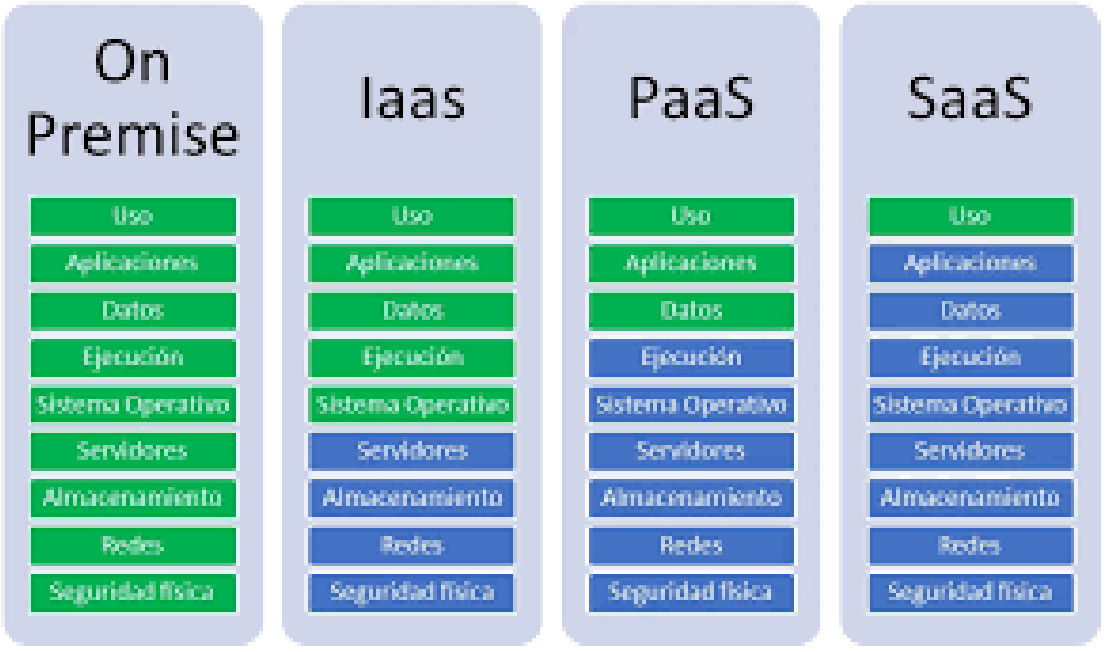
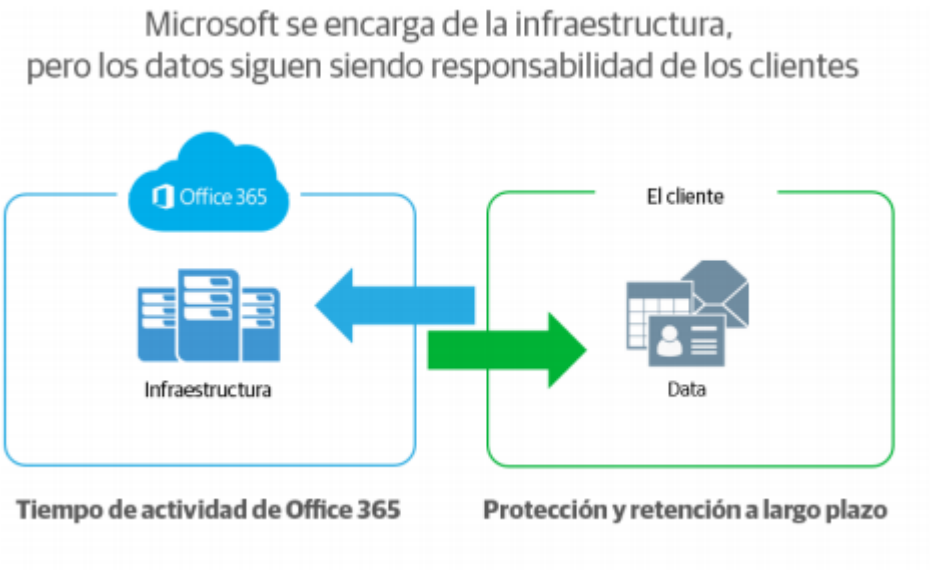
¿Utilizas Microsoft Office 365 para trabajar? ¿Ya has hecho un backup de tus datos?

Hoy queremos invitarte a reflexionar sobre **porqué es tan importante elaborar una estrategia de copia de seguridad y recuperación de datos**. Y es que pareciera ser que con Office 365 nuestros datos siempre estarán al alcance de un click, pero hay cierta tergiversación entre la responsabilidad percibida de Microsoft y la responsabilidad real del usuario en la protección y retención a largo plazo de sus datos de Office 365: Microsoft Office 365 permite que su empresa funcione desde cualquier lugar y en cualquier momento, sin necesidad de contar con su propia infraestructura de correo electrónico, archivos y SharePoint.
Si bien Microsoft alberga la infraestructura, es bueno saber que no abarca la responsabilidad de mantener un backup de los datos esenciales para tu empresa, los datos son responsabilidad del usuario SIEMPRE

MODELO DE RESPONSABILIDADES





Muchos confunden los acuerdos de nivel de servicio de disponibilidad de Microsoft con estrategias de copia de seguridad, mientras que muchos otros, no consideran necesario pensar en una copia de seguridad para la nube por tratarse de una tecnología avanzada. Pero el factor común será que las organizaciones sin un backup de sus datos, se exponen a los siguientes riesgos:

