pasiona

Cloud Management

GUÍA IMPRESCINDIBLE PARA
MIGRAR TU NEGOCIO A LA NUBE

MORE THAN **SOFTWARE DEVELOPERS**

DESARROLLO WEB & CLOUD · MOBILE DEVELOPMENT · OUTSOURCING IT · CLOUD COMPUTING · AGILE · UX · ACCESIBILIDAD WEB · CIBERSEGURIDAD

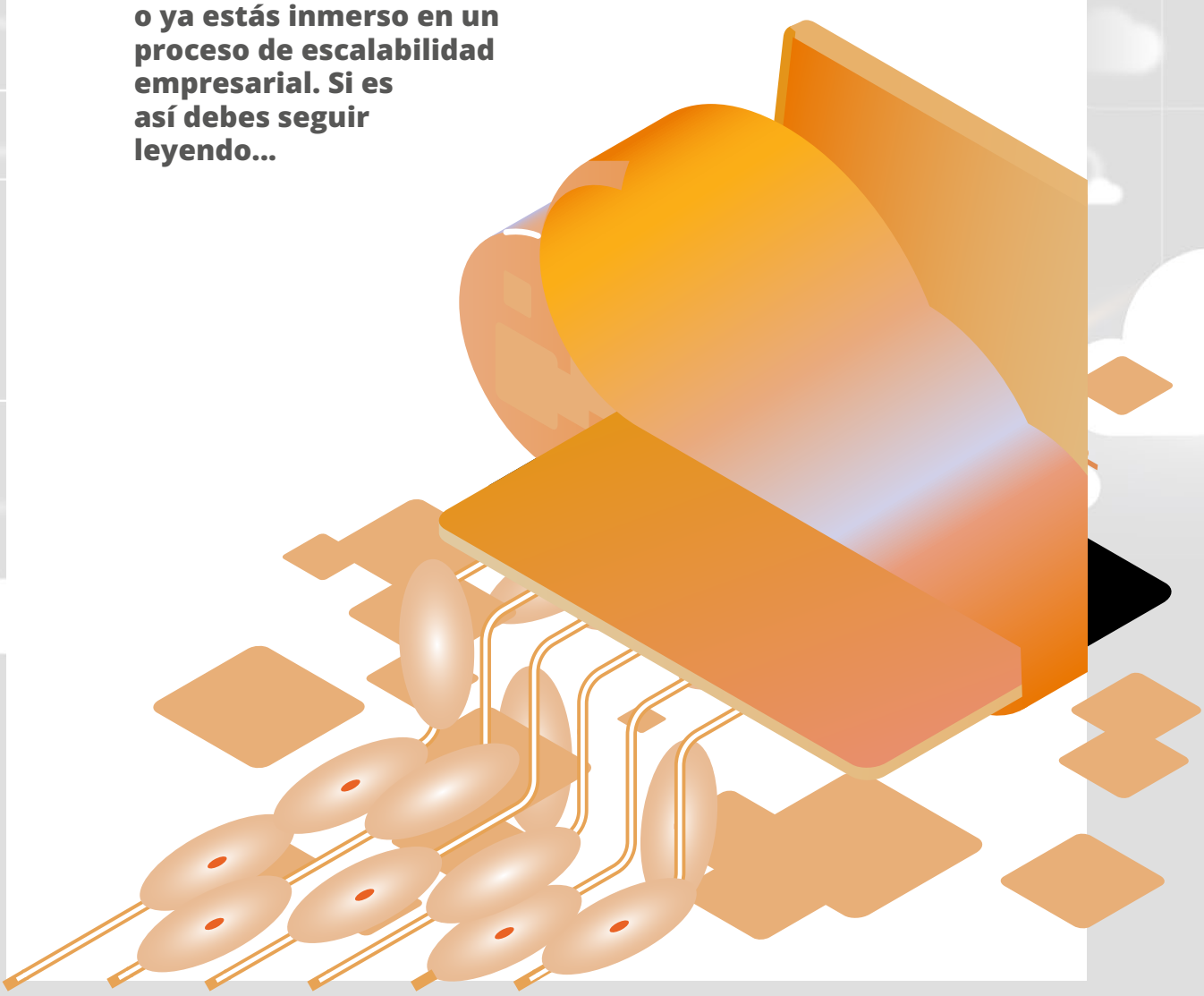
pasiona.com

pasiona

Este ebook te ayudará a dar tus primeros pasos en la migración de tu negocio al Cloud.

¿CÓMO SABER SI MI EMPRESA DEBERÍA IR A LA NUBE?

Quizá estás planteándote una nueva financiación en tu empresa, has de cambiar el hardware o ya estás inmerso en un proceso de escalabilidad empresarial. Si es así debes seguir leyendo...



ÍNDICE

pasiona

Herramientas clave para el teletrabajo

01

MORE THAN **SOFTWARE DEVELOPERS**

DESARROLLO WEB & CLOUD · MOBILE DEVELOPMENT · OUTSOURCING IT · CLOUD COMPUTING · AGILE · UX · ACCESIBILIDAD WEB · CIBERSEGURIDAD

pasiona.com

pasiona

HERRAMIENTAS DIGITALES PARA EL TELETRABAJO CON MICROSOFT TEAMS

Microsoft Teams es el complemento perfecto de Microsoft 365. De hecho, se ha convertido ya en uno de los términos mejor conocidos por parte de los teletrabajadores. A continuación, se comentan cuáles son las herramientas digitales para el teletrabajo que incluye.

¿Cómo elegir el mejor programa para teletrabajar?

El antedicho verbo es uno de los más conjugados desde la aparición de la pandemia de coronavirus. Muchos empresarios se vieron en la tesitura de elegir un programa eficaz. Entre otros requisitos, la opción elegida debe cumplir con los siguientes.

