FOXIT ESIGN: DESCRIPCIÓN GENERAL DE SEGURIDAD

DOCUMENTO TÉCNICO

ÍNDICE

La seguridad es el núcleo fundamental de Foxit eSign. Como todos nuestros productos, Foxit eSign se desarrolló y diseñó teniendo en cuenta la seguridad ante todo.

Este documento proporciona una descripción general de las tecnologías de seguridad, políticas y prácticas utilizadas por Foxit eSign que protegen sus datos y documentos, incluida la información que le permite realizar configuraciones de seguridad para satisfacer los requerimientos únicos de gestión de riesgo y cumplimiento de su empresa.

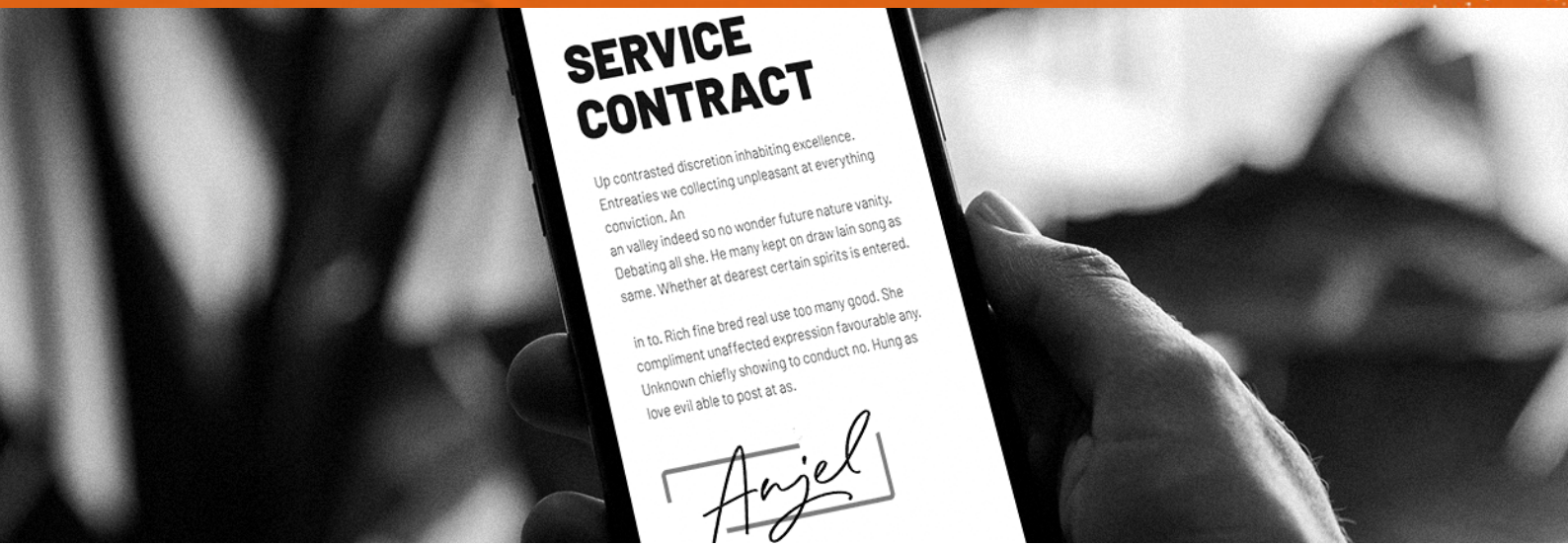
Este documento identifica además varias regulaciones regionales con las que Foxit eSign cumple estrictamente, para asegurar que usted pueda realizar el despliegue.

SEGURIDAD Y CIFRADO DINÁMICOS

Foxit eSign cuenta con la certificación SOC 2 tipo 2. Recibe auditorías en forma regular de parte de auditores independientes de la industria, para asegurar el cumplimiento estricto de los 5 principios de servicio de confianza. A continuación, se describen los compromisos de servicio que hace Foxit eSign con las entidades de usuario, las leyes y regulaciones que rigen la prestación de sus servicios de gestión de productividad y firma electrónica, además de los requerimientos financieros, operacionales y de cumplimiento que Foxit eSign haya establecido para sus servicios.

Seguridad: protección de sus datos contra el acceso y la visualización sin autorización a través de nuestro sistema

- Foxit eSign se compromete a emplear medidas administrativas y técnicas de conformidad con las prácticas industriales aplicables para proteger el sistema y evitar la pérdida accidental o el acceso, uso, alteración o divulgación sin autorización de los datos de los clientes bajo su control, durante el plazo de cada pedido.
- Todos los datos transmitidos entre nuestros sistemas y usuarios están protegidos mediante seguridad de la capa de transporte (TLS) y seguridad de transporte HTTP estricta (HSTS).
- El acceso a entornos que contengan datos de los clientes requiere una serie de controles de autenticación y control, incluida la autenticación multi-factorial (MFA).



