8 Excelentes Proveedores Cloud Para Datos Corporativos

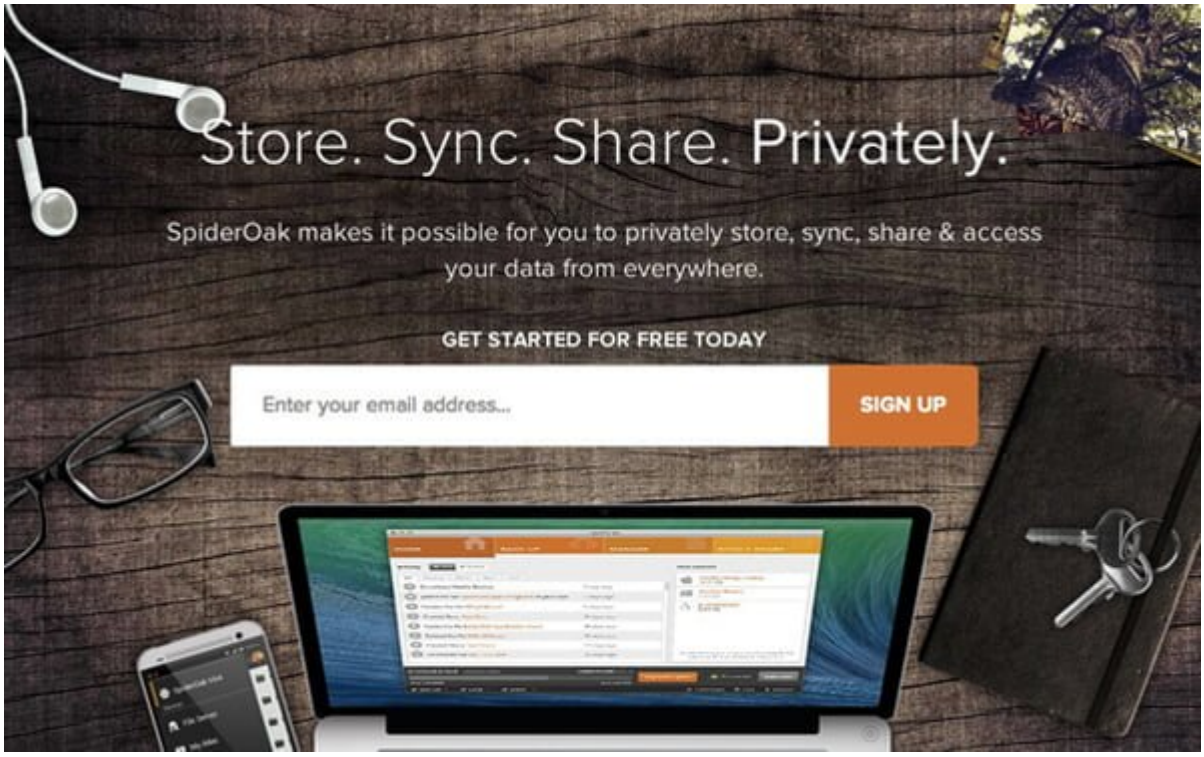
La mayoría de las organizaciones ahora almacenan los archivos digitalmente utilizando tecnología cloud para manejar la gran cantidad de datos generados. En esta era de abundante información digital, es importante que las empresas tomen las medidas necesarias para mantener los registros de clientes de forma privada y segura. Es de vital importancia que las empresas elijan un **proveedor Cloud** que cumpla con dos grandes características: **privacidad y seguridad**.

Los proveedores de almacenamiento en la nube toman una serie de medidas estrictas para garantizar que los datos transmitidos en los servidores son seguros. Sin embargo, algunos son mejores que otros para proporcionar privacidad y seguridad máxima. Los siguientes proveedores de almacenamiento en la nube son mejores opciones para cualquier organización preocupada por la seguridad de datos.

Nota: Los planes de precios son sobre basados en la investigación. Las cifras son iguales en el momento de la publicación.