- La **adaptabilidad**. Dependerá de los objetivos a alcanzar y del valor añadido que se quiera disfrutar.
- Una **instalación sencilla y la compatibilidad** con el software existente.
- La capacidad de **almacenamiento** del software de teletrabajo.
- **Seguridad**. La protección de los datos de la empresa es imprescindible. La opción de recuperar la información perdida, también.
- **La red que usará el teletrabajador.** Deberá ajustarse a las medidas de seguridad estipuladas.
- Un **panel de control claro** y fácil de entender.
- La opción de poder comunicarse con otros compañeros y con la empresa.

En Internet es posible encontrar diversos programas para teletrabajar, pero muy pocos incluyen todo lo anterior. Evitar el uso de opciones complementarias distrae a los empleados que prefieren **una única plataforma**. Tal y como ahora se comenta, hay una solución ideal para cualquier empresa que ya está ofreciendo óptimos resultados.

pasiona

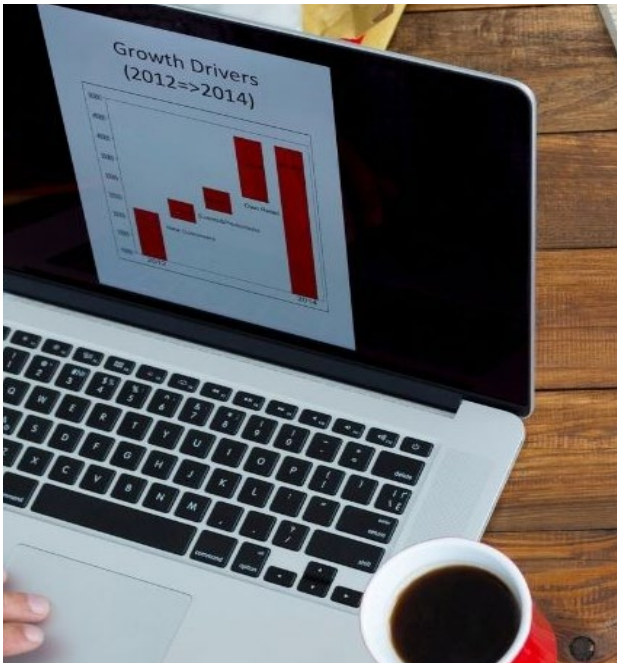
¿Por qué Microsoft Teams es la herramienta perfecta para el trabajo remoto?

Porque **une el trabajo en equipo con el teletrabajo sin dificultad**. A ello contribuye la interesante variedad de herramientas para trabajo remoto que ahora se detalla.

La conversación entre los teletrabajadores

El usuario únicamente tiene que acceder al panel principal, hacer clic en el nombre del compañero y comenzar a escribir. El proceso de enviar y recibir correos electrónicos ralentiza la actividad. La opción de compartir documentos en los que podemos colaborar y archivos en segundos **aumenta la eficacia y la productividad.**

La opción de realizar llamadas o videollamadas Solo es necesario hacer clic en la opción correspondiente. Es posible programar **videollamadas hasta para 250 participantes**. Los **eventos en línea admiten hasta 10 000**. La inclusión de subtítulos es imprescindible para aclarar mejor el contenido de cada llamada. Incluso es posible llamar al número de teléfono de la sala de reunión. Así, se evita la dependencia total de Internet.



La creación de grupos de trabajo

La interfaz principal permite agrupar a los teletrabajadores en grupos concretos. Cada envío de documentación, aviso o programación llegará a todos sus miembros. El uso de un repositorio de archivos facilita que cada profesional sepa qué debe hacer en todo momento. Se permite agregar un bot a cada equipo para que ofrezca las respuestas necesarias a quien tenga alguna duda. Debe subrayarse que el acceso a la plataforma como desarrollador es libre. Los equipos de trabajo tendrán la opción de crear **integraciones de Teams** para sus procesos comerciales y aplicaciones.

La integración con otros programas

No solo **funciona a la perfección con los programas de Microsoft 365** (Word, Excel, etcétera). También lo hace con otras **aplicaciones como SharePoint, Stream o Yammer**. La combinación de herramientas es siempre positiva para organizar mejor cada proyecto. Debe destacarse que Microsoft Teams no solo funciona bajo entorno Windows. Se ofrecen versiones para MAC, Android e iPhone. Basta con descargarse la alternativa compatible con el sistema operativo de los dispositivos que vayan a utilizarse. Posteriormente, es necesario suscribirse eligiendo entre las opciones disponibles.

El control de acceso al correo electrónico

Microsoft Teams ofrece **intercambio y alojamiento de correo electrónico,** así como una dirección con **dominio personalizado**. Se conecta con los servicios de administración de derechos para restringir el acceso a empleados concretos. Esto contribuye a mejorar la **seguridad** de cada intercambio de información.

El almacenamiento de archivos

El almacenamiento se basa en la plataforma SharePoint Online, creando **un site por canal**, donde podemos almacenar datos dentro de las limitaciones de la plataforma SPO.

El teletrabajo

Es suficiente con disponer de un móvil, tableta u ordenador portátil con conexión a Internet. El acceso al panel principal permite comenzar a teletrabajar de **inmediato**. La aplicación para teléfonos móviles admite mensajes de voz. La conexión permanente de los pertenecientes al mismo grupo de trabajo contribuye al éxito.

El vídeo empresarial

La aplicación permite crear, gestionar y compartir vídeos de la empresa. Las reuniones pueden grabarse con **subtítulos o transcritas a texto**. Los asistentes tendrán toda la información en distintos formatos y durante la reunión podrán prestar atención a lo que se les indique.

