

A series of eight yellow stars arranged in a curved path across the page, starting from the top left and ending at the bottom left.

GDPR

WHITE PAPER

QNAP

El nuevo Reglamento Europeo de Protección de Datos (GDPR): La solución completa de QNAP para apoyar a las empresas durante y después del plan de ajuste al Reglamento.



GDPR: ¿qué es?

GDPR (Reglamento General de Protección de Datos) es la normativa europea 2016/679 sobre la protección de las personas con respecto al tratamiento de datos personales y a la libre circulación de estos datos. El presente Reglamento sustituirá a la Directiva europea sobre protección de datos (Directiva 95/46 / CE) establecida en 1995 y derogará las disposiciones del Código para la protección de datos personales (Decreto Legislativo n. 196/2003) que será incompatible con ella. El reglamento fue adoptado el 27 de abril de 2016, y será convertido en pleno funcionamiento en la UE el 25 de mayo de 2018 después de un período de transición de dos años y, a diferencia de una directiva, no requiere ningún tipo de legislación de aplicación por los Estados miembros .

¡Las sanciones alcanzarán hasta el 4% de la facturación y hasta un máximo de 20 millones de euros!

El GDPR tiene como objetivo estandarizar y normalizar, dentro de la Unión Europea, las diferentes reglas que rigen el tratamiento de datos personales, regulando definitivamente las formas en que los datos y la información deben ser almacenados, protegidos y puestos a disposición por las empresas sino que también se aplica a las empresas no comunitarias que proporcionan bienes o servicios a los residentes de la UE.

Es importante tener en cuenta que las reglas de GDPR tienen un valor general y no prevén obligaciones específicas o diferenciadas por tamaño, tipo o sector de actividad de la empresa.

De acuerdo a los datos personales de la Comisión Europea cualquier información relativa a su vida de una persona conectada es privada, ya sea profesional o pública. Puede usted relacionarse con todo: nombres, fotos, direcciones de correo electrónico, datos bancarios, trabajo en los sitios web de redes sociales, información médica o direcciones IP de los equipos ".

Los pasos: desde el registro de las actividades de procesamiento al plan de ajuste

El objetivo principal de GDPR es asegurarse de que los datos personales no se dan a conocer, están protegidos y monitoreados constantemente: lo que podría tener importantes cambios organizativos e inversiones tecnológicas, las empresas requieren una planificación cuidadosa en un tiempo muy ajustado, dado que el período dentro del cual se puedan adaptar está cerca (aproximadamente seis meses).

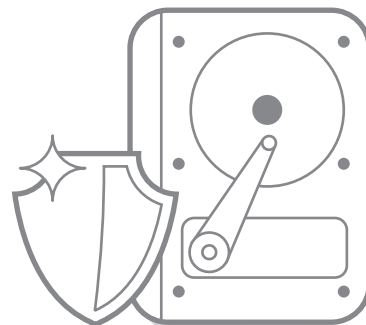
Las empresas deben tener un plan de cumplimiento a GDPR. Esta fase consiste en la evaluación del modelo actual de la organización, con el fin de definir un plan de acción detallado adecuado. Este plan de ajuste, que utiliza un enfoque estructurado, definitivamente debe considerar dos áreas importantes en la tecnología y la informática:

- El área de los procesos y reglas. Es sin duda una de las áreas más involucradas en las solicitudes de ajuste de GDPR: basta recordar la portabilidad de los datos, el incumplimiento de la gestión de datos, registro de procesamiento de datos y los derechos de los interesados. Muy importante es la privacidad desde el diseño, que es un nuevo enfoque requerido por GDPR que exige a las empresas la obligación de poner en marcha un proyecto que proporciona, de inmediato, la protección de las herramientas de datos personales.
- El área de la tecnología y herramientas adquiere una importancia vital, desde el punto de vista de las inversiones que se esperan en el plan de ajuste: la seguridad informática (antivirus, recuperación de desastres, cortafuegos, los datos apócrifos, cifrado de datos, los datos de violación de prevención y detección, la administración de identidades, etc.). seguridad física (por ejemplo. el control de acceso), la adopción de las herramientas informáticas de GRC (Gobierno, Riesgo y cumplimiento).

El GDPR establece un marco normativo centrado exclusivamente en las tareas y responsabilidades del responsable del tratamiento (el principio de "rendición de cuentas"). Las nuevas regulaciones requieren que la entidad no solo asegure el cumplimiento de los principios que contiene, sino también ser capaz de demostrar, la adopción de un conjunto de herramientas que sí indica GDPR.

