AIEP
DE LA UNIVERSIDAD
ANDRES BELLO

SEGURIDAD DE CABLEADO Y DATACENTER

Unidad 2

Seguridad de almacenamiento en el *datacenter*

ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yáñez

ELABORACIÓN

Experto disciplinar: Eder Morán Heredia

Diseñadora instruccional: Luisa García Ospina

Editora instruccional: Trinidad Marshall

VALIDACIÓN

Experto disciplinar: Gabriel Urra Varas

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Welearn

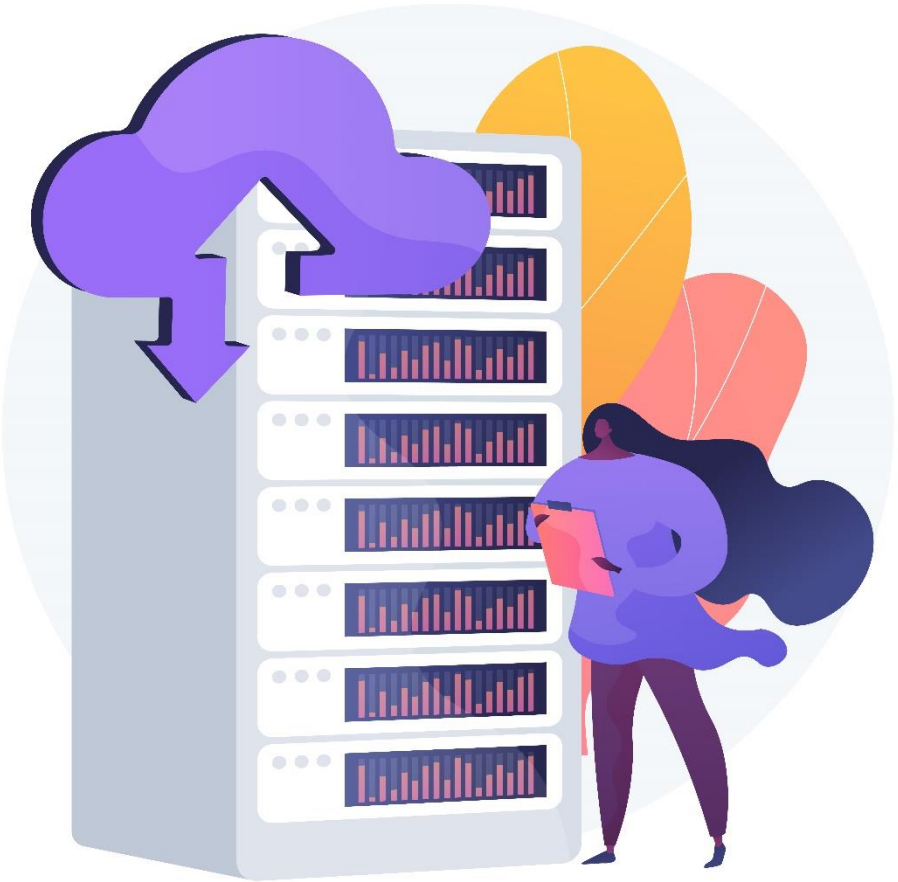
AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Aplicar **técnicas de diseño de red de *datacenter*** en la nube, basándose en la seguridad lógica y considerando procesos de implementación de red segura para acceso de datos.



Fuente: Freepik, (s.f)

Introducción

¿Cuáles son las ventajas del uso de la nube?

Cuando se habla de la **nube** se alude a un término con años de historia y que es una metáfora para nombrar al internet. Básicamente consiste en servicios de computación, tales como correos electrónicos, almacenamiento y todo lo que los servicios de **TI** ofrecen. Esta herramienta ha sido muy popular a nivel global y ha influido en el cambio de las organizaciones y en la gestión de estas.

En los últimos años, el ***Cloud Computing*** se ha masificado debido a la necesidad de generar nuevos formatos de obtención, almacenamiento y gestión de datos que permitieran cambiar la metodología de trabajo por el contexto de la pandemia del 2020. Estos servicios de información utilizada y almacenada, así como la mayoría de sus aplicaciones requeridas, son procesados por un servidor de internet. Se trata de una implementación que transforma como vemos la informática.

Este desarrollo se llevó a cabo en grandes organizaciones, quienes incluso llegan a cobrar por estos servicios. Por lo tanto, se establecen como un modelo de negocios que actualmente está en auge. Empresas como Amazon y Google construyeron su propia infraestructura de soporte, para lo cual se soportaron sobre granjas de servidores, que son un tipo de tecnología que cosecha datos y crea aplicaciones. Aunque la implementación es una idea reciente, no es nueva, ya que se ha discutido en el medio desde hace algunos años.

1. Estándares de seguridad para redes internas y de acceso a *datacenter*

La prestación de servicios de un *datacenter* no se limita al uso del *hardware*, sino que incluso llega a ofrecer a los clientes el servicio ***cloud***. Este es un sistema de almacenamiento para manipular la información sin la necesidad de estar físicamente en los equipos, los cuales están generalmente conectados por medio de una VPN desde el centro de computadores del cliente.

Modelos de *cloud*: cada modelo se adecúa rápidamente a los cambios que requieran las organizaciones. Uno de los factores más importantes para su uso es la característica de los medios de la información, es decir, son de acceso exclusivo o compartido.

Existen actualmente cuatro modelos convencionales de la nube que comercialmente se llaman *cloud*:

- **Nube privada**: los recursos y accesos son de uso exclusivo de la organización, los colaboradores y los proveedores, de manera que se utiliza de forma interna. El objetivo es gestionar en un entorno cerrado todas las diligencias comerciales y digitales para administrar el proceso productivo dentro de toda la organización.

- **Nube comunitaria**: los requerimientos de un conjunto de empresas, con alguna característica en particular, para conformar parte de dicha sociedad, obligan al distribuidor a compartir políticas concretas entre los usuarios de la nube comunitaria.

- **Nube pública**: los servicios se hayan en los servidores del distribuidor o en terceras piezas. La infraestructura de la nube es compartida por los diversos consumidores independientes y se debería garantizar la libertad de dichos conocimientos.

