

Backup Cloud: Copia de Seguridad

¿Qué es backup Cloud?

El respaldo en la nube es un servicio donde todos los datos y aplicaciones que se encuentran en el servidor de una empresa se respaldan y almacenan en un servidor remoto. El respaldo en la nube para empresas funciona mediante la copia y el almacenamiento de los archivos de su servidor en otro servidor que se encuentra en una ubicación física diferente. Las empresas pueden respaldar algunos o todos los archivos del servidor, dependiendo de su preferencia.

¿Qué es Cloud Backup?

Cloud backup (o copia de seguridad del equipo en la nube) es copiar tus archivos, aplicaciones, equipos virtuales o servidores y almacenarlos en una red remota y segura de recursos informáticos a los que usted accede vía Internet. Protege cualquier entorno virtual, físico y en el cloud, y permite la mayor seguridad de la información rápidamente sin costes por adelantado y con un modelo de negocio de pago por uso.

Te ofrecemos una plataforma que proporciona servicios de protección de datos con una facilidad sin precedentes. Con una sola instalación, usted y sus clientes pueden obtener acceso a los servicios de copia de seguridad, recuperación ante desastres, sincronización y uso compartido de archivos, así como servicios de notaría y firma electrónica, todo ello gestionado desde una única consola.



Proteje cualquier
carga de trabajo.

Cloud
Máquinas virtuales en el cloud
Office 365
Sitios web
In situ
Físicas
Virtuales
Aplicaciones
Entorno móvil

Características

- Copia de seguridad
- Restauración ante desastres
- Encriptación con Cifrado fuerte AES-256
- Copia Híbrida
- Cifrado de canal SSL 2048
- Protección contra Ransomware
- Sincronización de archivos

Características esenciales

Protección para cualquier carga de trabajo

Proteje Windows, Linux, Mac, seis hipervisores principales, iOS, Android, aplicaciones Microsoft, Office 365, sitios web. Protección contra ransomware basada en IA. Defiende los datos, sistemas y copias de seguridad frente al ransomware.



Copias de seguridad rápidas y fiables

Evita que los archivos de copia de seguridad resulten dañados, reanuda y detén trabajos de copia de seguridad en cualquier momento y realiza copias de seguridad a 500 MB/segundo y aún más rápidas.

Restauración instantánea

Recupera sistemas en unos segundos iniciando cualquier sistema directamente desde el almacenamiento de copia de seguridad.

Consola de gestión web centralizada

Reduce la carga de trabajo de TI con una sola consola web táctil y centralizada. Optimiza los tiempos de recuperación mediante el acceso a la consola web desde cualquier dispositivo, incluidas las tabletas.

Envío de datos físicos

Realice la recopilación inicial más deprisa enviando un disco duro con la copia de seguridad completa original a un centro de datos de clouds7.



Complemento DRaaS sencillo

Añada la funcionalidad de recuperación ante desastres al sistema de copia de seguridad en solo unos minutos a fin de que puedas acelerar los sistemas en el cloud.

Centros de datos en el cloud seguros

Los centros de datos de clouds7 están diseñados para Nivel IV y han recibido varias importantes certificaciones de seguridad.

Protección completa para Office 365

Aumenta fácilmente los ingresos ofreciendo servicios de copia de seguridad y recuperación de cloud a cloud eficientes y bajo demanda para Office 365.



Beneficios

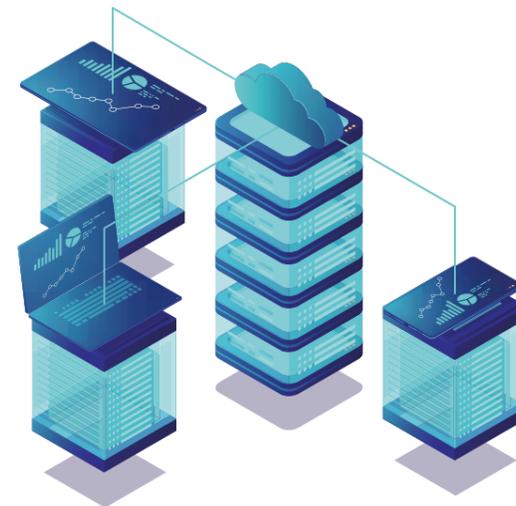
- Tu información se encuentra encriptada en nuestros servidores, ni nosotros podemos ver el contenido de sus archivos.
- Programa las copias de seguridad a la hora que desees.
- Administra todos los computadores de escritorio y portátiles de su empresa desde un mismo panel de administración
- Verifica el estado de las copias mediante el panel o mediante los reportes que enviamos a tu correo electrónico.
- Restaura archivos y carpetas de forma inmediata
- Cada archivo se almacena en 4 discos duros, en dos servidores distintos.
- Soporte para Windows y Mac.

