Arquitecturas de Acceso Remoto Seguro

1. INTRODUCCIÓN

Cada vez más empresas y organizaciones están apostando por implementar políticas de teletrabajo, lo que conlleva la necesidad de desplegar y configurar soluciones de acceso remoto. Dichos sistemas deben permitir a los empleados acceder de forma segura a los recursos empresariales que necesiten para desarrollar su trabajo, desde ubicaciones exteriores a las de la propia organización.

Tradicionalmente, las redes de las organizaciones tenían un perímetro que se correspondía con la ubicación física de dicha organización. Hoy en día, este perímetro es mucho más difuso debido a la necesidad de proporcionar acceso remoto a los trabajadores y al aumento del uso de la nube o *cloud*.

Permitir acceso remoto a los recursos empresariales conlleva riesgos de seguridad inherentes, que deben ser mitigados por las soluciones que se implementen. El objetivo del acceso seguro es proporcionar al usuario una buena experiencia y, a la vez, protección *Zero Trust*. Se trata de facilitar accesos simples y efectivos a la información, aplicaciones y servicios de la organización, sin compromiso de la seguridad. El modelo Zero Trust asume que nada fuera o dentro de la organización es confiable, y que se debe identificar y autenticar a cualquier persona o entidad que intente conectarse, antes de permitir su acceso.

Una solución de acceso remoto seguro debe:

- **Facilitar la movilidad de forma integrada**. La solución debe ser apta para cualquier tipo de dispositivo e independiente de la ubicación del usuario.
- **Proporcionar al usuario una experiencia satisfactoria:** facilidad de uso y eficiencia.
- **Constituir un punto de acceso único.** La solución debe constituir un único punto de acceso a todos los servicios, aplicaciones y recursos que el usuario pueda necesitar, independientemente de donde se encuentren.
- **Proporcionar seguridad** tanto a la información intercambiada con el usuario, como a los recursos accedidos, sin poner en riesgo el resto de los recursos de la red interna. Debe permitir la aplicación de las políticas de seguridad de la organización.

Este documento presenta las principales arquitecturas de acceso remoto que existen en la actualidad. No se entrará en el detalle de su implementación, puesto que este es un aspecto muy ligado a las soluciones de cada fabricante.

2. ESQUEMA GENERAL

A continuación, se incluye un esquema y un diagrama de las arquitecturas que serán abordadas a lo largo del documento.

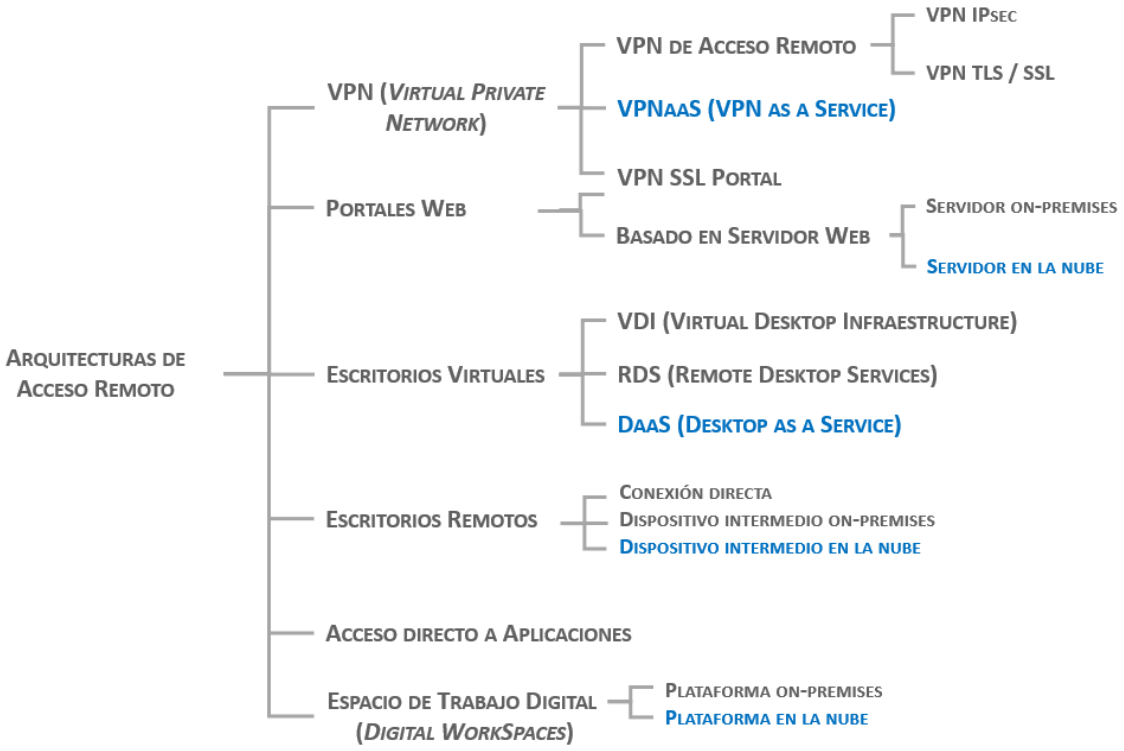

Figura 1. Esquema de las arquitecturas de acceso remoto

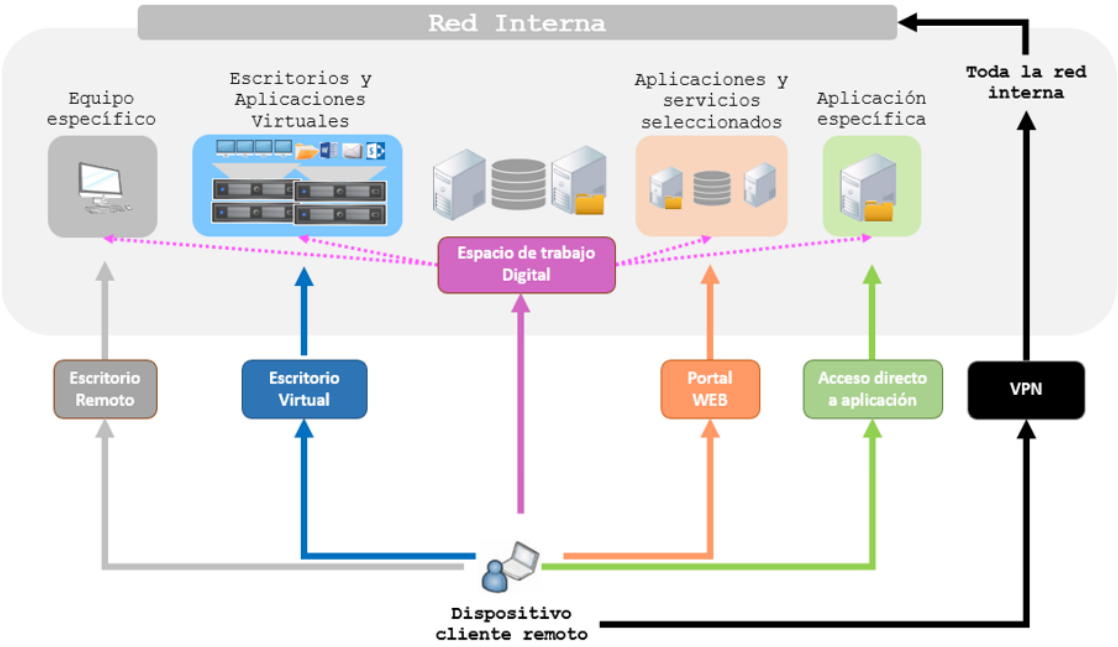

Figura 2. Diagrama de las arquitecturas de acceso remoto

3. VPN

Una Red Privada Virtual (VPN, *Virtual Private Network*) es una tecnología que establece una conexión virtual segura, conocida como "túnel", construida sobre una red física insegura (internet). La VPN proporciona los mecanismos de seguridad para proteger la información transmitida, y para permitir el acceso seguro y controlado a los recursos que protege.

Hay dos (2) tipos de VPN:

- **VPN *site-to-site***: VPN que se utiliza para unir redes mediante una conexión segura. Suele emplearse para conectar las redes de oficinas secundarias con una sede central.
- **VPN de acceso remoto**: VPN que se utiliza para conectar un dispositivo cliente remoto con la red de la organización. Es la empleada para permitir acceso seguro a los usuarios que trabajan de forma remota, a través de la infraestructura proporcionada por una red pública.

