Diseño de una infraestructura segura para proporcionar un servicio de teletrabajo

Autor: Abad Gutiérrez, Laura

Director/es: Rodelgo Lacruz, Miguel

Contacto: laura.abad@alumnos.uvigo.es

Resumen: Este trabajo trata de presentar una arquitectura para dotar de teletrabajo a cualquier organización con altos requisitos de seguridad. Para ello se propone el diseño de un sistema en el que de principio a fin se pone el foco en la seguridad, dotando a cada elemento de los mecanismos necesarios para garantizarla y dedicando un especial esfuerzo en realizar las pruebas adecuadas sobre el sistema implantado, que permitan evidenciar que tal seguridad existe.

Además, se basará en soluciones de virtualización de escritorios que por una parte permitirán el acceso a los servicios corporativos desde ubicaciones remotas, y por otro mantendrán una infraestructura *on-premise* que se podrá beneficiar tanto de la seguridad física como lógica que la organización ya viene manteniendo sobre sus instalaciones, sistemas e información.

La implementación de este sistema se realizará de manera integrada con los servicios que la organización presta de manera presencial. Los escritorios virtuales ofrecerán un modo de trabajo en el que la experiencia de usuario no se verá afectada, ni en la calidad del servicio ni en el modo en que se realizan las tareas habituales.

Todos los elementos, tanto hardware como software, que conforman la infraestructura se instalan siguiendo las guías de seguridad que sean de aplicación, y una serie de buenas prácticas, tratando siempre de emplear dispositivos acreditados. Sin olvidar por supuesto, cumplir con las diferentes normas y legislación aplicable tanto por la parte del teletrabajo como por la del propio centro de proceso de datos.

Palabras clave: VDI, teletrabajo, escritorio virtual, citrix, vmware

---

1. Introducción

Hace casi ya dos años, desde marzo de 2020, que el teletrabajo irrumpió de manera imprevista en la vida de muchas personas. La pandemia mundial ha supuesto el desencadenante de un cambio en la manera de trabajar de muchas organizaciones, y en pleno siglo XXI, este fenómeno repentino ha pillado a muchísimas empresas con el pie cambiado.

En el caso concreto de España, gozamos de una buena posición con respecto a la inmersión en tecnologías de la información. El informe del DESI 2020 [1] (Índice de la Economía y la Sociedad Digitales) nos coloca por encima de la media europea en el índice de digitalización de la economía y la sociedad, especialmente en el ámbito de la conectividad de muy alta capacidad, gracias al despliegue de infraestructura como la fibra, 4G y 5G. Lo cual nos indica que nuestro país se encuentra en una situación aventajada en cuanto al potencial de implantación de teletrabajo que no podremos dejar de aprovechar.

El planteamiento de los auténticos retos que supone el teletrabajo, es lo que me ha motivado a elegir este trabajo, para dar respuesta a una necesidad creciente de las organizaciones, poniendo especial énfasis en garantizar la seguridad de los datos y los sistemas.

2. Desarrollo

2.1. Tecnologías de aplicación

La primera cuestión que se nos plantea es referente al principal mecanismo para acceder a aplicaciones y datos corporativos, es decir: ¿cuál es realmente la mejor manera de proporcionar teletrabajo?

La respuesta a esta pregunta plantea una primera elección: ¿Una red privada virtual, Virtual Private Network (VPN), o una infraestructura de escritorios virtuales, Virtual Desktop Infraestructure (VDI)?

El primer caso supone acercar el puesto de trabajo de cada trabajador a su propia casa con unos cambios mínimos, permitiendo la conexión a la red local a través de un túnel VPN, del mismo modo que si estuviese en la oficina. En el segundo, el planteamiento implica un cambio importante en la infraestructura, no tanto en la parte del trabajador, que gracias a la tecnología de escritorios virtuales contará con una experiencia de usuario similar, sino en la parte de las TIC, que deberán desplegar esta nueva infraestructura e integrarla en su centro de proceso de datos.