- **Nube hibrida**: es una combinación entre nube pública, nube privada o con una nube comunitaria, que interactúan para proporcionar mayor flexibilidad en los servicios informáticos. Esta nube entrega información de manera uniforme con un único modelo operativo, pero pueden migrar datos a distintos tipos de nubes y de manera fluida.

Servicios de *cloud computing*: son todas las infraestructuras, plataformas, tecnologías o sistemas de *software* a los que acceden los usuarios a través de internet. Estos servicios no necesitan descargar un *software* adicional.

Generalmente son tres servicios de *cloud computing* ofrecidos por los principales proveedores empresariales:

1 **Infraestructura como Servicio** (IaaS): uno de los servicios más complejos y está destinado a usuarios expertos, otorgándoles un control absoluto al cliente. En este servicio hay otro proveedor que suministra los componentes de *hardware* al cliente.

2 **Plataforma como Servicio** (PaaS): en este servicio, el usuario solo tiene acceso a la plataforma, la cual da el proveedor. El usuario nunca tendrá el control ni permisos para usar la infraestructura de este mismo.

3 **Software como Servicio** (SaaS): el servicio más común y está enfocado en el usuario del día a día (los ejemplos más claros de este son los ofrecidos por *Google Drive* y *One Drive*).

1.1 Estándares

1.1.1.ITIL

ITIL es un acrónimo para ***IT Infrastructure Library*** (Biblioteca de Infraestructura de Tecnologías de la Información). Fue desarrollado por la **OGC** (*Office of Government Commerce*) por el gobierno inglés en 1989. A través de los años, se ha consolidado como un estándar mundial de la **Gestión de Servicios Informáticos**. Es un conjunto de buenas prácticas orientadas a la administración de servicios de tecnologías de la información, las cuales están definidas a colaborar con las organizaciones que proveen servicios de TI para lograr una mayor calidad y eficiencia en la gestión de sus servicios.

ITIL propone las buenas prácticas identificando el **Ciclo de Vida de los Servicios** y entrando en el detalle de los diferentes procesos y acciones que son propuestas en cada una de las 5 fases de este: **estrategia**, **diseño**, **transición**, **operación** y **mejora continua**.

1.1.2.COBIT

COBIT es un acrónimo para ***Control Objectives for Information and related Technology*** (Objetivos de Control para tecnología de la información y relacionada). Desarrollada por la Information Systems Audit and Control Association (**ISACA**) y el IT Governance Institute (**ITGI**), COBIT es una metodología reconocida mundialmente para el adecuado control de proyectos de tecnología, los flujos de información y los riesgos que estas implican. Ayuda a las empresas a la obtener los valores óptimos asociados a

TI, manteniendo un equilibrio entre la implementación de beneficios, recursos utilizados y los umbrales de riesgos asumidos.

La metodología COBIT se usa para planificar, implementar, controlar y evaluar el gobierno sobre las empresas de TI, incorporando diversos objetivos de control, auditorías, y medidas de rendimiento para obtener los respectivos desempeños.

1.1.3.ISM3

La publicación del **ISM3** (***Información Security Management***) es un estándar para la creación de sistemas de gestión de la seguridad de la información, el cual puede ser usado en forma independiente o en conjunto a otras metodologías como ITIL, ISO o COBIT. Este último está diseñado en niveles de madurez, de modo que cada empresa pueda decidir qué nivel es el más adecuado para su negocio, y de esta forma lograr objetivos en varias etapas.

ISM3 tiene como propósito alcanzar niveles de seguridad definidos, o denominados **riesgo aceptable**, en lugar de la búsqueda de la invulnerabilidad.

2. Redes virtualizadas en la nube

La nube (*cloud computing*) es el nombre que se le dio al procesamiento y almacenamiento masivo de datos en servidores que alojan la información del usuario. Esto significa que hay servicios, algunos gratuitos y otros pagados, que guardan tanto los archivos como la información del usuario de internet.

La idea de esto nace en el acceso instantáneo, y en todo momento, a los datos. Se ubica y se hace uso de los servicios en cualquier artefacto con acceso a internet. La nube fue creada para el usuario, que quiere soluciones rápidas y simples. Por este motivo, la mayoría de las plataformas que hacen uso de esta tecnología son intuitivos y fáciles de usar.

2.1 Características y limitaciones

Algunas características de la nube son:

- **Agilidad**: constantes mejoras en la oferta de recursos al usuario.
- **Disminución de costos**: tiene equipamiento de terceros.
- **Escalabilidad y elasticidad**: aprovisionamiento de recursos casi en tiempo real.
- **Dispositivos e independencia de la ubicación**: solo se necesita conexión a internet.
- **Virtualización**: se pueden realizar grandes cambios o la compartición de máquinas físicas.

- **Rendimiento**: control y optimización por parte del proveedor, además de proporcionar transparencia.
- **Seguridad**: es tan buena, o mejor, que en los sistemas tradicionales.
- **Mantenimiento de Aplicaciones**: es centralizada, y, por ende, más fácil y rápida.

También, algunas limitaciones de la computación en la nube son las siguientes:

- Pérdida o fuga de datos.
- El acceso de control **API** y la generación de las claves permiten una política de destrucción de datos.
- Dificultad para valorar la fiabilidad de los proveedores.
- El proveedor de servicios en la nube controla los accesos a los datos, los cuales son diferentes en muchos proveedores y circunstancias.
- Los mecanismos de autenticación no son muy fuertes, por lo tanto, un atacante puede fácilmente obtener la cuenta de usuario y acceder al sistema virtual.

2.2 ¿Por qué usar la Nube para las Redes?

El *cloud* ha venido para quedarse, ya que ha cambiado de manera radical la forma de emplear el soporte de datos tanto en la industria como en las aulas. Un ejemplo de ello es el actual uso de *GoogleDocs* para gestión y almacenamiento de información, y su traspaso a otras plataformas o computadoras.

Las empresas han migrado al *Cloud 365*, la gestión de los clientes se hace ahora en *Salesforce* y aún otros *softwares* están ingresando a la nube como soportes de negocios. Sin embargo, hay que tener en cuenta que algunos componentes deben permanecer en el entorno local para ser accesibles.