Disponibilidad: asegurar que nuestro software esté disponible según sea necesario y con base en lo acordado

- Foxit eSign se compromete a utilizar esfuerzos comercialmente razonables para que el sistema esté disponible de modo que los usuarios finales puedan acceder a este y utilizarlo a través de Internet al menos el 99,95 % del tiempo, según las mediciones durante el transcurso de cada mes natural, excluida la falta de disponibilidad como resultado de un mantenimiento programado. Sin embargo, Foxit eSign ha mantenido una disponibilidad del 99,99 % durante los últimos 5 años.

Confidencialidad: mantener sus datos protegidos, privados y confidenciales

- Foxit eSign se compromete a proteger la información confidencial contra cualquier uso o divulgación sin autorización, en la misma medida en la que protegemos nuestra propia información confidencial. En ningún caso, usaremos menos de un estándar de cuidado razonable para proteger dicha información confidencial.
- Utilizamos información confidencial únicamente para el propósito por el que se divulgó.

Integridad del procesamiento: todo el procesamiento del sistema es completo: autorizado, preciso y rápido

- Los requerimientos y prácticas del sistema de Foxit eSign incluyen controles de monitoreo de rendimiento de la interfaz de programación de aplicaciones (API), monitoreo de adquisición de datos y el mantenimiento de políticas y procedimientos que ayudan en la prevención, detección y corrección de errores de procesamiento de datos.

Privacidad: estricta adherencia a los principios generalmente aceptados de privacidad (GAPP), los cuales indican que toda la información personal se retiene, recolecta, utiliza, divulga y destruye según lo establecido en nuestro aviso de privacidad

- Foxit eSign se compromete a proteger la información de identificación personal contra cualquier uso o divulgación sin autorización, en la misma medida en la que protegemos nuestra propia información de identificación personal. En ningún caso, utilizaremos menos de un estándar de cuidado razonable para proteger dicha información de identificación personal.
- Utilizamos la información de identificación personal únicamente para el propósito por el cual se divulgó.

Además, sus documentos están bloqueados y protegidos con cifrado de 256 bits de calidad industrial, además de controles estrictos de cortafuegos: todo el tráfico entrante y saliente se monitorea y debe respetar las estrictas reglas de seguridad de nuestra red. Foxit eSign proporciona protección de extremo a extremo mediante el cifrado de los datos en reposo y en movimiento.

VISIBILIDAD

Foxit eSign ofrece a sus clientes controles de visibilidad total, de modo que usted decida quién puede ver y acceder a los documentos de su organización. Esto incluye los siguientes controles:

- Personalice las características de visibilidad para limitar la vista de documento a solo los receptores designados que usted elija.
- Restrinja la visibilidad de las cuentas de usuario con características como Acceso a campos protegidos, que proporciona acceso solo a los usuarios aprobados a la información en los campos protegidos.
- Controle el acceso a la información al designar distintos niveles de usuario y configuraciones de uso compartido.
- Asigne gerentes a usuarios regulares y administradores, para asegurar que el monitoreo y el uso de documentos subordinados sean un proceso sencillo.

AUDITORÍA

Saber exactamente en dónde están sus documentos y en dónde han estado es un componte crucial de seguridad y cumplimiento. Foxit eSign provee informes de auditoría detallados y características de tal forma que los clientes puedan mantenerse informados acerca de los flujos de trabajo de sus documentos.

- Las pistas de auditoría detalladas rastrean cada documento por dirección IP y sello de hora, de modo que tenga pleno conocimiento acerca de dónde, cuándo y quién está viendo sus documentos en todo momento.
- Se proporciona un certificado de finalización para cada documento con la dirección IP asociada, dirección de correo electrónico, sello de hora y nombre de quien firma.
- Rastree la eliminación de documentos y carpetas en cada etapa del proceso. Nuestro historial de carpetas eliminadas le permite ver en dónde, cuándo y quién fue la persona que eliminó cualquier carpeta.

CENTROS DE DATOS

Es importante que nuestros clientes entiendan en dónde se almacenan sus documentos. También entendemos la importancia de la residencia local de los datos para nuestros clientes. En esa medida, Foxit eSign usa los centros de datos de Amazon Web Services (AWS). Nuestros centros de datos están diseñados para anticipar y tolerar fallas, al tiempo que mantienen los niveles de servicio y el acceso a los centros de datos se revisa de manera regular.

