Teletrabajo Inteligente

Incremente la productividad sin renunciar a la seguridad

Índice

Introducción

El teletrabajo se ha disparado en España. Con la pandemia causada por el COVID-19 como catalizador principal, el número de personas que trabaja a distancia en el último año ha crecido de forma exponencial. Es algo que ponen de relieve todo tipo de estudios e informes. Según el último publicado por Adecco, realizado tomando como base la Encuesta de Población Activa (EPA), el número de personas que teletrabajaron el año pasado aumentó un 74,2% con respecto al año anterior.

2,86M
de personas trabajaban en remoto en España a finales de 2020

En total, 2,86 millones de personas trabajaban en remoto en España a finales de 2020, aunque solo lo hiciesen de manera puntual y no habitualmente. Esto, por supuesto, ha impactado directamente en la infraestructura tecnológica de las empresas, que han tenido que adaptarse (y siguen haciéndolo) a una nueva forma de trabajar que está exigiendo inversiones cuantiosas.

De hecho, según un informe de Gartner, la inversión en tecnología relacionada con el teletrabajo va a llegar a **332.000 millones de dólares este año**, un dato que facilitará el hecho de que las empresas vayan a ir retomando este año sus planes de expansión retrasados por la pandemia del COVID-19.

Mucha de esa inversión irá destinada, por supuesto, a equipamiento, pero, sobre todo, a software sobre el que construir la nueva empresa distribuida, esto es: la que llega al hogar de cada empleado. ¿Los principales retos a los que se enfrenta este tipo de empresa? No solo ser capaz de mantener la productividad de los empleados que forman parte de esta, sino, además, hacerlo con la máxima seguridad.

Los nuevos retos

Tras una situación excepcional, en 2021 y sobre todo 2022, muchas empresas afrontarán el reto de construir esa nueva realidad: una fórmula mixta. En esta nueva relación con las compañías, organizaciones y trabajadores tienen por delante unos cuantos retos por superar, comenzando por el de la seguridad informática. De hecho, según el **Barómetro de Empresas** elaborado por Deloitte, hasta el 80% de las compañías prevé invertir en una mejor protección del puesto de trabajo, tanto en la empresa como en el hogar. Además, hay otros obstáculos que se han hecho evidentes a lo largo del último año. Desde un punto de vista tecnológico, estos son los principales:

Problemas a la hora de utilizar redes VPN

Cuando se desarrolló la tecnología VPN en los años noventa, se diseñó para ofrecer un subconjunto de las aplicaciones corporativas a un subconjunto de usuarios móviles, remotos o de sucursales. En un escenario de teletrabajo masivo sin embargo, este tipo de conexiones se saturan y muchos usuarios tienen problemas para poder conectarse a su centro de trabajo y realizar su actividad con normalidad.

Las aplicaciones no funcionan como es debido

Que se desborden las conexiones VPN también tiene un impacto directo sobre las aplicaciones: algunas porque son “heredadas” y se diseñaron para clientes cercanos a un servidor en la red LAN y otras porque, al no poder contar con un procesamiento prioritario, tienen que competir con todo el tráfico de red del vecindario, ocasionando múltiples problemas.

Crece la complejidad en la gestión de contraseñas

Acceder desde casa a los recursos corporativos suele suponer una autenticación más frecuente o más estricta. Al no contar con herramientas de gestión eficientes, muchos usuarios se ven obligadas a recordar nuevas contraseñas que acaban olvidando o perdiendo, lo cual da lugar a un mayor número de incidencias y pérdida de productividad.

80%
de las compañías prevé invertir en una mejor protección del puesto de trabajo

Complejidad en la gestión de usuarios y privilegios

Habitualmente, las herramientas de supervisión de credenciales, privilegios y accesos requieren que los equipos permanezcan dentro de la misma red corporativa. En una situación de teletrabajo, la supervisión de los equipos que se mueven dentro de la red, entran en el terreno de la nebulosa.

