
White Paper

DocuWare Cloud

12 de diciembre 2019

Copyright © 2018 DocuWare GmbH

Reservados todos los derechos

El software contiene información propiedad de DocuWare. Se ha escrito con la licencia correspondiente y está protegida por las leyes de derechos de autor. El contrato de licencia contiene restricciones relativas a su uso y publicación. La reingeniería del software está prohibida.

Este producto se está desarrollando constantemente y la información que se ofrece aquí se puede cambiar sin previo aviso. Los derechos de propiedad intelectual e información que contiene este documento constituyen información confidencial, a la que sólo pueden acceder DocuWare GmbH y el cliente, y son propiedad exclusiva de DocuWare. Si observa algún error en la documentación, comuníquenoslo por escrito. DocuWare no garantiza que este documento no contenga ningún error.

Ninguna parte de esta publicación se puede reproducir de forma alguna ni por ningún medio (electrónico, mecánico, fotocopia, grabación u otros), ni se puede almacenar en un sistema de recuperación de datos ni transmitir sin el previo consentimiento por escrito de DocuWare.

Este documento se ha creado con AuthorIT™, Total Document Creation.

Renuncia de responsabilidad

El presente documento se ha redactado cuidadosamente y la información en él incluida procede de fuentes fiables. No obstante, no asumimos ninguna responsabilidad sobre la exactitud, exhaustividad o relevancia de la información. Por tanto, no se aceptarán reclamaciones a raíz del uso de la información contenida en este documento. DocuWare GmbH se reserva el derecho de modificar dicha información en cualquier momento sin previo aviso.

DocuWare GmbH
Therese-Giehse-Platz 2
82110 Germering
www.docuware.com

Contenido

1	Finalidad del White Paper	4
2	Introducción	5
3	Seguridad	6
3.1	Seguridad TI	6
3.2	Seguridad y protección de datos	8
4	Capacidad de ampliación	11
5	Capacidad de integración	12
6	Soporte de sistema con disponibilidad total	13
7	Transferencia de datos al final del contrato	15
8	Cumplimiento y legalidad	16

1 Finalidad del White Paper

DocuWare Cloud representa una solución en la nube de múltiples usuarios para la gestión de documentos y la automatización de flujos de trabajo. El presente White Paper describe las características técnicas de DocuWare Cloud, centrándose en las medidas técnicas y organizativas que DocuWare adopta en las áreas de seguridad (seguridad TI y protección de datos) y capacidad de ampliación. Otros temas incluyen Support, como la migración de datos y el cumplimiento y la certificación. El White Paper está dirigido, en concreto, a empleados técnicos de posibles clientes, empresas interesadas y socios de ventas, así como a consultores o medios especializados.

2 Introducción

DocuWare Cloud representa una solución de "Software as a Service" (SaaS). DocuWare, a su vez, utiliza los servicios de Microsoft Azure como "Platform as a Service" (PaaS) para su oferta. Todos los documentos, archivos y metadatos del cliente se almacenan en el Azure Storage. Las bases de datos están alojadas en Azure SQL (Managed Service).

El presente White Paper se limita a los servicios directos de DocuWare. En su propia página web, Microsoft describe los servicios de [Microsoft Azure](#), así como las [medidas asociadas a la seguridad TI y la protección de datos](#) en las que se basa DocuWare.

3 Seguridad

Los datos del cliente en DocuWare Cloud están protegidos de acuerdo con las reglas de tecnología generalmente aceptadas. Esto se garantiza mediante la infraestructura TI y las tecnologías de Microsoft Azure Security Services y DocuWare, así como su adecuación a las directivas actuales de protección de datos.

3.1 Seguridad TI

Mediante la codificación de documentos y comunicaciones, un concepto sofisticado de derechos, restricciones de acceso y auditorías de seguridad, DocuWare Cloud garantiza la seguridad de sus datos.

Codificación de documentos

Todos los documentos archivados en DocuWare Cloud se codifican automáticamente utilizando el método AES (Advanced Encryption Standard). Los documentos que se migran desde los sistemas DocuWare On-Premises se pueden codificar posteriormente. AES representa un método criptográfico simétrico que cumple con los requisitos de seguridad más exigentes. Como estándar de codificación, está autorizado, por ejemplo, por el gobierno de los EE. UU. para documentos con el mayor nivel de clasificación (Top Secret).