Una agenda individual

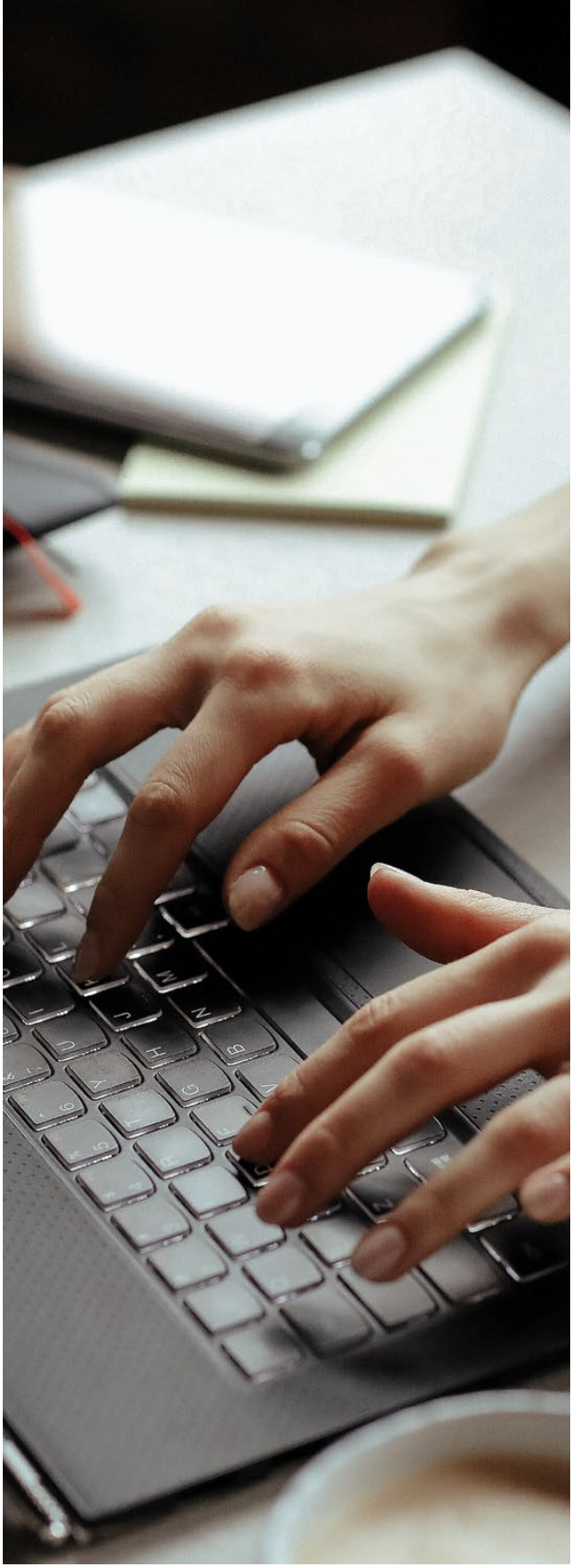
Planner es la aplicación que asigna las tareas pendientes de cada teletrabajador. Combinada con Microsoft Teams, hace posible disfrutar de una **agenda personalizada**. El objetivo es conseguir que los empleados organicen mejor su tiempo.

La seguridad

Los datos compartidos se cifran. Según configuración puede requerir un segundo factor de autenticación para tener acceso. Los datos empresariales y de los usuarios quedan protegidos.

