

# QNAP NAS

Manual de seguridad de la información




QNAP SYSTEMS, INC.

Gracias por utilizar productos de QNAP y por confiar sus datos a NAS QNAP para su protección. Agradecemos su apoyo y consideramos que la confianza que ha depositado en nosotros es nuestro activo más valioso. A este respecto, nos esforzamos en alcanzar la perfección mejorando constantemente nuestros productos y nuestra seguridad.

En el mundo actual, con un creciente número de ataques, malware y problemas de seguridad, sentimos la necesidad de proporcionarle la siguiente información con el fin de ayudarlo a que se defienda proactivamente y a que defienda sus activos digitales. Esperamos que la combinación de los consejos que aparecen en esta guía con unos hábitos de uso sensible de las TI, todos nuestros usuarios puedan defender sus dispositivos y datos ante las amenazas actuales y futuras.

QNAP Systems, Inc.



Director general

[www.qnap.com](http://www.qnap.com)

## Prácticas recomendadas para mejorar la seguridad

Los métodos de protección de datos intentan constantemente seguir el ritmo de la evolución de las técnicas de hackeo. Para mantener protegidos sus datos y sus dispositivos, los usuarios de NAS disponen de numerosas herramientas, como protección con contraseña, configuración de permisos, cifrado de nivel de archivos, actualizaciones del sistema operativo y del software, configuración de conexión de red y aplicaciones para la copia de seguridad de datos y recuperación ante desastres. Los productos de QNAP disponen de robustas características de seguridad de la información con múltiples facetas. A continuación se indican nueve (9) puntos de seguridad de la información para ayudar a que nuestros usuarios comprendan rápidamente la seguridad de la información.

1. Elimine cuentas de usuarios desconocidas o sospechosas
2. Elimine aplicaciones de NAS desconocidas o de uso poco frecuente
3. Deshabilite la configuración automática del router en myQNAPcloud
4. Configure controles de acceso a dispositivos
5. No divulgue el número de puerto predeterminado en Internet
6. Instale y ejecute la versión más reciente del Malware Remover
7. Cambie periódicamente las contraseñas de todas las cuentas de usuario
8. Actualice las aplicaciones instaladas a la versión más reciente
9. Asegúrese de que el sistema operativo y el software del sistema de sus dispositivos conectados en red siempre están actualizados

Más adelante explicaremos los distintos diseños de seguridad de la información de QNAP, de uno en uno, y elaboraremos un plan de defensa del NAS más completo.

## Utilice contraseñas complejas

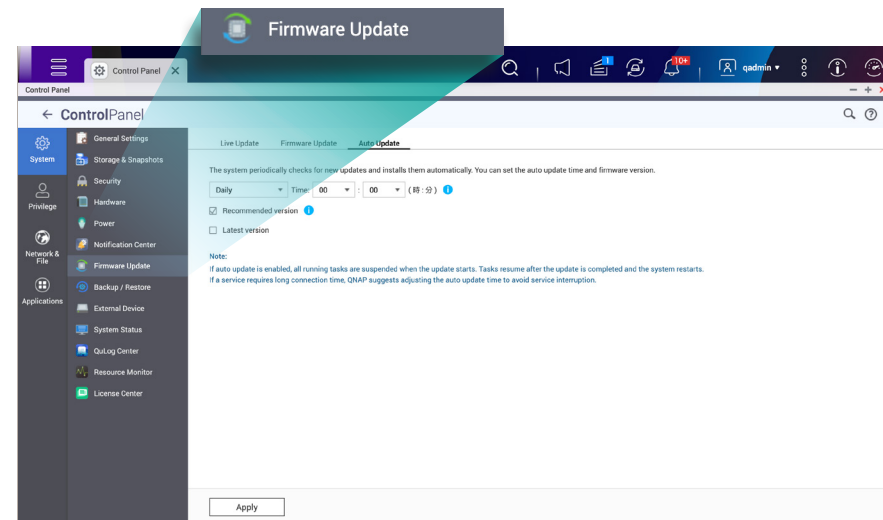
Tratar de acceder a la cuenta de un usuario es el vector de ataque más usado por los hackers. Suelen intentarlo probando con las contraseñas predeterminadas o con las frecuentes, o bien utilizando técnicas de ingeniería social (por ejemplo, si alguien usa el nombre de su hijo o de su mascota como contraseña, otra persona podría adivinarlo). Para mitigar la amenaza que supone poner en riesgo una cuenta de usuario, recomendamos desactivar la cuenta de administración predeterminada y exigir a todos los usuarios que definan contraseñas complejas como se describe a continuación.