El método AES genera un par de codificaciones asimétricas para cada archivo. A su vez, la codificación privada se utiliza para codificar las codificaciones simétricas que se generan al codificar los documentos de un archivo. La clave de codificación del archivo se vuelve a codificar con una codificación maestra.

A fin de lograr la máxima protección, DocuWare utiliza una longitud de codificación de 256 bits en la codificación con AES. Para la codificación de codificaciones simétricas, se utiliza una longitud de codificación de 1024 bits. Se genera una nueva codificación simétrica para cada documento. Como resultado, incluso con un criptoanálisis, no se pueden detectar patrones y, por lo tanto, no se pueden calcular codificaciones.

Codificación de la comunicación

En un centro de datos utilizado por DocuWare, todos los datos del cliente están protegidos mediante una VPN (Virtual Private Network). La infraestructura de red también está virtualizada y la red virtual está protegida desde el exterior.

Para la codificación del tráfico de datos entre los usuarios y el centro de datos, se utiliza el protocolo TLS actual (protocolo sucesor de SSL), siempre y cuando resulte compatible con el navegador correspondiente. TLS se utiliza para todo el tráfico basado en HTTP (HTTPS) y TCP. Los usuarios consultan inmediatamente en el navegador si su conexión está asegurada y validada: En una conexión segura, la barra de URL se vuelve verde (a excepción de Google Chrome).

Para mayor protección contra ataques externos, existen capas y funciones de seguridad adicionales, por ejemplo, HSTS como protección contra ataques de degradación de protocolo y secuestro de "cookies".

Concepto de derechos

DocuWare Cloud utiliza un sofisticado sistema de derechos. La distinción entre derechos funcionales y derechos de archivadores resulta fundamental para la gestión de derechos en DocuWare.

Los derechos funcionales se asignan por organización de DocuWare y hacen referencia a ciertas funciones. Estos incluyen, por ejemplo:

- Administrar usuarios
- Configurar archivos y bandejas
- Diseñar flujos de trabajo
- Utilizar sellos
- Configuraciones de componentes de DocuWare como, por ejemplo, crear y editar Connect to Outlook, Smart Connect o DocuWare Forms.

Los derechos de archivadores hacen referencia a un archivo específico y a los documentos almacenados en él. Los derechos de archivadores incluyen:

- Gestionar autorizaciones administrativas, como derechos o diálogos, o migrar documentos.
- Guardar, buscar, editar o eliminar autorizaciones generales con respecto a los documentos en el archivo, por ejemplo, documentos.
- Autorizaciones de superposición, como el sellado de documentos, la aplicación de anotaciones y elementos gráficos a los documentos o la eliminación de anotaciones.
- Las autorizaciones de los campos de índice, como cambiar los contenidos de los campos o usar entradas de campos que no están en una lista de selección.

Derechos para usuarios y administradores

Para todas las configuraciones de DocuWare Cloud, por ejemplo, bandejas, archivos o formularios, asigne autorizaciones, ya sea a los usuarios directamente o a través de roles. Existen dos tipos diferentes de autorizaciones: Con el derecho del usuario, se puede utilizar el objeto en cuestión. El derecho de administrador le permite cambiar el objeto o su configuración.

Restricción de acceso por separación de datos

DocuWare Cloud separa estrictamente los datos del cliente de los datos del sistema, es decir, una organización de DocuWare por cliente.

Los administradores de los sistemas de DocuWare Cloud solo tienen acceso a los datos del sistema que se necesitan urgentemente para el servicio. Consulte también el capítulo [Support > Mantenimiento](#).

Los administradores de DocuWare de los clientes tienen acceso completo a la configuración de sus respectivas organizaciones, pero no a la configuración del sistema de DocuWare.

Auditoría de seguridad

Las pruebas regulares de penetración externa e interna contribuyen a mantener la seguridad de los sistemas siempre al nivel de las reglas de tecnología generalmente aceptadas. Los

auditores externos examinan detenidamente los resultados de las pruebas de penetración durante la certificación regular para el estándar SOC2.

Además, Azure Security Services proporciona informes detallados de los riesgos para poder resolver rápidamente cualquier problema que surja con Microsoft Azure.