Información segura

Respaldos diarios, semanales y mensuales, así mantendrás segura la información de tu empresa segura en la nube, para evitar cualquier pérdida y consultarla desde cualquier equipo de cómputo o dispositivo móvil con conexión a internet.

Respaldos programados

Realiza respaldos automáticos o prográmalos de forma diaria, semanal o mensual. Después del primer respaldo solo se actualizarán los incrementos o modificaciones de tu información para un proceso más ágil.



Siempre disponible

Tu información respaldada estará disponible cuando lo necesites, desde cualquier computador o dispositivo móvil con conexión a internet.

Las empresas pueden correr el riesgo de perder datos importantes. La pérdida de datos genera costosos tiempos de inactividad, insatisfacción de los clientes, multas regulatorias y pérdida de ingresos. Como resultado, los profesionales de TI deben cumplir con expectativas extremadamente altas, tienen que mantener la empresa en funcionamiento las 24 horas del día.

Ofrecemos la protección de datos que cumple con las demandas actuales. Mantenemos tu negocio en funcionamiento, protegemos cualquier carga de trabajo, escalamos sin límites y te ahorramos dinero.

Backup en la nube para empresas

Aloja tus datos en el cloud de forma automática y segura. El servicio de copias de seguridad en la nube para empresas te permite realizar backups y restaurar servidores, bases de datos, ordenadores o solo algunas carpetas o archivos en el cloud, de forma fácil, automática y segura. Configura y gestiona tus copias de backup online, desde un único panel, para todos tus datos.

Copia de seguridad rápida

Actividad empresarial sin interrupciones.

Ejecuta copias de seguridad tan a menudo como lo necesites, sin afectar al rendimiento general. Mejora tu RPO y ahorra dinero en caso de desastre.

¿Puedes sobrevivir sin tus servidores esenciales?

La velocidad de su recuperación puede marcar la diferencia entre la pérdida de dinero y la quiebra. Evita el paralizante tiempo de inactividad al añadir la conmutación tras error en el cloud. Garantizará que sus aplicaciones empresariales esenciales estén siempre disponibles y listas para ejecutarse.



Seguridad

Replicación automática en dos centros de datos y encriptación de datos.

Restaura los datos tú mismo, de la última copia realizada o de la de hace un año.

Backup online de cualquier tipo: servidores, aplicaciones, PCs, carpetas, archivos, etc.

Fácil: Rápida de implementar, fácil de utilizar y no requiere formación.

Eficiente: Solución asequible sin inversiones en infraestructura.

Segura: Protección proactiva contra ransomware basada en IA y ML.

Tips de uso

En 3 sencillos pasos

Realizar copia de seguridad



Utiliza la clonación e imágenes de espejo para realizar un duplicado de tu sistema, capturando todos tus datos para realizar la migración del disco o la recuperación del sistema.

Almacenar



Realiza una copia de seguridad en una unidad local y en la nube para tener doble protección al tener siempre copias disponibles in situ y externas.

Restaurar



Recupera rápidamente todo el sistema o un archivo específico con confianza, sabiendo que la copia de seguridad es tan buena como el original.

Todas las herramientas. Una interfaz simple.

Ninguna otra solución ofrece una gama de herramientas de protección potentes, a través de un panel de control informativo y fácil de usar.



Versátil

Realiza una copia de seguridad de lo que desees y cómo desee con herramientas como la creación de imágenes completas, copias de seguridad a nivel de archivo o carpeta, clonación de discos activa, programación basada en eventos, copias de seguridad sin parar y un creador de medios de inicio.

Visual

Conoce todo sobre tu copia de seguridad de un vistazo. Realiza un seguimiento del estado de las copias de seguridad, ve el tamaño de los archivos, mide la velocidad de las copias de seguridad y mira el tipo de datos almacenado con códigos de colores.

Flexible

Controla dónde vas a almacenar tus datos, localmente o en un disco duro externo, una carpeta de red o un dispositivo NAS, externamente en el cloud, o una combinación para garantizar una protección total.

Compatible

Protege tus datos independientemente de dónde vivas con una solución que admite dispositivos Windows, Mac, iOS y Android, así como equipos virtuales y cuentas de redes sociales.