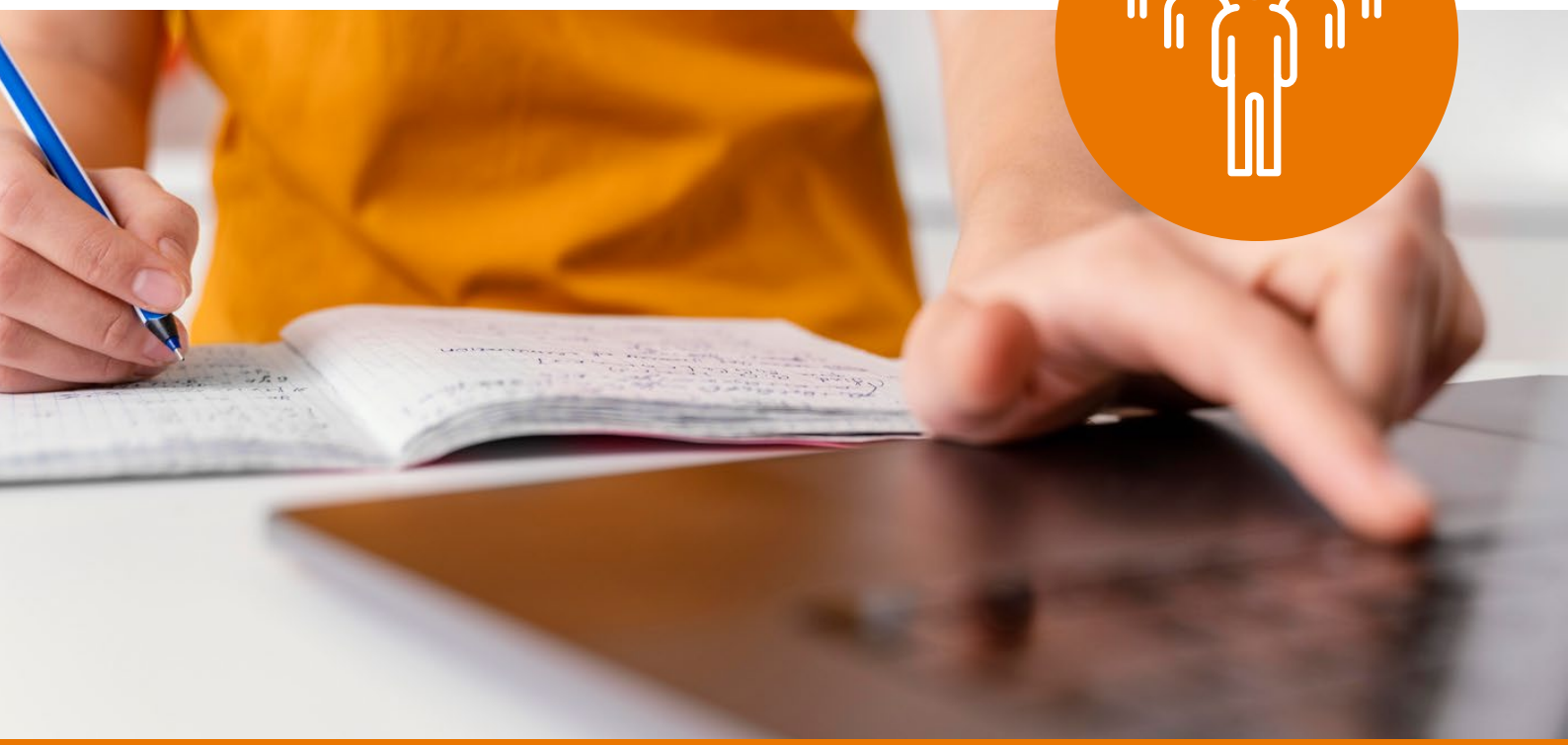
Escalabilidad

El programa se va adaptando a las necesidades de cada empresa a medida que se producen.



Puede afirmarse que **Microsoft Teams ofrece un conjunto de herramientas digitales para el teletrabajo de enorme utilidad**. Sirva la información anterior para confirmarlo y despejar cualquier duda al respecto.

pasiona



Gestionando equipos en remoto

02

MORE THAN **SOFTWARE DEVELOPERS**

DESARROLLO WEB & CLOUD · MOBILE DEVELOPMENT · OUTSOURCING IT · CLOUD COMPUTING · AGILE · UX · ACCESIBILIDAD WEB · CIBERSEGURIDAD

pasiona.com

ENDPOINT MANAGER: GESTIÓN DE EQUIPOS EN REMOTO

La gestión de equipos en remoto es uno de los servicios que ofrece Endpoint Manager, que incluye también Microsoft Intune. A continuación, se repasan las características y ventajas principales para los empresarios.

¿Cómo gestionar equipos a distancia?

Endpoint Manager es un servicio con base en la nube que **facilita la MDM (administración de dispositivos móviles) y la MAM** (administración de aplicaciones móviles). Desde la empresa es posible conocer cuál es el uso de los dispositivos (ordenadores portátiles, tabletas y teléfonos móviles) facilitados a los empleados.

Además, permite configurar el control de cada dispositivo y gestionar la recepción de mensajes o correos electrónicos de personas que no sean de la empresa. Si la compañía no ha facilitado ningún dispositivo, Endpoint Manager protege los datos empresariales aislándolos de los personales. En caso de facilitarlo, es posible hacer lo mismo dependiendo de las licencias.

Forma parte de **Microsoft 365**. Ello permite que todos los dispositivos contribuyan a aumentar la productividad y la seguridad. Además, hace posible:

- Establecer una serie de **reglas para el uso** de los dispositivos.
- **Mejorar y autentificar** las aplicaciones utilizadas.
- **Evitar** que la información de la empresa se comparta.
- Certificar que los **dispositivos empleados son seguros.**

pasiona

Teletrabajo: trabajar en equipos a distancia

Esta forma de trabajar se impuso con la llegada del coronavirus. Incluso los empleados más comprometidos tuvieron que adaptarse a un nuevo escenario.

Por ello, se convirtió en esencial el uso de herramientas de control de la productividad. Además, también crecieron otras opciones que facilitan la comunicación entre los profesionales de un mismo departamento.

Evidentemente, para **alcanzar los objetivos** hace falta un gestor que marque el camino a seguir. El uso de Endpoint Manager es imprescindible tanto para lo ya explicado como para adaptarse a las necesidades concretas de cada grupo de empleados.

Dispone de un sencillo panel de control que permite compartir archivos. La monitorización de la actividad es esencial para alcanzar el éxito.

Cómo dirigir el teletrabajo

Teletrabajo y gestión forman un binomio inseparable. Se recuerda que es necesario marcar unas pautas a los empleados sin olvidarse de la flexibilidad.

La generación de nueva información a diario conlleva que sea necesario usar una herramienta eficaz. Endpoint Manager es una de ellas, ya que permite:

- Asignar el **uso de cada aplicación** a cada empleado o departamento.
- **Configurar las aplicaciones** para que siempre se ejecuten correctamente con la configuración elegida.
- **Actualizar las herramientas** de uso habitual en la empresa.
- **Generar informes** para detectar cuál es la aplicación más empleada y saber cómo se utiliza.
- **Eliminar los datos de la empresa** de las aplicaciones si se desea.
- Crear un eficaz **control de accesos** en combinación con Azure AD.

Apostar por la presente alternativa exige la compatibilidad de los dispositivos móviles de los empleados. Tras cumplirse este requisito, se ofrece acceso a todos los productos de ofimática de la suite. Ello hace que los empleados puedan encontrar cualquier recurso para llevar a cabo su labor profesional sin problemas.

Las empresas consideran que la formación de expertos es clave para migrar sus soluciones a un sistema Cloud seguro

pasiona

Ventajas de Endpoint Manager

Aparte de contratar un único servicio, con el ahorro que ello supone para la empresa, hay otros beneficios como:

- Facilitarles a los trabajadores un **entorno seguro** en el que puedan desarrollar su labor.
- **Potenciar la productividad** tras ordenar las aplicaciones de manera automatizada que se deben realizar (tanto por parte de la empresa como por la de los empleados) de manera más lógica.
- Establecer **políticas de acceso** a los datos de la empresa.
- Proteger dispositivos de **todos los sistemas operativos** compatibles desde una única plataforma.
- **Evitar el gasto en mantenimiento o actualización** del servicio. Ambos procesos están automatizados.
- Controlar los mensajes enviados y recibidos tanto desde y hacia ubicaciones en la nube como locales.
- Hacer posible la puesta en práctica de la **política BYOD** (bring your own device) para que el empleado pueda usar su propio ordenador sin temor a poner en riesgo la seguridad de la empresa.
- Contribuir a gestionar los activos y las licencias adquiridas de manera más sencilla y eficaz.