Los clientes pueden llevar a cabo registros de documentos, archivos y organizaciones dentro de su organización y exportarlos para facilitar su lectura en formato CSV universal. Por ejemplo, es posible saber quién modificó una cierta configuración o guardó/eliminó los documentos. El registro, por ejemplo, demuestra el cumplimiento de las directrices legales.

Análisis de datos telemétricos

En los análisis de seguridad en tiempo real de los datos telemétricos, se comprueba si se producen eventos inusuales dentro de los sistemas de DocuWare en comparación con el servicio normal. En caso de detección de tales eventos, se tomarán las medidas adecuadas. Las investigaciones incluyen:

- Acceso a la base de datos (acceso y semántica de comandos)
- Índice de errores
- Modificaciones en el rendimiento
- Intentos de conexión
- Actualizaciones críticas del sistema
- Tráfico de red

3.2 Seguridad y protección de datos

DocuWare Cloud garantiza la seguridad, protección y recuperación de los datos del cliente de forma fiable cuando se configura y maneja adecuadamente. Por lo tanto, brinda apoyo al cliente en su cumplimiento con la ley de protección de datos regional válida. La protección de datos a través del diseño de tecnología (Privacy by design) ha representado un principio base para DocuWare desde la fundación de la empresa en 1988. Puede encontrar una descripción de las medidas técnicas y organizativas [aquí](#).

Seguridad de los datos

Todos los documentos utilizados por los clientes (datos productivos) se almacenan en un centro de datos de Microsoft Azure (ubicación principal). Esto se aplica tanto a los documentos en archivos como a los de las bandejas. Además, se almacenan dos copias de cada documento en este centro de datos inmediatamente después de modificarse o de llegar a DocuWare.

Además, a fin de salvaguardar todo el inventario de datos productivos para grandes daños, como terremotos o accidentes aéreos, se realizan tres copias de cada documento en un segundo centro de datos ubicado en una ubicación diferente pero en la misma región (almacenamiento georredundante, AGR).

Ambas ubicaciones siempre cuentan con la versión más actualizada de cada documento.

Protección de datos

El funcionamiento de los sistemas está sujeto a la ley regional de protección de datos. Los datos de los clientes de la región EMEA se alojan en centros de datos ubicados en la Unión Europea (UE). La ubicación principal actual es Dublín (Irlanda) y la ubicación AGR es Ámsterdam (Países Bajos). Los datos están sujetos al Reglamento General de Protección de Datos (RGPD) de la UE.

Los datos de nuestros clientes de la región de América del Norte y América del Sur se alojan en centros de datos ubicados en Estados Unidos. La ubicación principal actual se encuentra en el estado de Iowa y la ubicación AGR en Virginia. Los datos de clientes americanos están sujetos a la política de protección de datos de EE. UU.

Copia de seguridad

Si el cliente eliminó documentos accidentalmente, es posible restaurarlos en caso necesario. Incluso si los documentos se han modificado incorrectamente, se puede restaurar cualquier borrador anterior. En ambos casos, se aplican las siguientes restricciones.

Para permitir un restablecimiento, tanto las bases de datos como los documentos están respaldados por DocuWare como copias de seguridad en su propio Cold Storage. Dicho Cold Storage se encuentra en un centro de datos de Microsoft en la región correspondiente: para la UE actualmente en Ámsterdam (Países Bajos) o para América en el estado de Washington (EE. UU.).

Para ello, se realiza y se almacena una copia de seguridad de cada documento. Dicha copia se realiza poco después de que el documento se haya guardado o modificado en DocuWare. En el caso de una copia de seguridad tras la modificación del documento, se crea una nueva copia del documento. Dicha copia se guarda, además de las copias de seguridad existentes del documento. Esto siempre se aplica, tanto con la versión de documentos activada como no activada en DocuWare.

El Cold Storage se encuentra físicamente separado del dominio de DocuWare, lo que significa que la base de datos también está protegida contra posibles daños en el dominio de DocuWare. La generación de copias de seguridad en Cold Storage se supervisa continuamente de forma automática. Las copias de seguridad en Cold Storage se conservan durante, al menos, un año.

Al importar manualmente los datos de la copia de seguridad en el sistema productivo, una organización de DocuWare se puede restaurar completamente en cooperación con DocuWare Support. Si el cliente requiere datos de la copia de seguridad debido a un manejo inadecuado (por ejemplo, eliminación o modificación accidental de documentos), el cliente se hará cargo de los gastos de Support en la recuperación.