Protección moderna contra amenazas modernas

Consigue la única solución de copia de seguridad con una defensa contra ransomware basada en inteligencia artificial, que detecta, detiene e invierte automáticamente de forma activa los efectos de una encriptación no autorizada.

Protección contra Desastres

¿En qué consiste?

Protección contra desastres de clouds7 es una solución sencilla, completa y lista para utilizar, basada en clouds7 Backup Cloud. Puede proteger las cargas de trabajo de tus clientes poniendo en marcha instantáneamente los sistemas de TI en el sitio gestionado de recuperación en la nube y restaurándolas en un hardware similar o diferente.

Funciones principales

Recuperación ante desastres para cargas de trabajo físicas y virtuales

Cubre todas las cargas de trabajo más utilizadas, incluidos servidores físicos y máquinas virtuales Windows y Linux, los principales supervisores, así como aplicaciones empresariales de Microsoft.

Replicación de máquinas basada en copia de seguridad

Aprovecha la combinación perfecta de tiempos de recuperación, cortos y bajos costos en comparación con tecnologías de replicación sofisticadas.

Sitio de recuperación en la nube de clouds7

Reanuda la actividad normal en cuestión de minutos en caso de paralización del sitio simplemente trasladando tus cargas de trabajo de producción a máquinas del centro de datos de la nube de clouds7.



Mejora la eficacia operativa a través de una consola web fácil de utilizar.

Editor para arrastrar y soltar

Defina grupos de máquinas y secuencias de acción con estos grupos con el intuitivo editor para arrastrar y soltar.

Incluye todas las funciones de copia de seguridad

Copia de Seguridad de clouds7 es la base de Recuperación contra desastres, por lo que incluye todas las funciones de nuestra potente solución de copia de seguridad.



Fácil ampliación de redes locales al sitio de recuperación en la nube

Extiende tu red al sitio de recuperación para proporcionar acceso remoto transparente a los servidores de recuperación en modo de conmutación por error. Nuestro dispositivo virtual VPN lo hace muy fácil.

Organización de la recuperación ante desastres

La función de runbooks simplifica y acelera la conmutación por error de varias máquinas a un sitio de recuperación en la nube. Permite realizar operaciones eficaces para automatizar la conmutación por error y las pruebas, y garantiza que los sistemas se recuperan en el orden adecuado para gestionar las interdependencias entre las aplicaciones en máquinas distintas.

Pruebas sin interrupciones

Verifica la integridad de los planes de recuperación ante desastres mediante la ejecución de runbooks en modo de prueba a través de la consola web y aislando las pruebas de la red de producción.

Integración con sistemas PSA y RMM

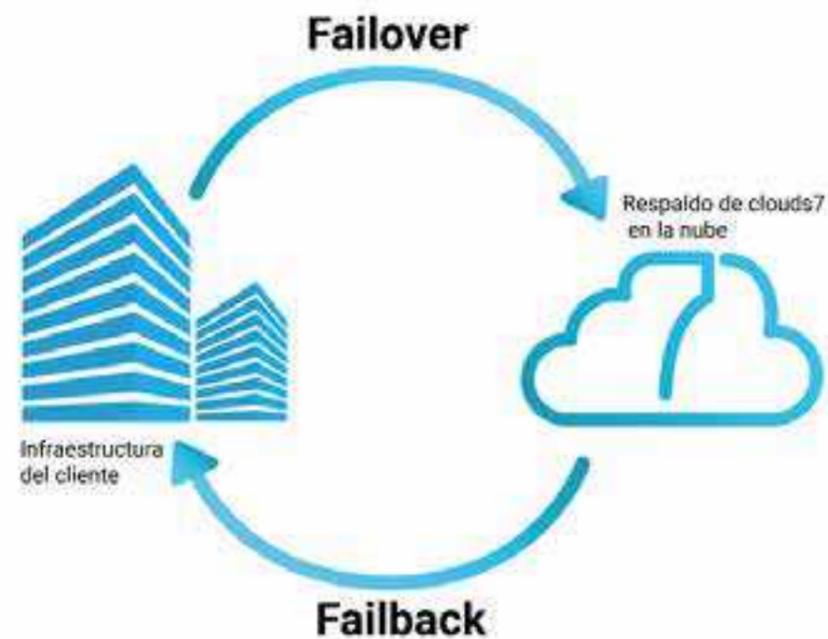
Proporciona servicios a tus clientes de forma instantánea gracias a la integración con Auto-task, ConnectWise Automate y ConnectWise Manage. *costo adicional

Pago por uso, sin complicaciones

Paga exclusivamente por los servicios que estás protegiendo con y solo cuando necesites protección. No se efectúan cargos por recursos informáticos si el servidor de recuperación no está activo.