1. SpiderOak

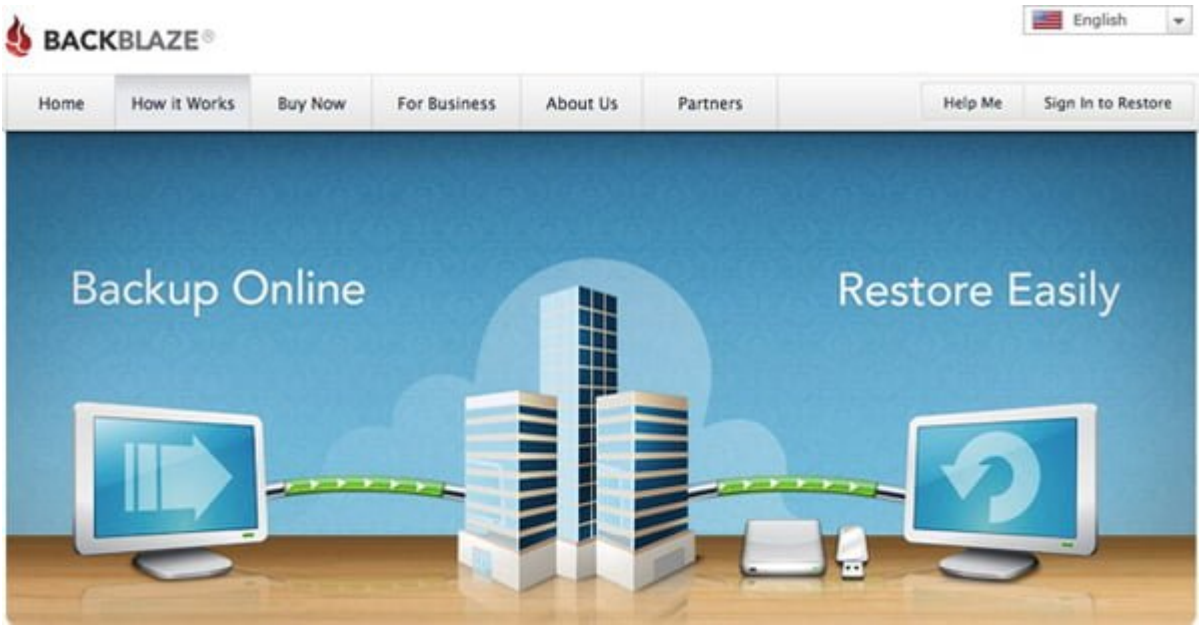
SpiderOak es uno de los **proveedores Cloud** más seguro, debido a sus prácticas de privacidad «zero-knowledge». **SpiderOak** no almacena las contraseñas de sus usuarios y claves de cifrado. Su «de-duplicated central storage repository» representa un almacenamiento en la nube segura.



Para los desarrolladores, los propietarios de **SpiderOak** proporciona una forma de crear aplicaciones escalables horizontalmente y verdaderamente privadas. La compañía Nimbus.io se dirige a almacenamiento a nivel de servidor y copia de seguridad; que proporciona almacenamiento en la nube a largo plazo combinado con un backend abierto. También han fundado la organización Zero Knowledge Privacy organization con el objetivo de promover los derechos de privacidad en línea a nivel mundial. [Planes de Precios]

2. BackBlaze

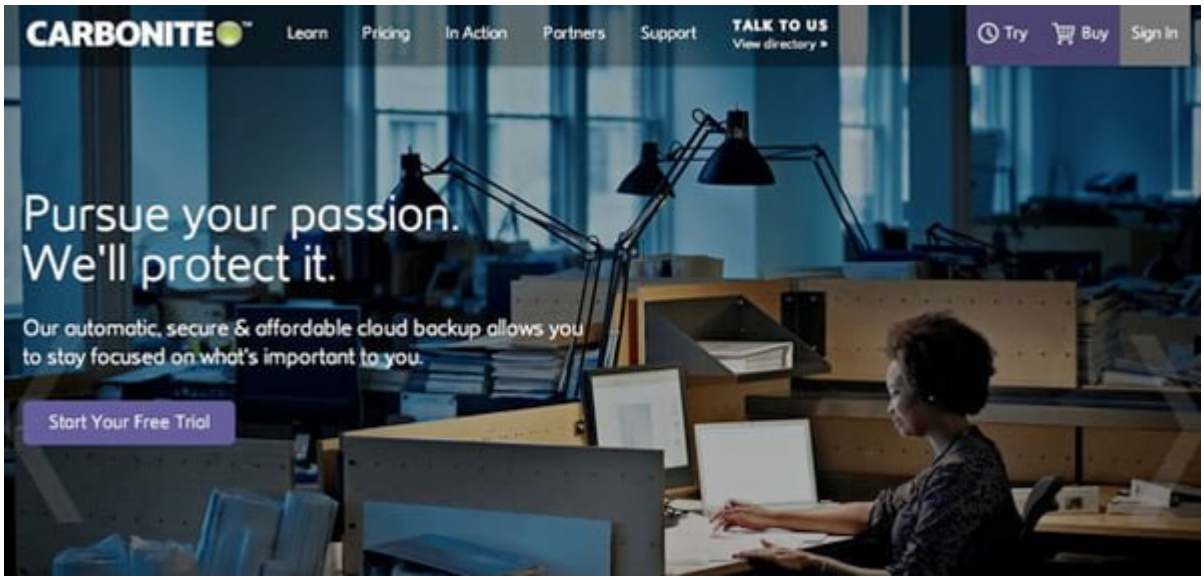
BackBlaze utiliza un centro de datos que se describe como un «Fondo de misión crítica», que emplea medidas de seguridad biométrica para el acceso del personal. Sus socios incluyen 25 proveedores de telecomunicaciones independientes para garantizar la transmisión segura de datos a su centro de datos. A su llegada, los datos se comprimen y se cifran con el cifrado de grado militar AES. A partir de ahí, los datos se mueve a la nube de servidor mediante una **conexión SSL segura**.