Crecen las amenazas de seguridad

A medida que los sucesos actuales aceleran drásticamente la transición hacia el teletrabajo, los empleados trabajan intercambiando y compartiendo datos desde diversos dispositivos personales no gestionados. Las amenazas de seguridad tanto para dispositivos, como para datos y la empresas en su conjunto, crece de forma exponencial.

Se ralentiza la gestión IT

Cuando se aplican parches y actualizaciones de gran tamaño desde la red corporativa a través de una intranet sobrecargada, se producen inevitables cuellos de botella que acaban convirtiendo el trabajo en los departamentos de IT en una experiencia muy frustrante.

VPN y VDI: dos aproximaciones a un mismo problema

A la hora de enfrentar estos retos y securizar el trabajo a distancia, cada vez son más los responsables tecnológicos que se preguntan cuál es la solución más adecuada para facilitar la productividad en la empresa distribuida. Pese a que, como hemos, visto el VPN tiene ciertos inconvenientes, también resulta una gran solución en múltiples ocasiones; por otro lado, los escritorios virtualizados también están creciendo con fuerza.

¿Cuál es entonces la mejor forma de asegurar ese trabajo a distancia? ¿Debería invertir en más y mejores licencias VPN, o deberían apostar por una gran solución de VDI? En términos prácticos, esta pregunta lo que significa en realidad es lo siguiente: cuando trabajan desde casa, **¿qué tecnología debería poner a disposición de los usuarios?**

La decisión no siempre es sencilla. Ambas soluciones tienen sus pros y sus contras, por lo que en lugar de explicar cuál es mejor, lo interesante es definir qué entendemos por "mejor". Dependiendo de las distintas compañías y sus diferentes necesidades, ese "mejor" es la respuesta a preguntas como:

- ¿Cuál es más rápida de desplegar?
- ¿Cuál es la más fácil de poner en marcha?
- ¿Y la más barata?
- ¿Cuál ofrece una mejor experiencia de usuario?
- ¿Cuál se adapta mejor a lo que necesitan nuestros trabajadores?
- ¿Cuál es más segura?

Es importante tener en cuenta que ninguna de las dos opciones ofrece un "Sí" rotundo a todas las preguntas a la vez, por lo que hay que tener en cuenta cuáles son las prioridades principales. Pero es que además, los profesionales de IT deberían ser capaces de responder a algunas preguntas adicionales como:

- ¿A qué aplicaciones es necesario dar soporte? ¿Son web-apps, aplicaciones para Windows, otras…?
- ¿Trabajamos solo con aplicaciones on-premises, o trabajamos también con aplicaciones cloud y SaaS?
- ¿Tenemos experiencia con entornos VDI? ¿Tendríamos que empezar desde cero, o contamos con un entorno previo?
- ¿Tenemos experiencia gestionando dispositivos corporativos fuera del perímetro de seguridad de nuestra organización?
- Y los empleados… ¿disponen ya de portátiles con los que trabajar desde casa o deberían hacerse con equipos nuevos? Y si no los tienen, ¿los va a proveer la empresa o va a incentivar su compra?
- ¿Cómo gestiona la empresa sus dispositivos en estos momentos? ¿Cuenta con una solución cloud moderna para hacerlo?

- ¿Dispone ya de licencias VPN? ¿Dispone de licencias suficientes para dar soporte a la plantilla completa? ¿Tiene un ancho de banda suficiente para todos ellos? Y si no lo tiene… ¿hay medidas sencillas que se pueden poner en marcha para liberar espacio?
- ¿Cómo se relacionan con estas soluciones los otros componentes de la infraestructura tecnológica? (Ej: el acceso a archivos "legacy" funciona mejor a través de VDI, mientras que el trabajo con soluciones como DropBox o OneDrive es más sencillo con un escritorio no virtualizado).
- ¿Existe en la organización, sector, etc. algún tipo de regulación o compliance que incline necesariamente la balanza hacia una u otra solución?

Al responder todas estas preguntas no sería extraño acabar por determinar que lo más interesante es trabajar con un escenario mixto: uno en el que el caso de uso para algunos usuarios estuviera muy claro en favor de VPN, mientras que para otros lo más interesante fuera apostar por VDI, o viceversa.

