

LI - Escritorios Virtuales

El presente lineamiento representa una guía de referencia dado que permite comprender distintos aspectos básicos de una tecnología específica, en este caso los Escritorios Virtuales.

La idea principal es disponibilizar un conjunto de recomendaciones y prácticas que permitan comprender cuál de las soluciones tecnológicas disponibles se adecúa a la resolución de la problemática relevada y los distintos aspectos técnico funcionales involucrados.

Escritorios Virtuales

Los escritorios virtuales son una tecnología que permite desvincular las terminales físicas de los usuarios con el sistema operativo que ellos utilizan. Estos escritorios no se encuentran alojados en las terminales de los usuarios, sino que se encuentran en uno o más servidores, facilitando distintos aspectos de la gestión dado que los activos se encuentran centralizados y se obtiene un único punto de falla.

Existen tres modalidades de implementar esta tecnología: el organismo puede poseer un centro de datos propio en donde virtualizar los escritorios. Por otro lado, puede también utilizar *housing*, es decir, alojar servidores propios en un centro de datos de un proveedor (por ejemplo en ARSAT). Por último, la tercera posibilidad, es contratar escritorios virtuales como servicio, comúnmente conocido con el nombre de DaaS (Desktop as a Service).

En ese orden, para las primeras dos modalidades se detallan a continuación distintas consideraciones propias de la tecnología tales como, recursos, dimensionamiento, arquitectura, seguridad, que deben ser tenidas en cuenta a la hora de utilizar servidores propios, ya sea con un datacenter propio o de un tercero para realizar una adecuada adopción tecnológica. Si la decisión del organismo es optar por la última modalidad, recomendamos la lectura del "LI - Servicios de nube".

Recursos necesarios. Los escritorios virtuales, como todo recurso de cómputo, consumen cuatro elementos básicos: el procesamiento (CPU), la memoria (RAM), el almacenamiento en disco para la imagen del sistema operativo (SO) de cada tipo de escritorio y el ancho de banda o tráfico de Internet (networking). Asimismo, se deberá considerar que si se requiere persistencia de los escritorios virtuales, la capacidad variará según se necesite una persistencia de las preferencias de escritorio de cada usuario, o una persistencia de los datos que genere el usuario durante el uso del escritorio virtual. Esto último requiere un cuidadoso relevamiento de las necesidades de los usuarios.

Dimensionamiento. La cantidad de recursos que consume un escritorio virtual depende de cuatro aspectos que se encuentran relacionados con las necesidades que se deben cubrir en los usuarios. Estas necesidades definirán las exigencias mínimas de consumo de recursos, las cuales se deben dimensionar para satisfacer la correcta realización de sus tareas. Los cuatro aspectos antes mencionados son:

- El sistema operativo (SO) que corre (Windows, Linux, etc.) y esto influye en la CPU y RAM que consumen, y en menor grado en el almacenamiento ya que se mantiene una única imagen para todas las instancias de un mismo escritorio virtual..
- Las aplicaciones que ejecutan la imagen de SO (una imagen de SO preparada para ejecutar aplicaciones de diseño gráfico virtualizadas ocupará más CPU y memoria, que una dedicada sólo a Ofimática). Es decir, las aplicaciones que se virtualicen en la imagen de SO, también influyen en la CPU y RAM que consumen los escritorios virtuales que se instancian a partir de ellos.
- La cantidad de datos que requiere almacenar cada usuario (influyen en la capacidad de almacenamiento requerido).
- El tamaño de los archivos que el usuario requiere enviar y recibir en el escritorio virtual (influye en el ancho de banda de Internet necesario).

Análisis de la arquitectura de una solución de escritorio virtual.. Los escritorios virtuales se alojan y se ejecutan en un centro de datos del cual consumen recursos de CPU, RAM, almacenamiento y ancho de banda de Internet. Los usuarios pueden encontrarse in situ, es decir dentro de los organismos y entidades del Sector Público Nacional, pudiendo utilizar equipamientos propios o dispositivos provistos por el organismo.

Esta tecnología también puede utilizarse para el trabajo remoto, es decir, cuando existen usuarios trabajando desde sus hogares con equipo propio (PC, notebook) y servicio de Internet hogareño.

El almacenamiento de datos puede tener tres formas: en primer lugar, se puede realizar en el centro de datos donde se ejecutan los escritorios virtuales. Una segunda opción es mediante la provisión de un servicio externo de nube contratado específicamente para ese fin (ARSAT, Google, Azure, AWS, etc.). Finalmente, se pueden almacenar los datos en los dispositivos personales de los usuarios. No obstante, siendo este último es menos recomendado porque se pierde principalmente la disponibilidad.

También se debe considerar que el ancho de banda de Internet y su disponibilidad depende de dos aspectos: el primero es la capacidad del enlace a Internet contratado

en el centro de datos en donde se alojan los Escritorios Virtuales; el segundo es la capacidad del enlace a Internet, dependiendo cual sea el caso puede ser aquel con el que se conecta el organismo del SPN (usuarios corporativos), o bien aquel con el que se conectan los tele trabajadores (servicio hogareño).