Condición	Descripción
Letras del alfabeto latino	Incluya una mezcla de caracteres en mayúsculas y en minúsculas
Números	Incluya al menos un número
Caracteres especiales	Incluya al menos un carácter especial (como <ADD SPECIAL CHARACTERS HERE>)
Evitar repetición	No use caracteres repetidos (como AAA o 111)
Excluir nombre de usuario	No use el nombre de usuario en ningún lugar de la contraseña, ni siquiera escrito en orden inverso. Por ejemplo, si el nombre de usuario es: usuario1 y la contraseña es: 1oirausu.
Longitud mínima	Se recomienda usar una contraseña de al menos 8 caracteres. La longitud máxima de una contraseña es 64 caracteres.

Además de usar contraseñas complejas, los usuarios también deberían cambiarlas periódicamente. Puede especificar en la configuración del sistema el número de días que es válida la contraseña de un usuario.

## Las actualizaciones de software son importantes

Ejecutar un software desfasado en el NAS y en otros dispositivos conectados en red pone en riesgo a toda la red. El equipo de desarrollo de QNAP monitoriza activamente y corrige potenciales vulnerabilidades para la seguridad tan pronto como se descubren, y publica actualizaciones para el sistema operativo y las aplicaciones lo antes posible. Recomendamos que los usuarios mantengan actualizadas sus aplicaciones en el Centro de aplicaciones, además de que activen las actualizaciones automáticas en la sección Actualización de firmware del sistema QTS. El sitio web de QNAP contiene Notas de la versión con información sobre las correcciones y mejoras realizadas en las nuevas versiones de software.

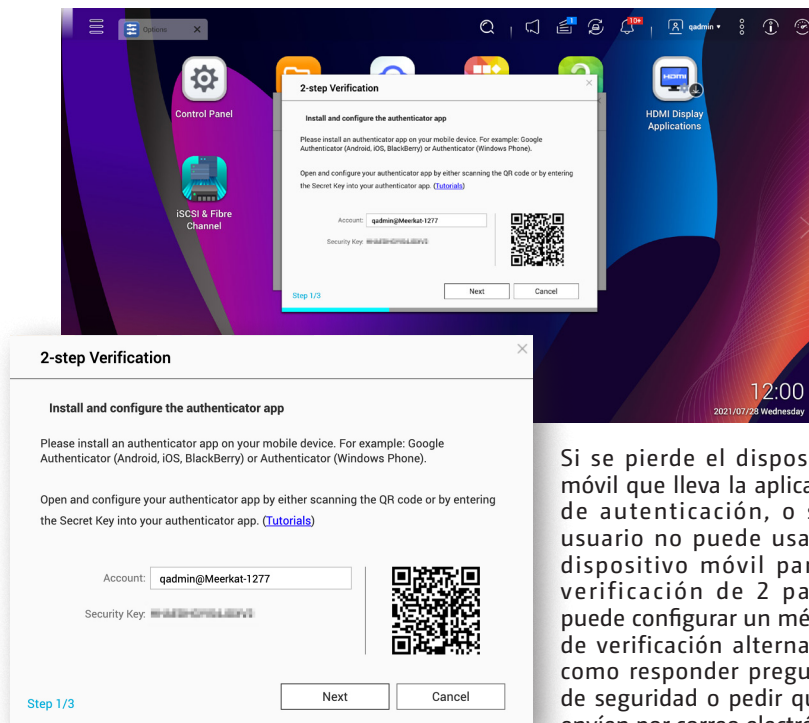


A partir de QTS 4.5.3, el Centro de aplicaciones actualiza automáticamente las aplicaciones con las nuevas versiones de forma predeterminada (los NAS que no se pueden actualizar más allá de QTS 4.5.3 pueden activar las actualizaciones automáticas con la interfaz de consola). Si su NAS no está conectado a Internet, puede descargar actualizaciones desde el Centro de descargas de QNAP e instalarlas manualmente en el NAS.