Los clientes tienen la opción de establecer una clave de cifrado personal, privada. Además, BackBlaze es desarrollado por sus propietarios para su entorno cloud que los «de-duplicates y porciones de datos en bloques; encriptados y transferidos para la copia de seguridad; se vuelven a ensamblar, descifrar, y los paquetes de los datos para la recuperación, y supervisa y gestiona toda la nube del sistema «. [Planes de Precios]

3. Carbonite

Planes de almacenamiento en línea de Carbonite están certificados **certified HIPAA** (Health Insurance Portability and Accountability Act). Sus centros de datos están protegidos por guardias 24/7/365 y el acceso humano a la instalación asegurada a través de la utilización de escáneres biométricos en los puntos de entrada de trabajo.



Seguridad de los datos se garantiza mediante estándares de encriptación Blowfish de 128 bits. Proporciona seguridad adicional a nivel de cliente a través de claves de cifrado personal. La transmisión de datos utiliza el estándar de tecnología Secure Socket Layer (SSL). [Planes de Precios]

4. Hightail

Hightail (antes YouSendIt) permite a los clientes compartir carpetas con la capacidad de limitar el acceso a archivos específicos. Los propietarios de cuentas también puede agregar una **fecha de vencimiento** para presentar el acceso y son

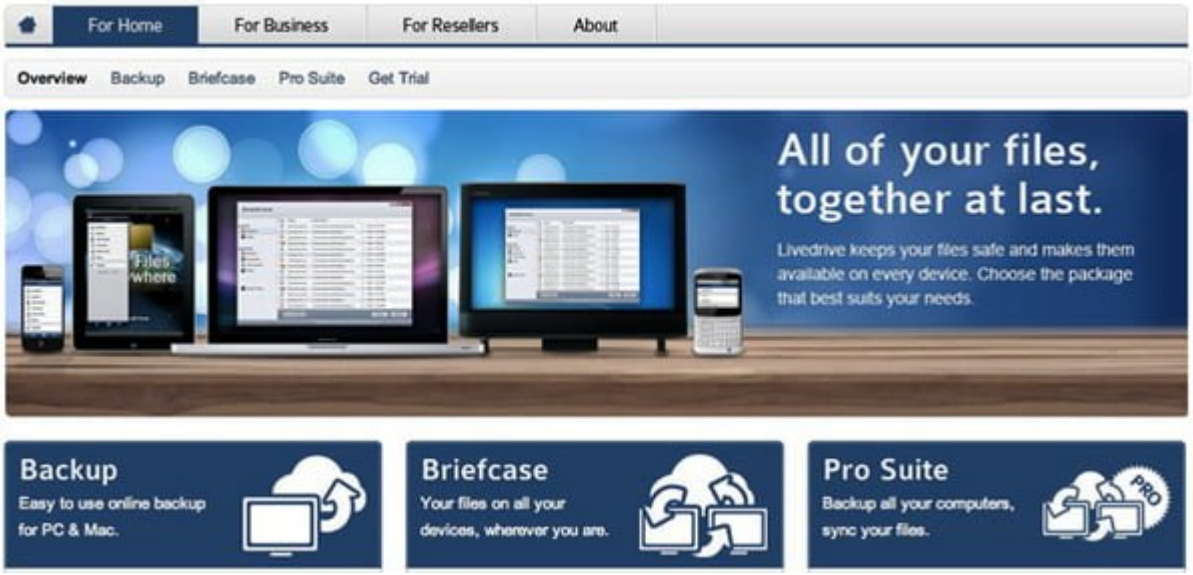
capaces de utilizar los **protocolos de verificación de identidad, protección de contraseña y los informes de seguimiento de archivos**.