Tu teletrabajo con VDI

Un infraestructura de VDI es un conjunto de tecnologías que virtualizan los escritorios de los empleados de una empresa, alojándolos normalmente en su propio centro de datos. De esta forma, normalmente utilizando un navegador web, los trabajadores pueden acceder al mismo escritorio que están acostumbrados a utilizar en su empresa (información, aplicaciones, correo corporativo, etc.) desde cualquier dispositivo. Las ventajas de trabajar de esta forma son evidentes:

- No importa con qué equipo se cuente en casa (un portátil de alta gama, una vieja torre de sobre mesa, una tablet…). Basta una conexión a Internet, una pantalla y un teclado para que la experiencia siempre sea idéntica.
- Conectarse a un escritorio VDI no exige ningún tipo de habilidad especial por parte del usuario. Si son capaces de recordar su nombre de usuario y su contraseña, pueden empezar a trabajar en su ordenador corporativo en pocos segundos.
- Un escritorio virtualizado es altamente seguro, ya que tanto las aplicaciones como los datos con los que trabaja el usuario se encuentran bien en los servidores de la compañía, bien en el cloud.

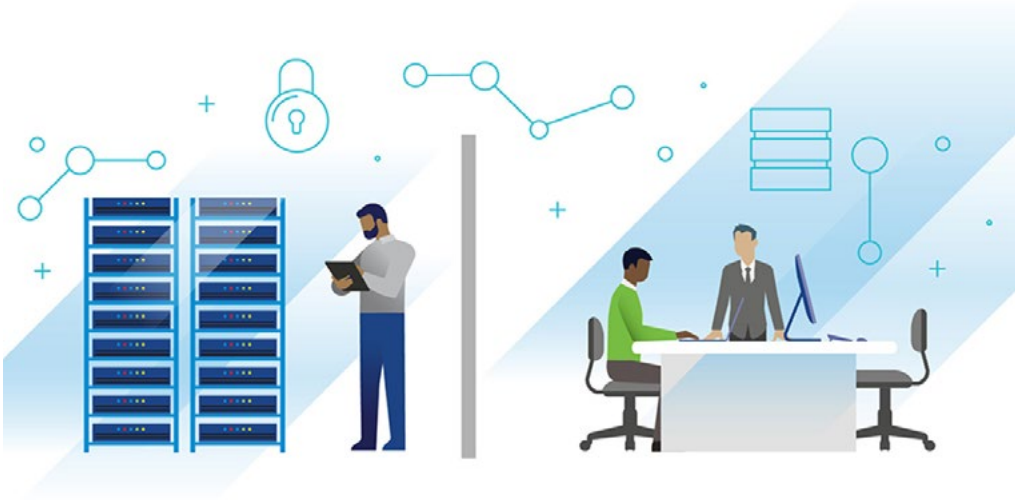
Que estas ventajas sean importantes y atractivas para muchas empresas no quiere decir que no existan ciertos inconvenientes que hay que tener en cuenta, principalmente los siguientes:

- Poner en marcha una infraestructura VDI puede ser complejo. Si no disponemos de una estructura previa, el proceso inicial puede ser costoso y necesita de expertos IT que nos vayan asesorando durante todo el proceso.
- Todos los teletrabajadores deben contar en su domicilio con una conexión a Internet de calidad. Una interrupción en el servicio implicará que no puedan hacer nada.
- VDI requiere más ancho de banda y potencia en los servidores, sobre todo a la hora de trabajar con grandes o múltiples pantallas. Si en el centro de datos de la empresa se producen "cuellos de botella", la experiencia de usuario se resiente.
- No todas las aplicaciones ofrecen una experiencia óptima en VDI.
- VDI supone en la práctica "pagar" por un portátil para cada usuario, alojado en el servidor de la empresa, por lo que si esos usuarios ya disponen de equipos corporativos validados, tal vez estemos pagando dos veces por los mismos equipos.