## Habilite la verificación de 2 pasos

La verificación de 2 pasos aumenta en gran medida la seguridad de las cuentas de usuario. Cuando está habilitada, se le pedirá a los usuarios que introduzca un código desde una aplicación de autenticación en sus dispositivos móviles para poder iniciar sesión en sus cuentas. Esto añade seguridad en las cuentas de usuarios que puede reducir en gran medida el potencial que tienen los hackers para acceder de forma ilegítima a las cuentas de los usuarios.

Para usar la verificación de 2 pasos, debe instalar una aplicación de verificación en su dispositivo móvil. Esta aplicación deberá usar un algoritmo TOTP (contraseña para una sola vez válida por tiempo limitado) para crear un servicio de autenticación. QTS admite Google Authenticator (Android, iOS y BlackBerry) y Authenticator (Windows Phone) para la verificación de 2 pasos.



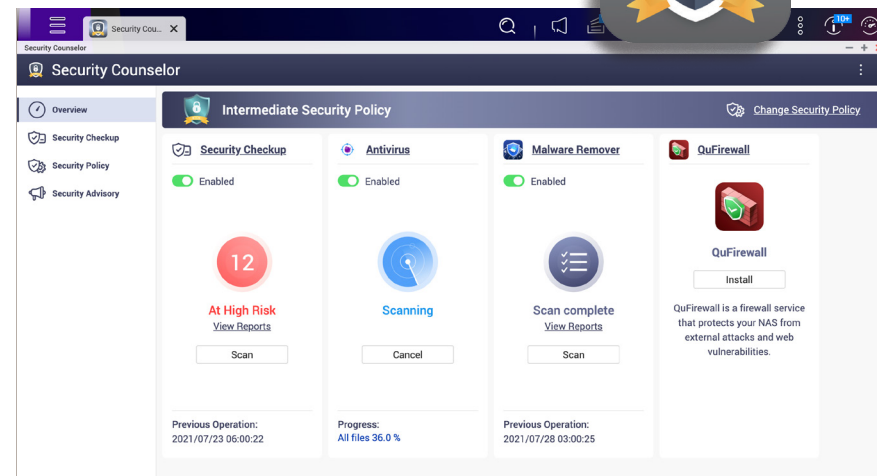
Si se pierde el dispositivo móvil que lleva la aplicación de autenticación, o si el usuario no puede usar un dispositivo móvil para la verificación de 2 pasos, puede configurar un método de verificación alternativo, como responder preguntas de seguridad o pedir que le envíen por correo electrónico un código de seguridad.

## Permítanos que evaluemos su seguridad

Existen riesgos para la seguridad inherentes al conectar cualquier dispositivo a Internet; por ello QNAP proporciona la aplicación Security Counselor. Esta aplicación audita las posibles vulnerabilidades de seguridad de su NAS y proporciona recomendaciones para realizar ajustes en la configuración del sistema con el fin de evitar que se ponga en riesgo el NAS.

En Security Counselor, puede especificar diferentes recomendaciones del nivel de seguridad en función de sus requisitos de uso del NAS. Se pueden efectuar análisis siguiendo un programa. También se puede ajustar otra configuración, como el bloqueo de IP, las credenciales de seguridad y políticas de contraseñas.