La recuperación de un documento solo es posible si el documento no se ha modificado o eliminado durante su copia de seguridad. La copia de seguridad de un documento nuevo o modificado se iniciará en no menos de cinco segundos después de que el documento se haya registrado en el archivador.

Para utilizar la versión correcta de la base de datos para la restauración, DocuWare requiere que el cliente proporcione información sobre cuándo el documento que restaurar todavía estaba visible en el archivador. Para que las entradas de la base de datos asociadas se

restauren, el cliente debe enviar la solicitud a Asistencia de DocuWare a más tardar 7 días después de eliminar o modificar el documento.

Además de los documentos, las copias de seguridad completas de las bases de datos de SQL se llevan a cabo en Cold Storage, principalmente los fines de semana y en horario nocturno en la región.

File Share Snapshots

Además de realizar copias de seguridad de los documentos, el servicio Azure Files de Microsoft genera File Share Snapshots una vez a la semana. Dichos archivos contienen las modificaciones con respecto al estado anterior. Las capturas se guardan durante, al menos, un año.

Por lo tanto, todos los documentos de un cliente se protegen varias veces en diferentes ubicaciones contra daños y en cumplimiento con la ley de protección de datos regional en cuestión.

DocuWare se reserva el derecho a modificar o ampliar las ubicaciones de los datos productivos, AGR y de copias de seguridad (en concreto, si se modifican las ubicaciones ofrecidas por Microsoft Azure) mientras permanezcan en el territorio económico correspondiente (UE o EE. UU.).

4 Capacidad de ampliación

Tanto DocuWare como Microsoft Azure en el marco de su infraestructura PaaS (Platform as a Service) ofrecen métodos y tecnologías de capacidad de ampliación extensiva.

Capacidad de ampliación por cliente

DocuWare Cloud es compatible con equipos de todo tipo y tamaño. Se puede adaptar de manera flexible en términos de volumen de almacenamiento y número de licencias de usuario al tamaño de la empresa en cuestión y al volumen de documentos.

Capacidad de ampliación del sistema Cloud

DocuWare Cloud se amplía automáticamente según la cantidad de usuarios, la cantidad de datos y el tamaño de la carga de procesamiento. Dado que DocuWare Cloud es una Public Cloud, la ampliación se realiza por sistema y no por organización del cliente.

Rendimiento y distribución de carga

La distribución de la carga en todos los servicios disponibles garantiza un alto rendimiento constante de todo el sistema DocuWare. DocuWare Cloud responde rápida y dinámicamente a condiciones de carga fluctuantes a través de una escala mayor o menor de los servicios existentes o la agregación de servicios completos.

5 Capacidad de integración

Para maximizar el uso de la administración de documentos y la automatización del flujo de trabajo, DocuWare Cloud se conecta a prácticamente cualquier aplicación empresarial. Esto funciona independientemente de si dicha aplicación funciona como un sistema local o basado en la nube. Para obtener más información, consulte [DocuWare White Paper Integration](#).

6 Soporte de sistema con disponibilidad total

Control

El centro de datos de Microsoft Azure controla constantemente todas las operaciones. Los incidentes destacados se notifican automáticamente al soporte del sistema de DocuWare. El control incluye:

- Controles constantes del rendimiento
- Pruebas completas regulares de las funciones básicas de DocuWare
- Encuestas estadísticas de patrones de uso de clientes, como la cantidad de acciones que realizan los clientes en una ventana de tiempo determinada (por ejemplo, búsqueda y archivado de documentos, inicio de sesión) para permitir mejoras de rendimiento.

En el caso de irregularidades, el soporte del sistema de DocuWare interviene inmediatamente con servicio ininterrumpido.

Revisiones y actualización

Una o dos veces al año, la nueva versión de DocuWare se importa a las organizaciones de los clientes. Para ello, la organización se desconecta, se realiza la actualización y, a continuación, la organización vuelve a conectarse con la nueva versión de DocuWare.

DocuWare informa a los clientes sobre la actualización planificada con cuatro semanas de antelación. En caso de error, la organización se volverá a poner en línea con la versión anterior de DocuWare, para evitar períodos de inactividad.