Tu teletrabajo con VPN

Una conexión VPN es ese ese "túnel" virtual que conecta los equipos de los trabajadores de una empresa con el centro de datos de la misma, cuando estos se encuentran en una oficina distante o, como en esta situación, se encuentran teletrabajando. Esto facilita que los usuarios utilicen equipos corporativos en su hogar, de forma local, a la vez que se securizan sus comunicaciones. Lo cual tiene muchas ventajas como que:

- Si los usuarios ya disponen de un "portátil de empresa", no tienen que hacer nada. Pueden seguir trabajando de la misma forma en la que lo harían en la oficina.
- Es una opción más barata que el VDI. No hace falta invertir en servidores dedicados o invertir en licencias VDI cloud que son bastante más caras.



Pero, como en el caso de los escritorios virtuales, trabajar con conexiones VPN también tiene aspectos "no tan bonitos" que hay que tener en cuenta:

- Como las aplicaciones corporativas se encuentran en los ordenadores de cada uno de los usuarios, se incrementan y se dificultan las tareas de mantenimiento.
- También hay que considerar el mantenimiento de los propios equipos o su reemplazo, en el caso de que se queden obsoletos.
- El usuario va a tener total libertad para poder trabajar con la información corporativa de su empresa de forma local, lo cual desde el punto de vista de la seguridad no es lo ideal.
- Una VPN pone el dispositivo del usuario en la red de la empresa, lo que implica que todos los parches de seguridad, las actualizaciones de las aplicaciones y del sistema operativo, la distribución de software en general… se realizan a través de este tipo de conectividad. ¿Podemos asegurar que estas tareas se están realizando con regularidad?
- Para los usuarios que no dispongan de un equipo corporativo puede ser todo un desafío replicar la configuración de los mismos.
- Si necesitamos adquirir nuevos equipos para los trabajadores, ¿estamos seguros de que nuestra imagen de Windows va a funcionar exactamente igual que en los equipos "antiguos"?

Lo cierto es que, en el caso de la VPN, algunas de las desventajas solo se presentan si lo que estamos utilizando es una plataforma tradicional, como puede ser Microsoft SCCM, GPOs, VPN on-prem, etc. Y, en gran medida, desaparecen si apostamos en cambio por **plataformas de gestión moderna como VMware Workspace ONE**, que aprovechan las capacidades cloud de Windows 10 que permiten a los usuarios inscribir automáticamente sus dispositivos en la red de la empresa, y que automatizan desde la nube todas las tareas de actualización de aplicaciones, seguridad y mantenimiento.

Pero incluso así no hay una respuesta sencilla. El departamento de IT debe apostar por aquella en la que crea que pueden sentirse más cómodo, lo que en grandes equipos de trabajo se traducirá en muchas ocasiones (e insistimos en esto), en una combinación de ambas soluciones.

Seguridad y teletrabajo: el gran problema al que se enfrentan las empresas

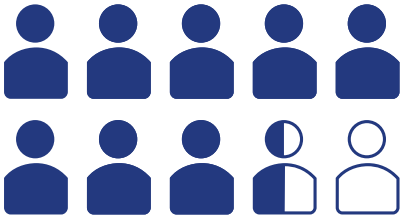
Trabajar con seguridad se ha convertido en todo un reto para la mayoría de las empresas. Ya lo era antes de la pandemia y ahora que el perímetro de seguridad llega a cada domicilio particular, la magnitud de ese reto se ha multiplicado en varios enteros.

Existe un gran número de herramientas informáticas que ayudan a los empleados a trabajar con cierta seguridad. Pero son los propios empleados y su grado de concienciación con respecto a los riesgos potenciales la mejor y principal línea de defensa en ciberseguridad.