Los datos se envían con el cifrado SSL de 128 bits y se almacena mediante el cifrado AES de 256 bits. El almacenamiento en la nube de Hightail está certificado con SAS 70 Tipo II, SSAE, SOC 2 Tipo 2, TRUSTe, PCI, HIPAA y GLBA cumplimiento. [Planes de Precios]

---

5. LiveDrive

Los usuarios de LiveDrive tienen una opción SSL en la conexión para asegurarse de toda la actividad entre sus dispositivos de computación y almacenamiento en la nube utilizan una conexión segura. Los datos se cifran mediante cifrado AES 256 y se almacena en más de un servidor de forma que un fallo de seguridad en un servidor no proporcionará acceso total a la información almacenada.



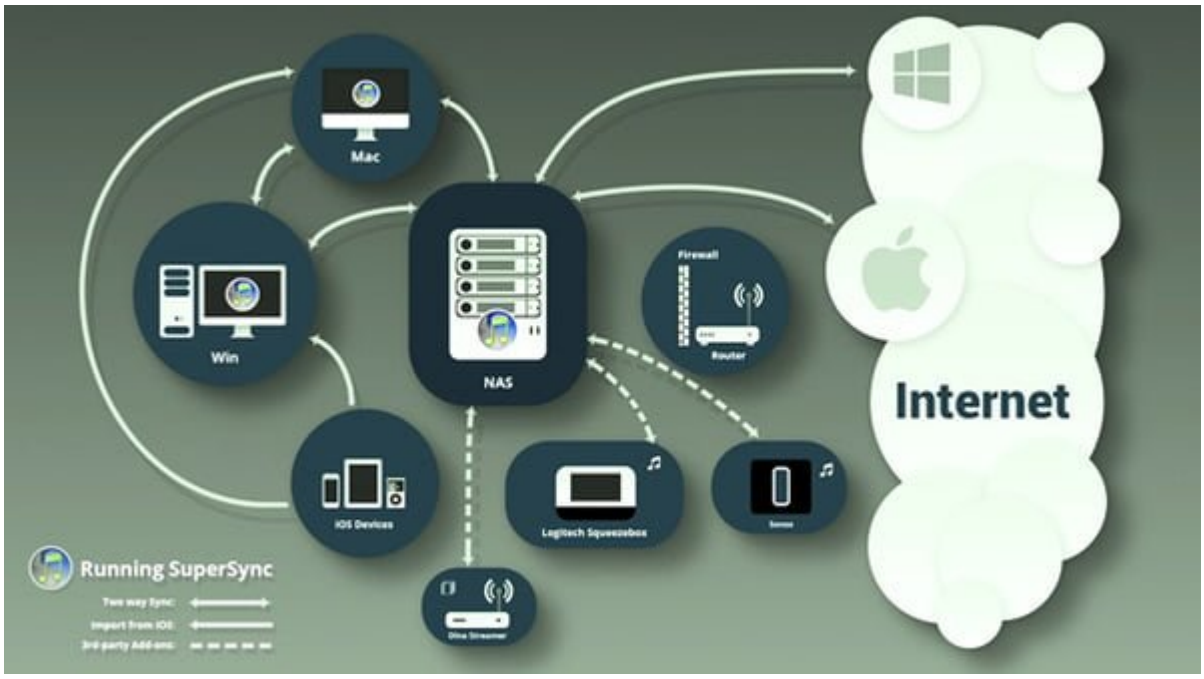
También se cifran las transferencias de datos entre dispositivos y la nube LiveDrive. Los clientes tienen la opción de crear sus propias cuentas FTP, sin embargo, esto podría dejar vulnerable de datos durante la transferencia FTP ya que no emplearia inherentemente protocolos de seguridad o cifrado. [Planes de Precios]

---

6. SuperSync

Al igual que con muchos otros **proveedores cloud**, SuperSync permite a los propietarios de las cuentas limitar el acceso de los demás a archivos específicos al compartir datos. Su panel de control de administrador proporciona **control de acceso** y un **registro de actividades** para todos los usuarios. Una característica única de sus planes está la opción de **borrar de forma remota todos los datos de un cliente en caso de un fallo de seguridad**.