### Security Counselor

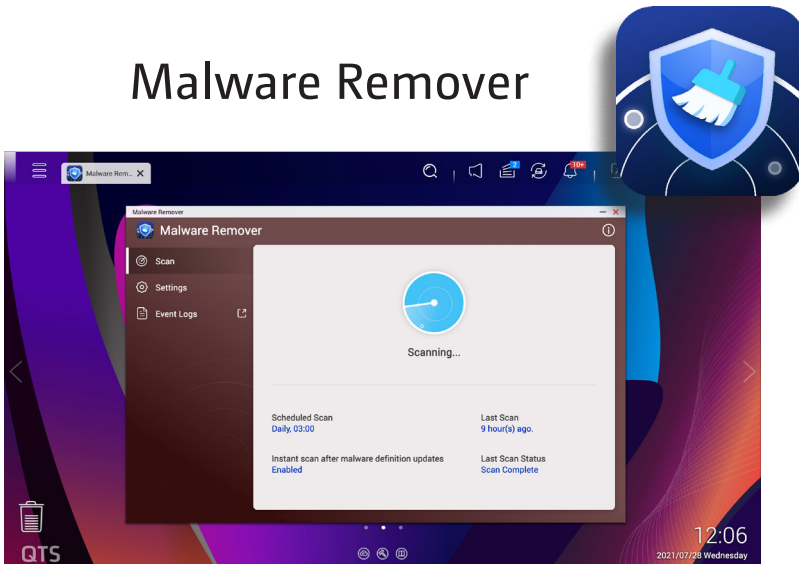




## Elimine amenazas al instante

Los análisis periódicos pueden ayudar a comprobar si el NAS ha sido afectado por malware, eliminándose el malware detectado. Malware Remover también descarga automáticamente las definiciones de malware más recientes para ofrecerle la máxima protección frente a las amenazas de malware nuevas y emergentes.

### Malware Remover



También puede configurar el envío de los resultados del análisis de Malware Remover a QNAP, para que así podamos actualizar nuestras definiciones de malware y ayudar a fortalecer la seguridad de todos los usuarios de QNAP NAS.

## Instale un firewall de seguridad para el NAS

Las amenazas de seguridad en red no diferencian entre redes internas y externas; por ello, los firewalls basados en red (límites) configurados en el borde de las redes locales son insuficientes para garantizar la completa seguridad. En la actualidad, el concepto de Zero Trust Networks está pasando a ser predominante; puede instalar y habilitar QuFirewall en dispositivos QNAP para crear un firewall basado en host (microlímite) para proteger sus datos y servicios esenciales.

### QuFirewall



QuFirewall es una aplicación para NAS QNAP gratuita que le permite configurar reglas de tráfico de red entrante para permitir/denegar conexiones y mejorar la seguridad del NAS conectado a Internet. QuFirewall también admite GeoIP, que se puede usar para detectar y denegar conexiones de regiones geográficas especificadas. Para aumentar aún más la protección, puede considerar la instalación del popular firewall de código libre pfSense de Virtual Machine Marketplace de Virtualization Station.

## No deje su NAS expuesto

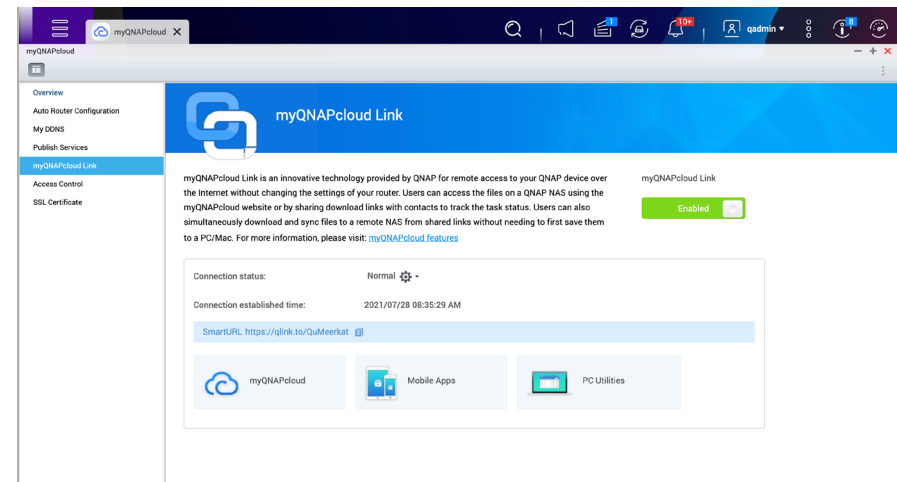
Su NAS QNAP es potencialmente vulnerable al snooping si se conecta directamente a Internet sin protección. Mediante el uso de botnets o sitios web tales como Shodan, los atacantes pueden bloquear dispositivos y lanzar ataques. Esto se controla en la configuración de reenvío de puertos de los routers y modems. Si habilita el reenvío manual, el reenvío de puertos automático (UPnP; Universal Plug and Play) o la zona desmilitarizada (DMZ), su NAS QNAP se conecta directamente a Internet. La conexión directa a Internet también se produce cuando el NAS QNAP obtiene una dirección IP pública directamente (estática/PPPoE/DHCP).