Los componentes instalados localmente (Desktop Apps) siempre deben mantener a los clientes actualizados. Los propios usuarios pueden realizar dichas actualizaciones de forma sencilla, siempre y cuando estén autorizados para instalar "software" localmente. De lo contrario, el administrador de TI puede realizar la actualización silenciosa (Silent Install) utilizando una solución de administración de software.

Mantenimiento

Ciertas actividades de mantenimiento requieren derechos de administración completos o avanzados a los sistemas DocuWare Cloud. Para garantizar la seguridad de los datos que cumple con las normas de tecnología generalmente aceptadas, el acceso de los administradores de mantenimiento está sujeto a registro.

Además, se aplican los siguientes mecanismos de seguridad:

- Todos los accesos a los sistemas de DocuWare Cloud se realizan a través de una sesión RDP.
- Para poder iniciar una sesión RDP, un administrador debe seleccionarla a través de direcciones IP definidas y especialmente protegidas en una VPN que esté protegida por certificados y solo esté disponible para los administradores.
- Cada administrador de DocuWare Cloud cuenta con su propia identificación. Por lo tanto, siempre se puede saber quién ha iniciado sesión en qué sistema.

- Todos los administradores están capacitados y han recibido formación específica sobre la manipulación cuidada y protegida de datos, como certificados y contraseñas.

7 Transferencia de datos al final del contrato

Los datos del cliente son siempre propiedad del cliente

En caso de que un cliente decida rescindir el contrato, DocuWare le brindará asistencia si desea descargar sus documentos de DocuWare Cloud System o migrarlos a otro sistema. Existen dos opciones para esto:

1. Las pequeñas cantidades de documentos que no necesitan procesarse a tiempo o en absoluto pueden exportarse y utilizarse con DocuWare Request en forma de archivos independientes. Esta opción está limitada a un máximo de 50 000 documentos o 10 GB de almacenamiento.
2. Los especialistas de DocuWare Professional Services prestan ayuda en caso de grandes volúmenes de datos y muchos documentos integrados en los procesos actuales. Sus servicios de pago ofrecen las siguientes ventajas:
 - Tras consultar con el cliente, el acceso a los documentos se realiza directamente en el centro de datos y, por lo tanto, se transfieren grandes cantidades de datos en el menor tiempo posible.
 - Los documentos dinámicos e integrados en los procesos actuales se migran a los procesos de un nuevo sistema de manera oportuna, minimizando así las interrupciones de los flujos de trabajo.
 - Se desarrollan soluciones a medida del flujo de trabajo y los tipos de documentos utilizados por los clientes.

Tras la rescisión del contrato, todos los datos del cliente dentro del sistema DocuWare Cloud y todos los datos de las copias de seguridad se eliminarán de manera segura e irrevocable: después de 60 a 90 días en la ubicación principal y en la ubicación AGR y, durante el siguiente trimestre, en Cold Storage.

La recuperación de los datos ya no resulta posible a partir de este momento.

8 Cumplimiento y legalidad

Certificaciones de DocuWare y DocuWare Cloud



Las certificaciones que hacen referencia a una versión de software no se ejecutan para cada nueva versión, sino que se renuevan regularmente. Encontrará más información sobre las certificaciones DocuWare en <https://pub.docuware.com/es/cumplimiento-y-certificaciones>.

Microsoft ha destacado en el sector por el establecimiento de requisitos claros de seguridad y privacidad, y por cumplir estos requisitos de forma constante. Azure cumple un amplio abanico de normas internacionales y específicas del sector, como el Reglamento General de Protección de Datos (RGPD), ISO 27001, HIPAA, FedRAMP, SOC 1 y SOC 2, así como normas específicas de cada país, entre las que se incluyen: IRAP en Australia, G-Cloud en el Reino Unido y MTCS en Singapur. Auditorías de terceros rigurosas, como las del Instituto Británico de Normalización, confirman que Azure se adhiere a los estrictos controles de seguridad que estos estándares exigen. Más información sobre las [certificaciones de Microsoft Azure](#).

Modificaciones de White Paper Cloud

DocuWare se reserva el derecho a modificar el contenido de White Paper Cloud por razones legítimas, en particular con respecto a los servicios y estándares descritos, siempre y cuando resulte razonable para el cliente. Existe una razón legítima en caso de avance técnico, introducción de nuevos servicios o estándares, modificaciones en la oferta de servicios de los proveedores de servicios utilizados (en particular, Microsoft) o prescripciones legales u oficiales modificadas.