¿Es Endpoint Manager la mejor alternativa disponible?

Todo dependerá de las **peculiaridades de cada empresa.** En términos generales, la respuesta a la pregunta es afirmativa.

Sin embargo, es habitual tener que **contar con algún programa complementario**. Endpoint Manager incluye todas las opciones necesarias para la administración de dispositivos a distancia. Que, además, funcione en la nube aumenta su eficacia y lo convierte en una opción digna de ser valorada.

Cualquier empresa que trabaje con equipos en entorno Windows debería probar esta opción. Incluir en un único panel de control el tiempo de uso de cada dispositivo es fundamental, ya que permite conocer la cantidad de accesos al equipo y a las aplicaciones realizadas.

Es importante subrayar que el programa también establece patrones de uso. Incluso, avisa de lo que podría suceder en el peor escenario posible. Conocer esta información de antemano es de gran ayuda.

La información anterior sirve para confirmar que la **gestión de equipos en remoto** y Endpoint Manager son sinónimos. Por un módico precio, es posible disfrutar de la última tecnología y crear un ambiente de trabajo ideal. El control de cada dispositivo aumenta la protección de los datos de la empresa. Si se le añade a este factor el de accesos y la mejora de la comunicación, el resultado no puede ser más positivo.

El **teletrabajo** deja de ser un problema gracias a la adaptabilidad de una herramienta prácticamente perfecta. Confiar en Endpoint Manager para la **gestión de equipos en remoto** es, sin duda, la mejor opción para afrontar la transformación digital de los procesos internos de los equipos de trabajo. La sencillez de su uso contribuye, directamente, a familiarizarse con su funcionamiento en muy poco tiempo.

pasiona

Cómo proteger tus datos de negocio

03

MORE THAN **SOFTWARE DEVELOPERS**

DESARROLLO WEB & CLOUD · MOBILE DEVELOPMENT · OUTSOURCING IT · CLOUD COMPUTING · AGILE · UX · ACCESIBILIDAD WEB · CIBERSEGURIDAD

pasiona.com

pasiona

CÓMO UTILIZAR MICROSOFT AZURE PARA PROTEGER LOS DATOS Y SERVICIOS DE TU NEGOCIO

Microsoft Azure para proteger tu negocio es una de las alternativas más fiables que existe, y que dispone de una red de servidores remotos conectados entre sí para funcionar como uno solo. A continuación, vamos a comentar las características de la función Backup y todas sus ventajas.

La importancia de las copias de seguridad

Trabajar con servidores físicos instalados en el propio negocio implica un riesgo. Cualquier ciberataque puede provocar la pérdida de toda la información almacenada. Sin embargo, Azure es una plataforma que se basa en la nube de Internet. Así, se consigue poder **disponer de una copia de seguridad** del entorno local, las máquinas virtuales los discos duros, recursos compartidos y bases de datos.

El entorno local

Usando el **agente MARS (Recory Services)** es posible obtener una copia de seguridad de archivos, carpetas y del sistema completo. **DPM de MABS (Azure Backup)** permite proteger máquinas virtuales como VMware, Hyper-V y otras cargas de trabajo a nivel local.

En 2019, la adopción de la nube entre las empresas fue del 94%

El 69% de las organizaciones han creado nuevos roles en sus departamentos de TI

Máquinas virtuales

Las extensiones de copias de seguridad permiten copiar **máquinas virtuales completas de Linux o Windows**. MARS permite añadir todas las carpetas, los archivos y los estados del sistema con mayor facilidad.

Los discos duros y los recursos compartidos

Gracias a **Azure Managed Disks** es posible tener una copia fiable de los discos duros instalados. **Azure Files** ayuda a guardar en una cuenta de almacenamiento los recursos compartidos de uso habitual.

Blobs

Los **blobs de Azure** son indispensables para su correcto funcionamiento. Realizar una copia de seguridad periódicamente contribuye a evitar daños imprevisibles.

¿Cuáles son las ventajas de confiar en Azure Backup?

Tras haber comentado todos los elementos susceptibles de ser copiados de forma fiable, habría que analizar las ventajas del programa.

La facilidad de uso

Las **copias de los recursos locales** en la nube se realizan en segundos, algo imposible con otros programas que exigen el uso de alternativas más complejas.

Las copias de máquinas virtuales

Hay que subrayar que no todas las copias se almacenan en el mismo espacio. Cada una es independiente y se aísla de las restantes para evitar el borrado accidental de los datos. **Recovery Services** incluye un panel de administración muy claro que incluye puntos de restauración. Configurar este servicio y adaptarlo a nuestras necesidades es bastante fácil; poder restaurar la copia necesaria, también.

Su disponibilidad

Cualquier sistema de almacenamiento físico exige un mantenimiento y una supervisión continua. Azure **automatiza ambos factores**, siempre está disponible y se adapta a la carga de trabajo correspondiente de inmediato.

Una transferencia de datos sin límites

Azure no cobra por la cantidad de datos de salida o entrada. Los datos de salida se refieren a los provenientes de **Recovery Services** durante la restauración. Es posible importar grandes cantidades de datos con un coste determinado. Tanto los datos en reposo como los que están en tránsito se encuentran siempre protegidos.

La centralización de las operaciones

La **supervisión** y la **alerta** están integradas en Recovery Services. No es necesario elegir una versión especial de Azure para disfrutarlas. Usando Azure Monitor es posible mejorar el tipo de supervisión y obtener informes más completos.