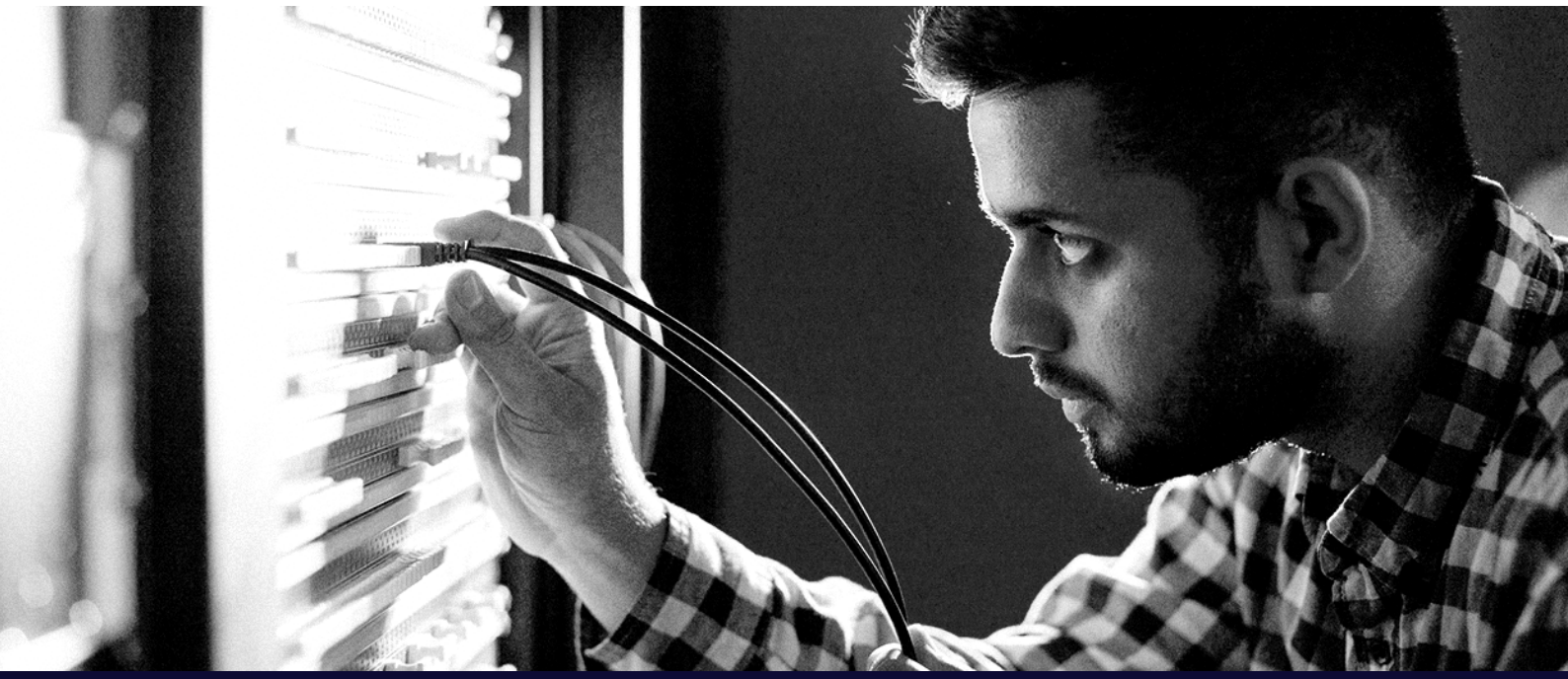
Ubicación de datos: Foxit eSign mantiene centros de datos de confianza en EE.UU. y Europa con instalaciones SSAE16 que cumplen con los estándares SOC 2 tipo 2 y PCI. En Estados Unidos, las aplicaciones se alojan en la plataforma AWS y operan principalmente en instalaciones ubicadas en Virginia del Norte (este de EE.UU.), Ohio (este de EE.UU.) y el norte de California (oeste de EE.UU.). En Europa, los centros de datos se encuentran en Frankfurt, Alemania. Estas instalaciones están bloqueadas y se monitorean a toda hora para asegurar que sus datos se almacenen solo en los servidores más seguros y protegidos.

