



## La seguridad en Documoto

### Protegiendo sus activos más valiosos

La tarea más importante en Digabit es la protección de sus datos. Combinamos las tecnologías de seguridad más avanzadas del mercado con las mejores prácticas de software para garantizar que sus datos están completamente seguros.

#### El centro de proceso de datos de Documoto

Digabit aloja sus sistemas de producción en una ubicación segura del *backbone* de Internet. En ella se dispone de una potente tecnología de red, múltiples sistemas de alimentación y proximidad a líneas de fibra completamente redundantes de proveedores de red Tier 1. Nuestro centro de datos está diseñado para alojar exclusivamente sistemas de misión crítica con un nivel de servicio superior al 99%. Puede confiar en nosotros, su información es inexpugnable y Documoto opera siempre eficientemente. Las medidas de seguridad son el fiel reflejo de nuestro compromiso. Nuestro alojamiento es totalmente redundante, cumple con PCI Nivel 1 y está certificado según SSAE 16 para garantizar que las políticas y procedimientos se actualizan a medida que evolucionan las tecnologías.

Verificado por una firma de auditoría independiente, el centro de datos de Digabit completó satisfactoriamente la auditoría SSAE 16 de su entorno de control interno. La firma auditó los procesos y políticas de hosting para garantizar la conformidad con los controles documentados, incluyendo inspecciones y pruebas locales.

#### Diseño del entorno

- » Centro de operaciones de red con personal presente 24 x 7 x 365
- » Proveedores de red redundantes, entre ellos Qwest, XO, Time Warner, Internap y MHO
- » Detección de incendios: Fike Cheetah Photoelectric + VESDA
- » Extinción de incendios: Pre-action dry pipe
- » Ventilación y refrigeración redundantes Liebert
- » Flujo de aire controlado en suelos elevados para estabilidad de la temperatura

#### Suministro eléctrico

- » Alimentación redundante N+1
- » 4 generadores Diesel con más de 88 horas de autonomía.
- » Sistema de test periódico

#### Seguridad

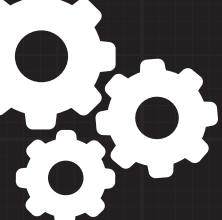
- » Personal de seguridad presente 24 x 7 x 365
- » Cámaras de seguridad en todo el edificio y exteriores
- » Acceso por tarjetas en las oficinas y pasillos del centro de datos
- » Pasillo de seguridad con trampa de intrusos
- » Escanners biométricos de manos



#### ¿Qué es SSAE 16?

SSAE 16, acrónimo de Statement on Standards for Attestation Engagements 16, es una norma de auditoría desarrollada por el American Institute of Certified Public Accountants (AICPA). SSAE 16 está concebida para que los auditores revisen los controles establecidos por los proveedores de servicios. Auditores independientes verifican los objetivos y actividades para garantizar que los controles son válidos y que se cumplen.

Los controles de Digabit incluyen: acceso/seguridad del edificio, del data center, del área de almacenamiento, de la información de los clientes y de los procedimientos de cambio en el hardware y el software.



## La plataforma software Documoto

Digabit aplica la mejores prácticas de la industria para proteger el almacenamiento y transmisión de los datos de sus clientes

### Seguridad de las Comunicaciones y Sistemas Operativos

Programamos nuestro software teniendo en cuenta los sistemas más actualizados para prevenir intrusiones en internet mediante cross-site scripting, JavaScript e inyecciones SQL.

Adicionalmente, **todas las comunicaciones entre el PC del cliente y nuestros servidores se efectúan en modo seguro mediante Secure Sockets Layer (SSL)**. Éste es un protocolo criptográfico para comunicaciones seguras en Internet que evita escuchas o manipulaciones de los datos. Todavía más, cada sesión es validada, reduciéndose enormemente la posibilidad de apropiación de la sesión por terceros.

El acceso al sistema de producción de Documoto se efectúa estrictamente bajo el principio de “el menor privilegio”, permitiendo el acceso únicamente a quienes lo necesitan y con solamente los privilegios que son absolutamente esenciales para su trabajo.

Los servidores de Digabit están protegidos acorde con las mejores prácticas. Hacemos tests de vulnerabilidad periódicamente, y las excepciones se corrigen según sea proceda. Las actualizaciones de los sistemas operativos y del código de programa se instalan durante paradas de mantenimiento planificadas. Todos los cambios se revisan concienzudamente antes de ser aplicados al entorno de producción.

### Los Objetos y la Seguridad de los Datos en un entorno Multi-Tenant

“Multi-tenant” y “Cloud” son términos habituales en el mundo del software moderno. Para entenderlo fácil, significa que múltiples clientes comparten una misma instancia física de una plataforma software sin que vean jamás los datos de los otros clientes.

Hemos diseñado Documoto sobre la base de un sistema multi-tenant seguro, creando muros de seguridad virtuales entre los tenants. A cada tenant se le asigna un Tenant Encrypted Key (TEK) que sirve como vía de acceso para únicamente sus propios datos.

Al crear usuarios, quedan asociados a un único tenant. Cuando acceden al sistema, éste garantiza que los datos a los que acceden son exclusivamente los del tenant al que pertenecen.

Además, nuestro modelo de seguridad permite un modo de acceso a la información y privilegios extremadamente granulares. **Usted controla quién de su organización tiene acceso a qué documentos, separándolos por grupos de usuarios y con sus propios controles de acceso.** Adicionalmente, no se almacenan contraseñas, claves ni ninguna otra información de seguridad en el PC del cliente. Todo está encriptado en el server. Esto implica que, por razones de seguridad, ni siquiera el personal de Digabit puede decodificar ningún password.

Los documentos de los clientes están en un repositorio blindado, y no se puede acceder a ellos sin autenticarse como usuario, ni tampoco escribiendo la URL en un navegador. Gracias a nuestra capa de seguridad en la aplicación es imposible que un usuario que está en un tenant pueda acceder a los documentos de otro tenant.



Con toda seguridad,  
¡sus datos están protegidos!

La seguridad en Digabit está siempre al día. Compruébelo en [www.digabit.com/learn-more/secure-your-data/](http://www.digabit.com/learn-more/secure-your-data/)