Si evaluamos comparativamente las diferentes características que ofrece cada alternativa desde varios puntos de vista, tenemos lo siguiente:

Hardware

VPN depende en gran medida del hardware del usuario, ya que todo el procesamiento se realiza en los dispositivos del cliente. El hardware antiguo y los sistemas operativos obsoletos pueden afectar al rendimiento y a la productividad. A esto debemos añadir la dificultad que supone mantener y administrar estos equipos remotamente.

Por otro lado, VDI tiene requisitos mínimos de hardware, y los dispositivos de los usuarios finales no suponen restricciones importantes para garantizar la experiencia de usuario. El procesamiento se realiza en el lado del servidor, utilizando recursos dedicados asignados a la máquina virtual que ejecuta el escritorio.

Almacenamiento de datos y seguridad

Hay una gran diferencia en la forma en que VPN y VDI manejan los datos. En el caso de VPN se protegen los datos mientras están en tránsito, enviándolos a través de un túnel cifrado. Mientras que los datos en el túnel llegan de forma segura al usuario, no tienen límites de seguridad una vez que están en el dispositivo del cliente. Pueden moverse y copiarse externamente sin restricciones. Tener archivos de la organización copiados localmente supone un peligro para la seguridad.

Cuando se utiliza VDI, las aplicaciones y los datos permanecen en la máquina virtual que ejecuta la estación de trabajo. Por lo tanto, los archivos están protegidos en los servidores de la organización. Los administradores pueden configurar los escritorios virtuales para restringir el movimiento de datos fuera de la red corporativa.

Rendimiento

Sin duda, VPN pierde la carrera en cuanto a rendimiento para las cargas de trabajo más grandes. Dado que las redes privadas virtuales dependen de los dispositivos de los usuarios finales, están limitadas a los recursos del usuario final y a la velocidad de conexión. Por lo tanto, diferentes usuarios tienen diferentes resultados de rendimiento dependiendo de su hardware y calidad de conexión. Además, el cifrado y descifrado de grandes cantidades de datos también puede afectar a la velocidad y al trabajo remoto.

VDI proporciona un entorno más rápido y una mejor experiencia de usuario porque cada usuario tiene asignados recursos para su estación de trabajo virtual. En lugar de tener que depender de los dispositivos del usuario, VDI utiliza recursos de servidor dedicados para mejorar las capacidades de personalización y rendimiento.

Gestión y mantenimiento

En lo que respecta a la gestión de la VPN, el servidor o infraestructura que la gestiona, es más fácil y menos costoso de mantener. Sin embargo, el mantenimiento de los dispositivos cliente es más complejo, ya que utilizan recursos externos. Esto requiere conectarse al dispositivo para solucionar problemas o realizar actualizaciones.

A diferencia de lo que ocurre con VPN, los administradores pueden actualizar y solucionar fácilmente los problemas de una infraestructura de escritorios virtuales porque disponen de una gestión centralizada del sistema. Los administradores pueden actuar sobre toda la infraestructura y tener un estrecho control sobre todo el entorno. Debido a la complejidad del sistema, esta solución requiere administradores cualificados que puedan garantizar que todo está bien configurado.

Coste

El coste puede jugar un papel importante a la hora de decidir entre VPN y VDI, ya que difiere drásticamente. Si se está buscando únicamente una solución rentable, VPN puede resultar la mejor opción. Debido a sus mínimos requisitos de hardware y a un mantenimiento menos costoso, pero normalmente se deben considerar otros factores que pueden justificar una mayor inversión.

Al contrario, VDI es una solución más cara, ya que incluye añadir toda una de una capa adicional de software y una nueva infraestructura para alojar el sistema VDI, hardware de servidor y recursos

dedicados para cada estación de trabajo, lo que requiere una alta inversión inicial, pero que se ve compensada a largo plazo por los ahorros en costes de administración y mantenimiento.