Quién necesita Protección contra desastres?

- Empresas que:
- Se basen en aplicaciones y datos de misión crítica.
 - Están sujetas a requisitos de cumplimiento regulados.
 - Son socias en cadenas de suministro rigurosas.
 - Están ubicadas en áreas propensas a desastres
 - Carecen de recursos técnicos.
 - Tienen una gran dependencia de TI para funciones de negocios
 - Falta experiencia en recuperación de desastres



Encriptación Cifrado AES-256

¿En qué consiste?

Advanced Encryption Standard (AES), también conocido como Rijndael (pronunciado Rain Doll en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.

La privacidad y la seguridad son dos de las principales razones para usar un servicio VPN para navegar por Internet. Pero no todas las VPN son creadas igual – diferentes proveedores utilizan diferentes estándares de cifrado que ofrecen distintos niveles de seguridad. Si tú te tomas en serio mantener tus hábitos de navegación y tus datos confidenciales en privado la elección de un proveedor de VPN con los mejores estándares de encriptación disponibles es crítico.

El VPN utiliza el algoritmo de cifrado AES-256 para proteger todo el tráfico que pasa por nuestros servidores. Uno de los protocolos de cifrado más avanzado disponible, AES-256, te ofrece la tranquilidad y el máximo nivel de seguridad posible.



Tu información es impenetrable

El AES es uno de los algoritmos más populares usados en criptografía simétrica.

Se transformó en un estándar efectivo el 26 de mayo de 2002.

Características

Extremadamente rápido.
Imposible de descifrar incluso si los servidores son hackeados.
No disminuye el rendimiento de tus equipos.
Protección completa en la nube
Fácil acceso



fig.1

Características esenciales

¿Qué tan seguro es AES?

Tiene un solo ataque exitoso registrado en 2011, realizado por un grupo de investigadores de Microsoft y de la Dutch Katholieke Universiteit Leuven. No es vulnerable al criptoanálisis diferencial y lineal. Es necesaria una gran cantidad de textos encriptados y gran procesamiento para su análisis.

Según investigadores, para romper el cifrado AES se necesitan un billón de ordenadores y que cada uno pueda probar mil millones de claves por segundo. Y unos 2000 millones de años para dar con un AES-128. Teniendo en cuenta que las máquinas actuales sólo pueden probar 10 millones de claves por segundo.

¿Cómo funciona el cifrado AES?

Cifrado Básico 1: Es una buena idea ocultar la relación entre tu mensaje real y tu mensaje "cifrado". Un ejemplo de esta confusión es el viejo y fiel "Cifrado del César": en claro: T T A C K A T D A W N ↓ cifrado: A ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ D W W D F N D W G D Z Q A + 3 letras = D

- Cifrado AES AES es un algoritmo de cifrado por bloques, los datos se dividen en segmento de 16 bytes (128 bits), y cada segmento se puede ver como un bloque o matriz de 4x4 a la que se llama estado. AE 03 1F 2A 1E 3F 01 7A 21 04 CF Bloque de 128 bits AE 1E 21 1C 03 3F 04 33 1F 1 CF 11 2A 7A 7A 27 Matriz de Estado 7A 1C 33 11 27

- En la ronda inicial calculo una OR-Exclusiva (XOR) de cada byte con el correspondiente de la clave para la primera ronda. AddRoundKey Estado Clave inicial 32 88 31 E0 2B 28 AB 09 19 A0 9A E9 43 5A 31 37 7E AE F7 CF 3D F4 C6 F8 E3 E2 8D 48 BE 2B 2A 08 F6 30 98 7 A8 8D A2 34 X O R 15 D2 15 4F 16 A6 88 3C =

- De ahí, necesito muchas claves para usarlas en rondas posteriores. Derivo todas ellas a partir de la clave inicial usando una técnica sencilla llamada SubBytes. Clave de 128 bits 2B 28 AB 09 7E AE F7 CF 15 D2 15 4F 16 A6 88 3C

- Para calcular la primera columna de la siguiente clave se aplica una operación llamada Rotword, que consiste en realizar una rotación del primer byte hacia el último lugar en la columna. 09 CF CF 4F → 4F 3C 3C 09.

- Para obtener la transformación S-Box de un byte se toman los primeros 4 bits como el índice de la fila de la tabla y los segundos 4 como índice de la columna de la tabla: Resultado después de la transformación S-Box CF 8A 4F 84 → 3C EB 09 01.