Las VPN utilizan protocolos de seguridad criptográficos (*tunneling protocols*) que son los que protegen la información transmitida. Los más extendidos son **TLS (*Transport Layer Security Protocol*)**[1] e **IPsec (*Internet Protocol Security*)**. Ambos proporcionan los siguientes servicios de seguridad:

- Protección de la **confidencialidad** mediante el uso de algoritmos de cifrado simétrico. Las claves para este cifrado se generan utilizando métodos de intercambio de claves (*Key Exchange*).
- Protección de la **integridad y autenticidad** mediante el uso de valores MAC (*Message Authentication Code*).
- **Autenticación** mediante el uso de certificados de clave pública X.509v3.
- **Protección anti-reenvíos**, mediante números de secuencia añadidos al mensaje.
- ***Forward Secrecy***[2] (secreto hacia adelante).
- **Control de sesión.**

Además, las herramientas o dispositivos que proporcionan la infraestructura VPN suelen añadir otros servicios adicionales de seguridad como:

- **Evaluación del estado de seguridad del dispositivo cliente (*Host Check*)**. Se comprueban las herramientas de protección de las que dispone el dispositivo, como un *software* antivirus actualizado, *firewalls*, y parches de seguridad. En función de los resultados de la comprobación, se puede permitir o denegar el acceso a la red interna, a cierta categoría de recursos o a recursos individuales.
- **Control de acceso granular** basándose en factores como la pertenencia a un grupo de usuarios, la dirección IP origen, los atributos del certificado cliente presentado, o el estado de seguridad del dispositivo cliente.

[1] También conocido como SSL, la versión antigua de TLS.
[2] Propiedad que asegura que, si la clave se descubre en un momento dado, no podrá ser usada para descifrar ninguno de los datos trasmitidos anteriormente.

- **Características de *proxy*** haciendo de intermediario entre la red pública y los recursos de la red interna.
- **Integración con otros elementos de seguridad corporativos,** a los que puede enviar información sobre el tráfico, el usuario, el dispositivo y la actividad que está realizando.

La infraestructura VPN de acceso remoto está normalmente formada por dos (2) elementos principales:

- **El servidor o *gateway* VPN**. Es el elemento básico en la infraestructura VPN encargado de establecer las conexiones seguras (túnel VPN) con los dispositivos de usuario.
- **El cliente VPN.** Es el *software* que debe instalarse en los dispositivos de usuario para poder establecer la conexión segura con el servidor VPN.

Las VPN de acceso remoto, tanto las VPN IPsec como las VPN SSL (TLS), establecen un túnel VPN que proporciona **conectividad de capa 3 completa a la red interna**. A este modo de despliegue se le llama "***VPN Tunneling***" y permite al usuario disponer del mismo nivel de acceso a la red corporativa, como si estuviese *in situ* en la oficina.

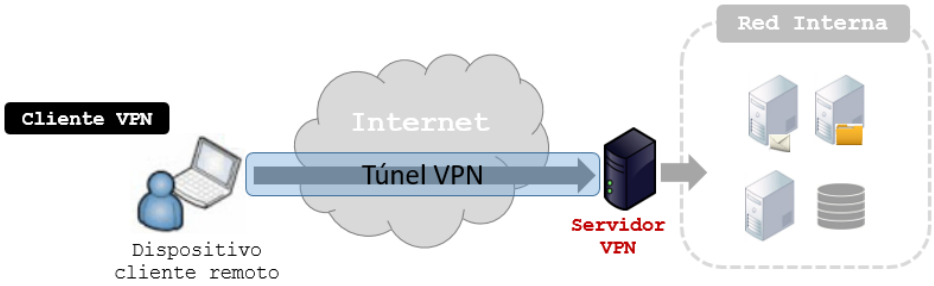

Figura 3. VPN de acceso remoto tipo túnel

Las VPN SSL tienen otro modo de despliegue llamado "***VPN SSL Portal***", que únicamente permite el acceso a aplicaciones y servicios determinados. Este modo levanta un Portal Web en el servidor VPN, que actuará como un *proxy* inverso al que el usuario se conecta y que le permite solo acceder al conjunto de aplicaciones y recursos para los que esté autorizado. En este caso, no es necesario un *software* cliente VPN ya que el usuario se conecta a través de un navegador o *web browser*. Normalmente permite acceder a aplicaciones basadas en web, servidores de ficheros u otras aplicaciones cliente/servidor como *Microsoft Outlook, Lotus Notes, Citrix XenApp*, etc.

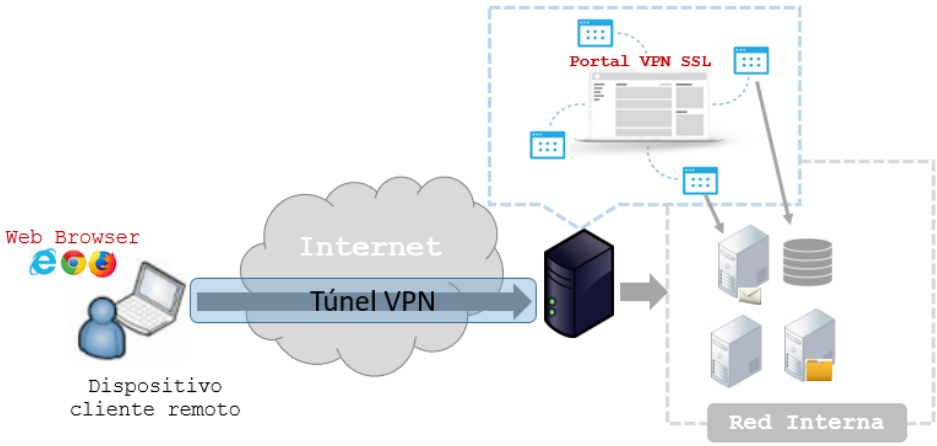

Figura 4. VPN de acceso remoto tipo portal

El *software* de cliente VPN permite varios modos de funcionamiento:

- *Túnel iniciado por el usuario*: es el usuario quien inicia el túnel cada vez que necesite acceder a los recursos internos de la organización.
- *Túnel permanente:* cuando el equipo arranca, automáticamente se establece la conexión VPN que el usuario no puede desactivar de forma manual. Todo el tráfico del dispositivo va a través del túnel VPN.
- *VPN con túnel dividido (split tunneling)*: permite que el tráfico dirigido al dominio corporativo pase por el túnel VPN, mientras que todo lo demás va por fuera del túnel y directamente a Internet.

Las opciones de *Túnel iniciado por el usuario* y *VPN con túnel dividido* se desaconsejan para escenarios de teletrabajo en los que no sea posible realizar un control de bastionado del equipo o se conecte a Internet desde una infraestructura de terceros no controlada.

El servidor VPN puede ser un equipo físico dedicado o ***appliance***, o puede ser un servicio dentro de otros dispositivos existentes en la infraestructura de la organización. Cada tipo de implementación tiene sus ventajas e inconvenientes. A continuación, se muestra una tabla con los puntos fuertes de cada una.

Appliance	En otro dispositivo de la infraestructura
Seguridad Un *appliance* dedicado cuya única función es la de administrar las conexiones VPN es, sin duda, la opción más segura. Si el dispositivo realiza más funciones que las de VPN, la probabilidad de que existan vulnerabilidades que puedan ser explotadas por un atacante aumenta.	**Escalabilidad** Se refiere a la capacidad de expandir la VPN para añadir más conexiones remotas, usuarios o equipos. En el caso de los *appliance* dedicados, la escalabilidad dependerá del equipo físico y sus características. En el caso de utilizar otros dispositivos de la infraestructura, no será complicado aumentar los recursos del equipo (agregar procesadores, memoria, etc.).

Appliance	En otro dispositivo de la infraestructura
Rendimiento La ejecución de las funciones VPN tiene un elevado consumo de recursos debido, principalmente, a las actividades de cifrado y descifrado de datos. En el caso de un *appliance* dedicado, éste estará dimensionado adecuadamente.	**Coste** En general los *appliance* dedicados son más costosos. Además del coste inicial de adquisición y despliegue de la solución, existen muchos factores que influyen en el coste final. Por ejemplo, la escalabilidad es un aspecto que tiene gran impacto en el coste, ya que, si la solución seleccionada no resulta escalable, el coste se elevará de forma muy acusada cuando la VPN supere su capacidad.
Capacidades de control En el caso de utilizar dispositivos de la infraestructura, se pierden capacidades de control relacionadas con el equipo físico o el *software* de base.	**Operación y mantenimiento** Aunque existen tareas comunes, los *appliance* dedicados requieren más actividades de mantenimiento. Hay que tener en cuenta que se añaden nuevos equipos a la infraestructura *hardware* de la organización. Además, son equipos muy específicos, que pueden incluso tener su propio sistema operativo, por lo que las tareas de operación se dificultan.

Tabla 1. Ventajas de servidor VPN en *appliance* vs en otro dispositivo de la infraestructura

En la actualidad, es habitual que el servidor VPN forme parte de las capacidades de los cortafuegos de nueva generación (NGFW, *Next Generation Firewalls*). Los **NGFW** son cortafuegos que han evolucionado incorporando muchas otras funcionalidades de seguridad como *Anti-malware*, IPS y VPN. Al tener el servidor VPN integrado, el cortafuegos puede realizar un análisis exhaustivo del tráfico para detectar y minimizar riesgos, problemas de seguridad, actividades sospechosas o fugas de datos. Esto otorga a la organización la visibilidad completa del tráfico, las aplicaciones, los puertos y los protocolos de red, sin ángulos muertos en el tráfico de los trabajadores remotos.