En definitiva, como podemos observar en los aspectos tratados, los mecanismos de control, acceso, seguridad y administración que ofrece VDI lo convierte en la opción más adecuada para utilizar en el diseño de un sistema en el que estas características son imprescindibles, sin olvidar que además el empleo de escritorios virtuales nos va a permitir mantener la experiencia del usuario al máximo nivel.

2.2. Proveedores

Si echamos un vistazo al mercado, la cantidad de opciones disponibles para proporcionar una infraestructura de escritorio virtual, es elevada y parece que cada vez los arquitectos de sistemas van a disponer de más opciones, ya que las alternativas no dejan de crecer.

Las características que debemos evaluar a la hora de elegir un determinado proveedor van a ser las siguientes:

- Una presencia consolidada en el mercado, con soluciones probadas, contrastadas y que ofrezca continuidad y estabilidad.
- Que disponga de un servicio de soporte de calidad y eficaz.
- Que disponga de técnicos cualificados, y sean capaces de prestar apoyo en las intervenciones que deban realizarse en la infraestructura.
- Que ofrezcan productos fáciles de implementar, integrar, y tengan capacidad de ofrecer soluciones adaptadas para cada cliente.
- Que dispongan de herramientas fáciles de gestionar y proporcionen una administración simplificada.
- Que cuenten con una oferta adecuada de formación completa y de calidad.
- Que proporcionen I+D+I suficiente para evolucionar sus productos y soluciones, renovando las tecnologías, adaptándose a las nuevas necesidades y ofreciendo continuamente tecnología actualizada e innovadora.

Si evaluamos los principales proveedores de soluciones virtuales que garanticen estas premisas, centramos el abanico de opciones en Vmware, Citrix y Microsoft. Todos ellos ofrecen productos estables de largo recorrido, y ampliamente conocidos. La mejor opción es combinar las fortalezas de cada proveedor y diseñar una solución combinando productos de cada uno de ellos.

De Citrix implementaremos la parte de virtualización de escritorio que ofrece gracias a su completa infraestructura de Citrix Virtual Apps and Desktops, una experiencia de usuario con el escritorio virtual cercana al PC tradicional. Vmware proporcionará su amplio conocimiento de hipervisores y será la tecnología empleada tanto para implementar los servidores que serán virtuales, como la infraestructura de clientes con vCenter y vSphere. Microsoft aportará toda la parte de distribución de software, aplicaciones, parches, y sistemas operativos dando soporte a los sistemas tanto en servidores como en clientes.

2.3. Implementación del teletrabajo

La virtualización de escritorio se trata de un modelo de virtualización basado en máquinas virtuales de sistemas operativos cliente. Este modelo de virtualización ofrece a los usuarios acceso remoto a escritorios completos de Windows (fundamentalmente) sin necesidad de disponer de

hardware potente en el origen, ya que los escritorios se ejecutan en el centro de datos, en un conjunto o clúster de servidores.

Se debe diseñar e implantar una infraestructura que abarque desde el puesto de cada teletrabajador, los sistemas de comunicaciones, controles de acceso, etc., hasta los servidores y sistemas de almacenamiento que darán soporte al sistema, logrando mantener en todo momento las condiciones de seguridad exigidas.

Dado que las ubicaciones en las que se podrá teletrabajar no pertenecen a la propia organización, ésta no tendrá ningún mecanismo de control sobre las medidas de seguridad física. Por ello se ha determinado definir un sistema en el que el puesto físico que utilice el trabajador no pueda albergar ningún tipo de información, más allá de la configuración para la conexión. Estos puestos serán ordenadores portátiles configurados para que no pueda realizarse ningún trabajo en local.

Como hemos avanzado en el punto anterior, el sistema estará basado en la tecnología de escritorios virtuales de Citrix (VDI), de manera que toda la información se mantendrá almacenada en el CPD de la organización.

