# Protéjase del Ransomware de Encripción


Synology

Neogénesys

## Que es Ransomware

**El riesgo de sufrir de infección de malware se mantiene en constante aumento con nuevas infecciones que se extienden rápidamente cada hora y cada día. Synology y Neogénesys hacen frente a este creciente problema de malware introduciendo potentes medidas de seguridad, como Security Advisor y Qualysguard Security Scan, así como ofreciendo regularmente actualizaciones de seguridad para proteger a los usuarios de posibles amenazas. A continuación explicamos cómo la completa solución de copia de seguridad multiversión de Synology puede recuperar su PC y su servidor NAS tras un ataque malicioso.**

# ¿Qué es un ransomware de cifrado?

El ransomware de cifrado, como CryptoWall, CryptoLocker y TorrentLocker, cifra los archivos almacenados en ordenadores e incluso en unidades de red. Una vez infectado, solo le queda la opción de pagar el rescate para recuperar el acceso a sus archivos o renunciar a los preciados datos que tuviera almacenados en el ordenador o en el dispositivo de almacenamiento.

## Prácticas cruciales contra los ataques de ransomware en sus equipos y servidores

### Actualice su Sistema Operativo

Los sistemas informáticos anticuados son relativamente más vulnerables a los ataques de ransomware. Por eso es fundamental actualizar regularmente el software y el sistema operativo para mejorar la seguridad de su ordenador.

### Instale un conjunto de seguridad respetable

Instale un buen software antivirus y un conjunto de seguridad respetable que le ayude a detectar y luchar contra las amenazas maliciosas, de forma que disfrute de una protección adicional.

### Evite archivos sospechosos

Manténgase alerta y piense dos veces antes de abrir adjuntos de correo o de hacer clic en archivos de fuentes desconocidas. Tenga cuidado con archivos sospechosos con extensiones de archivo ocultas como ".pdf.exe"

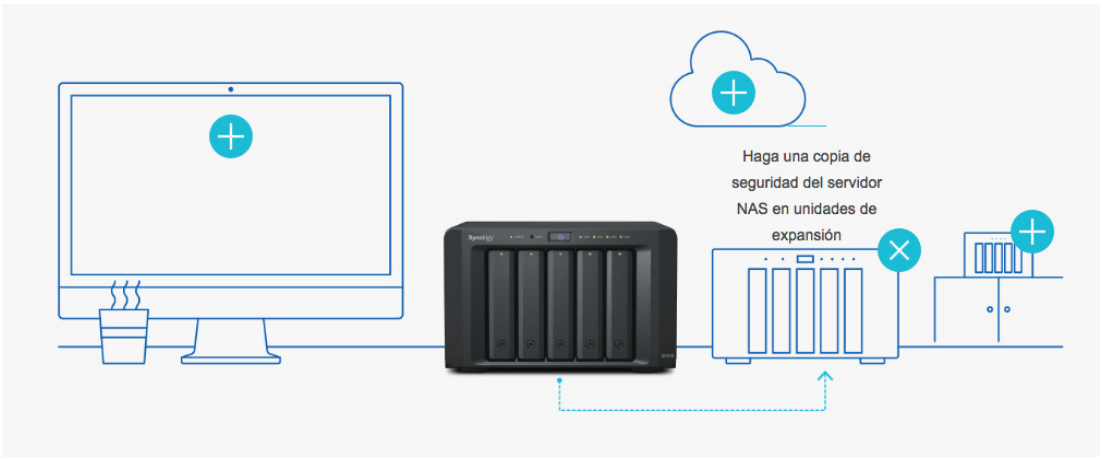
### Deshabilite el acceso remoto

Con frecuencia el malware va dirigido a ordenadores que utilizan el protocolo de escritorio remoto (RDP, Remote Desktop Protocol). Mantenga el protocolo RDP deshabilitado si no necesita el acceso remoto. Lo mismo aplica para aplicaciones que dan acceso remoto a sus equipos o servidores. En ocasiones este punto no es posible, ya que este es el método de acceso por excelencia por empresas de todo tamaño y giro. Si no hay manera de des-habilitar este servicio, cambie el puerto por default (3389) por alguno otro de su elección y establezca esquemas de seguridad y privacidad de usuarios y passwords en la medida de lo posible. Si usa una aplicación como TSPlus para el acceso remoto, le recomendamos implementar el esquema de acceso basado en el Módulo Gateway, que permite la autentificación de sesión sin exponer a la internet los servidores de aplicaciones TPSPlus o similar logrando un aislamiento de los mismos.

Si necesita mayor información, consulte tsplus.mx o envíenos un correo para que le expliquemos cómo implementar el Gateway como protección del acceso remoto TSPlus.

# Copia de seguridad multiversión: su mejor arma contra el ransomware

El ransomware de cifrado se está volviendo más sofisticado y puede que no sea detectado a tiempo por el software antimalware. Una vez infectado, no podrá acceder a sus propios datos y además, no tendrá ninguna garantía de poder recuperarlos, incluso después de pagar el rescate. Es muy recomendable realizar copias de seguridad regulares para poder restaurar los archivos infectados y minimizar los daños. Utilice la copia de seguridad multiversión, una robusta solución de copia de seguridad que le permite restaurar versiones anteriores de los datos infectados.