Si necesita acceder remotamente al NAS, el modo más seguro es establecer una conexión de VPN segura o usar la aplicación myQNAPcloud Link. Si no usa estos métodos de conexión, deberá instalar el NAS QNAP detrás de su router y firewall. Si el NAS está detrás de un router pero se conecta a Internet mediante reenvío de puertos, deberá especificar un nuevo número de puerto en el router. No utilice los números de puerto 22, 443, 80, 8080 o 8081.

## Sugerencias de seguridad para las conexiones remotas

Uno de los mejores aspectos acerca del NAS es el acceso universal a sus archivos y servicios desde cualquier dispositivo en cualquier momento. Para facilitar la conexión remota y hacerlas más seguras, hemos desarrollado la aplicación myQNAPcloud Link, que se conecta al NAS (a través de una conexión P2P) para que pueda conectarse con seguridad al NAS sin solicitar una configuración de firewall adicional ni dejar directamente expuesto al NAS.

La conexión remota mediante los servicios DDNS solía precisar unos procesos de configuración tediosos; sin embargo, myQNAPcloud Link ofrece una conexión remota sencilla con la que podrá conectarse a su NAS QNAP allá donde se encuentre, como si lo llevara consigo.

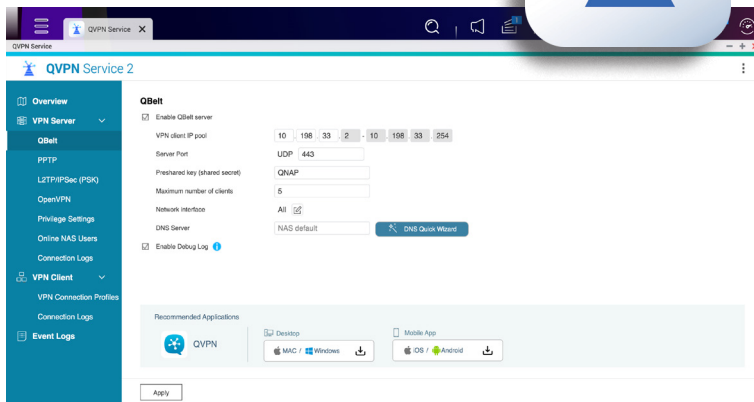


## Establezca una conexión VPN segura

Además de la conexión remota de myQNAPcloud Link, configurar su propio servidor de red privada virtual (VPN) en su NAS QNAP mediante el servicio QVPN ofrece un superior nivel de conexión segura, que ofrece unas comunicaciones más seguras entre sus dispositivos y el NAS. Además, también puede conectar su NAS QNAP a otros servidores VPN.

QBelt, el protocolo de VPN exclusivo para QVPN de QNAP, puede reducir aún más la posibilidad de que se detecten las conexiones VPN. Un ordenador o dispositivo móvil puede usar el cliente del dispositivo QVPN para conectarse al servidor VPN en el NAS QNAP o al servicio QuWAN.