Existen múltiples productos VPN propiedad de fabricantes, y existen otras soluciones de código abierto (*open source*) gratuitas o de coste muy bajo. Un ejemplo de producto de código abierto es OpenVPN, con licencia GPL (*General Public License*) para la implantación de VPNs basadas en SSL/TLS.

No obstante, en aquellos sistemas bajo el alcance del ENS o que manejan Información Clasificada deberán emplearse productos cualificados para el ENS o productos aprobados para el manejo de Información Clasificada. Estos productos se encuentran en el Catálogo de Productos y Servicios STIC (CPSTIC).

3.1. VPN CLOUD / VPNaaS

La VPN de acceso remoto es, por lo tanto, un método seguro, tradicional y, relativamente sencillo, de proporcionar al usuario remoto acceso a los datos, aplicaciones y servicios alojados en el centro de datos de la organización.

El problema se plantea cuando el usuario no solo requiere acceso a esos recursos, sino también a otros que se encuentran fuera de la red corporativa, como es el caso de aplicaciones y recursos en

la nube. Para acceder a este tipo de recursos, la arquitectura de VPN tradicional de acceso remoto no resulta eficiente.

Al usar la arquitectura tradicional de VPN, el tráfico del usuario hacia un servicio que es accesible desde internet, sigue un recorrido muy ineficiente: **(1)** la petición va del usuario al Servidor VPN de la sede, **(2)** de ahí sale por el cortafuegos perimetral hacia internet y la aplicación en la nube, **(3)** la respuesta de la nube llega al cortafuegos que la redirige al servidor VPN, y **(4)** del servidor VPN al usuario.

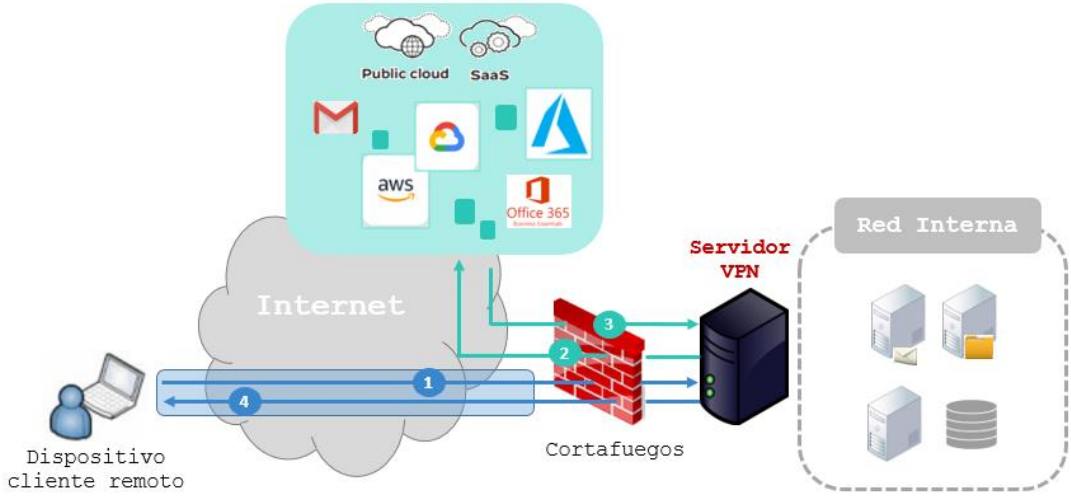

Figura 5. Acceso a servicios en la nube con una VPN de acceso remoto tradicional.

Esta ineficiencia habitualmente hace que el usuario, tras una experiencia poco satisfactoria, no utilice la conexión VPN más que cuando tenga que conectarse a la red interna, y deje de utilizarla cuando deba conectarse a recursos en internet. Cuando esto ocurre, la organización pierde visibilidad sobre el uso de aplicaciones y servicios por parte de los usuarios, además de no poder aplicar a este tráfico las políticas de seguridad corporativas.

Por ello, han surgido las soluciones de VPN en la nube (*VPN Cloud*), también llamadas *Hosted VPN* o *VPN as a service (**VPNaaS**)*. Este es un nuevo tipo de tecnología VPN especialmente diseñada para entornos *cloud*.

VPNaaS se utiliza, no solo para proporcionar al usuario remoto una conexión segura VPN con los servicios en la nube o recursos en internet, sino también para establecer conexiones seguras VPN entre redes corporativas y proveedores de la nube, o conexiones *cloud to cloud*. En la actualidad, estas soluciones han evolucionado y también ofrecen conexión VPN a los recursos de la red interna corporativa (*on-premise*).

VPNaaS proporciona al usuario remoto, por tanto, un punto único de acceso seguro VPN ya sea al centro de datos, a Internet o a las aplicaciones alojadas en los entornos de nube pública, privada e híbrida. Además, da visibilidad de todo el tráfico a la organización, permitiendo inspeccionar de forma exhaustiva el tráfico registrado en todos los puertos y protocolos.

Este tipo de soluciones normalmente utiliza un *software* cliente en el *endpoint* del usuario que se conecta a la solución *VPNaaS* de forma automática en cuanto detecta que el *endpoint* tiene conexión

a internet, sin intervención del usuario. Para la conexión con los servicios y recursos del centro de datos de la organización, puede requerir de algún tipo de conector, dependiendo de la solución.

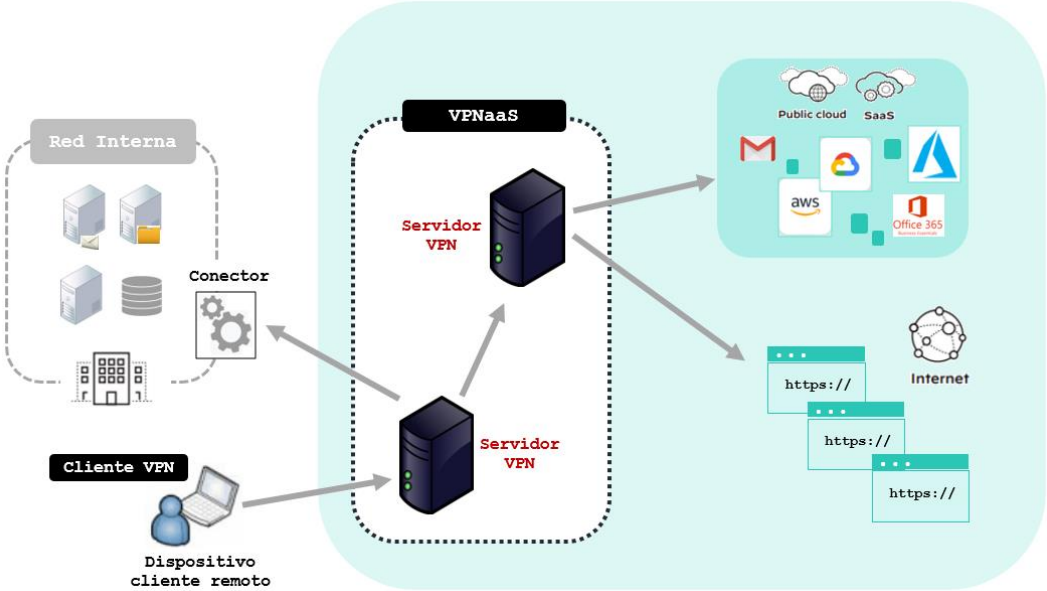

Figura 6. *VPNaaS*

Aunque la solución basada en VPNaaS mejora las prestaciones del servicio, tiene la contrapartida de que todo el tráfico y la información de la organización es procesada por un sistema de información perteneciente al proveedor del servicio cloud (CSP[3]), ajeno a la organización, por lo que deberá valorarse, caso por caso, la idoneidad del uso de dicha solución.

4. PORTALES WEB

Cuando las necesidades del usuario remoto no requieren el acceso a todos los recursos de la red interna de la organización, sino a un conjunto determinado de aplicaciones o servicios, se pueden usar los **Portales Web**.

Estas soluciones ofrecen una interfaz web centralizada que proporciona acceso a un conjunto específico de servicios y contenidos como, por ejemplo, acceso al correo electrónico, noticias y comunicaciones internas, formación, información sobre los empleados, directorios, carpetas compartidas, etc. Para proporcionar acceso a estos recursos, el portal web ejecuta una serie de aplicaciones cliente que establecen las conexiones con los servidores, bases de datos y repositorios internos de la organización. De este modo, el portal hace la función de capa de presentación ante los usuarios.