- Entonces, se hace XOR de la columna con una "Constante de Ronda" (RCON) que es diferente para cada ronda. RCON 01 02 04 08 10 20 40 80 1B 35 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 El resultado de esta operación será la primera columna de la siguiente clave: 2B 8A 01 A0 7E 84 00 FA XOR XOR = 15 EB 00 FE 16 1 00 17.



- De ahí, necesito muchas claves para usarlas en rondas posteriores. Derivo todas ellas a partir de la clave inicial usando una técnica sencilla llamada SubBytes. Clave de 128 bits 2B 28 AB 09 7E AE F7 CF 15 D2 15 4F 16 A6 88 3C

- Para calcular la primera columna de la siguiente clave, se aplica una operación llamada Rotword, que consiste en realizar una rotación del primer byte hacia el último lugar en la columna. 09 CF CF 4F → 4F 3C 3C 09.

- Para obtener la transformación S-Box de un byte se toman los primeros 4 bits como el índice de la fila de la tabla y los segundos 4 como índice de la columna de la tabla: Resultado después de la transformación S-Box CF 8A 4F 84 → 3C EB 09 01.

- Entonces, se hace XOR de la columna con una "Constante de Ronda" (RCON) que es diferente para cada ronda. RCON 01 02 04 08 10 20 40 80 1B 35 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 El resultado de esta operación será la primera columna de la siguiente clave: 2B 8A 01 A0 7E 84 00 FA XOR XOR = 15 EB 00 FE 16 1 00 17.

- Las otras columnas son más fáciles. Solamente se hace un XOR de la columna anterior con la misma columna de la clave de la ronda previa: 28 A0 88 AE FA 54 XOR = D2 FE 2C A6 17 B1 A0 88 23 2A FA 54 A3 6C FE 2C 39 76 17 B1 39 05 Clave de la primera ronda.

- Luego, se empieza con las rondas intermedias. Una ronda es simplemente una serie de pasos que se repite varias veces. El número de repeticiones depende del tamaño de la clave

- Para ocultar la relación de cada byte, se usa la transformación S-BOX, que lo traducirá a un byte diferente. 19 A0 9A E9 D4 E0 B8 1E 3D F4 C6 F8 27 BF B4 41 E3 E2 8D 48 11 98 5D 52 BE 2B 2A 08 AE F1 E0 30 SBOX Luego desplazo las filas hacia la izquierda usando "Shift Rows". D4 B8 27 BF B4 41 11 AE E0 98 5D 52 F1 E0 30 ↓ D4 E0 B8 1E BF B4 41 27 5D 52 11 98 30 AE F1 E0 1E

- A cada columna del estado se le aplica una transformación lineal, esto es multiplicarlo por una matriz predeterminada en el campo GF. A este proceso se le conoce como MixColumns: 02 03 01 01 01 02 03 01 01 01 02 03 03 01 01 02 D4 X BF 5D 30 04 = 66 81 E5.

- Al final de cada ronda, se aplica un XOR, a la clave resultante, con la primera clave de la ronda. En la ronda final, se salta el proceso de MixColumns, ya que no incrementará la seguridad, solamente ralentiza el proceso. Determinar el número de rondas, siempre implica varios compromisos.

"La seguridad siempre implica un coste en rendimiento."

-Vicent Rijmen.



Copia Híbrida

Protege tu entorno de nube híbrida es fácil. Simplemente instala Copia de seguridad, basada en web consola en un servidor Windows® o Linux®, PC, máquina virtual o instancia en la nube.

Agrega los dispositivos que deseas proteger a la consola, desplegando agentes a locales o sistemas físicos remotos, máquinas virtuales e instancias de la nube. También puede proporcionar agentes de nivel de hipervisor para VMware vSphere® y Microsoft Hyper-V®.

Después de la instalación, programa tus copias de seguridad y selecciona tus destinos de almacenamiento:

- Discos locales para una rápida recuperación.
- Discos de red para backup de centrales u oficinas remotas.
- Clouds7 Storage para seguridad de almacenamiento de sitio y copia de seguridad de su nube, así como usuarios remotos. Los dispositivos de cinta también son compatibles. Puedes establecer tu política de retención, hacer copias de seguridad a múltiples ubicaciones y habilitar el cifrado, para mayor seguridad y tranquilidad.

Gestión

Incluso una pequeña empresa puede tener más de cien dispositivos con datos críticos y la copia de seguridad con herramientas tradicionales puede ser un reto, Copia Híbrida de clouds7 incluye tableros personalizables, avanzados informes, políticas de copia de seguridad y más características para ayudarte a proteger tu crecimiento.