### Servicio QVPN



## Funciones de seguridad incorporadas

Además de las numerosas aplicaciones que mejoran la seguridad ya mencionadas, los sistemas operativos del NAS de QNAP (QTS y QuTS hero) cuentan con una amplia gama de configuraciones de seguridad incorporadas para añadir capas adicionales de protección al NAS.

- **Lista negra y lista blanca de IP:** Utilice la lista blanca para restringir las conexiones y solo autorizar las direcciones IP, mientras que la lista negra se puede usar para bloquear automáticamente determinadas direcciones IP para evitar que se conecten al NAS.
- **Bloqueo automático:** Configure el NAS para que bloquee los usuarios/direcciones IP que no hayan podido iniciar sesión al cabo de un número de intentos especificado. Esto resulta útil para evitar ataques de fuerza bruta y garantizar la seguridad de los dispositivos.
- **Conexión HTTPS:** Habilite una conexión HTTPS al NAS y podrá elegir cifrar su conexión con un certificado TLS autofirmado o de myQNAPcloud/Let's Encrypt para aumentar la seguridad.
- **Múltiples soluciones de copia de seguridad:** Realice una copia de seguridad completa del NAS de distintas formas, como con instantáneas y realizando copias de seguridad/sincronizando en un servidor remoto o en un servicio de almacenamiento en la nube.
- **Control de permisos:** Además de los controles de seguridad para la información, configurar permisos de carpetas otorga a los usuarios más privacidad, lo que no solo garantiza la seguridad de la información confidencial, sino que también cumple con los requisitos normativos.
- **Registros y notificaciones:** El sistema cuenta con registros de eventos y notificaciones totalmente incorporados, lo que asegura una detallada trazabilidad de las operaciones y ahorra tiempo para el mantenimiento de IT.



## Elimine riesgos desconocidos

Las cuentas de usuario deben monitorizarse y modificarse basándose en sus necesidades. Debe eliminar las cuentas que ya no necesite o revocar todos sus permisos si la cuenta se va a necesitar más tarde. Esto se hace en "Panel de control" > "Permisos" > "Usuarios". También debe monitorizar las aplicaciones que los usuarios han instalado y verificar si se necesitan una vez eliminada la cuenta de un usuario. Si, en algún momento, encuentra una cuenta de usuario que no reconoce o que no recuerda haber creado, deberá eliminarla de inmediato.

## Instale software antivirus

Además del antivirus gratuito ClamAV incorporado en QTS, también puede comprar el antivirus McAfee, un conocido software antivirus, para aumentar la protección. Los usuarios de QNAP pueden realizar manualmente o programar análisis para proteger sus datos ante virus, reparar archivos que hayan sido infectados, poner en cuarentena archivos infectados y recibir las últimas definiciones de virus para protegerse contra virus nuevos y emergentes. Se pueden adquirir licencias del antivirus McAfee en QNAP Software Store, con una duración de hasta 3 años.

### Antivirus McAfee

Escanee su NAS en busca de malware o bien manualmente o según un programa con el sistema antivirus McAfee.

Esencial	Pro	Premium
Antivirus Annual Suscripción para el NAS	Antivirus BIANUAL Suscripción para el NAS	Antivirus trianual Suscripción para el NAS
USD \$25.00 /Año	USD \$50.00 /2 Años	USD \$70.00 /3 Años
SUSCRÍBASE AHORA	SUSCRÍBASE AHORA	SUSCRÍBASE AHORA