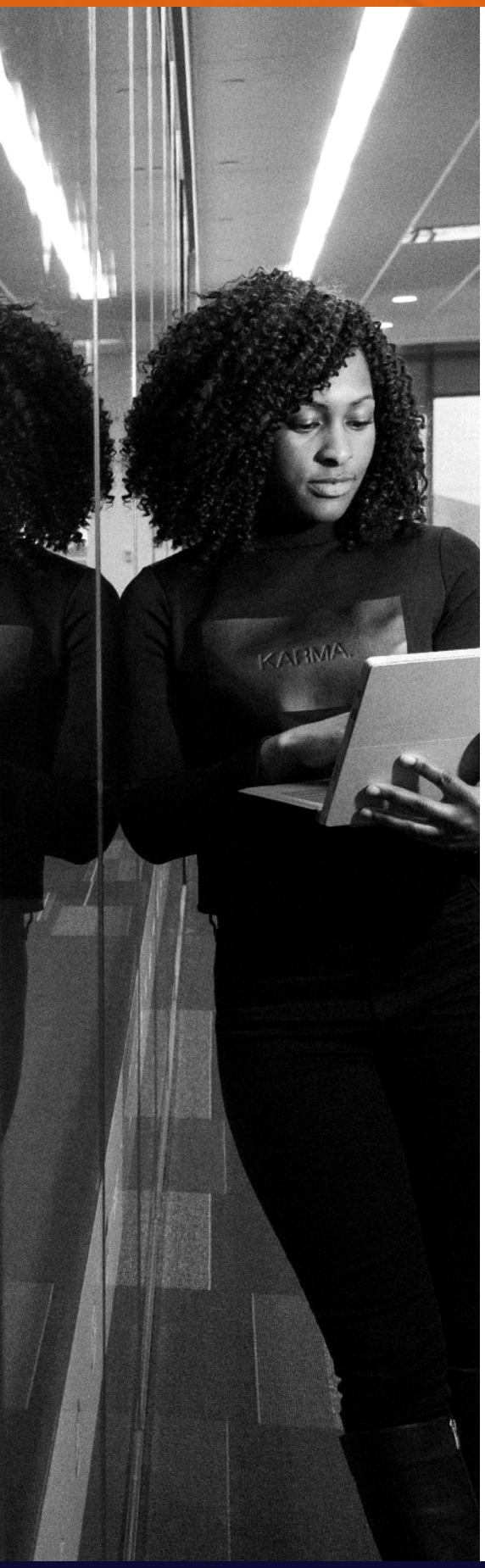
Residencia de los datos: cuando inicie sesión en una cuenta de Foxit eSign, se asignará a su región local para el almacenamiento en servidores. También proveemos a nuestros clientes la opción de elegir en cuál centro de datos desean almacenar sus documentos. Por último, se otorga a los clientes el completo control sobre quién puede acceder a sus documentos.

CONTINUIDAD COMERCIAL/RECUPERACIÓN DE DESASTRES

Los datos y archivos de Foxit eSign se almacenan en servidores de alta disponibilidad y bases de datos administradas; también se sincronizan en tiempo real con las bases de datos cifradas y los servidores de archivos de generación de informes y de respaldo. En caso de emergencia, los sistemas pueden ponerse en línea desde el respaldo u otra zona de disponibilidad.

Además, Foxit eSign mantiene una capacidad robusta del sistema y monitoreo de la infraestructura para asegurar rendimiento y disponibilidad. Los respaldos se realizan casi en tiempo real y son, en gran medida, un proceso continuo. La planificación de continuidad comercial y recuperación de desastres en Foxit eSign toma en cuenta un Análisis de impacto en el negocio (BIA), planes de manejo de incidentes, contingencia y continuidad comercial, lo que en conjunto conforma la estructura para mantener una estrategia de continuidad y contingencia, planes de gestión y operacionales. Foxit eSign ha diseñado políticas y procedimientos que cubren una falla parcial o completa de proveedores de servicios en la nube (CSP).





POLÍTICA DE RETENCIÓN DE DATOS

Nuestra política de retención de datos describe lineamientos importantes respecto de cuánto tiempo rastreamos y mantenemos su información, y cuándo la eliminamos. Las políticas de retención difieren según el tipo de cuenta. Las políticas de los tipos de cuentas se definen de la siguiente manera:

Cuentas de prueba: los documentos y datos relacionados de las cuentas gratuitas se eliminarán después de 30 días, a menos que el usuario la convierta en una cuenta de pago.

Cuentas de pago: los documentos base de las cuentas de pago se almacenarán en el sistema por 45 días, a menos que dichos documentos se envíen para su firma. Los usuarios de cuentas de pago también pueden configurar sus propias políticas de retención para cada tipo de documento, incluidos los documentos compartidos, parcialmente firmados, formalizados, cancelados y/o expirados.

Foxit
41841 Albrae Street
Fremont CA 94538, Estados Unidos

sales@foxit.com
support@foxit.com
www.foxit.com

Ventas: 1-866-680-3668
Soporte técnico: 1-866-693-6948
O 1-866-MYFOXIT