Las aplicaciones y servicios accesibles desde el portal, deben estar basados en Web (*Web-based*) o poder ser accedidos mediante interfaz Web. Para aplicaciones no basadas en Web, será necesario que el servidor disponga de funciones de conversión de un protocolo a otro.

Los componentes básicos de esta solución son:

a) **Servidor que implementa el portal**.

[3] *Cloud Service Provider*

b) **Aplicaciones cliente instaladas en este servidor**, que acceden a los servicios y recursos de la red interna.

c) No se requiere ningún software cliente para que el usuario acceda al portal. Normalmente se usa un navegador (*web browser*).

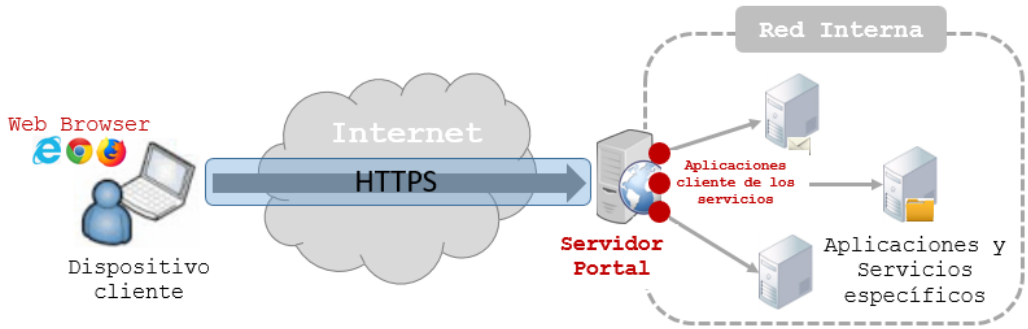

Figura 7. Arquitectura general de los Portales Web.

El dispositivo que implementa el portal normalmente es un **servidor Web HTTPS**, aunque también puede ser implementado por un **servidor VPN SSL**, tal y como se ha comentado en el apartado anterior relativo a las VPN. Este servidor VPN levanta un portal web al que el usuario accederá a través de un navegador.

El servidor o dispositivo que implementa el portal web es el que proporciona los servicios de seguridad a este tipo de solución:

- **Realiza funciones de *proxy* inverso**. Esto significa que no se establece conexión directa entre el cliente y los recursos internos. Es el *proxy* quien establece ambas conexiones, por un lado, con el dispositivo cliente (recibe sus peticiones de información) y, por otro lado, con las aplicaciones, solicitando la información y enviándosela posteriormente al cliente.
- **Proporciona protección a la comunicación con el dispositivo cliente**, utilizando servicios de cifrado, integridad y autenticación, entre otros. Generalmente para ello, se utiliza el protocolo HTTPS/TLS.
- Añade otras características de seguridad a la implementación, como el **control de acceso** y la **autenticación**, pudiendo usar certificados, contraseñas o a través de servidores de autenticación. En algunos casos, también pueden revisar la postura de seguridad de los dispositivos cliente utilizando *plug-in* del navegador o a través del cliente VPN en el caso del Portal VPN SSL.
- **Impide el almacenamiento de información sensible en el dispositivo cliente** ya que, aunque puede configurarse de otra forma, por defecto, el portal web está configurado para no permitir al usuario descargar información y almacenarla en su dispositivo.

Los servidores del portal web pueden estar alojados en las instalaciones de la organización (*on-premise*) o en la nube.

En el caso de alojar el servidor del portal *on-premise*, **deberá ubicarse en una DMZ** desde la que tendrá acceso a la red interna de la organización. De esta forma, podrá comunicarse con los recursos

que sea necesario y ofrecer los diferentes servicios disponibles a través del portal web, a la vez que protege al resto de recursos de la red interna.

En el caso de que el servidor del portal esté alojado en una infraestructura en la nube, para poder acceder a los diferentes recursos internos de la organización, se deberá establecer una conexión segura con la red interna de la organización, para lo que se utilizará un conector.

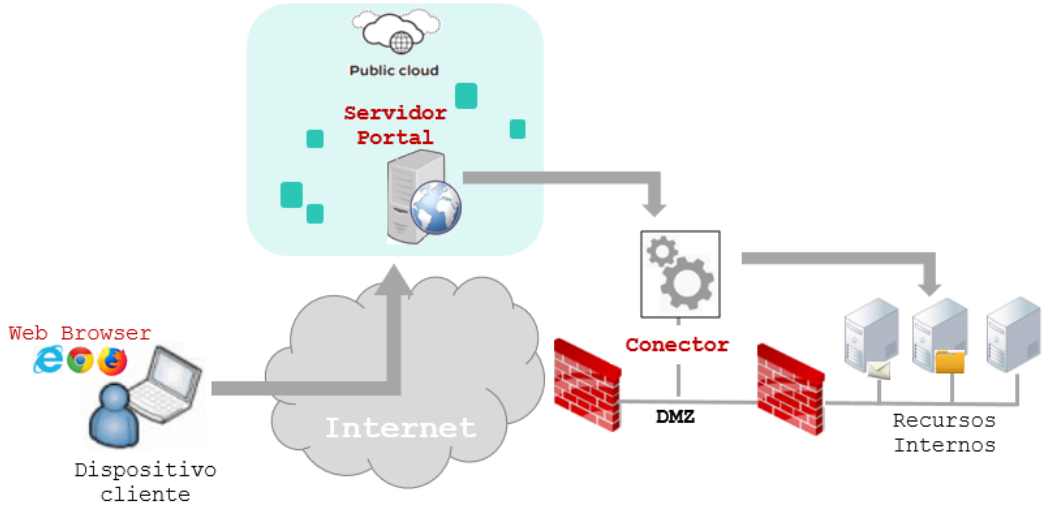

Figura 8. Portal Web alojado en la nube.

5. ACCESO DIRECTO A APLICACIONES

Cuando el usuario solo necesita acceder a un conjunto muy reducido de aplicaciones, se puede implementar un acceso directo desde el exterior a la aplicación en concreto.

Uno de los ejemplos más comunes de este tipo de implementación es el correo web (*webmail*). El usuario abre un navegador y se conecta a un servidor web que proporciona el acceso al correo electrónico. Este servidor web utiliza HTTPS, de forma que la comunicación con el dispositivo cliente está protegida con TLS. La aplicación de *webmail* en el servidor autentica al usuario antes de permitirle acceso a sus buzones de correo.

En este caso, es la aplicación la que proporciona todas las medidas de seguridad necesarias, como la protección de las comunicaciones con el dispositivo cliente, la autenticación, el control de acceso, etc. Para el acceso, el dispositivo cliente puede necesitar un *software* cliente, aunque normalmente se usa el navegador ya que suelen ser aplicaciones basadas en web.

Esta opción es recomendable solo si los servidores de la aplicación a la que se accede están localizados en el perímetro de red de la organización (DMZ), y no en la red interna. Estos servidores, directamente accesibles desde internet, deben ser bastionados adecuadamente para reducir la posibilidad de compromiso.

En general, esta opción se utiliza para aplicaciones que son ampliamente usadas por los usuarios y concebidas para ser accesibles desde cualquier ubicación, como el correo electrónico. Otras aplicaciones más sensibles deben ser accedidas usando otros métodos más seguros como el túnel VPN o los portales web.

6. ESCRITORIO VIRTUAL

Los **escritorios virtuales**[4] son una opción que permite a los usuarios el acceso remoto a un entorno de escritorio completo con las aplicaciones y recursos que necesitan.

La tecnología de escritorio virtual se basa en que los recursos *hardware* y *software* que soportan y ejecutan los escritorios virtuales se encuentran en servidores en el centro de datos de la organización. El usuario accederá desde su dispositivo cliente a estos servidores, los cuales le asignan un recurso de escritorio, y le envían su información gráfica y multimedia.

El procesamiento se produce, por lo tanto, en los servidores. El almacenamiento de datos se produce en los servidores remotos, de forma que el cliente no almacena ningún dato sensible en su dispositivo. De esta forma, el dispositivo cliente no requiere de capacidades de procesamiento ni almacenamiento, por lo que se utilizan dispositivos muy sencillos con los recursos necesarios para establecer la conexión. Se denominan ***Thin Clients*** (clientes ligeros) y tienen recursos mínimos de almacenamiento, memoria, procesamiento y sistema operativo. Otro tipo de clientes aún más ligeros son los ***Zero Clients***, que no llegan a tener ni sistema operativo, y utilizan un *firmware* específico para poder establecer la conexión.

Las tecnologías de escritorio virtual también proporcionan acceso a aplicaciones *software* sin necesidad del entorno de escritorio completo. De esta forma, a través de las tecnologías de escritorio virtual, los usuarios pueden hacer uso de aquellas aplicaciones que necesitan para completar sus tareas.

Existen muchas tecnologías de escritorio virtual. Las más extendidas son VDI (*Virtual Desktop Infraestructure*) y RDS (*Remote Desktop Services*).