Cómo protege QNAP la información

Gracias a la función de codificación de datos en el NAS QNAP, permite implementar en los volúmenes de disco el cifrado AES de 256 bits. Los volúmenes cifrados sólo se pueden utilizar para el acceso normal de lectura / escritura con una contraseña autorizada. El cifrado protege los datos confidenciales de acceso no autorizado, incluso cuando se roban los discos duros o todo el NAS.



- **Cifrado AES 256**

La característica de cifrado de datos en un NAS QNAP le permite cifrar volúmenes de discos en el NAS con el cifrado AES de 256 bits. Los volúmenes de discos cifrados solamente se pueden montar para acceso normal de lectura/escritura con la contraseña autorizada. La característica de cifrado protege los datos confidenciales de acceso no autorizado, incluso si los discos duros o todo el NAS fuese robado.

Algunos modelos también soportan el motor de cifrado acelerado por hardware AES-NI, para la protección de datos más rápida, económica y segura.

- **Cifrado de unidad USB / eSATA externo**

Para evitar la pérdida de datos, puede hacer una copia de seguridad de sus archivos importantes desde su NAS QNAP a unidad externa. QNAP ahora es compatible con el cifrado de discos duros eSATA / USB para evitar el acceso no autorizado a los contenidos en caso de pérdida o robo. El administrador de redes puede elegir si desea cifrar un volumen de disco o una partición con el cifrado: AES-128, AES-192, AES-256.

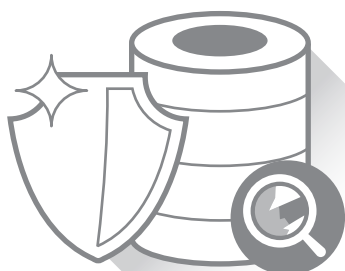
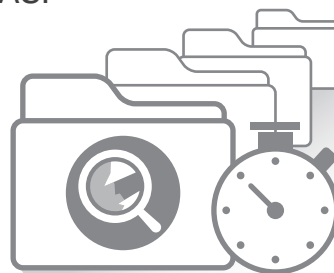
- **Protección de nivel militar**

El cifrado FIPS 140-2 validado a nivel militar, considerado como la certificación de seguridad vigente más alta para el cumplimiento con las actuales normas, se adopta automáticamente para el cifrado de discos duros tanto internos como externos.

Cómo QNAP gestiona sus datos

- **Qsirch - Qsirch es un potente motor de búsqueda en el NAS.**

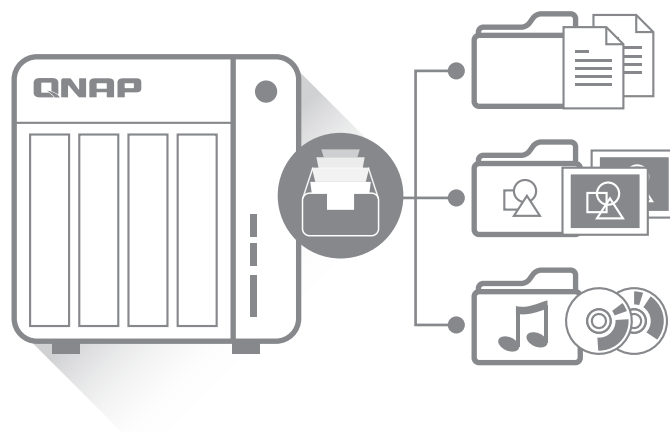
Para las empresas, los beneficios son muchos, sobre todo en la capacidad de encontrar los documentos y archivos que desea para crear propuestas, informes, contratos y mucho más. Qsirch le permite aumentar inmediatamente la productividad y la eficiencia en el trabajo.



Qsirch opera en línea con los permisos de carpetas compartidas y cuentas de usuario de QTS. Protege eficazmente la privacidad de los datos y resultados de la búsqueda ya que muestra sólo los archivos autorizados para cada usuario. Los administradores pueden añadir y eliminar carpetas específicas compartidas para Qsirch. Excluye de forma flexible las carpetas compartidas de la indexación para garantizar la seguridad de los datos.