El escritorio virtual que se mostrará a cada usuario será una simulación de su puesto de trabajo físico que tendría en modalidad presencial. Contará, salvo alguna excepción justificada, con los mismos accesos, servicios y aplicaciones de los que disponía habitualmente.

El sistema se compone de cuatro partes principales:

1) Puesto de trabajo de usuario asegurado.

Aunque se podría tratar de cualquier dispositivo, por homogeneizar, se va a concretar en un equipo portátil (puede ser del mismo tipo y modelo de los usados de manera habitual en la organización), con sistema operativo Windows 10 y fuera de dominio. Este equipo estará asegurado utilizando los siguientes mecanismos de aseguramiento y gestión:

- Cifrado del disco duro mediante CRYHOD
- Bastionado con las guías CCN-STIC-599B19
- Gestionado mediante el cliente de SCCM de Microsoft
- Con cliente Citrix EPA
- Agente Antivirus McAfee
- McAfee DLP Endpoint
- McAfee Endpoint Security

De esta forma se trata de garantizar la integridad del mismo y que se evite que el usuario pueda ex filtrar información en formato digital del equipo. Este equipo no podrá realizar ningún trabajo en local y solo podrá trabajar una vez se conecte con la infraestructura de la organización.

2) Sistema de comunicaciones cifradas seguro.

Junto al puesto de usuario se encuentran los dispositivos que facilitarán las comunicaciones con los sistemas corporativos de manera segura. Para el acceso a la red (Internet) se ha optado por utilizar un dispositivo 4G ya que se trata de la manera de conexión más independiente.

Además las comunicaciones seguras serán posibles a través de un sistema basado en el uso de cifradores personales EPICOM EP960, proporcionados con los equipos de teletrabajo, que están

configurados para conectarse a unos cifradores EP430DIC en las instalaciones centrales de la organización.

Este sistema de cifra se trata de una versión comercial, que está certificado por el CCN-CERT [2] para versiones con cifra nacional. Además, el sistema cuenta con cortafuegos para proteger los cifradores. Este sistema de comunicaciones se apoya en el acceso externo con que ya cuenta la organización y las infraestructuras existentes, como son los balanceadores F5, que proporcionan alta disponibilidad y diversidad de accesos a Internet.

3) DMZ.

Esta zona proporciona un nivel extra de seguridad al servir de puerta acceso a los equipos de teletrabajo antes de acceder a los sistemas e información corporativos de la organización.

Esta capa de acceso cuenta con:

- Balanceadores NetScaler que validarán el acceso de los miembros de la organización en teletrabajo a través validación con usuario y contraseña del dominio.
- Servidor de actualizaciones de seguridad de los portátiles (WSUS) y distribución de software.
- Servidor gestor del software seguridad del portátil (antivirus, control de puertos, etc.) EPO.
- Servidores que prestarán los servicios de seguridad del CCN-CERT (CARMEN).
- Servidor de licencias Microsoft KMS para licenciar los equipos portátiles.

4) Infraestructura de virtualización de escritorios

Podemos ver la arquitectura en la Figura 1. Muy brevemente, vemos como consta de cuatro capas diferenciadas:

- **Capa de usuario**: Compuesta por la parte de equipos clientes que disponen de Citrix Receiver bajo el que se accede a los recursos disponibles para un usuario dado.
- **Capa de acceso**: Las implementaciones típicas para usuarios externos requieren que éstos realicen conexiones cifradas seguras que admitan el protocolo HDX, como Citrix Gateway. En el acceso se establece un canal desde el dispositivo cliente, a través de un protocolo llamado ICA que es el que permite establecer ese dialogo virtual, presentando la máquina virtual al cliente como si fuera un video interactivo, y proporcionando así esa seguridad de que los datos no viajarán fuera de la organización.
- **Capa de control**: La capa de control se utiliza para agrupar y presentar los principales componentes de la implementación de Citrix Virtual Apps and Desktops, que son los recursos. Aquí se encuentra el servidor Delivery Controller que es el intermediario que maneja las solicitudes de sesiones de usuario, tanto a aplicaciones como a escritorios virtuales. También gestiona el equilibrio de carga y la disponibilidad y las conexiones a los recursos que se ofrecen. En esta capa también se encuentran la base de datos SQL y el servidor de licencias Citrix, encargado de mantener y suministrar licencias para las conexiones de los usuarios.
- **Capa de recursos**: La capa de recursos es una presentación de todos los recursos a los que los usuarios autorizados pueden acceder . También es la parte de la arquitectura donde los administradores establecen la mejor manera de administrar y controlar los

