netdocuments®

CIFRADO DE DOCUMENTOS Y POR QUÉ ES IMPORTANTE

El cifrado es crucial para el papel que desempeña en la seguridad, el cumplimiento y la prevención de pérdidas.

Seguridad

El almacenamiento seguro de documentos de negocios es una alta prioridad. A medida que los archivos se comparten digitalmente entre personas y dispositivos, hay cada vez más oportunidades para que los malos actores ataquen los sistemas y roben información. El cifrado es una **capa esencial** de protección para mantener su contenido seguro, incluso si se violan otros controles de seguridad.

Gobernanza y cumplimiento

La seguridad y la gobernanza de la información son requisitos operativos fundamentales para las organizaciones. Conformadas por directrices a nivel estatal, federal e internacional, las empresas necesitan herramientas para almacenar, gestionar y disponer de forma defensiva de los documentos. El cifrado es una **herramienta clave** para el cumplimiento de estas normas.

Prevención de pérdidas

El costo de las violaciones de datos va mucho más allá de la simple mejora de la seguridad. Las violaciones de los datos socavan la confianza del público y pueden tener un efecto increíblemente perjudicial en la reputación de una empresa, lo que puede poner en peligro las relaciones con los clientes y los ingresos actuales y futuros. El cifrado **puede evitar** que un incidente de seguridad se convierta en una violación de datos.

netdocuments®

Cómo maneja NetDocuments el cifrado de documentos

Mantener sus archivos seguros es nuestro trabajo. Con la computación de confianza cero, NetDocuments utiliza prácticas de cifrado líderes en la industria para proteger su negocio contra las violaciones de datos, además de proporcionar una infraestructura de cifrado de próxima generación y gestión de claves. Puede estar seguro de que los documentos de su empresa están protegidos en los niveles más altos disponibles hoy en día dentro del Servicio de NetDocuments.

Cifrado multicapa y gestión de la clave de cifrado (EKM)

NetDocuments aplica múltiples capas de cifrado y utiliza una tecnología innovadora, incluido un generador de números aleatorios cuánticos (QRNG, por sus siglas en inglés), para crear una clave de cifrado única para cada documento y correo electrónico guardado en el Servicio. El QRNG utiliza la mecánica cuántica para generar claves de cifrado AES-256 totalmente entrópicas, a diferencia de la aleatorización basada en software que puede ser descifrada por los agentes nacionales estatales.

El Servicio de NetDocuments realiza el cifrado y descifrado de cada documento, en lugar de utilizar métodos de seguridad de bajo valor como el cifrado a nivel de disco. Este proceso oculta todos los archivos digitales a los administradores de almacenamiento y de la red, lo que no es posible con el cifrado a nivel de disco.

Cada documento guardado en NetDocuments está cifrado con su propia y única clave de cifrado de objetos (OEK, por sus siglas en inglés) AES-256. Después del cifrado, el documento se escribe en la matriz de almacenamiento de datos ("almacén de objetos"), mientras que la OEK se almacena por separado en una base de datos de claves seguras.

Antes de ser almacenados en la base de datos de claves, las OEK son a su vez cifradas utilizando una Clave maestra de cifrado (MEK, por sus siglas en inglés), que proporciona una capa adicional de seguridad de cifrado. NetDocuments salvaguarda y gestiona las MEK en los Estándares Federales de Procesamiento de Información (FIPS, por sus siglas en inglés) 140-2 Módulos de seguridad de hardware (HSM, por sus siglas en inglés) de nivel 3 con acceso restringido, utilizando la arquitectura de raíz de confianza para proteger completamente la MEK. Las MEK se rotan cada seis meses. Los FIPS son una norma mundialmente reconocida para los controles de seguridad de cifrado; el nivel 3 permite la separación física y lógica para maximizar la seguridad de la clave de cifrado.

La computación de confianza cero se logra almacenando claves de cifrado totalmente entrópicas en un HSM clasificado en el nivel 3 de FIPS 140-2 y utilizando los controles operativos del servicio de NetDocuments.

Claves de cifrado gestionadas por el cliente

Los clientes pueden tener requisitos de seguridad únicos y granulares. El cifrado puede utilizarse para aislar diferentes conjuntos de contenido de otros documentos. Cumplimos con este requisito ofreciendo a los clientes la opción de utilizar Claves de cifrado gestionadas por el cliente (CMEK, por sus siglas en inglés), gestionadas a través de los HSM de NetDocuments o los HSM gestionados por el cliente.

netdocuments®

Cuando se utilizan las CMEK, el Servicio de NetDocuments aplica tres capas de cifrado separadas a cada documento. Los clientes controlan cuándo se aplican las CMEK a los documentos confidenciales que corresponden a las políticas de regulación, cumplimiento u otras políticas de gobernanza de datos obligatorias.

Los clientes pueden asignar y revocar las CMEK a proyectos o grupos de documentos específicos cuando sea necesario. La gestión de claves de cifrado granulares basadas en metadatos permite a las empresas revocar el acceso a un contenido específico mientras que el resto del contenido sigue siendo accesible y está protegido por su propio cifrado.

Cifrado en tránsito

NetDocuments no solo protege sus documentos mientras están almacenados en la aplicación, sino que el Servicio también protege sus documentos mientras se transmiten hacia o desde el Servicio mediante el cifrado de todas las transmisiones del Servicio a través de Internet. NetDocuments requiere que todas las conexiones al Servicio utilicen HTTPS y solo permite el cifrado mediante los actuales protocolos de seguridad TLS (actualmente TLS 1.2) para la seguridad de la transmisión de documentos.

Almacenamiento resiliente de documentos

Un elemento clave de la arquitectura de almacenamiento de NetDocuments es el uso de la tecnología de almacenamiento de objetos. Cuando se coloca un archivo en el Servicio de NetDocuments, se cifra inmediatamente y luego se guarda en un almacén de objetos, donde se replica automáticamente o se codifica su borrado (dependiendo del tamaño del archivo) a través de múltiples centros de datos y múltiples dispositivos de almacenamiento físico dentro de cada centro de datos. Esta dispersión a través de centros de datos geográficamente separados y altamente seguros asegura la completa disponibilidad de los datos, la integridad del contenido y los más altos niveles de seguridad.

Asegurarse de que se utilice el cifrado en todo el Servicio de NetDocuments hace que los documentos confidenciales sean indescifrables e inaccesibles para cualquier parte, incluido el personal de NetDocuments.

El cifrado es uno de los muchos elementos de un plan de seguridad sólido y de confianza cero

Si bien el cifrado y el almacenamiento de objetos son elementos esenciales de cualquier servicio seguro, representan solo una capa de la gobernanza de datos de los servicios de NetDocuments. NetDocuments proporciona controles para gestionar el acceso de los usuarios a los documentos y la protección contra la pérdida de datos (DLP, por sus siglas en inglés) para minimizar el riesgo de una fuga de datos accidental o maliciosa.

Además, NetDocuments mantiene las certificaciones de seguridad ISO 27001, 27017 y 27018, la nueva certificación ISO 27701 para demostrar el cumplimiento de la normativa GDPR, y es auditada regularmente para validar el cumplimiento de los controles SOC 2, de modo que usted tenga la comodidad y la seguridad de saber que la infraestructura de seguridad de NetDocuments ha sido validada independientemente por auditores acreditados, y que su organización puede reclamar los beneficios de la completa arquitectura de seguridad de NetDocuments mediante el cumplimiento de la normativa de transferencia de datos.

Descubra cómo nuestra cifrado líder en la industria puede proteger aún más su negocio.

Programe hoy una demostración de NetDocuments >