6.1. VDI (VIRTUAL DESKTOP INFRAESTRUCTURE)

VDI es una tecnología que utiliza Máquinas Virtuales (MV) *host-based,* es decir, alojadas en un servidor centralizado en el centro de datos (*data center*). Estas MV son las que llevan a cabo la provisión y gestión de escritorios virtuales (*Virtual Desktops*) a los usuarios. Estos podrán acceder al escritorio virtual desde cualquier localización o dispositivo y todo el procesamiento se realiza en el servidor central. La imagen del escritorio virtual viaja a través de la red hasta el equipo del usuario, desde el que este puede interactuar con el escritorio, las aplicaciones y el sistema operativo subyacente, como si fuesen locales.

Las características generales de una infraestructura VDI son las siguientes:

- Los escritorios virtuales se encuentran dentro de las MV alojadas en un servidor centralizado en el centro de datos.
- Cada escritorio virtual incluye una imagen de un sistema operativo de usuario.
- Las MV son creadas, ejecutadas y gestionadas por un hipervisor instalado en el servidor VDI. Estas MV encapsulan los escritorios virtuales.

[4] Escritorio virtual no es lo mismo que virtualización de escritorio (*Desktop Virtualization*). La virtualización de escritorio es la ejecución de una Máquina Virtual invitada (*guest VM*) en nuestro equipo, normalmente para poder disponer de dos (2) sistemas operativos: el del ordenador y el de la máquina virtual.

- Un componente de la implementación (*Gateway, Controlador o Connection broker*), asignará a cada cliente un escritorio virtual dentro del *pool* de recursos al que el cliente podrá conectarse tras la correcta autenticación en el entorno VDI.
- Los usuarios deben estar conectados de forma permanente al servidor central para mantener el acceso a los escritorios virtuales que aloja.

VDI puede ser persistente o no persistente:

- **VDI persistente**. El usuario se conecta al mismo escritorio siempre y puede personalizarlo y adaptarlo a sus necesidades, ya que los cambios se guardan una vez la conexión termina. Los escritorios en un entorno VDI persistente actúan exactamente como el escritorio personal físico.
- **VDI no persistente**. Los usuarios se conectan a escritorios genéricos y los cambios no permanecen una vez finaliza la sesión. Es más sencillo y más barato, ya que no es necesario mantener escritorios personalizados entre sesiones. Este entorno es apropiado para organizaciones con trabajadores que realizan tareas limitadas y repetitivas y no requieren de un entorno personalizado.

Existen muchas soluciones VDI, cada una de ellas con su propia arquitectura. En general, hay tres (3) componentes principales: la capa de recursos, la capa de control y el protocolo de presentación.

A continuación, se incluye un diagrama de la arquitectura general de la tecnología VDI.

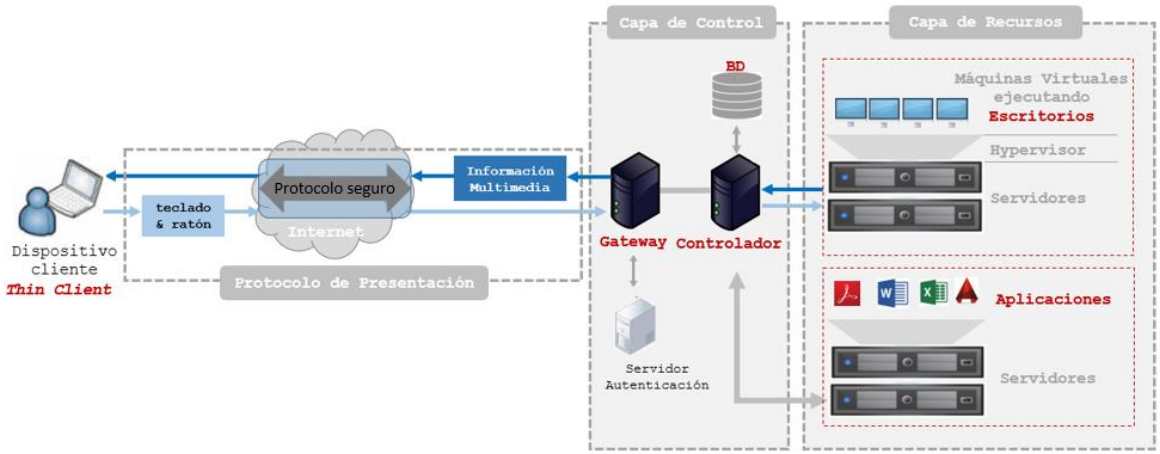

Figura 9. Arquitectura genérica VDI

- **Capa de recursos**

La capa de recursos la forman todos los componentes, *hardware* y *software*, que alojan los escritorios y aplicaciones virtuales accesibles de forma remota. Estos componentes incluyen servidores, hipervisores y recursos de almacenamiento, así como otros recursos que las diferentes aplicaciones necesiten para su funcionamiento, como pueden ser servidores de archivos y repositorios.

La capa de recursos está gestionada en todo momento por la capa de control, que suministra de forma dinámica los recursos necesarios para ofrecer el servicio a los usuarios finales. En caso de que ambas capas estén físicamente separadas, la conexión se llevará a cabo mediante un conector que encapsule el tráfico de forma segura entre la capa de recursos y la capa de control.

- **Capa de control**

La capa de control es la encargada de gestionar los recursos (escritorios y aplicaciones) y distribuirlos a los usuarios. Sus funciones principales son las siguientes:

- Autenticar a los usuarios y gestionar sus permisos de acceso a los recursos. Para ello, puede conectarse a servidores de autenticación.
- Conectar cada usuario con una de las MV de acuerdo con unas políticas predefinidas u otros criterios establecidos por el administrador.
- Monitorizar el estado de conexión de las MV y gestionar su reasignación una vez finaliza la sesión del usuario actualmente conectado. También actúa como gestor de *failover*, es decir, asigna al usuario un nuevo recurso en caso de fallo del recurso al que está conectado.
- Gestionar los protocolos de presentación.
- Almacenar información sobre los usuarios y las conexiones establecidas.
- Gestionar el estado de los recursos.

Los componentes de la capa de control varían en función del fabricante y de las soluciones concretas. Algunos componentes habituales son los siguientes:

- Un componente *gateway*, encargado de gestionar las peticiones de conexión de los usuarios, autenticar a los mismos y establecer las conexiones entre los usuarios y los recursos.
- Un componente de gestión, habitualmente denominado controlador, encargado de distribuir y gestionar los recursos.
- Bases de datos que contengan información sobre usuarios y licencias, entre otros.

En algunas soluciones, la función del *gateway* y controlador la realiza un único componente llamado "*Broker de conexión*" o ***Connection Broker***.

- **Protocolo de presentación**

El protocolo de presentación se encarga de transmitir toda la información necesaria para que el usuario pueda interactuar con el escritorio o aplicación remota. Estos protocolos transportarán fundamentalmente información multimedia, así como todos los movimientos de ratón y pulsaciones de teclado que el usuario remoto lleve a cabo. También envían información de señalización para el correcto establecimiento de la sesión.

Algunos de los protocolos más extendidos son los siguientes: *RDP (Microsoft), ICA (Citrix), VNC (de código abierto)* y *PCoIP (VMWare).*

El enlace entre el usuario remoto y el *gateway* se lleva a cabo sobre internet, por lo que es necesario dotar de confidencialidad e integridad a los datos transportados. Existen varias opciones, una opción bastante habitual es el uso de SSL/TLS para transportar de forma segura los paquetes de los protocolos de presentación mencionados con anterioridad, normalmente a través de una *VPN SSL Portal*, que permite el acceso al escritorio virtual.

6.2. RDS (*REMOTE DESKTOP SERVICES*)

Remote Desktop Services, RDS, es una tecnología de *Microsoft*. Se conoce también como RDSH (*Remote Desktop Session Host*) y anteriormente se conocía como *Terminal Services*.

Con RDS los usuarios acceden de forma remota a escritorios y a aplicaciones Windows centralizadas en un servidor con sistema operativo de *Microsoft Windows Server*. Los recursos del servidor se dividen entre todos los usuarios que dispongan de una sesión activa. A todos los usuarios se les presenta el mismo escritorio virtual, que se sirve a través del protocolo de escritorio remoto de *Microsoft* (RDP, *Remote Desktop Protocol*).

Desde una perspectiva de usuario, VDI y RDS son idénticos. La diferencia es que VDI se basa en una infraestructura de máquinas virtuales que implementan un sistema operativo. Sin embargo, RDS se basa en sesiones de usuarios concurrentes en un mismo sistema operativo de servidor. Con RDS el aislamiento es a nivel de sesión y todos los usuarios comparten el sistema operativo y los recursos del servidor. Con VDI cada usuario se conecta a una instancia de sistema operativo separada, por lo que el aislamiento es a nivel de sistema operativo.