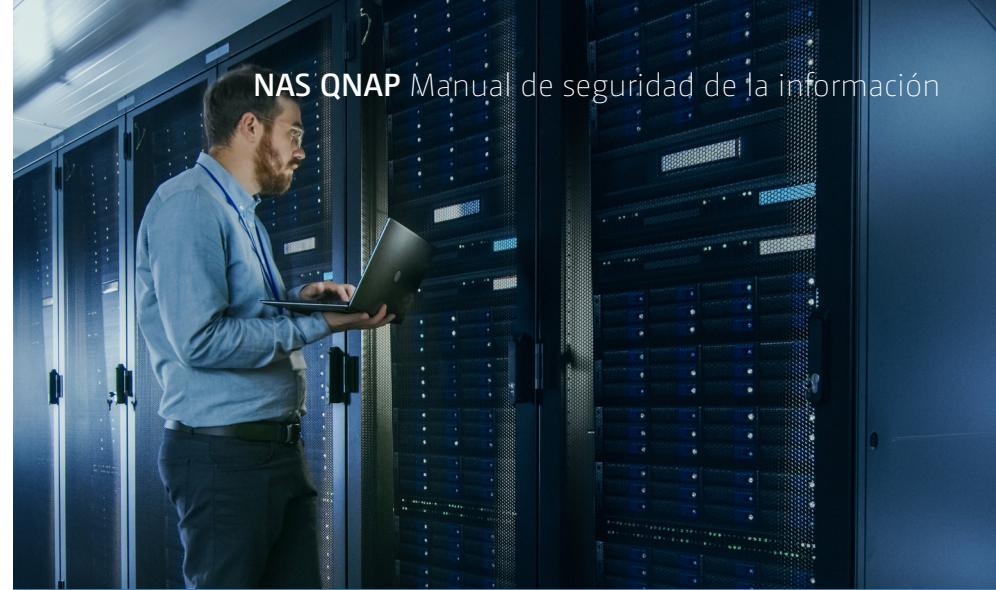


## El equipo de seguridad de QNAP está preparado en todo momento

QNAP ha recibido la certificación en 2018 de MITRE, una organización internacional sin ánimo de lucro, como autoridad de numeración de CVE. Esto permite a QNAP asignar identificadores de CVE por problemas de seguridad en productos de QNAP. El equipo de respuesta ante incidentes de seguridad del producto de QNAP (PSIRT) recibe notificaciones de seguridad con información en tiempo real de todo el mundo, investiga vulnerabilidades de forma proactiva, hace pública las amenazas y responde a notificaciones de vulnerabilidades en el plazo de 24 horas desde que se reciben.

Recomendamos que los usuarios comprueben periódicamente el boletín de seguridad de la información de QNAP y se suscriban al boletín de seguridad de la información de QNAP para obtener la información más actualizada y las actualizaciones. En caso de un incidente de seguridad, siga las prácticas recomendadas del equipo de QNAP PSIRT para ayuda a evitar que un incidente de seguridad ponga en riesgo su NAS.

Advisory	Status	Impact	CVE	Last Updated	Affected Product(s)
<p>Improper Access Control Vulnerability in Legacy HBS 3 (Hybrid Backup Sync)</p> <p><b>QNAP SA ID:</b> QSA-21-19</p> <p><b>First Published:</b> 2021-07-06</p> <p><b>Summary:</b> An improper access control vulnerability has been reported to affect certain legacy versions of HBS 3 (Hybrid Backup Sync). If exploited, this vulnerability allows attackers to compromise the security of the operating system. We have already fixed this vulnerability in the following versions of HBS 3: QTS 4.3.6...</p> <p><a href="#">Learn More</a></p>	Resolved	Critical	CVE-2021-28809	2021-07-06	Certain QNAP NAS
Multiple Command Injection Vulnerabilities in QTS and QuTS hero	Resolved	Medium	CVE-2021-28802 CVE-2021-28804	2021-06-25	Certain QNAP NAS
Stored XSS Vulnerability in QuLog Center	Resolved	Medium	CVE-2020-36196	2021-06-25	Certain QNAP NAS
Stored XSS Vulnerability in Q-center	Resolved	Medium	CVE-2021-28803	2021-06-25	Certain QNAP NAS
XSS Vulnerability in QTS and QuTS hero	Resolved	Medium	CVE-2020-36194	2021-06-25	Certain QNAP NAS
DNSpoof Vulnerabilities in QTS	Resolved	Medium	CVE-2020-25684 CVE-2020-25685 CVE-2020-25686	2021-06-28	Certain QNAP NAS