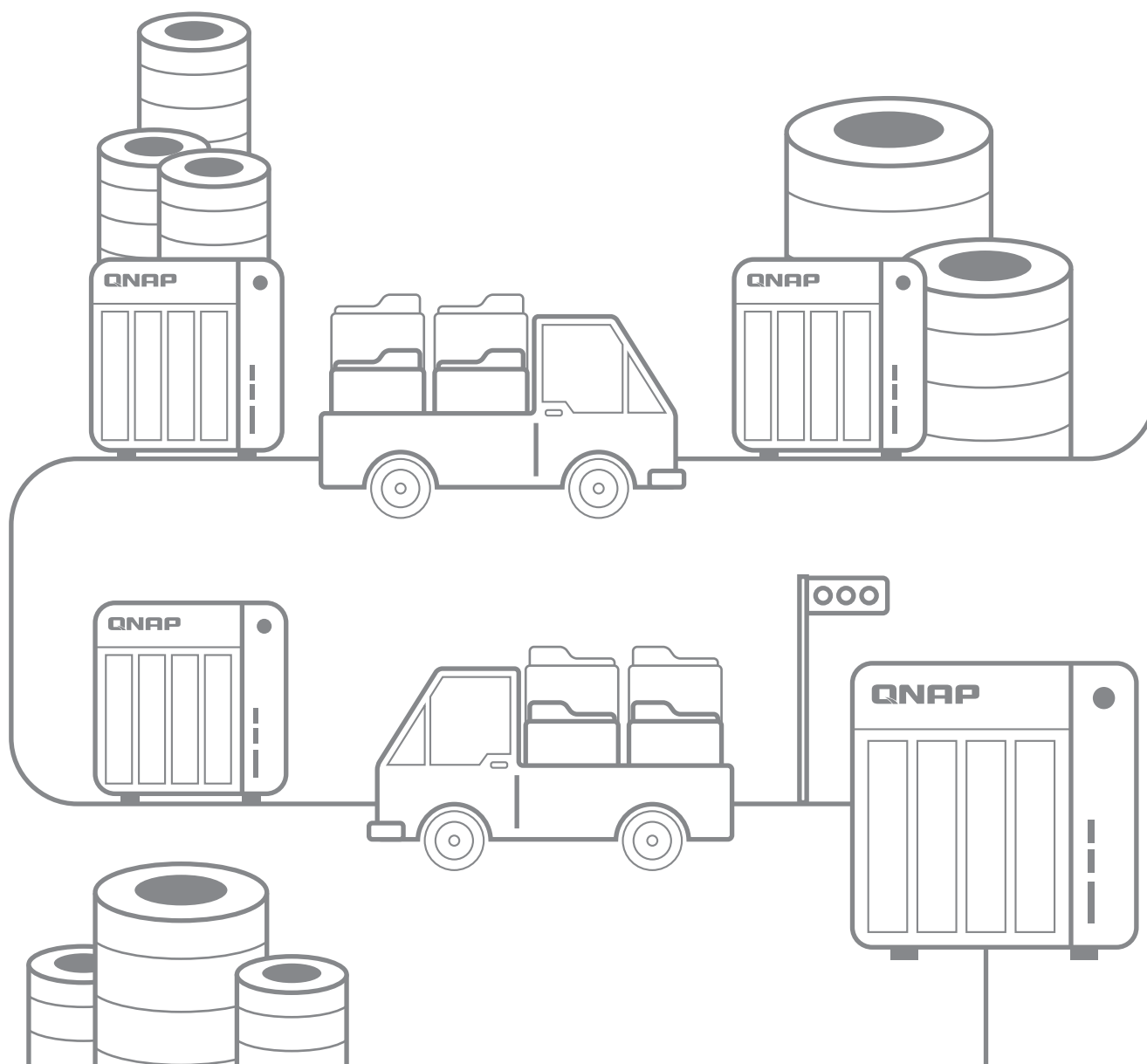
- **Qfiling** - Qfiling automatiza la organización de los archivos de manera eficiente

Al usar NAS QNAP como un almacén de archivos central, la posibilidad de organizar de manera eficiente los ficheros es un principio fundamental para la gestión de archivos y su uso todos los días. Sin embargo, existen un gran número de archivos distribuidos en varias carpetas y se hace cada vez más difícil, costoso, en términos de tiempo y agotador, clasificar y almacenar. Ahora, con la organización de archivos Qfiling es automática y eficiente.



