



# EXPLICACIÓN RESUMIDA DE SERVICIOS Y SEGURIDAD

**netdocuments®**

**NetDocuments es un sistema de gestión de documentos (DMS) basado en la nube** que ofrece gestión de documentos y correo electrónico, así como soluciones de productividad. Los usuarios pueden acceder a los documentos desde cualquier dispositivo aprobado con conexión a Internet mientras disfrutan de los beneficios de cumplimiento y seguridad líderes en la industria que ofrece NetDocuments.

Este resumen de seguridad describe cómo NetDocuments protege sus datos y redes de servicios para que pueda estar seguro de que su información siempre estará protegida cuando utilice NetDocuments DMS.

## Protección de los datos del cliente

NetDocuments se creó sobre una base de seguridad e innovación, con el entendimiento de que la innovación no puede suceder a expensas de la seguridad. La plataforma NetDocuments está diseñada para proteger sus documentos con medidas de seguridad sólidas que incluyen múltiples capas de cifrado y custodia controlada de forma independiente de las claves de cifrado.

Cada documento que coloca en el DMS está cifrado con su propia clave única de cifrado de objetos AES-256 (OEK). Cada OEK tiene un mayor cifrado con una clave maestra AES-256 MEK que se almacena en un módulo de seguridad de hardware altamente seguro o Módulo de Seguridad Hardware (HSM, por sus siglas en inglés).

NetDocuments ofrece a los clientes la opción de cifrar aún más los documentos seleccionados con una tercera capa de cifrado utilizando una clave de cifrado AES-256 administrada por el cliente o CMEK. Todas las CMEK se almacenan en un segmento completamente restringido de HSM de NetDocuments al que solo puede acceder el cliente, o en un HSM propiedad del cliente. Cuando los datos del cliente están en tránsito a través de Internet, están protegidos mediante https con protocolos de seguridad TLS.

## SEGURIDAD DE LA RED DE LA PLATAFORMA

NetDocuments emplea una amplia gama de procedimientos, herramientas y servicios independientes para proporcionar seguridad líder en la industria para los documentos dentro de la plataforma.

### 1. Seguridad de la red

- Firewall de aplicaciones web independientes de terceros
- Protección contra Ataque de denegación de servicio (DDoS, por sus siglas en inglés)
- Firewalls internos, redundantes y con monitoreo de estado
- Equilibradores de carga (firewalls sin monitoreo de estado)
- Sistema de detección de intrusiones (IDS)
- Todos los servidores web se alojan en una zona desmilitarizada



## 2. Seguridad de la infraestructura

- Infraestructura completamente redundante sin un solo punto de falla
- Monitoreo en tiempo real
- Registro de actividad con revisión de registros y retención de registros extendida
- Contraseñas seguras
- Acceso restringido
- Revisiones periódicas de las reglas de firewall
- Imágenes de servidor reforzado que se actualizan e implementan periódicamente
- Implementación automatizada que incluye la destrucción y el reemplazo periódicos de todas las máquinas virtuales (VM)



## 3. Seguridad del centro de datos

- Barreras perimetrales físicas
- Acceso cerrado, monitoreado y controlado
- Visitas solo con cita preautorizada, validadas por una identificación con foto emitida por el gobierno
- Todos los invitados acompañados por empleados del centro de datos en todo momento
- CCTV interno y externo 24x7 en todas las entradas y áreas de acceso clave, monitoreadas y registradas
- Guardias de seguridad en vivo con patrullas de seguridad regulares
- Zonas de seguridad segregadas que requieren acceso autorizado
- Generación de energía de respaldo redundante en el sitio con suministros de combustible extendidos
- Conexiones de acceso de ISP redundantes

## 4. Seguridad de la aplicación

- Seguridad aplicada en múltiples capas: Documentos individuales, contenedores, perfil/metadatos, proyecto/materia, clientes
- Permisos administrados por el cliente: Listas de control de acceso (ACL), firewalls éticos
- Autenticación: Inicio de sesión único o inicio de sesión de múltiples factores implementado por el cliente mediante identidad federada con aplicaciones compatibles con SAML 2.0, ADFS o RSA
- Revisiones de código estáticas y dinámicas antes de cada lanzamiento
- Capacitación continua para desarrolladores sobre las mejores prácticas de seguridad de OWASP
- Registros de auditoría