Cloud ofrece un modo alternativo a los servicios de TI de consumo regular. Para ello, las empresas deben abandonar el modelo local para pasarse al modelo del *cloud* que algunos proveedores descargan por ellos. Tradicionalmente, los clientes gestionan instalación y funcionamiento del *hardware*, energía, el cableado, actualizaciones, copias de seguridad, migraciones y redundancia. Lo hacen porque los *routers switches*, controladores, puntos de acceso, herramientas de gestión, puertas de enlace, concentradores y otros servicios, se aseguran de tener conectividad, ancho de banda adecuado, seguridad e integración en todos los sistemas. Además, se ocupan de la supervisión, solución de problemas, inventarios, gestión de problemas de asistencia y planificación del ciclo de vida de todo de principio a fin. Entonces, viendo su dimensión, nos daremos cuenta del tamaño del manejo e implementación de los datos, el cual necesita de la red para ejecutar una labor de gran magnitud.

Asimismo, alivia las demandas de los modelos de implementación al cambiar la carga de funcionamiento de todos los servicios, además de ser sumamente transparente para el cliente. Por otro lado, el que suministra el servicio se deshace de los gastos que implica y de la complejidad de las soluciones, y así los grupos de TI pueden centrase en solucionar los problemas de la empresa en lugar de abordar las dificultades de los servidores.

Su soporte tiene mayor flexibilidad y velocidad porque no tiene que realizar migraciones del sistema, actualizaciones, fallos repentinos, períodos de mantenimiento nocturno, reversiones ni otro tipo de inconvenientes. Estos

afectan al proceso de elaboración de un proyecto o del trabajo continuo del el día a día en las operaciones normales en la empresa. Por lo tanto, el *cloud* disminuye las problemáticas generadas por las migraciones de datos u otras situaciones que ralentizan el trabajo. Desde el punto de vista de la infraestructura, solo pasa ser responsabilidad de una persona, la cual debe ser especialista en servidores y centro de datos.

También, la nube mejora los flujos de trabajo diario, como el inicio de sesión sin necesidad de una VPN, el registro de dispositivos nuevos, la configuración y aplicación de políticas centralizadas la gestión de licencias y el disfrute de una visión centralizada.

2.2.1. Resistencia

El proveedor de la nube debe simplificar la gestión del sistema y garantizar, por lo general en un 99.9% o más, el tiempo de actividad. Las soluciones a los inconvenientes están construidas sobre arquitecturas de plataformas e infraestructuras muy fiables ofrecidas por operadores de confianza como *Amazon*, *Microsoft* y *Google*.

Además, existen versiones diferentes de **arquitecturas de la nube**, ya que no todas se crean del mismo modo. Sin embargo, el uso para los clientes es sumamente fiable porque presenta una resistencia inherente frente a fallos y redundancia.

2.2.2. Escalabilidad

Se trata del cambio que lleva a una red hacia nuevos niveles de funcionamiento, como ampliar o cambiar el dispositivo o la población del usuario. Otros casos de **escalabilidad** del *cloud* son los nuevos requisitos

empresariales de picos en eventos o alarmas, añadir ubicaciones/centros, nueva visibilidad de los datos, notificación de los requisitos o simplemente iniciar sesión con más frecuencia. El crecimiento también lleva a un riesgo durante su acumulación peldaño a peldaño.

La nube sustituye el paradigma de los recursos fijos del *hardware* en el entorno local y aborda la escalabilidad usando un paradigma de **recursos adaptables y flexibles**. Estos pueden supervisarse de cerca y es apto para la integración de herramientas automáticas para la solución de algún inconveniente.

Las soluciones que suministran los proveedores evolucionan de manera continua según las nuevas aplicaciones y los requisitos de los usuarios. Pero las resoluciones tradicionales frenan esta evolución con las limitaciones en sus recursos, y siempre existirán retos para ampliar las cajas de soluciones incluso en las máquinas virtuales. Los recursos del *hardware* pueden agotarse, lo que podría requerir un nuevo ciclo presupuestario para justificar gastos adicionales.

Las **soluciones de escalado** son mucho más sencillas de manejar para los administradores de red ya que suelen ser transparentes y se dan en forma lineal. Solo se necesita añadir una licencia y conectar los dispositivos. Además, los encargados pueden establecen actualizaciones de manera dinámica, considerando que los servicios en la nube son modulares y las limitaciones de escalado pueden usarse con recursos adicionales o con cambios de arquitecturas.

2.2.3. Coste

La **arquitectura *cloud*** es provechosa para muchas empresas, ya que el costo económico de su implementación es bajo y permite ahorrar en el uso de otros

mecanismos de almacenamiento de datos más caros. Las empresas optan por este tipo de servicio por que pueden hacer frente a otras situaciones en el entorno tecnológico con un presupuesto menor y accesible incluso para las pequeñas y medianas empresas. Con la llegada de la nube, el precio comercial de los recursos de procesamiento, memoria y disco son más bajos y accesibles para los usuarios.

Además, es más fácil proveer y gestionar costes, ya que la nube evita el crecimiento no lineal en arquitecturas tradicionales. Por ejemplo, en el caso que tu aplicación pueda funcionar en 1000 dispositivos, pero tu nuevo diseño necesita que se usen en 1025. Las licencias en las nubes se venden normalmente en unidades lineales como suscripciones, evitando así gastos de capital (**Capex**) inesperados para la infraestructura. El aspecto más importante relacionado con los costos es que permite pasar a gastos operativos (**Opex**) en lugar de iniciar elevados gastos de capital, que son habituales en las soluciones locales.

2.3 Arquitectura

Arquitectura de la nube: es el conjunto de capas acopladas entre sí, para brindarle funcionalidad al sistema. Por lo tanto, es similar a la arquitectura de la red, desde el nivel físico hasta el nivel de aplicación. Además, usa protocolos similares a internet como medios de comunicación, ya sea basado en web o no.

Se considera que una arquitectura genérica del *cloud compúting* tiene las siguientes capas mencionadas de abajo hacia arriba:

- **Recursos físicos**: servidores, almacenamiento, red, entre otros.
- **Virtualización**: infraestructura virtual como un servicio.
- **Plataforma**: componentes de aplicación como servicio.
- **Aplicación**: servicios basados en la web y *software*.