Las principales características de Qfiling son:

- **Velocidad** ▶ Completa todos los ajustes con unos pocos clics .. rápido y fácil.
- **Organización Aumento de la** ▶ Completa todos los ajustes con unos pocos clics .. rápido y fácil.
- **Productividad** ▶ La organización de archivos es automática y periódica. No más tiempo o esfuerzo.
- **Optimizado** ▶ Mantenga sus archivos organizados para encontrar fácilmente los archivos necesarios y obtener el máximo rendimiento de cada archivo.



Cómo gestiona QNAP sus usuarios

NAS QNAP es compatible con numerosas características para proporcionar seguridad para el sistema, el acceso a los datos y ficheros almacenados. El acceso encriptado protege las conexiones y comunicaciones del sistema, el bloqueo de IP impide la entrada de usuarios sospechosos y el cifrado de la unidad externa reduce el riesgo de apropiación indebida de los datos en caso de robo de discos duros. Además, QNAP ha apoyado la detección de los virus más recientes y creado actualizaciones de seguridad para sus dispositivos. Todas estas medidas están orientadas a lograr un lugar seguro la información.

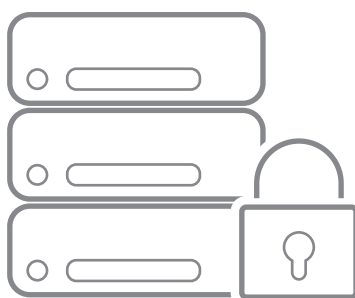
protección Acceso a la red



El administrador puede configurar la lista de conexiones para permitir un adecuado acceso a múltiples usuarios al NAS QNAP a través de la dirección IP. Funciona como un bloqueo de IP basado en políticas automáticas, lo que permite la protección de acceso a redes de control. Por ejemplo, el comando se puede configurar: "entre 1 minuto, después de 5 intentos fallidos, bloquear la IP durante 1 hora, 1 día o para siempre."

Una vez que se rechaza una dirección IP, el host ya no volverá a conectarse al servidor, independientemente de puertos de conexión que utiliza.

Protege los datos en entornos mixtos

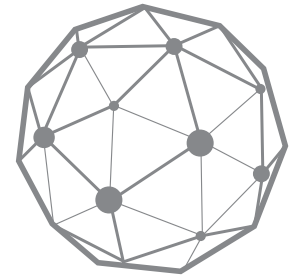
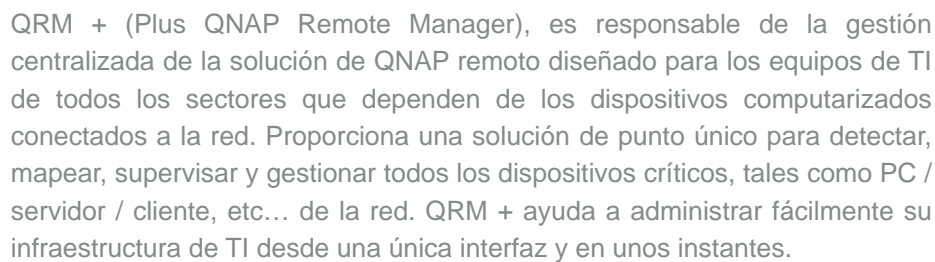


En general, todos los usuarios de negocios instalan software de antivirus en tiempo real. Sin embargo, los virus crecen más allá de todas las expectativas y los intentos deliberados por los usuarios a acceder a sitios web maliciosos son difíciles de evitar. Dado que el virus de archivos infectados en un entorno mixto puede causar un daño significativo, es esencial disponer de una solución antivirus para NAS QNAP que proporciona el intercambio de archivos entre plataformas. Detección inteligente: La solución antivirus integrada para el NAS QNAP asegura la continuidad del negocio a través de la detección de virus, malware, gusanos y troyanos más reciente con actualizaciones gratuitas continuas de la base de datos de virus. Además de las diversas tareas de exploración con una selección de carpeta personalizada y la exploración programada,

protección del sistema mejorado



Por lo general, un NAS con varios puertos LAN permite a todos los servicios de red habilitados acceder a los contenidos del servidor a través de cada puerto LAN. Esto reduce la protección de datos. En las empresas, los datos importantes sólo deben ser accesibles a ciertas personas que utilizan el protocolo de red por defecto, es decir, una dirección IP interna. NAS QNAP ofrece a los administradores la flexibilidad necesaria para permitir o bloquear los servicios específicos de las interfaces de red designados para garantizar la seguridad del sistema.

