. D
20. C
21. A
22. C
23. B
24. A
25. A
26. D
27. B
28. D

Referencias

[1] Hypervisor.
https://en.wikipedia.org/wiki/Hypervisor

[2] RPO & RTO.
https://www.bluelock.com/blog/rpo-rto-pto-and-raas-disaster-recovery-explained/

[3] Seguridad por niveles: Seguridad de acuerdo al modelo de capas TCP/IP.
Alejandro Corletti Estrada.