Eso incluye recomendaciones generales que sirven bajo cualquier circunstancia: no abrir archivos adjuntos de remitentes desconocidos, no conectar dispositivos de almacenamiento que puedan ser inseguros, cambiar periódicamente las propias contraseñas y actualizar el sistema y las aplicaciones de terceros que emplee la organización. Pero, más allá de estos consejos generales, el acceso remoto a una red corporativa requiere de precauciones extra para los equipos, conexiones y sistemas:

- El equipo que intente conectarse debe estar protegido con soluciones avanzadas. De otra manera, podrían estar poniendo en peligro los activos de la empresa.
- La conexión entre el equipo y la red corporativa debe estar asegurada en todo momento por medio de una conexión VPN o un escritorio VDI.
- Las contraseñas que usamos para acceder a los servicios corporativos, y siempre en general, deben ser complejas y difíciles de descifrar para evitar ser descubiertos. Si además se cuenta con una solución de autenticación multifactor, mucho mejor.
- Los sistemas firewall, ya sean virtuales o físicos, monitorizan el tráfico entrante y saliente y deciden si se debe permitir o bloquear un tráfico específico en función de un conjunto de lógicas de seguridad previamente definidas.
- Los servicios de monitorización de sistemas, redes, aplicaciones y usuarios son más necesarios en un entorno de teletrabajo debido a la mayor cantidad de dispositivos y procesos que se deben vigilar. Esto incluye el control de los datos de carácter personal desestructurados en los equipos, que pueden contener información sensible o confidencial y estar más expuestos al encontrarse los equipos fuera del perímetro de la organización.

85%
de CISOs han tenido que rebajar sus medidas de seguridad y sacrificar la ciberseguridad para que fuese posible el teletrabajo en sus empresas



La seguridad informática en entornos de teletrabajo crece (y mucho) en complejidad. No resulta extraño así descubrir informes como el elaborado por Newtrix, en el que se asegura que el 85% de los CISOs han tenido que rebajar sus medidas de seguridad y sacrificar la ciberseguridad para que fuese posible el teletrabajo en sus empresas.

VMware Future Ready Workforce: una nueva forma de trabajar

Como hemos visto a lo largo de este documento, las compañías que quieren poner en marcha una estrategia inteligente de teletrabajo tienen que considerar un gran número de factores y tomar unas cuantas decisiones estratégicas. Y cuando la seguridad entra en la ecuación, la complejidad crece tanto que son muchas las empresas que se ven obligadas a hacer malabarismos para que la productividad de sus empleados no se resienta.

Y sin embargo esto no tiene por qué ser así. Soluciones como **VMware Future Ready Workforce** ponen en manos de las empresas todo lo que necesitan para que sus empleados puedan trabajar a distancia manteniendo su productividad y con total seguridad. Lo hace bien de forma directa, bien a través de partners y socios estratégicos como Anadat, capaces de ofrecer servicios de valor añadido.

Veamos cuáles son las principales principales características que encontramos dentro de este conjunto de soluciones.

Adaptar el acceso a las aplicaciones y los datos

La capacidad de adaptar el acceso a los datos y las aplicaciones con rapidez permite a las organizaciones seguir funcionando. Además de ser una herramienta crucial para responder en tiempos de crisis, esta capacidad es también necesaria para establecer con éxito una estrategia de teletrabajo. Si utiliza la infraestructura digital correcta podrá adaptarse para respaldar a los empleados y brindarles las herramientas necesarias dondequiera que estén, proporcionándoles acceso a las aplicaciones y los datos requeridos para realizar las tareas esenciales desde cualquier parte.

Las soluciones **VMware Future Ready Workforce** ofrecen un acceso seguro, fiable y adaptable mediante las mejores tecnologías de área de trabajo digital, como por ejemplo, gracias a la infraestructura de escritorios virtuales **VMware Horizon y Horizon Cloud**, que permiten a los equipos de TI distribuir rápida y eficazmente escritorios y aplicaciones virtuales seguros a través de una plataforma centralizada de gestión y que ofrece un solo plano de control para tener una visibilidad completa.

Estas soluciones agilizan la experiencia de los empleados porque ofrece a los teletrabajadores, allí donde se encuentren, un acceso seguro a todos los recursos que necesitan desde cualquier dispositivo. Además, la gestión versátil de la nube ofrece escalabilidad, rendimiento y flexibilidad empresariales.