La diferencia de coste es también notoria, ya que una sola instancia de *Windows Server* proporciona el entorno virtual a tantos usuarios simultáneos como soporte el *hardware* del servidor. Sin embargo, en VDI hace falta una instancia (y licencia) por cada usuario. Por otro lado, no todas las aplicaciones que el usuario necesite pueden ejecutarse en un Windows Server.

Los principales componentes de RDS se muestran en el siguiente diagrama.

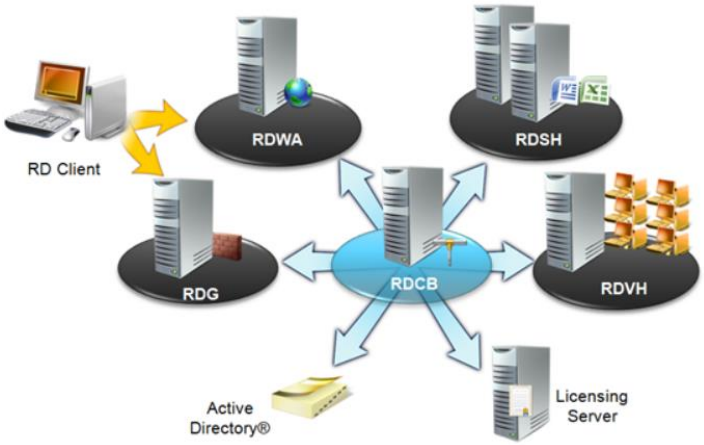

Figura 10. Arquitectura RDS

Este diagrama, así como la descripción detallada del funcionamiento de cada uno de los componentes de la solución RDS de *Microsoft*, se puede encontrar en la web de documentación de *Microsoft*[5].

6.3. VDI CLOUD / DAAS

La solución VDI puede tener la capa de control y la capa de recursos alojadas en el centro de datos de la organización (*on-premise*) o también pueden alojarse en la nube.

Se denomina **VDI Híbrido** cuando solo la capa de control está en la nube y los recursos se encuentran *on-premise*. En este caso, es necesario instalar un componente denominado **conector** en las instalaciones donde se ubiquen los recursos para que puedan comunicarse con la capa de control en la nube. Dicho componente se ejecuta en una máquina independiente, y su función es establecer

[5] https://docs.microsoft.com/es-es/archive/blogs/latam/arquitectura-de-remote-desktop-services-rds-y-sus-roles-principales

una conexión segura con la capa de control, para llevar a cabo las funciones de gestión y control de los recursos.

En este tipo de arquitecturas, los usuarios remotos establecen una conexión con un *gateway* ubicado en la nube. Tras la asignación de recursos al usuario remoto por parte de la capa de control, el *gateway* establece una conexión segura con dichos recursos, ubicados *on-premise,* haciendo pasar el tráfico a través de él.

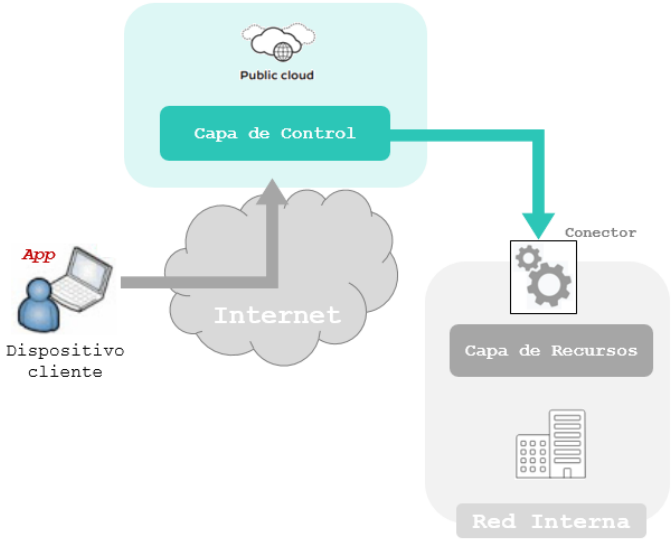

Figura 11. VDI Híbrido.

DaaS (*Desktop as a Service*) es la tecnología VDI alojada en la nube al completo, tanto la capa de control como la capa de recursos. En caso de que la solución deba acceder a alguna aplicación o recurso *on-premise*, también hará uso de un conector.

DaaS es un modelo de escritorio virtual bajo demanda que los usuarios consumen directamente en sus dispositivos fijos y móviles sin importar el sistema operativo, la ubicación o el tipo de red de acceso. Es suficiente con instalar una app para poder acceder a los escritorios virtuales corporativos que se hayan definido según la política. Es un modelo de pago por uso que se fija según los despliegues realizados y los usuarios concurrentes.

El uso de esta arquitectura permite a la organización asumir una menor carga de administración TI, al delegar la gestión de la infraestructura VDI en un servicio en la nube. Además, posibilita el acceso de los usuarios remotos al servicio a través de diferentes POPs (*Point-of-Presence*) en la nube, en función de su ubicación geográfica.

7. ESCRITORIO REMOTO

La tecnología de Escritorio Remoto (*Remote Desktop*) permite al usuario controlar de forma remota un equipo de la organización, normalmente el suyo. El usuario tiene el control del teclado y el ratón del ordenador remoto y ve su pantalla en el dispositivo cliente. El escritorio remoto permite al usuario acceder a todas las aplicaciones, datos y otros recursos que normalmente están disponibles desde su equipo en la oficina.

En general, en el dispositivo cliente se instala un *software* cliente o un *plug-in,* para acceder al equipo remoto dentro de la red interna de la organización.

Figura 12. Escritorio Remoto

El escritorio remoto se utiliza para labores de mantenimiento, donde es necesario conectarse a una máquina remota para solucionar cualquier tipo de problema que pueda tener, o bien para hacer uso de algún *software* específico que únicamente esté instalado en un determinado equipo dedicado. No se recomienda utilizar para el trabajo en remoto de usuarios, ya que hay opciones mucho más seguras y controladas.

Estas tecnologías también utilizan un protocolo de presentación, como VDI, para la entrega de la información multimedia y la transmisión de órdenes de teclado y ratón. El Escritorio Remoto de *Microsoft* utiliza RDP (*Remote Desktop Protocol*).

Los únicos requisitos que hacen falta para un escritorio remoto son:

- **Conexión a Internet**, necesaria para establecer la conexión remotamente con la otra máquina.
- **Habilitar la opción de escritorio remoto en los dos equipos.** Si el equipo destino no tiene habilitada la opción que permita la conexión remota, no se podrá llevar a cabo.
- **Tener permiso para llevar a cabo la conexión.** Si se trata del usuario administrador lo tendrá por defecto. Si no fuera así, habría que indicar qué usuarios podrán llevar a cabo la conexión remota.
- **El equipo remoto deberá estar siempre encendido.** Tampoco puede estar en modo hibernación ni suspensión. Si entra en estos estados, no sé podrá realizar la conexión.

Las soluciones de escritorio remoto se encargan de proteger la comunicación con el dispositivo cliente y de la autenticación para asegurar que ningún usuario no autorizado se conecta al equipo remoto. No obstante, esto implica un cifrado extremo a extremo, por lo que el contenido de la comunicación no podrá ser analizado por los dispositivos de control del perímetro, como cortafuegos o IDS.

Es recomendable utilizar algún **dispositivo intermediario**, que implemente una autenticación más robusta y proporcione la seguridad a la comunicación entre la máquina remota y el dispositivo cliente, por ejemplo, a través de protocolos seguros como TLS o IPsec.

Estos dispositivos intermediarios pueden ser proporcionados por la organización, o por un proveedor *cloud*, que actúa como agente (*broker*) para establecer la conexión entre el dispositivo cliente y el equipo al que se quiere acceder. Una vez establecida la conexión, la sesión continúa entre los dos *endpoints* transmitiendo los paquetes directamente.

Cada equipo de la organización que deba ser accedido de forma remota ha de ser bastionado de forma apropiada, tal y como se hace con cualquier servidor expuesto a Internet. Aun así, este tipo

de soluciones conlleva muchos riesgos. Por ello, se recomienda evitar este tipo de acceso remoto siempre que sea posible.

8. ESPACIO DE TRABAJO DIGITAL (*DIGITAL WORSPACES*)

Un espacio de trabajo digital (*Digital Workspace*) es un marco de trabajo o *framework*, que integra varias tecnologías para entregar a los usuarios aplicaciones, datos y escritorios virtuales de forma unificada en un **único espacio de trabajo**. Permite a los empleados acceder a sus aplicaciones y datos en cualquier dispositivo y desde cualquier lugar.