## ¿Qué debería hacer si mi NAS sufre un ataque de cifrado?

Los ataques de ransomware pueden variar en sus efectos y en sus vectores de ataque, por lo que es difícil definir una respuesta general recomendada a un ataque. Para prepararse frente a ataques potenciales, recomendamos encarecidamente seguir las prácticas recomendadas para la copia de seguridad y la recuperación ante desastres: copias de seguridad diarias, guardar las copias de seguridad en varios dispositivos, usar instantáneas y copias de seguridad de las instantáneas. Recuerde también suscribirse al boletín de noticias de seguridad de la información de QNAP para obtener las actualizaciones más recientes.

Si sospecha que se ha puesto en riesgo su NAS u otros dispositivos conectados a red (como un uso de la CPU anormalmente alto provocado por aplicaciones o servicios desconocidos, fallos en el inicio de sesión, archivos desconocidos en carpetas o el cifrado no autorizado de archivos), deberá quitar inmediatamente el NAS de la red y desconectar la red de Internet. Debe apagar\* inmediatamente el NAS y contactar con el QNAP Helpdesk para obtener más información. También debe verificar la integridad de las copias de seguridad y comprobar potencialmente si se han puesto en riesgo.

La aplicación Malware Remover se puede usar para eliminar potencialmente el malware del sistema. Asegúrese de que utiliza la versión más actualizada de Malware Remover.

Si habitualmente utiliza la función de instantáneas, y ha confirmado que sus archivos de instantáneas no se ha visto afectado, puede usar la función de recuperación de instantáneas para recuperar sus valiosos datos.

\* En la mayoría de los casos, lo mejor es apagar inmediatamente el NAS en cuanto se detecta un ataque. Pocos ataques de cifrado pueden hacer que el NAS pierda la clave de descifrado después de apagarse. Se recomienda a los usuarios que presten atención al boletín de seguridad de la información del QNAP.



## La seguridad de la información es la máxima prioridad de QNAP

El compromiso de QNAP con la seguridad es máximo. Mantenemos activamente la seguridad de la información y combinamos los puntos fuertes de nuestros socios y la comunidad para garantizar la seguridad de los productos de QNAP para su tranquilidad.



# QNAP SYSTEMS, INC.

TEL.: +886-2-2641-2000 FAX: +886-2-2641-0555 Correo electrónico: [qnapsales@qnap.com](mailto:qnapsales@qnap.com)

Dirección: 3F, No.22, Zhongxing Rd., Xizhi Dist., New Taipei City, 221, Taiwán (China)

QNAP puede realizar cambios en las especificaciones y en las descripciones de los productos sin previo aviso.

Copyright © 2021 QNAP Systems, Inc. Todos los derechos reservados.

QNAP® y otros nombres de productos QNAP son marcas comerciales o marcas comerciales registradas de QNAP Systems, Inc.

Otros productos y nombres de empresas aquí mencionados son marcas comerciales de sus respectivos propietarios.

## Países Bajos (Servicios de almacén)

Correo electrónico: [nlsales@qnap.com](mailto:nlsales@qnap.com)  
TEL.: +31(0)107600830

## China

Correo electrónico: [cnsales@qnap.com](mailto:cnsales@qnap.com)  
TEL.: +86-400-028-0079

## Japón

Correo electrónico: [jpsales@qnap.com](mailto:jpsales@qnap.com)  
FAX: 03-6435-9686

## EE.UU.

Correo electrónico: [usasales@qnap.com](mailto:usasales@qnap.com)  
TEL.: +1-909-595-2782

## India

Correo electrónico: [indiasales@qnap.com](mailto:indiasales@qnap.com)

## Francia

Correo electrónico: [frsales@qnap.com](mailto:frsales@qnap.com)

## Tailandia

Correo electrónico: [thsales@qnap.com](mailto:thsales@qnap.com)  
TEL.: +66-2-5415988

## Alemania

Correo electrónico: [desales@qnap.com](mailto:desales@qnap.com)