## 5. Protección de datos

- En reposo: Documentos cifrados con cifrado AES-256 por la Aplicación mediante claves aleatorias totalmente entrópicas
- En tránsito: Documentos cifrados con HTTPS mediante uso de los protocolos de seguridad TLS actuales
- Todos los documentos se conservan en una infraestructura de almacenamiento de objetos de alta seguridad mediante la codificación de borrado que, según el tamaño del documento, escribe de forma síncrona los documentos en varios centros de datos dispersos geográficamente o divide matemáticamente los documentos en varios segmentos de datos que se distribuyen en varios centros de datos geográficamente dispersos
- Todos los archivos o secciones de datos se ocultan al colocar de forma aleatoria archivos individuales en más de un millón de directorios lógicos dentro de cada centro de datos utilizando una estructura de archivos no enumerada dentro del almacén de objetos de almacenamiento.

## 6. Mejores prácticas

- Retención de soportes defectuosos (DoD 5520)
- Acceso de operador reforzado (acceso MFA, túnel VPN, desactivación de medios extraíbles)
- Pruebas de penetración independientes dos veces al año
- Análisis mensuales de vulnerabilidades
- Entrenamiento regular
- Verificaciones anuales de antecedentes y crédito para todos los empleados
- Requisitos de complejidad de la contraseña
- Se requiere un cambio de contraseña obligatorio cada 90 días
- Aceleración de Internet (Akamai)
- Auditorías anuales de tipo 2 SOC 2 para seguridad, disponibilidad y privacidad
- Certificación ISO 27001 con los controles adicionales de ISO 27017, ISO 27018 e ISO 27701
- Certificación independiente del cumplimiento de los requisitos de seguridad aplicables de HIPAA y HITECH

## 7. Segregación de responsabilidades y acceso

- Hardware: operadores de centros de datos
- Aplicación: ingeniería y control de calidad
- Red - I.T. Personal
- Servidores y almacenamiento - I.T. Personal
- Seguridad: acceso de dos factores por parte del personal de seguridad con auditoría del equipo de cumplimiento independiente
- Cumplimiento y auditorías: equipo de cumplimiento independiente

## 8. Planificación para el futuro

- Ampliación de protocolos y políticas de seguridad
- Gestión de correo electrónico integrada en la nube
- Funcionalidad OCR integrada
- Mensajería instantánea integrada para una colaboración segura vinculada a documentos o proyectos
- Desarrollo activo de funciones y características adicionales



## CERTIFICACIONES DE SEGURIDAD Y CUMPLIMIENTO NORMATIVO

NetDocuments se somete a auditorías anuales de tipo 2 SOC 2 para seguridad y disponibilidad y auditorías anuales de certificación ISO 27001 que incluyen los controles adicionales de ISO 27017, 27018 y 27701. La certificación ISO 27001 también incluye todos los centros de datos utilizados por NetDocuments.

Además de estas auditorías anuales, NetDocuments revisa activamente los requisitos de seguridad de la industria aplicables, así como las regulaciones de seguridad locales, estatales y nacionales para determinar los esfuerzos de cumplimiento apropiados. Los ejemplos incluyen requisitos de seguridad individuales de varios estados dentro de los EE.UU., el Reglamento General de Protección de Datos (GDPR) adoptado por la UE y los requisitos de seguridad establecidos por la Dirección de Señales de Australia.

NetDocuments modifica y amplía regularmente sus controles de seguridad para mantener los niveles más altos de seguridad para los datos de los clientes en todo el mundo mediante el cumplimiento de las normas y regulaciones adecuadas.

## TU SOCIO DE SEGURIDAD

NetDocuments se asocia con sus clientes para implementar y demostrar los niveles de seguridad requeridos. Esto incluye revisar los requisitos de seguridad únicos y respaldar las auditorías de cumplimiento de seguridad del cliente.

NetDocuments se compromete a proporcionar a sus clientes el sistema de gestión de documentos más funcional y seguro disponible. Puede obtener más información sobre las iniciativas de seguridad y cumplimiento en NetDocuments visitando [netdocuments.com](https://netdocuments.com) o comunicándose con el Equipo de Cumplimiento en NetDocuments en [compliance@netdocuments.com](mailto:compliance@netdocuments.com).