3. Creación de instancias en ambiente de nube

¿Qué es una **instancia en *cloud*?** Es un nuevo término y, por correspondiente, un nuevo paradigma en cuanto al alojamiento. Para que se entienda mejor, vamos a hacer una pequeña comparación entre un servidor y una instancia en *cloud*.

Los servidores son máquinas físicas que pagas mensualmente para poder acceder a ella y tienen recursos físicos establecidos como 8 GB de RAM y 500 Gb de disco duro. Es decir, son ordenadores que puedes alquilar y calcular mensualmente.

Una vez que comprendamos esto, podemos compararlo con una instancia en *cloud*. No obstante, antes debemos de conocer algo: el *cloud computing* no es físico, no puedes tocar un ordenador. La nube está compuesta por decenas (o centenares) de ordenadores que juntan sus discos duros. En el procesamiento, juntan toda su memoria RAM y una vez que está todo junto, deciden como repartir los datos.

Pues bien, una instancia en *cloud* se podría definir como un servidor virtual (no físico) que podemos alquilar solo unas horas (no es necesario un largo tiempo) y a la vez ser un ordenador, con el que podemos pasar de tener 10 Gb de RAM a tener 1250 GB de RAM con el simple uso del ratón.

3.1 Características de las instancias en *cloud*

- Está totalmente virtualizado, no es físico, por lo que podemos aumentar los recursos de 10GB a 200GB de RAM.
- A diferencia de los servidores y los VPS, suelen funcionar por horas. Puedes tener un ordenador con Ubuntu con 200 GB de RAM y 50 procesadores y pagar solamente dos horas de uso.
- Al no ser físico, no tenemos que preocuparnos de si se rompe un disco duro (como puede ocurrir en los servidores físicos), ya que nuestros datos están duplicados en varios discos duros.
- Al estar virtualizados, podemos hacer un ***backup*** de nuestro sistema. Esto se conoce como **imagen.**

3.1.1. ¿Qué es una imagen de una instancia?

Se pueden categorizar en *backups*, no obstante, hay una gran diferencia entre un *backup* y una imagen. El primero lo podemos hacer únicamente de los datos importantes (bases de datos, ficheros de una web, etc.). Es decir, solo guardamos lo esencial. Por otro lado, el segundo es una copia de todo el sistema. Exactamente igual que si clonáramos un disco duro, se hace una copia de todos los ficheros, incluso de los que son del sistema operativo.

Esto nos hace preguntarnos, si una instancia es una copia del sistema entero, ¿la existencia de dicha imagen no tendría que copiarse dentro de la imagen (si hacemos dos *backups*) y ocasionar un bucle?

Para entender cómo funciona vamos a ver características de las imágenes:

- Lo más importante es comprender que, a diferencia de muchos *backups*, las imágenes no se guardan en la instancia, si no que se encarga de gestionarlo la empresa proveedora.
- Puesto que no se guardan en la instancia, no tendrás que duplicar el espacio (disco duro virtual) de esta.
- Sin embargo, puesto que una imagen ocupa espacio (aunque no procesamiento), tendrás que pagar por cada imagen que crees.
- Una vez creada la imagen, podrás dar de baja la instancia (dejar de pagar) y seguir donde la dejaste, al cabo de un año, gracias a la imagen.

3.1.2. Crear una Instancia a partir de una imagen

Después de un uso prolongado de una imagen para el proyecto de una empresa, se crea una específica para ese proyecto, así que decidimos hacer una imagen (*backup*) de esa instancia y damos de baja la instancia (para no seguir pagando).

Pues bien, en el caso de que el proyecto se detuviera, podríamos hacer lo que se conoce como **lanzar una instancia a partir de una imagen**. Esto significa tomar la imagen que habíamos creado hace un año y crear una instancia a partir de una imagen.

El resultado sería que tendríamos exactamente la misma instancia que teníamos hace un año, antes de parar el proyecto, por lo que podríamos seguir dicho proyecto sin perder tiempo.

Lógicamente, las instancias no solo se realizan cuando paras un proyecto durante un año, también puedes hacerlas antes de actualizar el sistema o la web, para que, si algo no funciona bien, puedas regresar a un punto anterior.

3.1.3. Almacenamiento de instancias

El dispositivo de la instancia contiene la imagen usada para arrancarla. El dispositivo raíz es un volumen ***Amazon Elastic Block Store*** (*Amazon EBS*) o un volumen de almacén de instancias.

La instancia puede incluir volúmenes de almacenamiento local, conocidos como **volúmenes de almacén de instancias**, que puede configurar el aumento del lanzamiento con un mapeo de dispositivos de bloques.

Si la instancia da error o se termina, los datos de estos volúmenes quedan como datos temporales. Para proteger la información importante, es conveniente utilizar una estrategia de replicación entre varias instancias, o bien almacenar los datos persistentes en volúmenes de un almacenamiento conocido (como lo realiza *Amazon*).

4. Redes seguras definidas por *software* y *hardware* en un *datacenter* de la nube

Las **redes SDN** son una nueva arquitectura de red que elimina la rigidez actual de las redes tradicionales, permitiendo un comportamiento más flexible de la red y más adaptable a las necesidades de cada organización o usuario. Su diseño centralizado permite recopilar información sobre la red y utilizarla para mejorar y adoptar sus políticas de forma dinámica.

Se afirma que las SDN es una arquitectura diseñada para adaptarse a los nuevos requerimientos tecnológicos. Separa el plano de control del plano de datos, permitiendo que los operadores de red la puedan programar y gestionar de manera centralizada. Se basa en el uso de interfaces abiertas en cuyo estudio se fundamenta el soporte y la flexibilidad para SDN. Estas interfaces abiertas son las llamadas **API**, que se comunican con el controlador y de esta manera los dispositivos saben que acción realizar.