Copias de seguridad ajustadas a cada aplicación

Azure Backup no hace copias genéricas que luego hay que corregir para que todo vuelva a funcionar. Cada copia se completa con la **configuración de la aplicación** que usa los datos correspondientes. La reducción del tiempo de restauración ayuda a pasar al tiempo de ejecución de forma directa.

La posibilidad de almacenar los datos de manera personalizada

Es posible retenerlos a **largo o a corto plazo**. Además, Azure no es excluyente, permitiendo que los datos se almacenen a nivel local si así se prefiere. El sistema automatiza la asignación y la administración de las copias siendo esta opción de pago por uso.

Sus alternativas de replicación

Son tres las que contribuyen, directamente, a poder sacarle el máximo partido posible esta herramienta tan práctica:

- **LRS.** El almacenamiento con redundancia local se encarga de copiar los datos tres veces en una unidad de escalado de almacenamiento perteneciente a un centro de datos. Es la opción más económica para evitar los daños provocados por los errores del hardware a nivel local.
- **GRS.** Se denomina así al almacenamiento con redundancia geográfica. Es la más recomendable. La replicación se lleva a cabo en una región situada a cientos de kilómetros de la ubicación de los datos originales. La durabilidad de los datos es mayor, así como la protección frente a una interrupción a nivel regional.
- **ZRS.** Las siglas hacen referencia a almacenamiento con redundancia de zona. Los datos se replican en zonas de disponibilidad, por lo que su residencia y resistencia se encuentran en la misma región. Sin tiempo de inactividad, las cargas de trabajo críticas se adaptan muy bien a esta variante.

Otros beneficios a tener en cuenta

Si bien ha quedado demostrado que Azure es una opción ideal, hay otros aspectos dignos de mención como:

- **El cumplimiento del RGPD.** La LOPD (Ley Orgánica de Protección de Datos) es bastante estricta y su incumplimiento conlleva sanciones de diversa cuantía. En caso de ataque cibernético, es posible recuperar la información protegiendo los intereses de los clientes.
- **Su escalabilidad.** La versión estándar es más que suficiente para una PYME, pero Azure se adapta a distintas cargas de trabajo. El pago por fracciones de almacenamiento garantiza un servicio fluido y sin interrupciones.
- **El ahorro.** Las alternativas locales implican la compra de nuevos discos duros periódicamente. Asimismo, hay que disponer de un espacio concreto que tenga unas características concretas. La nube permite disponer de todo lo anterior de manera ilimitada. Además, las actualizaciones y el mantenimiento están incluidos en el precio.

Así, se confirma que el uso de **Microsoft Azure para proteger tu negocio** es una sabia decisión. Todo sea por convertir el almacenamiento de los datos en un proceso más sencillo y fiable. De ello dependerá el poder seguir superando retos y afrontar nuevas etapas con las máximas garantías de éxito.

pasiona

CÓMO Y POR QUÉ CREAR COPIAS DE SEGURIDAD EN LA NUBE PARA EMPRESAS CON MICROSOFT AZURE

Las copias de seguridad en la nube para empresas ayudan a afrontar situaciones críticas, como un ataque informático, sin perder competitividad. Detallamos, a continuación, cómo Microsoft Azure es una herramienta ideal para conseguir fácilmente este objetivo.

Qué tener en cuenta en los sistemas de backup para empresas

A la hora de encontrar un sistema de **backup en la nube para empresas** hay una amplia oferta. Sin embargo, consideramos esencial responder a:

- **¿Qué tipo de programa necesita la empresa?** Dependerá de la cantidad de información que quiera almacenarse y de las tareas que pueda desempeñar.
- **¿Cómo se realizan las copias de seguridad?** Podemos elegir entre un respaldo completo, una copia de seguridad diferencial o incremental.
- **¿Cuál es la periodicidad más adecuada de la copia de seguridad?**
- **¿Dónde se guardará la información?** La nube es una alternativa ideal.
- **¿El proceso será automático o manual?**

Cómo hacer un plan de copias de seguridad para empresas

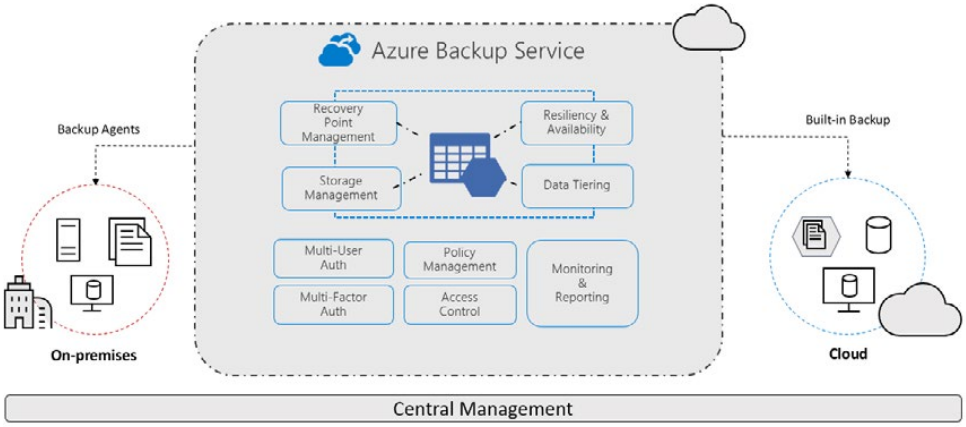
El plan previo a realizar un **backup en la nube para empresas que permiten recuperar desastres** debe contener distintos puntos. Para que sea eficaz y permita obtener los resultados oportunos hay que detallar:

- **Los detalles del plan.** Deberíamos incluir el propósito y el alcance del programa.
- La **política de respaldo de datos** de la compañía.
- Las **copias de seguridad de datos**. Especificamos cuáles son las que queremos realizar. Progresivamente, añadiremos los cronogramas con la periodicidad elegida.
- La **recuperación de los datos**. Es esencial que aclaremos los detalles del proceso de recuperación de los datos.
- El **mantenimiento y la revisión del plan**. Concluimos el plan añadiendo cómo se va a controlar la funcionalidad del plan ejecutado.
- Los **apéndices**. Incluimos detalles de contacto de los equipos implicados, ubicaciones del respaldo de datos y recursos que deben respaldarse.