Ambiente sin esfuerzo extra. Puede delegar la gestión de forma remota a oficinas y administradores locales y reducir aún más la carga.



47%

De las compañías son atacadas por ransomware

68%

De las compañías usan copias de seguridad híbridas.

+21

Plataformas soportadas

+500.000

Compañías que usan esta tecnología para proteger sus datos y sistemas.

Recuperación del sistema

Cuando se trata de recuperación clouds7 es la solución más completa disponible.

Clouds7 Universal Restore no sólo restaura tu copia de seguridad en el mismo hardware, si no también en un hardware diferente, incluyendo diferentes hipervisores, máquinas físicas, o nubes públicas, tales como Microsoft Azure® y Amazon EC2®.

Además de recuperar máquinas virtuales, también puede recuperar todo VMware y Hyper-V hipervisor hosts.

Recuperación de archivos

Si necesita restaurar un solo archivo o carpeta, clouds7 hace que sea fácil de navegar.

Copia de seguridad ubica el archivo deseado o expediente. Para resultados aún más rápidos, puedes buscar los contenidos para el archivo específico o carpeta que deseas recuperar.

Application Item Recovery

Si tus sistemas incluyen aplicaciones, como Microsoft Exchange®, clouds7 creará copias de seguridad conscientes de la aplicación que siguen pautas del usuario tales como truncamiento registros de transacciones y el ahorro necesario metadatos. Esto permite restaurar artículos de la aplicación de forma individual más adelante, incluyendo:

- Buzones de correo de Microsoft Exchange®, carpetas y correos electrónicos
- Bases de datos Microsoft SQL®.
- Documentos de Microsoft SharePoint®.
- Buzones de correo de Microsoft Office 365® y correos electrónicos.
- Bases de datos Oracle®, espacios de tabla, y registros, entre otros.



Sistemas soportados

- Windows Server® 2016, 2012/2012 R2, 2008/2008 R2*
- Windows Small Business Server 2011, 2008
- Windows MultiPoint Server 2012, 2011, 2010
- Windows Storage Server 2012/2012 R2, 2008/2008 R2
- Windows 10, 8.1, 8, 7
- Linux x86_64 con kernel

Microsoft Windows

- Windows Server 2016, 2012 R2, 2012, 2008 R2, 2008, 2003 R2, 2003*
- Windows Small Business Server 2011, 2008, 2003 R2, 2003
- Windows MultiPoint Server 2012, 2011, 2010
- Windows Storage Server 2012 R2, 2012, 2008 R2, 2008, 2003
- Windows 10, 8.1, 8, 7, Vista, XP SP3

Linux

- Linux with kernel from 2.6.9 to 4.9 and glibc 2.3.4 o posterior
- Various 32-bit (x86) and 64-bit (x86_64) Linux distributions including:
 - Red Hat® Enterprise Linux 4.x - 7.3
 - Ubuntu® 9.10 - 16.04
 - Fedora® 11 - 23
 - SUSE® Linux Enterprise Server 10 - 12*
 - Debian® 4 - 8.5
 - CentOS® 5.x - 7.3
 - CloudLinux 7, 7.1
 - ClearOS 5.x, 6.x, 7, 7.1
 - Oracle Linux 5.x - 7.3 (incluyendo UEK)

Exploradores web

- Google Chrome® 29 or later
- Mozilla Firefox® 23 or later
- Opera 16 or later
- Windows Internet Explorer® 10 or later
- Microsoft Edge® 25 or later
- Safari® 8 or later (running in Apple OS X and iOS)

Mac OS X / macOS

- OS X 10.08 o posterior

Sistemas móviles

- iOS 8 o posterior
- Android® 4.1 o posterior

Hypervisors

- VMware vSphere ESX(i) 6.5, 6.0, 5.5, 5.1, 5.0, 4.1, including vSphere Hypervisor (free ESXi)*
- Microsoft Hyper-V Server 2016, 2012 R2, 2012, 2008 R2, 2008
- Microsoft Windows Server 2016, 2012 R2, 2012, 2008 R2, 2008 con Hyper-V
- Microsoft Windows 10, 8.1, 8 (x64) con Hyper-V
- Citrix XenServer® 4.1-6.5*
- Red Hat Virtualization 2.2-4.0
- Linux KVM
- Oracle VM Server 3.0-3.3

