**Investiga y explica cómo se lleva a cabo la seguridad en los medios de almacenamiento online DAS, NAS, SAN y Virtualización del almacenamiento. Contenido y extensión a criterio del alumnado.**

El almacenamiento de datos es el proceso tecnológico donde se graban, archivan y guardan bits de información que contienen imágenes, texto, video, programas, hojas de cálculo, entre otros archivos digitales de múltiples formatos. Existen diversas arquitecturas y dispositivos de almacenamiento para cumplir este propósito.



**Almacenamiento de datos en red**

Este tipo de almacenamiento cuenta con una gran velocidad de transmisión de datos en una red. Existen tres tipos:

# **NAS (Network attached storage)**

La forma más sencilla de describir un NAS es definirlo como un disco duro conectado directamente a una red LAN.

Por lo que estos discos duros conectados a nuestra red LAN nos permite trabajar con la información que tenemos guardada en él. Dando a todos los usuarios que están conectados a esta red LAN, el poder de compartir archivos y trabajar sobre ellos.

Por lo que los sistemas NAS están orientados a manejar un gran conjunto de pequeños documentos y podemos deducir que son perfectos compañeros de oficina o domésticos. Tiene las ventajas de que es de tamaño reducido y no requiere de un mantenimiento como los servidores. Además de que tiene un menor consumo eléctrico, compatible con la mayoría de sistemas operativos y es más sencillo de administrar.

* Copias de seguridad.
* Un sistema Cloud privado.
* Compartir archivos
* Servidores Web (aunque de baja potencia)

# **DAS (Direct Attached Storage)**

La principal diferencia entre un DAS y un NAS es que los primeros no disponen de funcionalidades Webs. Se podría decir que el sistema DAS es el más sencillo de los tres y prácticamente todos lo hemos usado sin saberlo. Consiste en una conexión directa del ordenador a los datos, en lugar de conectarlo con un router o NAS. Por lo que podemos decir que son discos duros externos que tienen la función de compartir los datos entre los usuarios.

* Mayor velocidad de acceso y transmisión de información.
* Más sencillo y menos costoso que un NAS
* Desventajas no sirve de como servidor web

# **SAN (Storage área network)**

Un SAN es un conjunto de dispositivos junto con un software especializado para crear una red enfocada al intercambio de datos mediante bloques. Es una tecnología perfecta para conectar servidores.

Estos sistemas contienen red de alta velocidad, equipos de interconexión como switches y conmutadores, discos duros donde almacenar los datos

* Una mayor eficiencia
* Mayor protección para tus sistemas y datos
* Gran escalabilidad
* Encriptación
* Backup
* Su capacidad es casi ilimitada y puede alcanzar miles de terabytes de capacidad
* Compartir datos entre varios equipos de la red sin afectar el rendimiento ya que el tráfico SAN está separado del tráfico del usuario.

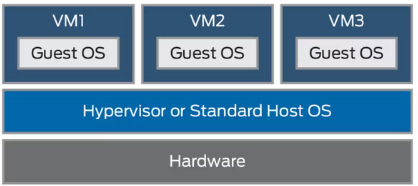
**Virtualización de Seguridad**

La virtualización es el proceso de ejecutar varias instancias virtuales de un dispositivo en un solo recurso de hardware físico. La virtualización de la seguridad hace referencia al proceso, al procedimiento y a las políticas que garantizan que la infraestructura de hardware virtualizada esté segura y protegida.



# **¿Qué puede hacer con la virtualización de la seguridad?**

La virtualización de la seguridad ejerce de barrera para proteger el acceso de perímetro a la red. Proporciona servicios de seguridad específicos y garantiza el aislamiento del tráfico dentro de la nube, además de ofrecer controles de firewall personalizables como servicio de gestión adicional. Las empresas y los proveedores de servicios pueden aprovechar su inversión en virtualización para crear un perímetro de seguridad granular mediante la asignación de recursos de seguridad dentro de una arquitectura de nube a los inquilinos y suscriptores del servicio.



# **¿Cómo funciona la virtualización de la seguridad?**

Un sistema de virtualización está compuesto por un sistema operativo host, un hipervisor y un sistema operativo invitado.El host es el hardware subyacente del sistema de virtualización que ofrece recursos de computación (tarjetas de interfaz física, CPU, memoria, puertos de gestión, sistema operativo, software de terceros e hipervisor). Todo esto permite al host contener una o más máquinas virtuales (o particiones) y compartir recursos físicos con ellas.

# **Problemas que aborda la virtualización**

La virtualización centraliza las tareas administrativas y mejora la escalabilidad y las cargas de trabajo. Además, permite la consolidación de la infraestructura de red, reduce los gastos operativos (OpEx) y simplifica la gestión. Ahora bien, la virtualización también plantea desafíos de seguridad para los cuales los sistemas de seguridad físicos no están preparados:

* El intercambio de archivos entre hosts e invitados no es seguro.
* El aislamiento entre componentes, como los OS y las aplicaciones de los invitados, los hipervisores y el hardware se debilita.
* Se consolidan varios servidores, lo que supone un mayor riesgo de que una vulneración pueda propagarse desde las aplicaciones de un mismo host.
* En cuanto a los sistemas de prevención de intrusiones (SPI), el malware dirigido a máquinas físicas y virtuales causa la infección mediante la red virtual. Otras amenazas de seguridad incluyen: el acceso no autorizado, la denegación de servicio y vulnerabilidades de seguridad..