- **Pérdida de datos y violaciones a la seguridad**. O365 no está libre de violaciones a la seguridad: es vulnerable tanto a amenazas internas (borrado accidental de datos, represalias de ex empleados o accesos indebidos) como a amenazas externas (malware o ransomware)

- **Retención de datos y el cumplimiento normativo**. Microsoft ofrece una política de retención de 90 días que no cumple con las normativas más estrictas en materia de retención de datos para determinados sectores, como servicios financieros, salud, comercio minorista y gobierno. Contar con una copia de seguridad proporcionada por un tercero puede ayudar a las organizaciones a estipular sus propias políticas de retención en función de sus necesidades empresariales, además de garantizar el cumplimiento de las normativas europeas en torno a los datos.

- **Falta de control de los datos en los despliegues híbridos:** La supervisión y el control completos de los datos son una prioridad

para todos los directivos, y este es el primer paso en el camino a transformarse en una empresa impulsada por datos.

Considerando los riesgos mencionados, elaboramos los **7 motivos por los cuales tu empresa debería realizar un backup de Office 365**.

1- Existe una alta probabilidad de que se de una **eliminación de datos accidental**. Si se elimina a un usuario, ya sea de forma intencional o no, esa eliminación se replica en la red junto con la eliminación de su cuenta de OneDrive for business y su casilla de correo. La papelera de reciclaje nativa y las versiones de historiales incluidas en Office 365 solo pueden brindarle protección contra la pérdida de datos de manera limitada, lo que puede convertir una simple recuperación con un backup adecuado en un gran problema una vez que Office 365 haya eliminado los datos para siempre a través de la redundancia geográfica o una vez que se agote el periodo de retención.

2- Puede darse cierta **confusión y brechas en la política de retención**, resultante del ritmo acelerado de los negocios en la era digital, que lleva a una continua evolución de las políticas, incluidas las de retención, que no son difíciles de seguir y mucho más de administrar. Al igual que la eliminación temporal y permanente, Office 365 tiene políticas limitadas de backup y retención que solo pueden repeler ciertas situaciones de pérdida de datos y no pretenden ser una solución de backup integral.

3- La idea de una **amenaza de seguridad**, por lo general, nos lleva a pensar en hackers y virus. Sin embargo, las empresas experimentan amenazas desde su interior y suelen ocurrir más a menudo de lo que usted cree. Las organizaciones han sido víctimas de amenazas provocadas por sus propios empleados, tanto intencional como accidentalmente. Microsoft no tiene manera de saber la diferencia entre un usuario frecuente y un empleado despedido que intenta eliminar los datos críticos de la empresa antes de su partida.

4 -Luego están las **amenazas de seguridad externas** como el malware, los virus, y el ransomware entre otros. Las amenazas externas pueden ingresar sigilosamente a través de correos electrónicos o archivos adjuntos y no siempre resulta suficiente educar a los usuarios sobre el

cuidado que se debe tener, especialmente cuando esos mensajes infectados parecen ser tan atractivos. Las funciones limitadas de recuperación/ backup de Exchange Online no son adecuadas para manejar ataques serios

5 -Algunas veces tendrá la necesidad de **recuperar correos electrónicos, archivos u otros tipos de datos en medio de una acción legal** de forma inesperada. Algo que usted piensa que nunca va a pasar, hasta que ocurra. Microsoft ha integrado un par de redes de seguridad (retención y conservación de elementos por litigios). Sin embargo, esto no es una solución de backup sólida para mantener a su empresa a salvo de los problemas legales.

6- El manejo de implementaciones de correo híbrido y migraciones a Office 365, generalmente necesitan cierto espacio de transición entre Exchange en las instalaciones y Office 365 Exchange Online. La implementación de estos correos híbridos es común, pero plantea desafíos adicionales de administración. La solución adecuada de backup para Office 365 debería ser capaz de manejar las implementaciones de correo híbrido y también tratar los datos de intercambio, de forma que la ubicación original se vuelva irrelevante

7- Microsoft Teams se está implementando cada vez más y está creciendo con el aumento del trabajo remoto, por lo cual se vuelve indispensable tener una estructura de datos para Teams. Hoy más que nunca, las personas eligen Teams para proyectos e iniciativas especiales a un ritmo acelerado. Pero una vez que complete un proyecto, es probable que necesite conservar una copia del proyecto terminado para necesidades a largo plazo, como requisitos legales y de cumplimiento. Lo que sucede con frecuencia es que estos Teams se eliminan por error o se aplica incorrectamente la retención, lo que genera que otros archivos o documentos esenciales no estén disponibles.

¿Sabías que 60 % de los datos confidenciales en la nube se almacenan en documentos de Office, y a 75 % NO se le realizan backups? Con Backup para Microsoft Office 365 tendrás la capacidad de realizar backups de Office 365 de forma segura en cualquier ubicación, incluso en las instalaciones, en una nube de hiperescala o en un proveedor de servicios.

Al implementar Microsoft Office 365, ya has tomado una decisión empresarial inteligente, ahora vamos a acompañarte a implementar la solución de backup que te permitirá acceder y controlar de forma segura tus datos de Office 365 para evitar riesgos innecesarios de pérdida de datos.