Aplicaciones

- Oracle Database 12, 11*
- Microsoft Exchange Online
- Microsoft Exchange Server 2016, 2013, 2010, 2007 – Incluyendo configuraciones de cluster
- Microsoft SQL Server® 2016, 2014, 2012, 2008 R2, 2008, 2005 – Incluyendo configuraciones de cluster
- Microsoft SharePoint 2013, 2010 SP1, 2007 SP2, 3.0 SP2

Almacenamiento

- Discos locales– SATA, SCSI, IDE, RAID
- Networked storage devices – SMB, NFS, iSCSI, FC
- Dispositivos móviles– ZIP®, Rev®, RDX®, etc.
- Discos externos y SSDs – USB 3.0/2.0/1.1 and IEEE1394 (Firewire)
- Unidades de cinta, cargadores automáticos y bibliotecas, incluye gestión de medios y código de barras.
- Almacenamiento en clouds7

Sistemas de archivos

- FAT16/32
- NTFS
- HFS+ *
- ReFS *
- ext2/ext3/ext4
- ReiserFS3, ReiserFS4 *
- XFS *
- JFS *
- Linux SWAP

Cloud

- Office 365mailboxes
- Amazon Web Services EC2 Instances
- Microsoft Azure VMs

Cifrado de canal SSL 2048

Seguridad absoluta

Cuando se trata de hacer una copia de seguridad de tus datos quieres tener el control. La mayoría de hemos escuchado que los datos pueden ser filtrados, accidentalmente o no, o pueden ser obtenidos ilegalmente por criminales que quieren explotarlos. En clouds7 entendemos que pueden tener esta preocupación, por eso ponemos todos los controles a tu disposición y podemos asegurarte que nuestra infraestructura para sus datos es muy segura. Incluso si tus datos son interceptados, utilizamos mecanismos para hacer tales intentos. Esto se logra principalmente mediante el uso de cifrado de datos y un canal seguro para ellos.



Tus datos totalmente asegurados

Con clouds7 puedes estar seguro de que tus datos no serán accedidos por alguien que no debería tener acceso.

Puede encriptar datos en el dispositivo y enviarlos con un cifrado de forma segura a la nube mediante un canal seguro. Estos datos en la nube serán adicionalmente asegurados a través de una estricta política de seguridad del centro de datos.



Restaura fácilmente cualquier archivo afectado

Dos días es el período de inactividad que causa en promedio en las empresas.

Tras bloquear el ataque de ransomware clouds7 te ayudará a restaurar cualquier archivo que pueda haber quedado alterado o infectado. Nuestra herramienta busca la versión del archivo más reciente y puede recuperar copias intactas a partir de la caché, los archivos temporales o la copia de seguridad. Al realizar automáticamente una copia de seguridad de tu carpeta Documentos en el cloud cada cinco minutos, la Protección contra ransomware de clouds7 logra salvaguardar tus archivos más importantes y ofrecerte una protección única de dos capas.

El Ransomware, también conocido como Rogueware o Scareware, restringe el acceso a su sistema y datos cifrándolos para exigir el pago de un rescate y así devolver su información a la normalidad (cosa que en el 92% de los casos nunca resulta positiva). Los ataques más peligrosos los han causado Ransomware como NotPetya, Jaff, GandCrab, GoldenEye, WannaCry, CryptoLocker, Locky, Petya, Crysis, zCrypt, PowerWare, HydraCrypt, Cerber, RAA ransomware, CryptoWall, KeRanger, LeChiffre, Spider, TeslaCrypt, TorrentLocker, ZCryptor, Dharma.

Protege el equipo contra el ransomware

Ransomware es malware del equipo que restringe el acceso al equipo (o incluso te impide que lo uses) o cifra tus archivos. A continuación, intenta obligarte a que pagues dinero (un rescate) para recuperar el acceso a él.

Entre las formas en las que ransomware puede infectarte se incluyen las siguientes: Visitar sitios web falsos, no seguros o sospechosos. Abrir correos electrónicos y datos adjuntos de correos electrónicos que no esperas o de personas que no conoces, abrir vínculos incorrectos o malintencionados de correos electrónicos, Facebook, Twitter y otras publicaciones de redes sociales, o en los chats de mensajería instantánea, como Skype.

A menudo puedes reconocer un correo electrónico y una página web porque la ortografía es incorrecta, o simplemente su aspecto es inusual. Presta atención a si hay nombres de empresas escritos de forma extraña (por ejemplo, "PayePal" en lugar de "PayPal") o espacios, símbolos o signos de puntuación inusuales (como "Servicio de atención al cliente de iTunes" en lugar de "Servicio de atención al cliente de iTunes"). El ransomware puede dirigirse a cualquier equipo, equipo doméstico, equipos en una red de empresa o servidores que usa un organismo gubernamental.