Seguridad de los datos. En todos los casos de adopción de nuevas tecnologías es importante garantizar la confidencialidad, integridad, y disponibilidad de los datos. Particularmente, con este tipo de tecnología se deben considerar los siguientes aspectos:

Confidencialidad: para asegurar que los datos confidenciales son accedidos solo por el personal autorizado, se debe tener en cuenta algunas recomendaciones:.

- Por parte del centro de datos:
 - Crear políticas de acceso a los datos que definan qué escritorios virtuales y qué usuarios tienen permisos para acceder a qué datos.
 - Encriptar las conexiones entre los servidores del centro de datos y los browsers de los usuarios (instalar certificados SSL en los servidores web).
 - Encriptar el tráfico entre los usuarios y el centro de datos (instalar gestor de túneles VPN “red privada virtual” para brindar conexión segura a los teletrabajadores).
- Por parte de los usuarios corporativos o tele trabajadores, se recomienda utilizar herramientas de software que permitan establecer conexiones seguras entre el cliente y el centro de datos, ya sea que este último sea propio o público. Algunas herramientas a considerar podrían ser las “Conexiones seguras del tipo SSL”, generalmente ya incluidas en el browser del usuario y los “Cliente VPN” que es un software cliente a instalar en el equipo del usuario.

Integridad. Para asegurar la integridad de los datos, es decir que los datos no sean alterados por usuarios no autorizados, se recomienda considerar los siguientes aspectos:

- Por parte del centro de datos: crear políticas de acceso a los datos que definan qué permisos tienen los usuarios sobre los archivos a los que acceden (lectura, escritura, eliminación, creación, etc.).
- Por parte de los usuarios corporativos o teletrabajadores: utilizar herramientas de software que permitan establecer conexiones seguras entre el cliente y el centro de datos, de modo que no haya posibilidad de

alteración de los datos en tránsito entre el equipo del usuario y el centro de datos, ya sea que este último sea propio o público. Las herramientas a brindar a los usuarios son las mismas que para brindar confidencialidad (conexiones seguras tipo SSL y clientes VPN).

Disponibilidad de los datos. Para asegurar la disponibilidad de los datos, se recomienda considerar las siguientes acciones.

- Implementar redundancia en el centro de datos para evitar indisponibilidades del servicio por fallos en el hardware, o exigir un porcentaje de disponibilidad mínimo en caso de tratarse de servicios en la nube.
- Contar con políticas de resguardo que contemplen la realización de *backups* periódicos de los datos.

Finalmente, se realizan una serie de consideraciones respecto de algunos aspectos destacados que posee esta tecnología, destacándose que la adopción de los escritorios virtuales puede generar más dedicación en una primera instancia de instalación, pero conduce a una mayor eficiencia a largo plazo.

Hardware. Las aplicaciones y el sistema operativo centralizado de un escritorio virtual facilitan el uso compartido de computadoras y, por lo tanto, es necesario comprar menos PC. Contrariamente, no es una ventaja si se va acceder en modo teletrabajo y se le va a entregar un dispositivo a cada usuario.

Aplicaciones. La mayoría de las aplicaciones son fáciles de virtualizar y se integran sin problemas en escritorios virtuales, como las aplicaciones que requieren pocas modificaciones, tienen procedimientos de configuración simples y no tienen hardware físico.

Administración. Los ahorros más significativos de la implementación de los escritorios virtuales se encuentran en la administración del sistema. El sistema operativo y las aplicaciones se utilizan en la misma imagen, lo que las hace menos costosas de administrar. El sistema se controla de forma centralizada y se necesita menos personal para completar las reparaciones. Asimismo, los administradores pueden solucionar problemas de forma eficaz sin tener que ir al escritorio del usuario, lo que ahorra tiempo y, en consecuencia, reduce el trabajo.

Movilidad. Los usuarios deberían ver un aumento en su productividad a largo plazo con escritorios virtuales dada a la movilidad mejorada. De esta manera, los usuarios que pueden conectarse de forma segura a un escritorio virtual desde cualquier dispositivo y en cualquier lugar, tienen un proceso optimizado para sus tareas y no necesitan tener dispositivos separados.

Interrupciones. Para el usuario individual, las interrupciones de la PC serán un problema menor porque los datos y las aplicaciones están centralizadas. Por lo tanto, si ocurriera una interrupción, los usuarios pueden simplemente pasar a otra PC y continuar con su trabajo. A largo plazo, las interrupciones del sistema disminuyen con los escritorios virtuales. Los sistemas se vuelven menos vulnerables a los ataques y la administración centralizada hace que sea más probable que los problemas se detecten antes de que provoquen interrupciones.

Seguridad. Los escritorios virtuales protegen mejor la información porque son posibles menos ataques. El robo de datos se vuelve menos probable ya que hay menos dispositivos abiertos.

Planificación futura. Los escritorios virtuales son más adaptables porque los cambios en el sistema son más rápidos, lo cual es ventajoso en el entorno actual donde la adaptación es esencial.