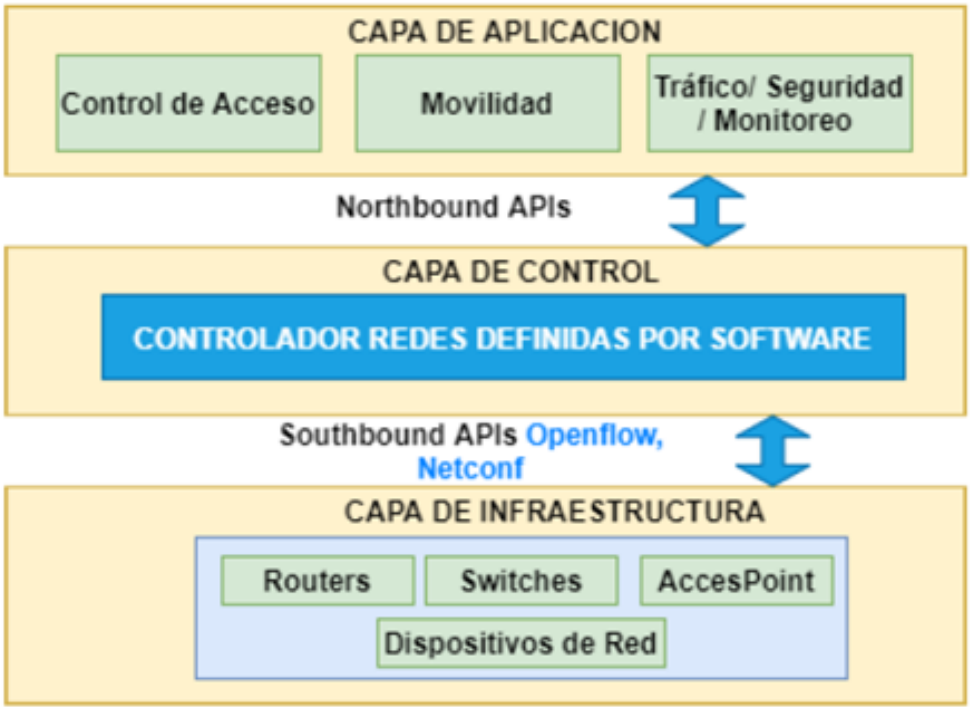
4.1 Arquitectura SDN

Una **arquitectura SDN** se divide en tres planos distintos, empezando desde la capa inferior donde se encuentra el plano de datos (*data plane*). Aquí se encuentran tanto el *hardware* como los conmutadores. Después a esta capa le sigue el plano de control (*control plane*), cuya función es enlazar el controlador y los dispositivos. En la capa superior está el plano de aplicación (*aplication plane*), que involucra aplicaciones individuales en constante uso y monitoreo de la red.

Se explica cómo la arquitectura SDN se comunica mediante la transmisión de **flujos**, lo que se puede definir como una secuencia de paquetes que viajan a través de la red y comparten campos en sus encabezados. El proceso de comunicación comienza cuando el usuario realiza una solicitud de un servicio. El conmutador recibió esa solicitud y se comunica con el controlador SDN que proporciona las instrucciones a seguir para el servicio especificado.

La comunicación entre el conmutador y el controlador se realiza a través del protocolo ***OpenFlow*** mediante un canal seguro. En siguiente imagen se describen los componentes principales de una arquitectura SDN:

Figura 1: Arquitectura SDN



Fuente: Francisco Aguirre en ResearchGate (s.f)

4.1.1. Capa de aplicación

La capa de aplicación se relaciona con las aplicaciones requeridas para el negocio y la personalización por parte del usuario. Las aplicaciones usan servicios de comunicación SDN a través de un ***Northbound* API** en la capa de control como **REST**, **JSON**, **XML**, etc.

Esta capa permite que los servicios y aplicaciones simplifiquen y automaticen tareas de configuración para administrar nuevos servicios de red, ofreciendo a los operadores nuevas fuentes de ingresos y diferenciación.

4.1.2. Capa de control

La capa de control se encarga de establecer el tratamiento de los flujos a través del *software* de control de SDN (controlador). La transmisión de las instrucciones al *switchs* se realiza a través de un protocolo estandarizado llamado *OpenFlow*. Se la conoce también como plano de control y es la inteligencia de la red en forma de controlador SDN centralizado y basado en *software*. Se puede instalar en sistemas basados en **UNIX**, que se ejecuta en cualquier *hardware*. La capa de control administra el *hardware* de reenvió e instala las reglas de reenvió través de API.

4.1.3. Capa de infraestructura

También llamada como plano de datos, involucra reenvió de *hardware*, conmutadores y enrutadores. La conmutación se realiza en los llamados **nodos de red** en donde también se realiza el enrutamiento proporciona programabilidad por medio de **API *Southbound*** como el protocolo *OpenFlow*.

4.2 Componentes

El **controlador SDN** es una entidad de *software* que tiene el control exclusivo sobre un conjunto abstracto de recursos del plano de datos y donde se generan las políticas de información de tratamiento. Equivale a la inteligencia de la red que controla todas las comunicaciones entre las aplicaciones y los dispositivos.

El controlador se encarga de traducir las necesidades o requisitos de la capa de aplicación a los elementos de la red y de proporcionar información relevante a las aplicaciones SDN. Es un canal de comunicación seguro, como ***Secure Sockets Layer*** (SSL) que conecta el software de control y el conmutador a través del protocolo *OpenFlow*.

4.3 Un conmutador compatible con *OpenFlow*

En SDN los controladores son la inteligencia de la red. Por tal motivo, nos brindan una visión total de esta. La red aparece frente a las aplicaciones como un conmutador lógico que beneficia a las empresas, ya que no dependen de los proveedores. La gestión se hace desde un punto lógico, facilitando el diseño y la gestión de redes mediante SDN, el cual se simplifica también en dispositivos de **RED** y de altos protocolos con estándares que se cambian por instrucciones de controladores.

4.4 Comunicación con el controlador

Se realiza a través de:

- **API *Southbound*** (SBI): se describe como un habilitador de SDN ya que, por medio de esta, el plano de control se comunica con el plano de datos. Esta API se usa para enviar información de configuración e instalar entradas de flujos en el plano de datos. Facilita al controlador configurar o manipular los procesos de *switch*. Es la forma en que SDN programa la red, en donde un ejemplo de una API programable SBI es *OpenFLow*.