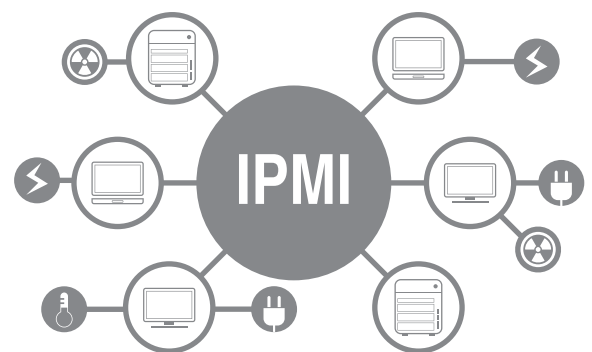


The diagram illustrates the integration of quantum random number generation into a storage system. On the left is a QNAP storage device. A line connects it to a central sphere labeled 'QRM+', which represents the quantum random number generator. From the 'QRM+' sphere, two lines branch out to the right, connecting to two computer monitors. The top monitor displays the Windows logo and the word 'Windows'. The bottom monitor displays the word 'Linux'. This setup indicates that the QRM+ provides random data to both Windows and Linux operating systems.

QRM + puede generar una lista de dispositivos IT vinculados permitiendo a los administradores controlar rápidamente cada dispositivo conectado y asegurar la integridad de todos los dispositivos. QRM + también permite la monitorización en tiempo real, con el fin de poder verificar el estado de cada punto final tantas veces como sea necesario. Con QRM +, la gestión remota de los equipos informáticos es seguro, rápido y fácil.

Controlar todos los parámetros críticos del servidor a través de IPMI

QRM +, una de las pocas soluciones disponibles en el mercado para la gestión centralizada de los dispositivos habilitados para IPMI, proporciona una solución como un único punto para la detección, la cartografía, el seguimiento y la gestión de todos los dispositivos IPMI en la red. QRM + soporta IPMI 2.0, que permite la gestión de sus dispositivos compatibles IPMI, con independencia del estado del sistema operativo. Ayuda a controlar los sensores críticos del sistema, tales como sensores de temperatura, velocidad de los ventiladores, sensores de tensión, estado de la alimentación y las notificaciones de eventos IPMI.



The illustration shows a QNAP Network Attached Storage (NAS) unit in the background. In the foreground, a laptop screen displays a web interface with a prominent warning icon (an exclamation mark inside a triangle) and a notification bubble in the top right corner containing the number '1'.

Alertas y notificaciones: Recibir alertas de antemano antes de que ocurra un desastre

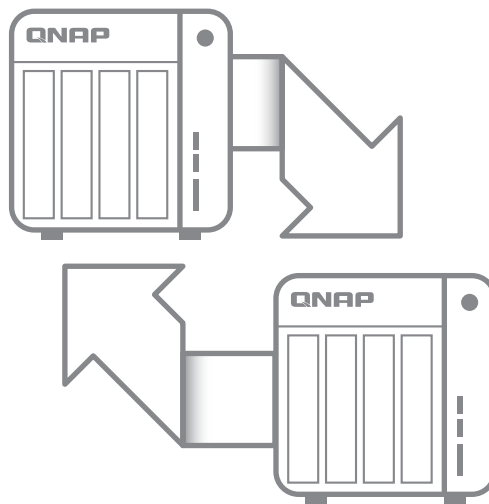
QRM + ofrece alertas para corregir problemas de rendimiento antes de que afecten a los usuarios, las aplicaciones y la empresa, lo que permite beneficiarse de una mayor productividad, la mejora de la colaboración y la recuperación más rápida de tiempo muerto del equipo o el rendimiento del sistema.

En caso de pérdida de datos, NAS QNAP soporta varios métodos de conservación de la copia para la recuperación

RTRR o rsync:

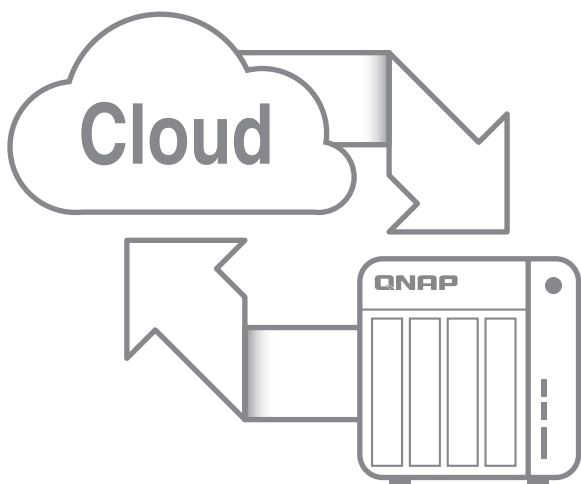
Puede hacer una copia de seguridad de sus datos de QNAP NAS en otro servidor QNAP NAS o FTP remoto en tiempo real a través del servicio de Replicación Remota en Tiempo Real (RTRR) de QNAP o un servidor rsync estándar programado por el protocolo rsync.