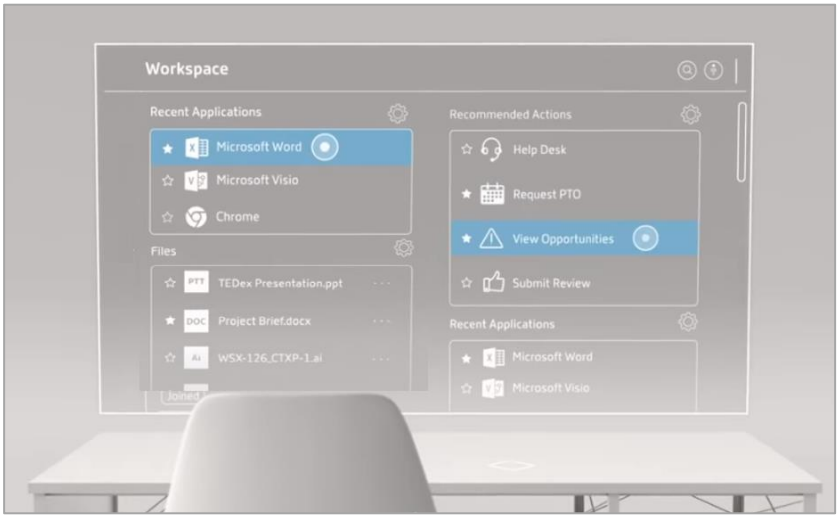

Figura 12. Interfaz de usuario de un *Digital Workspace*

Un espacio de trabajo digital combina varias tecnologías de las vistas hasta ahora (portal web, VDI, etc.), para proporcionar lo siguiente:

- **Punto único de acceso**, ya que todo lo que los usuarios necesitan para su trabajo está contenido en un único interfaz, independientemente de si los recursos a los que se acceden están *on-premise* o en la nube.
- **Compartición de ficheros y contenidos** de forma colaborativa entre los empleados.
- **Virtualización de escritorios y aplicaciones**.
- **Autenticación y *Single-Sign-On* (SSO)**. Los usuarios solo se registran una vez y pueden acceder a todo lo que necesitan. El usuario obtiene una buena experiencia y el entorno permanece seguro.
- **Análisis de Seguridad**. Además de usar mecanismos para proteger las comunicaciones con los usuarios y para autenticación robusta, el espacio de trabajo analiza el patrón de cómo el usuario habitualmente interactúa con los datos y aplicaciones. Esto ayuda a detectar amenazas internas o externas de forma preventiva, antes de que se produzca algún incidente de seguridad.
- **Gestión centralizada de los terminales de usuario**. Los equipos TI tienen un control centralizado sobre cada dispositivo utilizado para acceder al espacio de trabajo, lo que permite a los usuarios trabajar de forma segura en los dispositivos de los que dispongan. Permite desplegar configuraciones automatizadas, y aplicar políticas, parches y actualizaciones sobre los dispositivos.

- **Inteligencia**, al incorporar machine *learning* y *microapps* que permiten un aprendizaje automático sobre la actividad del usuario para crear flujos de trabajo guiados y automatizados.

El espacio de trabajo digital se implementa a través de una plataforma de tecnologías combinadas que puede encontrarse *on-premise* o puede ser proporcionada por un proveedor en la nube. Al igual que las arquitecturas de escritorio virtual, constan de una capa de control que gestiona un número determinado de recursos. Estos recursos pueden estar compuestos por aplicaciones en la nube (SaaS) y también por aplicaciones, datos y servicios *on-premise*. Para que el proveedor del espacio de trabajo digital pueda conectarse a estos recursos internos, deberá emplear un conector instalado en la red interna, similar al indicado en otras soluciones.

9. VENTAJAS E INCONVENIENTES DE LAS ARQUITECTURAS DE ACCESO REMOTO

A continuación, se muestran las principales ventajas e inconvenientes de las arquitecturas de acceso remoto descritas en este documento.

VPN de Acceso Remoto	
Ventajas	**Inconvenientes**
▪ Permite acceso total a la red interna de la organización, como si estuviese físicamente en la oficina. Aunque el servidor VPN puede restringir el acceso a segmentos de red o a servidores particulares. ▪ Es una solución, en general, no muy costosa, ya que los usuarios pueden mantener su dispositivo y únicamente es necesario el despliegue del servidor VPN, que puede realizarse dentro de uno de los dispositivos de red ya existentes (típicamente en unos cortafuegos). ▪ El servidor VPN proporciona la protección del tráfico con el dispositivo cliente, mediante el túnel VPN. ▪ El servidor VPN proporciona una autenticación robusta (MFA) y un control de acceso granular. ▪ El *software* cliente permite un chequeo de la postura de seguridad del dispositivo cliente.	▪ El despliegue y mantenimiento es más complejo que otras soluciones. ▪ El uso del cliente VPN puede resultar complejo para el usuario. ▪ El acceso total a la red interna, conlleva riesgos de fuga de datos y propagación de *malware*. Por ello, es fundamental que el dispositivo cliente esté equipado con una protección *antimalware* adecuada. ▪ El procesamiento se realiza en el dispositivo cliente por lo que es dependiente de los recursos del dispositivo cliente. ▪ El usuario puede almacenar datos de la red interna en su dispositivo cliente, por lo que deben tenerse en cuenta mecanismos adicionales para la protección de estos datos.

Tabla 2. Ventajas e inconvenientes de arquitectura VPN de acceso remoto

Portales Web	
Ventajas	**Inconvenientes**
▪ Los usuarios pueden acceder a estos portales de forma simple, desde cualquier dispositivo con acceso a Internet y un navegador web.	▪ Las aplicaciones y servicios accesibles desde el portal, deben estar basados en Web (*Web-based)* o poder ser accedidos mediante interfaz Web. Esto provoca que, a veces, este

Portales Web	
Ventajas	**Inconvenientes**
▪ El servidor del portal se puede configurar para que el dispositivo cliente no almacene datos de los recursos internos, y que estos se almacenen en el servidor. De esta forma la organización puede tener control sobre los datos sensibles. ▪ El servidor del portal web proporciona la protección del tráfico con el dispositivo cliente, típicamente a través de HTTPS. ▪ El servidor del portal web proporciona una autenticación robusta y un control de acceso en capas: al portal y a las distintas aplicaciones que ofrece. ▪ Al proporcionar acceso a recursos limitados, reduce la exposición de la red interna. ▪ En algunos casos se pueden usar *plug-in* del navegador para chequear algunos aspectos la postura de seguridad del dispositivo, aunque mucho más reducidos que el chequeo de una VPN.	tipo de soluciones resulte insuficiente para los trabajadores remotos.

Tabla 3. Ventajas e inconvenientes de arquitectura de Portales Web

Acceso directo a aplicaciones	
Ventajas	**Inconvenientes**
▪ Esta solución es fácil de implementar y de mantener y es poco costosa. ▪ Normalmente el usuario se conecta a través de un navegador web, sin necesidad de utilizar ningún *software* cliente. ▪ Al igual que los portales web, se puede configurar para no almacenar datos en el dispositivo cliente. ▪ Al proporcionar acceso a aplicaciones reducidas, reduce la exposición de la red interna.	▪ La solución proporciona un acceso limitado y no es apta para todas las aplicaciones y servicios. ▪ La seguridad no es muy robusta, ya que es la propia aplicación la que debe proporcionar la seguridad a las comunicaciones y el control de acceso.

Tabla 4. Ventajas e inconvenientes de arquitectura de acceso directo a aplicaciones

Escritorios Virtuales	
Ventajas	**Inconvenientes**
▪ Buena experiencia de usuario, ya que el entorno que los usuarios remotos manejan es un escritorio virtual similar al que tienen en la oficina. ▪ Permite configurar los escritorios virtuales y los recursos a los que los usuarios tendrán acceso, evitando exposición de otros recursos de la red interna.	▪ No se proporciona un acceso total a la red interna, sino limitado. Para determinados usuarios puede ser insuficiente. ▪ Aunque los protocolos de presentación han mejorado mucho a lo largo del tiempo, siguen existiendo problemas con la distancia y la velocidad de conexión que pueden

Escritorios Virtuales	
Ventajas	**Inconvenientes**
▪ Los recursos de cada usuario están ajustados a sus necesidades y aislados, a través de las máquinas virtuales. ▪ La organización puede asignar de forma dinámica los recursos (licencias, *hardware*, etc.) en función de sus necesidades. ▪ El procesamiento se realiza en los servidores, por lo que es la solución adecuada cuando las tareas del usuario requieren potencia de procesamiento. ▪ El almacenamiento de datos se realiza en los servidores, eliminando el riesgo de fuga que supone almacenar datos sensibles en el dispositivo cliente. ▪ No depende del *hardware* del dispositivo cliente, de hecho, se suelen utilizar *Thin Clients.* ▪ La solución proporciona protección del tráfico con el dispositivo cliente (normalmente con HTTPS), control de acceso y autenticación robusta.	generar lentitud y, en consecuencia, mala experiencia al usuario. ▪ La infraestructura VDI tiene un coste elevado y es compleja de mantener para el departamento TI, especialmente cuando el número de usuarios es elevado, ya que añade mucha infraestructura a la organización. Es inviable como solución única para empresas de gran tamaño, en las que deberá combinarse con otras soluciones como la VPN.