recursos que se ofrecen, mediante la creación de políticas para otorgar o restringir funciones a los usuarios.

- **La capa de hardware**: La capa de hardware proporciona la infraestructura virtual que necesitan el resto de capas: de acceso, control y recursos. Supone el "canal de suministro hardware" para todo el entorno.

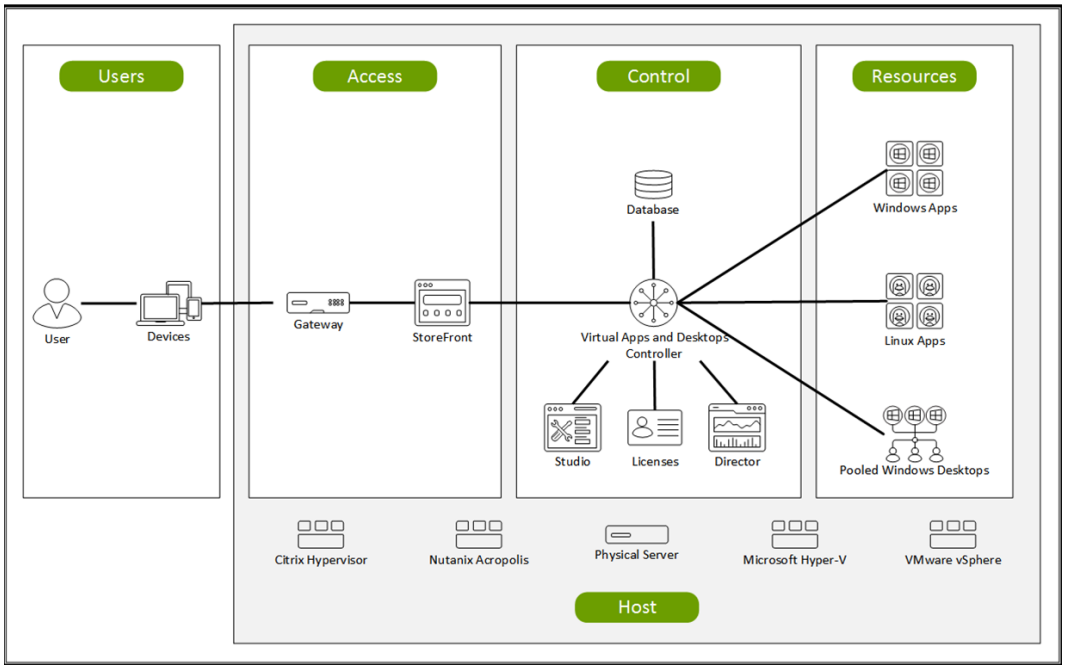

Figura 1. Arquitectura VDI.

3. Resultados

El principal objetivo de este trabajo se basa en dos grandes pilares: Servicio de teletrabajo y seguridad. Hemos visto en el apartado anterior de manera esquemática como se implementaba una infraestructura como solución de teletrabajo. Para poder dar por alcanzados los objetivos debemos además garantizar la seguridad.

Para ello, se plantea implementar mecanismos que permitan proteger los sistemas y conocer la respuesta de dichos sistemas ante acciones o situaciones no previstas que puedan poner en riesgo la seguridad. Debemos medir cuánto de seguro es, ya que sin esas medidas no será posible conocer las capacidades que se realmente ofrecen, ni llevar a cabo acciones correctivas.