Gracias RTRR, el Turbo NAS supervisa los archivos de origen, incluyendo los archivos de las carpetas de copia de seguridad de Time Machine y Qsync, y sincroniza los cambios en el servidor de destino. Los administradores de TI puede realizar copia de seguridad instantánea y programada.



Copia de seguridad en la nube:

QTS ofrece soluciones de copia de seguridad en la nube seguras, fáciles de usar y con numerosas funciones que le permiten realizar copias de seguridad de datos en diversos servicios de almacenamiento en la nube de clase empresarial, incluidos Microsoft Azure, Amazon Glacier, Amazon S3, ElephantDrive, Google Drive, Dropbox * e IBM SoftLayer. También es compatible con soluciones de almacenamiento en la nube privada compatibles con OpenStack Swift y WebDAV. QTS es la puerta de enlace de almacenamiento en la nube que le permite crear planes de recuperación simples y accesibles además de la retención de datos sin problemas con fines regulatorios y de archivo.



Por último, en el diseño de su plan de ajuste a GDPR, las empresas pueden optar por trabajar simplemente para cumplir con las nuevas regulaciones en el sentido estricto o explotar las oportunidades de creación de valor para la organización en su conjunto, lo que ayuda a difundir una nueva cultura en el procesamiento de datos personales y lograr una "transformación digital" real de los procesos comerciales que gestionan datos de clientes y empleados. Los cibercriminales están buscando constantemente debilidades y desarrollan sin cesar los ataques cada vez más específicos.. Las soluciones de seguridad sostenibles deben evolucionar y adaptarse actualizando con frecuencia y explotando la información de amenazas tan pronto como esté disponible. La seguridad es realmente innovadora solo si permite la detección de amenazas, desencadena una reacción y proporciona protección global para toda la instalación, desde puntos finales hasta redes y nubes híbridas.

¿Necesita realizar un backup remoto en territorio nacional?

La máxima de la implementación de esta ley es que siempre debe existir un modo confiable de poder borrar los datos personales a petición del propietario de los mismos. De este modo, se garantiza que la información personal, que es privada, no es utilizada por terceros sin el consentimiento expreso de la persona. Esto obliga a los integradores de sistemas y empresas relacionadas con el campo de la tecnología a disponer de un método efectivo de borrado de estos datos.

Los proveedores internacionales de almacenamiento en nube son una solución generalmente económica, eficiente y que provee de una gran disponibilidad de los datos. Sin embargo, no es siempre posible establecer compromisos legales vinculantes que aseguren el cumplimiento de la GDPR y sus posibles actualizaciones en determinados casos. Los proveedores de almacenamiento en data center nacionales, además de una disponer de soluciones más flexibles ante desastres (envío de discos duros por correo express certificado, requerimientos personalizados, etc), cuentan un ancho de banda dedicado a sus clientes para optimizar las velocidades de transferencia.

En lo que concierne a la GDPR, los data center locales hacen posible cumplir la ley de protección de datos mediante requerimientos de privacidad vinculantes específicos, que se pueden confirmar directamente con la empresa receptora de los datos. En España, QNAP ya cuenta con un primer data center de backup remoto certificado por QNAP, que cumple con el protocolo de transferencia remota RTRR de QNAP, certificación Tier II y asegura las máximas garantías de seguridad y redundancia con un 99.749% de disponibilidad, redundancia en alimentación, refrigeración y conexión, y con un máximo de 22 horas de downtime por año. Los datos almacenados en este data-center cuentan con una encriptación end-to-end, por la cual el cliente puede disponer de una clave única de descifrado de los datos, lo cual le confiere un acceso exclusivo sin que el data center pueda acceder a esta información o transferirla a terceros para su distribución.



Más información sobre esta solución en www.bsbdata.com

Consulte y contacte con QNAP en https://www.qnap.com/es-es/before_buy para más información sobre la gestión de backups remotos