- **API de *Northbound*** (NBI): permite que las aplicaciones tengan control de la red y proporciona una interfaz común entre el controlador y el plano de administración. Además, ayuda a la información de los dispositivos subyacentes para el desarrollo de aplicaciones y facilitar la innovación. También, aporta a la integración eficaz de la red, de manera que el control de SDN es más fácil y dinámico a través de la interfaz SBI. La interfaz NBI ha tenido menos esfuerzos de estandarización porque es un ecosistema de *software*.

4.5 *OpenFlow*

Es el protocolo más usado en SDN. Se comunica mediante *Southbound* API a la capa de control y facilita la programabilidad de la red configurando, gestionando y controlando el flujo desde un *software* centralizado.

Permite particionar el tráfico, elige la mejor ruta y mejora la forma en que se procesan los paquetes. Se enfoca en nuevas formas de enrutamiento de seguridad, control de tráfico y esquemas de direccionamiento, entre otros. Se puede comparar con el conjunto de instrucciones de una CPU especifica,

instrucciones básicas que pueden ser usadas por una aplicación de *software* externa para programar el plano de envío.

5. Nube híbrida: red local y *datacenter* en la nube

Una **nube híbrida** consiste en un entorno que cambia entre una nube pública y una privada, para realizar y compartir diferentes funciones y datos entre ellos. Esto permite obtener las características que ofrecen ambos modos juntos, logrando así un mejor desempeño y eficiencia.

Algunas de las principales ventajas que se obtienen al implementar una nube híbrida es la no necesidad de incurrir en gastos innecesarios para la atención de flujos de información esporádicos. Esto se debe a que en ocasiones se cuenta con información delicada que se quiere mantener en un entorno local y no en manos de un tercero.

Se debe tener en cuenta que la nube privada se puede integrar fácilmente con la nube pública o viceversa ya que, al momento de seleccionar el proveedor de la nube pública, este permite la fácil integración con entonos privados.

Como parte de una estrategia, la nube hibrida se ha movido al desarrollo de una nube dinámica altamente disponible con tres objetivos de diseño en mente:

- Diseño de aplicaciones y el entorno de alojamiento para arreglo automático.
- Diseño de la nube hibrida para satisfacer una demanda impredecible automáticamente.

- Diseño de aplicaciones, compatibles con la nube, que admitan interrupciones de la infraestructura y que puedan estar activas simultáneamente en múltiples ubicaciones.

Los analistas de la industria están de acuerdo en que los servicios en la nube híbrida son el estado futuro en las infraestructuras de TI. Por otra parte, los líderes de TI saben que este es su destino, pero lo que no está claro es como llegar allí. En algunos casos, este problema se ve agravado por los proveedores de soluciones de servicios en la nube privada, que impulsan implementaciones que protegen al propietario y a los enfoques.

Para tener éxito, una estrategia de servicios en la nube privada se debe abstener los procesos y a la tecnología existente, y así evitar las problemáticas identificadas por los líderes de TI. Además, las soluciones de servicios en la nube deben ser lo suficientemente flexibles como para adaptarse a los requisitos cambiantes, mientras proporcionan capacidades de servicios que satisfagan sus desafíos específicos.

5.1 Construir servicios en la nube híbrida

Después de haber virtualizado los centros de datos, cada vez más organizaciones de TI están tomando la decisión de construir servicios en la nube privada, al mismo tiempo que permiten la funcionalidad hibrida. Los servicios del modo hibrido permiten a las empresas aprovechar los servicios en la nube pública fuera de las instalaciones, mientras utilizan la nube privada dentro de las instalaciones para obtener lo mejor de ambas.

La escalabilidad y la elasticidad de los servicios en la nube pública son eficientes para el cambio rápido de los requerimientos del negocio. Por otro

lado, la visibilidad y la seguridad de los servicios en la nube privada se utilizan para la gestión de datos sensibles o regulados.

Sin embargo, existen dificultades para la construcción de servicios en la nube hibrida. A medida que los lideres comienzan a evaluar las soluciones de servicios en la nube privada, descubren que los proveedores de soluciones ofrecen opciones limitadas que a menudo encierran en una arquitectura especifica.

5.2 Arquitectura de los centros de datos

5.2.1. Centro de datos para cloud computing

Las plataformas de *hardware* que contienen el soporte a la computación en la nube necesitan unos recursos muy superiores a los centros de datos convencionales. Estas instalaciones no pueden diseñarse como una simple colección de servidores, ya que el *hardware* y *software* tienen que trabajar en forma coordinada.

Estos centros de datos deben ser tratados como un gran computador del tamaño de un gran almacén (***WSC: warehouse-escale computer***). Los centros tipo WSC dan soporte actualmente a los servicios online ofrecidos por compañías tales como *Google*, *Amazon*, *Yahoo* y *Microsoft*. Se diferencian de los centros de datos tradicionales en los siguientes hechos:

- Pertenecen a una misma organización.
- Usan una plataforma de *hardware* y *software* relativamente homogénea.
- Comparten una capa de gestión común del sistema.

- Ejecutan un número.

5.2.2. Arquitectura de un centro de datos de tres capas

La arquitectura de los centros de datos tradicionales consta de tres niéveles:

- **Nivel de red**: proporciona acceso seguro y fiable de los usuarios.
- **Nivel de computación**: proporciona los recursos del proceso.
- **Nivel de almacenamiento**: proporciona los servicios de la base de datos.

5.3 Estructura física de un centro de datos para *cloud computing*

La implementación *hardware* de un WSC difiere significativamente de una instalación a la siguiente:

- Incluso dentro de una misma organización, como puede ser *Google*, los sistemas desplegados en años diferentes usan elementos básicos distintos, reflejando las mejoras de *hardware* proporcionadas por la industria.
- Sin embargo, la organización arquitectónica de estos sistemas ha sido relativamente estable en los últimos 5 años.
- El sistema de refrigeración es un aporte significativo de un SWC.
- Los modernos centros de datos disponen de sistemas adaptativos de control para la refrigeración de la instalación.