Además del aseguramiento del puesto del usuario y los servicios prestados en la DMZ, se implementarán una serie tanto de medidas compensatorias, como aplicación de buenas prácticas, que permitirán garantizar la seguridad y realizar un seguimiento de los eventos de seguridad, dotando a los responsables de seguridad TIC de la capacidad de detección y respuesta antes incidentes de seguridad. Destacamos las siguientes acciones:

- Cifrar los ficheros de configuración y datos de las máquinas virtuales, así como sus instantáneas, para asegurar la seguridad de los datos críticos.
- Todos los sistemas alojados en una misma infraestructura virtual deben estar separados a través de firewalls, que filtren el tráfico de red y permitan solamente las comunicaciones definidas en cada uno de los sistemas, de modo que los aísle adecuadamente e impida la ejecución de código dañino e intentos de ataques o explotación de vulnerabilidades.

- Se debe contar con una correcta auditoria de los sistemas, que permita disponer de un registro que permita tanto realizar un análisis forense de un incidente como investigar un determinado comportamiento.
- Se debe mantener para todos los usuarios el principio de menor privilegio, dotando a cada grupo de usuarios los roles adecuados para su función y segregando correctamente dichos roles.
- Debe contarse con un adecuado plan de contingencia que permita la recuperación de los servicios en caso de desastre. En la política de copias de seguridad debe estar definido el plan de actuación que incluirá una copia remota de los datos a suficiente distancia que deberá mantenerse periódicamente.
- Se debe configurar el mayor nivel de auditoría asumible en cada dispositivo (cifradores, servidores, equipos, etc.).
- Se deben aplicar las guías STIC en cada sistema instalado que disponga de ella.
- Se debe configurar DLP en los equipos y deshabilitar cualquier tipo de conexión inalámbrica, así como protocolos que no deban utilizarse, como SSH, RDP, etc.
- Incorporación de sistemas de seguridad de aprendizaje autónomo que facilitan un continuo análisis de comportamientos y detectan las anomalías.

4. Conclusiones

Mi propósito al elegir y desarrollar este TFM no es otro que el de proporcionar un marco de referencia que pueda servir como base para diseñar un modelo, de las múltiples opciones posibles hoy en día, para implantar un sistema de teletrabajo con la mayor garantía de seguridad posible.

Hemos sido testigos a lo largo de estos dos últimos años de la necesidad de disponer en las organizaciones de mecanismos y sistemas que posibiliten esta nueva forma de trabajar. En este punto, debo resaltar varios datos que he observado durante mi investigación para este trabajo. Uno de ellos es el bajo nivel de penetración del teletrabajo que hay en nuestro país y en muchos otros aún hoy en día.

Dado que existen muchas vías de proporcionarlo, he de reconocer que me sorprende que sea así, por un lado porque en lo que a tecnologías respecta, hemos podido comprobar que el mercado actual cuenta con multitud de proveedores con soluciones aplicables a todos los niveles. Por otro lado, porque garantizar la seguridad resulta sencillo, puesto que este modelo permite aprovechar los mecanismos de seguridad con los que ya se contaba en las organizaciones, ya que básicamente la información y los sistemas permanecen en el centro de datos.

Partiendo de este como diseño posible, y acompañado del auge de las comunicaciones, es previsible y deseable que este modo de trabajo se extienda y se normalice como un estándar en las empresas que puedan adoptarlo. Espero que con el tiempo lo habitual sea esta modalidad y, como incluyo en una de las líneas futuras, no exista diferencia entre teletrabajo y presencialidad, aprovechando la flexibilidad que ofrecen estas tecnologías.

Referencias

1. Comisión Europea: Índice de la Economía y la Sociedad Digitales (DESI), 2020.
2. CCN-CERT. CCN-STIC-105. Catálogo de Productos y Servicios de Seguridad de las TIC. Diciembre 2021.