¿De qué tipo de información podemos hacer un backup?

Aunque pensamos que solo puede efectuarse el respaldo de los datos, es posible aumentar su alcance. Así, tenemos la opción de respaldar:

- Una **página web.**
- Todo el **almacenamiento local.**
- **Máquinas virtuale-**
- **Ficheros.**
- Entornos **cloud.**
- Entorno **híbrido.**



pasiona

¿Qué ofrece Microsoft Azure?

Como **Microsoft Partner**, es un alojamiento en la nube que permite a los usuarios realizar un respaldo de datos de:

- Los **recursos pueden almacenarse en distintas regiones del mundo**. Actúa en Norteamérica, Asia y Europa. También en Oriente, el Reino Unido y en Asia. Cada almacén debe estar presente en la misma zona donde se vaya a hacer una copia de seguridad.
- Facilita el **control de acceso basado** en el rol de RBAC de Azure y Azure.
- Los **recursos ejecutados en distintos entornos**. Podemos crear almacenes independientes para desarrollador, no producción y producción.
- Un **gran número de máquinas virtuales** de Azure (hasta 1000).
- La protección de **hasta 2000 cargas de trabajo distintas.** Se incluyen cargas como bases de datos SQL o SAP HANA de las máquinas virtuales de Azure.

¿Cuáles son los riesgos de no llevar a cabo un backup?

Los **sistemas de backup para empresas** tienen como objetivo guardar la información para recuperarla en caso de ataque o problema técnico.

Apostar por el almacenamiento local supone que no sea posible recuperar nada si el problema también les ha afectado.

Un repaso a las ventajas del uso de Azure Backup

Las **copias de seguridad para empresas** gracias a esta herramienta son mucho más sencillas. Azure permite realizar las siguientes funciones.

Descargar una copia de seguridad local

Las **copias del almacenamiento local** son más fáciles de descargar. Pueden obtenerse copias con el plazo elegido sin necesidad de implementar nada.

Copias de seguridad de máquinas virtuales de IaaS de Azure

Las **copias se aíslan** para que no se puedan destruir los datos originales por accidente. Se encuentran en Recovery Services que incluye puntos de recuperación.

Escalabilidad y eficacia

Azure combina **la escala sin límites de su nube** con la máxima eficacia. Sin necesidad de mantenimiento o supervisión, los datos son accesibles en segundos.

El gasto global en servicios de nube pública se duplicará en 2023

Los servicios de infraestructura en la nube son los servicios de más rápido crecimiento, con más del 40% de crecimiento

Una transferencia de datos sin límites

No hay un límite en la cantidad de datos de entrada o de salida. No se cobra por las transferencias.

La protección de los datos

Tanto en reposo como en tránsito, se nos ofrece una opción que permite supervisarlos y administrarlos. Puede aumentarse la escala de la supervisión e informes gracias a Azure Monitor.

Copias de seguridad coherentes con la aplicación

No necesitamos hacer una corrección adicional para la restauración de datos. Así se acorta el tiempo de cada proceso.

Retención de los datos

Tanto a corto como a largo plazo gracias a **Recovery Services**. Adicionalmente, Azure se encarga de asignar y administrar el almacenamiento de cada copia de seguridad.

Distintas opciones para almacenar los datos

La replicación de datos se divide en tres tipos principales. La **LRS** (con redundancia local) hace una copia por triplicado en una unidad de escalado ubicada en un centro de datos.

La **GRS** (con redundancia geográfica) conlleva que los datos se almacenen a cientos de kilómetros de la ubicación de la empresa. La **ZRS** (con redundancia de zona) copia los datos en zonas disponibles. La residencia y la resistencia de los datos están en la misma región.

Lo anterior confirma que Azure Backup es una opción ideal para ejecutar, en segundos y sin problemas, las **copias de seguridad en la nube para empresas.**

pasiona

Configurando un plan de recuperación de desastres

04

MORE THAN **SOFTWARE DEVELOPERS**

DESARROLLO WEB & CLOUD · MOBILE DEVELOPMENT · OUTSOURCING IT · CLOUD COMPUTING · AGILE · UX · ACCESIBILIDAD WEB · CIBERSEGURIDAD

pasiona.com

pasiona

CÓMO IMPLEMENTAR UN PLAN DE RECUPERACIÓN DE DESASTRES CON AZURE SITE RECOVERY

Azure Site Recovery es una de las funciones más interesantes de la plataforma. Es clave conocer cómo implementar un plan de recuperación en caso de desastre.

¿Qué es un plan de recuperación?

Es la mejor manera de acortar el tiempo de inactividad de una página. El objetivo es crear una **réplica exacta del sistema en funcionamiento** en una localización distinta. Las copias de seguridad locales no ofrecen las garantías suficientes al ser parciales. Suelen provocar errores que terminan por alterar la estabilidad del sistema. De preguntarse si es, o no, necesario su diseño, la respuesta es siempre afirmativa. Resulta imprescindible para:

- Proteger **todos los servicios críticos de una empresa.**
- Mantener activo una **herramienta de seguridad** que no altere el ritmo de trabajo o de ingresos.
- **Paliar las consecuencias de un ataque** y solucionar la disrupción del servicio en el menor tiempo posible. Tras la identificación de la alteración, se toman las medidas necesarias para solucionar la incidencia.
- **Cumplir con los RTOs** (recovery time objectives) o tiempo de recuperación. En el plan se especifica el tiempo máximo en que un servicio debería estar inactivo. En caso de no cumplirse, se apostaría por otra estrategia.