Tabla 5. Ventajas e inconvenientes de arquitectura de Escritorio Virtual

Escritorios Remotos	
Ventajas	**Inconvenientes**
▪ La implementación es muy sencilla y con poco coste. Sólo requiere un *software* en el equipo al que el usuario se quiere conectar, y una mínima configuración. ▪ El usuario puede acceder a todos los recursos internos como si estuviese en la oficina. ▪ El usuario se conecta, normalmente, a través de un *software* cliente. El manejo y almacenamiento de datos se realiza en el equipo remoto. ▪ La experiencia de usuario es buena porque se conecta a su propio equipo de la oficina, y lo maneja como si estuviera delante de él.	▪ Es la solución que conlleva mayor riesgo en la seguridad. La red interna queda expuesta, por lo que no debe emplearse como solución para el trabajo remoto, sino solo para casos excepcionales que requieran la conexión a un equipo concreto, por ejemplo, para uso de *software* específico o mantenimiento. ▪ Cada equipo remoto al que se accede debe ser bastionado de la forma apropiada, ya que será accesible desde internet, lo cual puede resultar tedioso y complicado. ▪ La aplicación de escritorio remoto se encarga de proteger las comunicaciones con el dispositivo cliente y proporcionar la autenticación. Sin embargo, es recomendable, en lugar de usar una conexión directa, implementar un dispositivo intermedio que permita proporcionar servicios de seguridad más robustos.

Tabla 6. Ventajas e inconvenientes de arquitectura de Escritorio Remoto

Espacio de Trabajo Digital (*Digital Workspace*)	
Ventajas	**Inconvenientes**
▪ Proporciona muy buena experiencia al usuario, al constituir una interfaz única de acceso a toda la información, aplicaciones y recursos que el usuario necesita, e implementar SSO (*Single Sign On*). ▪ Es muy configurable ya que permite el acceso solo a los servicios, aplicaciones y recursos que necesita el usuario. Se evita, por tanto, la exposición de otros recursos de la red interna. ▪ La solución proporciona múltiples servicios de seguridad. Además de la protección del tráfico con el dispositivo cliente y de la autenticación, realiza análisis de seguridad mediante el estudio de los comportamientos de usuario, para la detección de amenazas. ▪ Permite automatizar tareas y crear flujos de trabajo guiados mediante mecanismos de inteligencia, como *machine learning*. ▪ Permite a los equipos TI controlar de forma centralizada, los dispositivos cliente que acceden a la plataforma y desplegar configuraciones automatizadas, aplicar políticas, parches y actualizaciones sobre ellos.	▪ No se proporciona un acceso total a la red interna, sino limitado. Para determinados usuarios puede ser insuficiente. ▪ Solo se pueden desplegar directamente en el portal aplicaciones modernas (por ejemplo, *cloud-based*) con integración SAML. Aplicaciones tradicionales que requieren de un sistema operativo *Windows* deben ser desplegadas en el espacio de trabajo, usando las tecnologías VDI. ▪ Dada la combinación de tecnologías que incorpora, la plataforma tiene un coste elevado y es compleja de desplegar y mantener para el departamento TI.

Tabla 7. Ventajas e inconvenientes de arquitectura de Espacio de Trabajo Digital

10. CONCLUSIONES

Como se ha visto a lo largo de este documento, existen múltiples arquitecturas de acceso remoto que permiten acceder de forma más o menos segura y más o menos operativa a los recursos y aplicaciones de la organización.

A la hora de planificar su arquitectura de acceso remoto, una organización no solo debe tener en cuenta el grado en que cada solución de acceso remoto puede satisfacer los requisitos operacionales y proporcionar una buena experiencia al usuario, sino también qué implicaciones tiene sobre la seguridad de la información y de los recursos de la organización. También deben considerarse otros factores como la facilidad de despliegue y mantenimiento y, por supuesto, el coste.

El tipo de acceso proporcionado por las arquitecturas varía desde el acceso completo a la red interna a solo un conjunto restringido de aplicaciones o solo a una aplicación determinada.

La usabilidad también varía según la arquitectura. Por ejemplo, una VPN suele ser compleja de manejar para el usuario, mientras que arquitecturas basadas en web resultan más sencillas, ya que se accede a través de navegador web. Las arquitecturas de escritorios virtual generan, además, muy buena experiencia al usuario al presentarle un entorno familiar.

Respecto a la seguridad, algunas arquitecturas proporcionan una seguridad más robusta que otras. Aunque todas ellas proporcionan protección de las comunicaciones, autenticación y control de

acceso, los mecanismos usados para ello son, en algunos casos, como VPN o VDI, más robustos. También se debe tener en cuenta el grado de exposición de la red interna que presenta cada arquitectura y los mecanismos de seguridad adicionales que algunas arquitecturas aportan y resultan interesantes, como el chequeo de la postura de seguridad del equipo cliente, en el caso de VPN.

A continuación, se incluye una tabla en la que se puede comparar, entre las diversas arquitecturas *on-premise*, algunos aspectos clave a tener en cuenta[6].

	VPN *on-premise*	Portal Web	Escritorio Virtual	Escritorio Remoto	Acceso directo apps	*Digital Workspace*
Acceso a la red interna y sus recursos	Completo	Restringido	Restringido	Completo	Muy Restringido	Restringido
Seguridad	Alta	Alta	Alta	Baja	Baja	Alta
Facilidad de despliegue y mantenimiento	Complejo	Sencillo	Complejo	Sencillo	Sencillo	Complejo
Facilidad de uso para el usuario	No	Sí	Sí	Sí	Sí	Sí
Exposición de la red interna	Alta	Baja	Baja	Alta	Baja	Baja
Almacenamiento de datos en dispositivo cliente	Sí	No	No	No	No	No
Necesario software cliente	Sí	No	No	Sí	No	Sí
Chequeo de postura de seguridad en dispositivo cliente	Sí	Sí	No	No	No	Sí
Coste	Medio	Medio	Alto	Bajo	Bajo	Alto

Tabla 8. Comparativa entre soluciones de acceso remoto

Como se puede observar en la tabla, la arquitectura perfecta no existe. Cada arquitectura de acceso remoto tiene sus ventajas y sus inconvenientes. Dependiendo de las necesidades de acceso remoto que tengan los usuarios y de las capacidades y características de la organización, unas arquitecturas serán más apropiadas que otras.

En realidad, lo más conveniente suele ser implementar una combinación de ellas. Por ejemplo, una organización puede escoger proporcionar un acceso directo a las aplicaciones con bajo nivel de riesgo que son ampliamente usadas por los usuarios, como el email, y una VPN o un Portal Web para proporcionar el acceso a otras aplicaciones que podrían suponer un excesivo nivel de riesgo si fuesen directamente accesibles desde internet.

[6] Los aspectos se han evaluado para configuraciones estándar. Hay que tener en cuenta que pueden modificare según la implementación de cada fabricante, o incluso la configuración de cada implementación.

Respecto a las arquitecturas basadas en la nube, son adecuadas cuando, además de acceso a los recursos *on-premise*, se debe proporcionar acceso a aplicaciones SaaS, *cloud* públicas, privadas o híbridas.

Como se ha indicado en apartados anteriores, las arquitecturas *on-premise* no son eficientes para proporcionar un acceso seguro de los usuarios a los servicios y aplicaciones en la nube, ya que no están diseñadas para eso. Los usuarios podrían establecer canales directos a estos servicios sin pasar por los dispositivos de protección *on-premise* y sin beneficiarse, por tanto, de la seguridad que aportan. Esto supone un riesgo ya que la organización pierde visibilidad sobre ese tráfico.

La gran ventaja de las arquitecturas basadas en la nube, es que proporcionan al usuario un punto único de acceso a los recursos, independientemente de donde se alojen estos: *on-premise*, en los entornos de nube pública, privada e híbrida, o en internet.

Estas arquitecturas tienen otras ventajas típicas de todo servicio en la nube, como la facilidad de escalado, mayor flexibilidad, y un despliegue más rápido que las soluciones *on-premise*, ya que no requieren de un gran esfuerzo dentro de la organización. Sin embargo, la organización debe ceder parte del control al proveedor *cloud* y delegar en la provisión de parte de los servicios de seguridad.

Contacto

Correo electrónico CCN-PYTEC	ccn-pytec@cni.es
Twitter	@CCNPYTEC
LinkedIn	https://www.linkedin.com/company/CCN-PYTEC
Catálogo CPSTIC	Enlace web

#SALIMOS MÁS FUERTES