Distribuir, gestionar y proteger los terminales

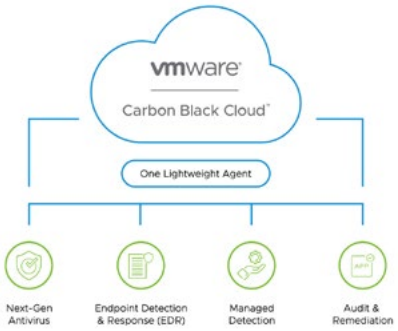
La modernización de la gestión y la seguridad de los terminales es imperativa para aquellas organizaciones que busquen adaptarse y acelerar las estrategias de teletrabajo y empresariales.

Dado que los empleados de un entorno de trabajo disperso deberían poder elegir los dispositivos que quieren utilizar (sin que el departamento de TI los controle), las organizaciones actuales que priorizan el teletrabajo deben integrar la seguridad en la distribución y gestión de estos dispositivos.

La seguridad intrínseca protege a todos los dispositivos remotos que tienen acceso a los recursos y, además, ofrece áreas de trabajo digitales seguras que proporcionan a los trabajadores las herramientas necesarias para que puedan comprometerse y ser productivos desde su primer día de trabajo.

Workspace ONE™

Las soluciones **VMware Future Ready Workforce** incluyen todas las funciones de **VMware Workspace ONE**. Se trata de una combinación líder de gestión moderna y seguridad del área de trabajo para que los equipos de TI puedan proteger de forma proactiva las identidades, las aplicaciones y los terminales de los usuarios.



La detección de amenazas y la respuesta ante ellas en Workspace ONE proporciona un **enfoque de confianza cero** para la protección de los terminales, además de brindar una experiencia de usuario excepcional. Finalmente, la combinación de características de **VMware** y **Carbon Black** ofrece datos sobre la conformidad y las amenazas.

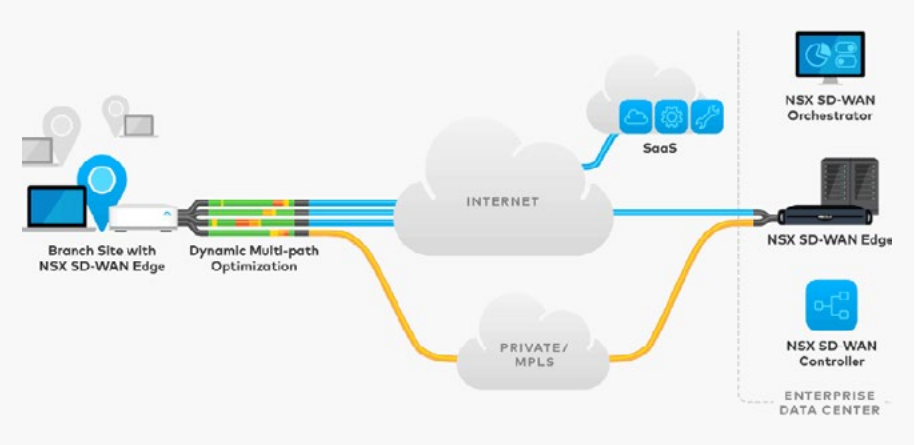
A partir de estos datos, es posible generar acciones basadas en la inteligencia, bien a través del motor de automatización, bien mediante productos de consulta en tiempo real, con el fin de corregir de forma eficaz cualquier amenaza presente. Además, Carbon Black Cloud ofrece el ciclo de protección completo de refuerzo, prevención, detección y respuesta para terminales y cargas de trabajo repartidos por todo el mundo.

Optimizar el perímetro de red

Dado que actualmente las organizaciones que priorizan el teletrabajo han ampliado sus fronteras hasta los hogares de los empleados, optimizar el perímetro de red se ha convertido en un requisito para responder con estrategias de teletrabajo, así como para adaptarlas y acelerarlas. Lo que esto conlleva es una estrategia de red y acceso moderna y flexible, con diseños de red adaptables que se centran en los usuarios, la identidad y el acceso uniforme, y que puede ampliarse globalmente.