6. Sistemas de monitoreo de equipamiento y servidores en la nube

Actualmente existen diferentes soluciones de monitoreo, algunas las cuales requieren la configuración de servidores y de los agentes de monitoreo. A continuación, se mencionan algunos d ellos sistemas de monitoreo actualmente existente:

- ***Logic Monitor***: sistema de monitoreo que funciona en los Estados Unidos y presenta una gran variedad de elementos para monitorear en las categorías de monitoreo de la red, aplicaciones, almacenamiento, servidores, bases de datos, balanceadores de carga e infraestructura de potencia.

- ***Copperegg***: herramienta de monitoreo comercial que funciona en los Estados Unidos. Controla únicamente las métricas básicas de servidores como uso de disco, CPU, tráfico de red y memoria. Una de las ventajas que ofrece este sistema es que presenta las estadísticas en tiempo real en una sola página.

- ***Cloudability***: permite a los **CSC** tener informes centralizados del consumo en dólares de los servicios adquiridos en una gran variedad de nubes. No ofrece monitoreo de infraestructura, si no que su foco principal se encuentra en los informes de consumo de **dinero.**

- ***Monitis***: herramienta de monitoreo en la nube muy fácil de usar. Presta los servicios básicos de monitoreo al igual que otros ya mencionados, y también otros que los demás no tienen, como el monitoreo de servicios web

con tan solo una URL, permitiendo mostrar estadísticas **HTTP**, **PING**, ***e-mail***, entre otros. Su servicio principalmente también se da en los Estados Unidos.

- ***Cloudkick***: otra herramienta comercial que presta variedad de servicios de monitoreo sobre servidores físicos y virtuales, presentando estadísticas en un lugar centralizado. Además, este sistema presenta facilidades para los principales **CSP**.

- **PCmosns**: Nace como herramienta de *software* libre, con el fin de monitorear nubes privadas. Se enfoca en recolectar y mostrar información y se basa en el uso de herramientas como *Nagios*. La desventaja de este sistema es que se requiere que su instalación y configuración sea dentro de la nube

- **SNMP**: protocolo cuyo fin es el de monitorear y configurar distintos elementos de red y de infraestructura. Este protocolo implica que cada elemento responda a ciertas métricas (por medio de **MIBS**), que son estandarizadas y mostradas en un servidor centralizado. Esta es la principal funcionalidad de algunas herramientas comerciales como **PRTG** y abiertas como **MRTG**.

6.1 Los desafíos del *logging* en arquitecturas basadas en la nube

La actividad más importante para garantizar el monitoreo y la respuesta es la recopilación y el análisis de datos de *logs*. Todas las reglamentaciones de cumplimiento exigen esta actividad de alguna forma, por lo tanto, las organizaciones que migran a la nube deben comprender como se modificará el entorno con respecto a estos *logs*.

A continuación, haremos una descripción exhaustiva de los aspectos de las arquitecturas de la nube que afectan el proceso de *logging*, el procesamiento y la respuesta ante un evento de seguridad que escape al horizonte técnico:

- **La naturaleza efímera de los activos**: las infraestructuras y las aplicaciones locales son relativamente **estáticas**. Las direcciones y puertos IP internos, las entradas DNS, las asignaciones de VLasn y los sistemas operativos tienden a ser configurados y rara vez modificados. De hecho, la mayoría de las tiendas dedicadas a TI evitan realizar cambios siempre que sea posible, por temor a que un cambio pequeño (por ejemplo, modificar la dirección de una subred) ocasione una interrupción al romper un *script* que ya todos habían olvidado. Su implementación en la nube tiene como objetivo ofrecer flexibilidad y agilidad. Los objetos van y vienen, según el diseño, y en algunos casos se introducen fallas de manera deliberada y periódica.

- **Diferencias en la tecnología**: Algunas construcciones en las infraestructuras de TI locales tienen un rol fundamental en la inserción de la seguridad y extracción de registros. Entre ellos están:

    - Inserción en la red a través de puentes.

    - Monitoreo de puertos SPAN.

    - Agentes implementados dentro de un conjunto limitado de sistemas operativos autorizados en la capa de virtualización.

- **Tasa de cambio y automatización**: los activos de la nube son efímeros por la naturaleza cambiante de esta. En particular, las aplicaciones en sí cambian, a diferencia de las aplicaciones locales que se actualizan un par

de veces al año, mediante un proceso en cascada. Las aplicaciones en la nube cambian a diario, lo que dificulta su modelado y complica distinguir un comportamiento normal. Por ello el proceso de cambio es dinámico, lo que significa que no es viable insertar puntos de control dirigidos por seres humanos.

- **Aumento de volumen de datos**: el movimiento de los datos en las arquitecturas de la nube es generalmente mayor que en los centros de datos tradicionales, lo que genera un problema de escalabilidad. Una metodología de seguridad que funciona en las instalaciones podría no funcionar en la nube, sencillamente porque no es escalable. Esto sucede porque los usuarios no han seguido el ritmo del aumento de responsabilidades asociados con la seguridad.

- **Falta de contexto**: los picos de tráfico pueden suscitarse por diversas razones, incluso después de haber realizado operaciones de ajuste en el sistema de infraestructura. Estos dan las soluciones en la nube pública, y pueden resultar imprecisas, por lo tanto, es posible optar por pasar horas rastreando para buscar patrones o adoptar una solución de terceros que le ofrezca contexto.

6.2 OpenStack

Es una colección de proyectos *cloud computing* cuyo fin es cubrir el ciclo completo para despliegues de la nube tanto en modo privado como público. Surge en 2010 de la mano de la organización *Rackspace Cloud* y de la Nasa para proporcionar IaaS. Actualmente, es gestionada por la fundación sin fines de lucro *OpenStack*, encargada de la distribución, desarrollo y adopción de *Openstack* como sistema operativo *cloud*.

Además, utiliza la licencia **apache v2** y es un *open source*, en el cual la comunidad colabora con lanzamientos de desarrollo con una frecuencia semestral. Esta tecnología se impone sobre el resto de la plataforma IaaS gracias al apoyo de los usuarios, a pesar de ser una tecnología reciente y que presta enormes expectativas.

6.2.1. Arquitecturas conceptual y lógica de Openstack

OpenStack utiliza **API públicas** (proyectos) para comunicar todos sus servicios, aunque no es necesaria la instalación de todos ellos. Únicamente son necesarias unas cuantas funciones para dar respuesta a necesidades particulares.