¿Por qué no es suficiente con una copia de seguridad de los datos?

Lo habitual es programar una copia de seguridad de los discos duros de forma periódica y alojarla en un espacio distinto. Durante la misma solo se copian los datos, pero no las funciones, los programas y las aplicaciones que se usan para dar el servicio. Azure apuesta por **replicar los servidores en su totalidad**. Es decir, en caso de alteración en el sistema, en minutos es posible volver a usarlo tal y como estaba momentos antes. Las copias de seguridad solo permiten acceder a la última almacenada, lo que conlleva una pérdida de información valiosa. Todo dependerá de la periodicidad elegida. Al usar la nube de Internet, el acceso a los datos es inmediato y no depende de otros factores externos que sí afectan a los servidores físicos. De hecho, el fallo de estos puede estar provocado por incendios, inundaciones o averías diversas. Estas circunstancias no pueden suceder en Azure dada su continua actualización y su mantenimiento.

Tener configurado un sistema de confianza de copias de seguridad y recuperación antes desastres permite:

80%

Reducir en un 80% el tiempo promedio de recuperación de datos

370%

Obtener un ROI del 370% en 5 años

97%

Reducir un 97% la pérdida de productividad de los usuarios por la pérdida de datos

La sencillez de uso de Azure

Solo es necesario acceder a **Azure Portal** y replicar una instancia de Azure Virtual Machines en otra región. Site Recovery se actualiza de manera automática a medida que se renueva el sistema. Los problemas de recuperación se verán minimizados. Es posible secuenciar el orden de las aplicaciones multinivel ejecutadas en las máquinas virtuales. El plan de recuperación resultante puede probarse sin que ello afecte a la funcionalidad de la web o a los usuarios. Las aplicaciones seguirán siempre disponibles, incluso durante las interrupciones con recuperación automática, tanto entre regiones como en el entorno local de Azure. Para lograrlo, habría que seguir los siguientes pasos.

Configurar las copias de seguridad

La plataforma permite seleccionar **el tipo de copia de seguridad** que debe realizarse. Site Recovery facilita el proceso. No es necesario añadir las directrices correspondientes. De forma automática, el sistema se encarga de realizar las copias de las áreas relacionadas con las cargas de trabajo en entornos de la nube o híbridos. Así, opciones como Azure Virtual Machines, las bases de datos SAP y SQL, las máquinas VMware y los servidores de Windows locales estarán mejor protegidos.

Establecer las normas de seguridad integradas

Es posible seleccionar las normas de privacidad y seguridad correspondientes. Las máquinas virtuales se pueden conmutar por error a la nube o bien hacer lo mismo entre centros de datos en la nube. Usar **grupos de seguridad de red** contribuye a protegerlos mejor. El complemento Azure Backup protege los datos ante el ransomware, la eliminación y el aislamiento de los datos de copia de seguridad. La eliminación accidental y la autenticación multifactor son evitables de manera más sencilla.

Los puntos de recuperación y los objetivos de tiempo de recuperación

Ambos contribuyen a que la carga de trabajo de una empresa sea más fácil de recuperar. Además, favorece el **coste de implementación**, aplicación de revisiones, supervisión y escalado de la infraestructura de recuperación ante desastres a nivel local. No es necesario administrar recursos relacionados con las copias de seguridad o crear un segundo centro de datos. Sin infraestructura física y con enorme flexibilidad, es posible mejorar el almacenamiento de cada copia.

El cumplimiento de la norma ISO 27001

El plan de restauración de copias de seguridad obedece al cumplimiento de la **norma ISO 27001**. Al habilitar Site Recovery entre las distintas regiones de Azure es posible conseguir que el usuario final no se percate del error. Es posible personalizar la cobertura incluyendo aplicaciones que se consideren esenciales. Además, Azure proporciona la posibilidad de restaurar los datos en segundos, un respaldo de disponibilidad y un soporte técnico.

El ahorro en costes

Supervisar, aplicar revisiones, establecer una infraestructura de recuperación e implementar los planes de prevención es mucho más económico. **Mantener un centro de datos**, a un encargado de su gestión y todo lo relacionado con este tipo de infraestructuras es bastante costoso. Solo es necesario pagar por los recursos de proceso que vayan a usarse.

La apuesta por la máxima funcionalidad posible

Diseñar un plan de contingencia es sinónimo de tener una garantía total de adaptabilidad a cualquier tipo de situación. Como ejemplo de un servicio crítico, **la página web de un negocio** es la vía de entrada que usarán los clientes para realizar pedidos, reclamaciones o comentarios. Cualquier página puede fallar, pero lo más importante es que el error sea casi imperceptible y que los servicios se restauren más rápidamente. Teniendo en cuenta que los costes son más asequibles y que la plataforma se adapta con facilidad a cualquier tipo de negocio, el resultado no puede ser más favorable. **Azure Site Recovery** es imprescindible para cualquier empresa que quiera ser competitiva y moderna. El plan de contingencia que propone esta herramienta se ha convertido en uno muy fiable. De su puesta en práctica puede depender el éxito de un negocio al afrontar incidencias de diversa índole.

pasiona

¡CONTACTA CON NOSOTROS!

info@pasiona.com

pasiona.com

+34 902 731 731
+34 648 888 777

MORE THAN **SOFTWARE DEVELOPERS**

DESARROLLO WEB & CLOUD · MOBILE DEVELOPMENT · OUTSOURCING IT · CLOUD COMPUTING · AGILE · UX · ACCESIBILIDAD WEB · CIBERSEGURIDAD