En la era del teletrabajo, las redes para perímetros tradicionales serán vulnerables; por ello, las soluciones **Future Ready Workforce** presentan un enfoque de seguridad de confianza cero que combina funciones inteligentes para dispositivos, usuarios y redes, con el fin de ofrecer un acceso más sencillo para intentos de menor riesgo, y más protección para los que planteen un riesgo mayor. Las organizaciones pueden funcionar con más seguridad que la que ofrecen las meras combinaciones de nombre de usuario y contraseña, sin comprometer la experiencia de usuario.

Las soluciones **VMware Future Ready Workforce** también se han creado para cumplir las expectativas cada vez más exigentes de los empleados dispersos, no solo en lo referente a la conectividad, sino también al acceso fiable a todas las aplicaciones (tradicionales y de nube), desde cualquier lugar.



Esto significa que la plataforma de servicios **VMware SD-WAN by VeloCloud** para empleados de sucursal y teletrabajadores, además de permitir que el personal de TI ofrezca entornos flexibles y de alta calidad con una conectividad sin riesgos y un servicio sin interrupciones, también proporcione acuerdos de nivel de servicio (SLA) de conexión a Internet para todos. Además, es segura gracias a las funciones integradas de cortafuegos, que no solo garantizan la productividad de las soluciones de software como servicio (SaaS), sino también que el tráfico de las aplicaciones de trabajo se enrute de forma óptima para obtener el máximo rendimiento.

En definitiva, si no sabes si a tu empresa le conviene apostar por conectividad VPN o VDI o de qué forma puedes asegurar el trabajo de tus empleados, tal vez lo más interesante sea optar por algunas de las soluciones que VMware ofrece en **VMware Future Ready Workforce**.

Las soluciones Future Ready Workforce te permiten establecer una base unificada (que abarca cualquier aplicación, nube y dispositivo) para que la empresa pueda implementar plataformas ágiles que se adapten a cada uno de sus objetivos de la transformación digital.

6. Anadat: el socio ideal para la transformación digital en tu empresa

Cualquier proceso de transformación digital precisa contar no solo con la mejor tecnología disponible en el mercado, sino también de un partner en el que poder confiar y que asegura que, desde la planificación y puesta en marcha hasta la configuración y soporte de la solución, se establece una relación de confianza. En el caso de las soluciones que forman parte de **VMware Future Ready Workforce**, uno de los partners más destacados es Anadat.

Anadat Technology, fundada en el año 2002, es una compañía global de servicios de IT que gestiona y moderniza las infraestructuras tecnológicas integrándolas con nuevas plataformas digitales, multiplicando las capacidades de las empresas mediante la innovación en sus negocios. Como misión principal, liderar la transformación digital de nuestros clientes, ayudándoles a aplicar la tecnología en sus negocios con el objetivo de mejorar su competitividad para liderar sus mercados.

Es importante destacar en este sentido que los servicios de Anadat abarcan todos los dominios TI y ayudan a las empresas a superar los continuos retos asociados con la gestión de tecnologías dispersas y procesos empresariales en continua evolución, manteniendo un rendimiento homogéneo de sus aplicaciones y posibilitando el acceso seguro a la información. Para ello:

- Sus profesionales le aconsejan sobre formas óptimas de utilizar la tecnología y los servicios para transformar su entorno de TI y lograr niveles más altos de innovación.
- Desarrollan un plan estratégico que alinee sus inversiones y su estrategia de TI con sus prioridades empresariales.
- Desarrollan estrategias específicas para la movilidad, la nube y la TI como servicio para ayudar a destrabar el potencial de estas tecnologías emergentes.
- Diseñan junto a sus clientes, una solución holística que integre nuevas tecnologías con el entorno preexistente, conforme a su estrategia de TI.
- Identifican los cambios requeridos en la infraestructura de TI, desde la red, las comunicaciones y la seguridad hasta el centro de datos, la informática del usuario final, las aplicaciones y la gestión de servicios.

En definitiva, aportan un enfoque disciplinado y sistemático con evaluaciones, metodologías, marcos y mejores prácticas probadas en el tiempo para lograr coherencia y calidad durante todo el proyecto.

¿A qué esperas para poner en marcha tu próximo proyecto de transformación digital?