El archivo de seguridad es proporcionado con acceso de sólo

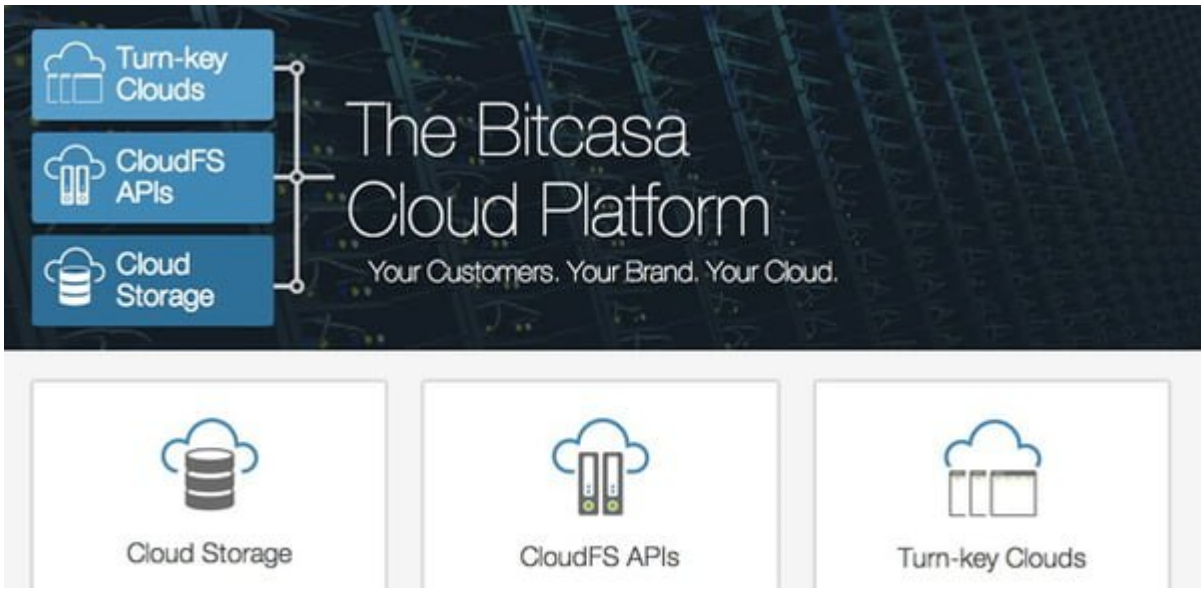


lectura, estándar de la industria de seguridad (SSL 3.3) de encriptación de datos de seguridad de nivel de transporte, 256-bit AES durante el envío, y el protocolo de reconocimiento para verificar la comunicación segura durante la transmisión a través de Internet. [Planes de Precios]

---

7. Bitcasa

Con una características de copia de seguridad sin esfuerzo que permite reflejar cualquier carpeta de un disco duro, Bitcasa es muy fácil de usar, mientras que también es seguro para el **almacenamiento de datos**. La empresa utiliza un programa propietario que emplea el cifrado a nivel de bloque antes de la transferencia a sus servidores.



Todos los archivos almacenados son encriptados antes de ser subidos y una vez que lleguen a los servidores de Bitcasa, nadie puede acceder a ellos, salvo el propietario de la cuenta. [Planes de Precios]

---

8. SOS Online Backup

Aunque SOS Online Backup está más orientado hacia el usuario personal, es una opción buena y economica para una pequeña empresa. Esta empresa de almacenamiento en línea asegura la privacidad de sus datos mediante el cifrado de 3 veces: una vez a nivel local, una vez que durante la carga en sus servidores y una vez más en el nivel del servidor (a lo que SOS denomina como «**UltraSafe**«).

Sus centros de datos utilizan equipos de calidad y de seguridad

de medidas militares. Los clientes que utilizan SOS son automáticamente compatibles con HIPAA y los servicios cumplan con todas las normas regulatorias SEC (Securities & Exchange Commission) . [Planes de Precios]

Finalmente

Siempre habrá un riesgo cuando se transmiten los datos en cualquier lugar, de cualquier manera. Sin embargo, mediante la utilización de las mejores medidas de encriptación y de seguridad disponibles, los **proveedores de almacenamiento en la nube** de hoy en día están haciendo todo lo posible para mitigar los riesgos que pueden afectar o extraer los datos importantes de cualquier empresa.