# Haga una copia de seguridad de los datos de su PC en el servidor NAS

El hecho de tener una copia de seguridad de sus datos le evitará tener que pagar un rescate para poder acceder a sus propios datos. Cree una copia de seguridad multiversión para poder restaurar los datos rápidamente. Synology Cloud StationBackup es la solución perfecta para hacer una copia de seguridad de los datos almacenados en su ordenador en los servidores Synology NAS. Puede almacenar hasta 32 versiones históricas de un único archivo, lo que le permitirá restaurar los archivos en un estado anterior. Más información sobre Cloud StationBackup

# Guarde una copia de seguridad de los datos del servidor NAS en otros destinos

Es posible que la copia de seguridad local no sea suficiente en caso de que un ataque de ransomware más destructivo comparta carpetas de su servidor NAS accediendo a los servicios de archivos de su PC. La mejor forma de evitar esto consiste en añadir otro nivel de protección más: tener las versiones de copia de seguridad no infectadas almacenadas en una ubicación fuera de las instalaciones. Si es víctima de un ataque de ransomware, podrá seguir accediendo a los datos almacenados en otras ubicaciones.

Con los equipos Synology usted podrá almacenar dichas copias en otros servicios de almacenamiento en la nube como Google Drive, Drop Box, etc. Y con esto incrementar la seguridad y recuperación de sus datos y archivos.

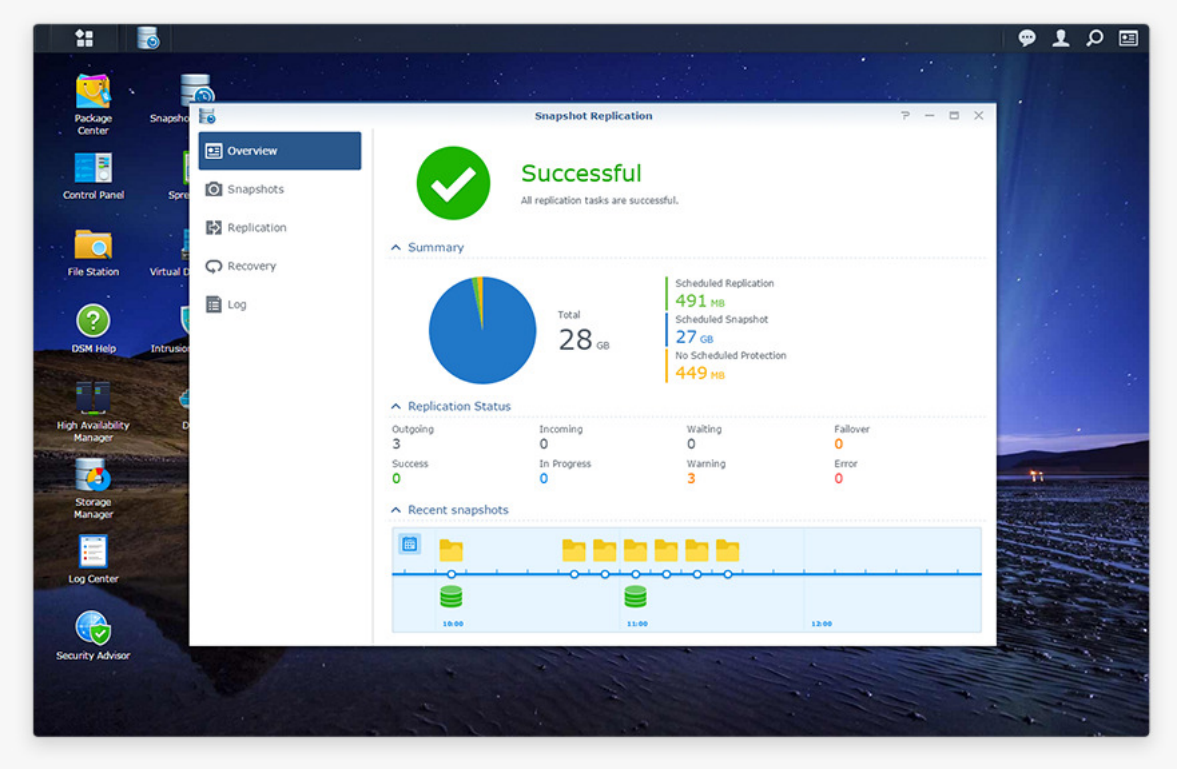
# HyperBackup

HyperBackup le permite disfrutar de una amplia variedad de destinos de copia de seguridad multiversión: carpetas compartidas locales, unidades de expansión, discos duros externos, carpetas compartidas de red, servidor rsync y servicios de nube pública.

HyperBackup también ofrece una sólida protección de la copia de seguridad local. Puede aislar los datos de las amenazas de Internet configurando en su PC los privilegios de acceso a determinadas carpetas compartidas de Synology NAS para evitar que alguien externo acceda a los datos de copia de seguridad críticos almacenados en la carpeta compartida de su servidor NAS. Más información sobre HyperBackup

# SnapshotReplication

El vanguardista sistema de archivos Btrfs admite la tecnología de copia de seguridad de última generación en determinados modelos de servidor NAS. SnapshotReplication le permite replicar los datos de un sitio principal en una ubicación fuera de las instalaciones con una frecuencia máxima de 5 minutos y 15 minutos para LUN, lo que garantiza que todos sus datos críticos en carpetas compartidas y máquinas virtuales en iSCSILUNs se puedan recuperar rápidamente en caso de desastre. Obtenga más información sobre SnapshotReplication




Permítanos ayudarle a implementar una solución Preventiva de ésta situación ANTES de que sea Demasiado Tarde!