¿Cómo reconocer el ransomware?

Es obvio cuando su dispositivo ha sido infectado con ransomware, ya que probablemente no podrás acceder a él.

¿De dónde procede el ransomware?

El ransomware lo crean estafadores con un gran conocimiento en programación informática. Puede entrar en tu PC mediante un adjunto de correo electrónico o a través de tu navegador si visita una página web infectada con este tipo de malware. También puede acceder a tu PC a través de su red.

¿Cómo evitar el ransomware?

Asegúrate de que todo el software de tu equipo está actualizado, incluyendo su sistema operativo, su navegador y cualquier complemento de barra de herramientas que utilice.

Asegúrate de que su software antivirus y tu protección cortafuegos están actualizados.

Haz respaldos de toda tu información con Clouds7 backup cloud, en tu caso de un ataque puedes recuperar toda tu información sin necesidad de pagar el rescate por ella.

Sincronización de Archivos

¿En qué consiste?

Proporciona a oficinas y usuarios móviles funciones de acceso seguro, sincronización y uso compartido en una solución sencilla, completa y fiable, alojada en la nube. Sincronización de Archivos de clouds7 permite trabajar con el contenido que necesite independientemente de su ubicación y del dispositivo que utilicen: smartphone, tablet, portátil, PC o Mac®. Gracias a Sincronización de Archivos de clouds7, podrá incrementar la productividad de tus empleados, mejorar el servicio al cliente, atraer clientes nuevos y aumentar tus ingresos.

¿Por qué elegir clouds7 para sincronizar tus archivos?

Es la única solución de sincronización y uso compartido de archivos (FSS) que a la vez ofrece la seguridad y la privacidad que exigas para sus datos.

Contenido siempre disponible

Permite a los empleados autorizados acceder, sincronizar y compartir contenido que reside en los servidores, archivos corporativos, SharePoint®, dispositivos NAS (Network Attached Storage) y servicios de interoperabilidad de gestión de contenido (CMIS), como Alfresco® y EMC® Documentum®, utilizando cualquier dispositivo: smartphones iPhone®, Windows® o Android®, tablets, portátiles, PC o Mac®.



Cientes compatibles

- iPad 2 y posteriores
- iPhone 4S y posteriores (iOS 11 o superior)
- Teléfonos y tablets Android (Android 4.1 o superior)
- Windows: 7, 8, 8.1, 10
- Mac OS X 10.6.8 y superiores
- Navegadores web: Firefox®, Internet Explorer, Google® Chrome y Safari®

Servidores compatibles

- Windows Server® 2008, 2012 y 2016
- Plataforma de servidor Intel®/AMD
- Compatibilidad con entornos de virtualización

Edición web mediante Microsoft Office Online

Advanced incluye ahora una opción para permitir a los usuarios ver, editar y crear archivos de Office mediante editores web de Microsoft Office Online. Microsoft Office Online puede ejecutarse también in situ con Office Online Server.

Más posibilidades de colaboración y control

Los usuarios tienen más flexibilidad y control sobre el material compartido. El departamento de TI puede definir directivas con relación al tipo, tamaño y propiedades.

Anotación y edición seguras en la app

Los usuarios pueden crear y editar documentos de Office e incluir anotaciones en los archivos PDF desde la aplicación móvil de Clouds7 File Advanced, lo que convierte el dispositivo móvil en una verdadera plataforma empresarial.

Previsualización web segura

Los usuarios disponen de una vista más rápida y segura de los archivos importantes y confidenciales mediante sus navegadores web autorizados, sin necesidad de descargar antes el documento. Se trata de una función imprescindible para las empresas que deben cumplir directivas de seguridad y normativas exigentes.

Seguridad y control avanzados

El motor de archivos de clouds7 proporciona funciones de administración granular para crear directivas de seguridad y garantiza el control y el cumplimiento de las normativas sobre contenido, usuarios y dispositivos.

Seguimiento y pistas de auditoría

Clouds7 Files Advanced proporciona una pista de auditoría y un historial de categoría empresarial de todas las transacciones, con funciones de búsqueda, filtrado y exportación, lo que permite al equipo de TI ver las actividades de los usuarios, los documentos a los que acceden y con quién los comparten.

Cifrado

Cifrado inalámbrico o en el dispositivo, incluido cifrado certificado con FIPS 140-2 para iOS.

Interfaces fáciles de utilizar

Una interfaz de usuario intuitiva y moderna fácil de utilizar y natural para los empleados. Además, prácticamente no requiere formación.