Los proyectos más importantes son:

- **Horizon**: provee servicios de portal web (*dashboard*) para interactuar con las demás funciones.
- **Nova**: responsable de la gestión del ciclo de vida completo de las instancias de cómputo (*compute*) en el entorno *OpenStack*.
- **Neutron**: provee una API para la definición de configuraciones de la red (*networking*) y ofrece conectividad con los demás servicios *OpenStack*.
- **Swift**: almacena y recupera datos (*objects traje*) a través de una API REST basadas en HTTP.
- **Cinder**: permite la creación y gestión de dispositivos de almacenamiento (*block storage*) para las instancias en curso.

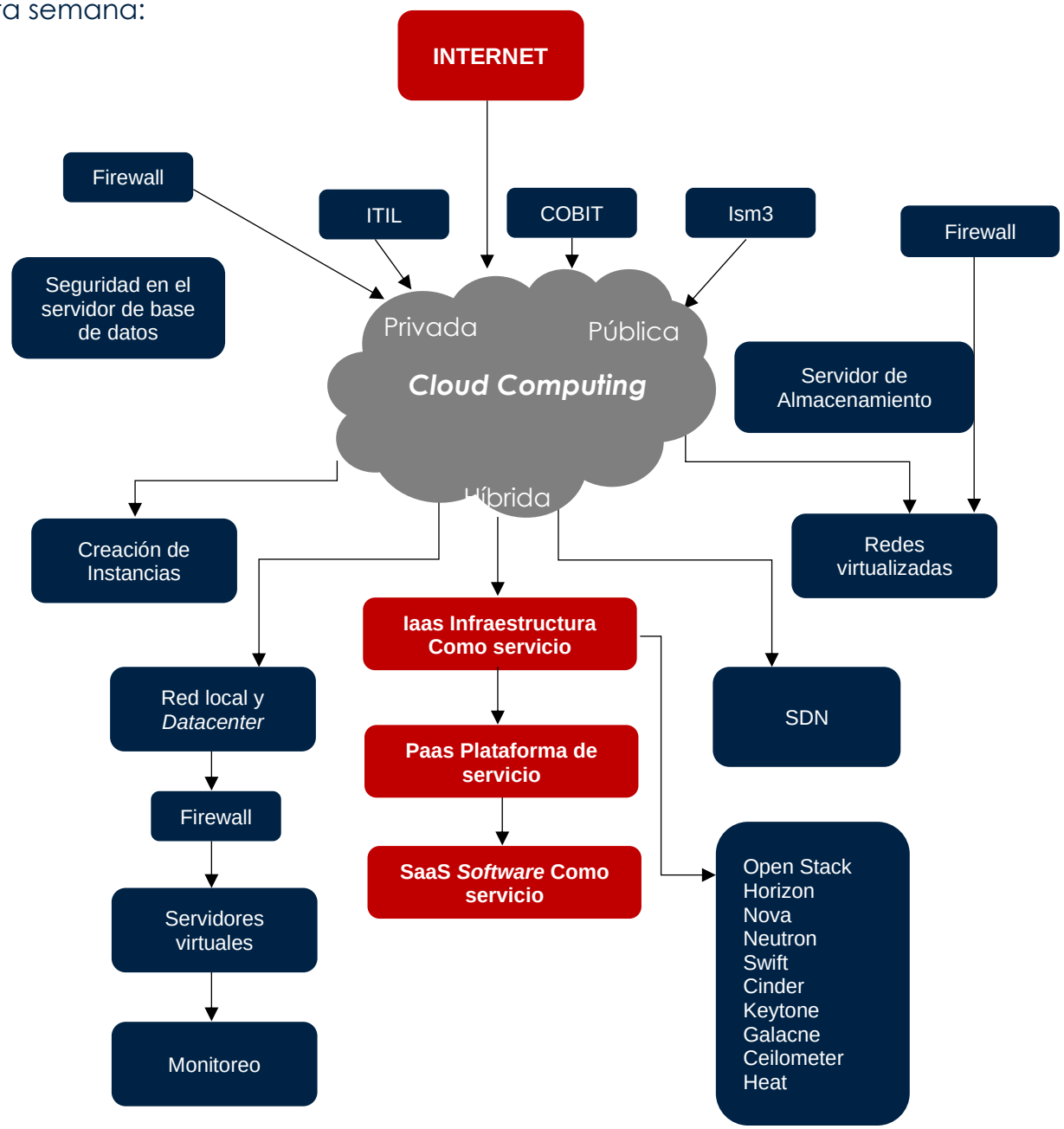
- **Keytone**: ofrece un servicio de autenticación y autorización a los servicios desplegados.
- **Galacne**: el encargado de almacenar y recuperar las imágenes de disco de las máquinas virtuales (al crear instancias).
- **Ceilometer**: desplegada con *OpenStack*, actúa como monitor de la nube, pudiendo realizar tareas de facturación comparativas de mercado.
- **Heat**: permite la orquestación con otros servicios de alto nivel, como los proporcionados por **AWS** (Ancon Web Services), en la nube, usando plantillas como formato nativo **HOT.**

6.2.2. Organización y planteamiento

Dependiendo del tamaño de la organización, debemos tener en cuenta de qué vamos a organizar en nuestro *cloud*, qué servidores se encargarán del cómputo almacenamiento, control de red, etc. *OpenStack* requiere de dos a cuatro CPU, un mínimo de ancho de gigas de RAM, un mínimo de cien gigabytes de almacenamiento y dos tarjetas de red. Para esta instalación se han utilizado dos servidores de 8 núcleos 32 gigas de RAM y 300 GB de disco duro.

Cierre

Por medio del siguiente organizador gráfico, se destacan las ideas clave de esta semana:



Referencias bibliográficas

- Abts, D. (2011). *High performance datacenter networks: architectures, algorithms, and opportunities*. Obtenido de https://bit.ly/3oqlVSL
- Mark A. Sportack. (2003). *Fundamentos de enrutamiento IP*. Madrid: Pearson Educación.
- TIA. (2005). *TIA Standard: Telecommunications Infrastructure Standard for Data Center*. Obtenido de: https://manuais.iessanclemente.net/images/9/9f/Tia942.pdf