Resumen sobre la seguridad de Adobe Acrobat DC con los servicios de Document Cloud

Índice de contenido

Aunque Adobe Sign es parte de los servicios de PDF de Document Cloud, sus funciones de seguridad son independientes.

Resumen ejecutivo

En Adobe, nos tomamos la seguridad de tu experiencia digital muy en serio. Las prácticas de seguridad están profundamente integradas en nuestro desarrollo de software interno, nuestros procesos de operaciones y nuestras herramientas. Nuestros equipos multifuncionales siguen estas prácticas estrictamente para ayudar a evitar, detectar y responder a incidentes de forma oportuna. Estamos al día de las últimas amenazas y vulnerabilidades a través de nuestro trabajo de colaboración con partners, investigadores líderes, instituciones de investigación sobre seguridad y otras organizaciones del sector. Incorporamos de forma habitual técnicas de seguridad avanzadas a los productos y los servicios que ofrecemos.

Los servicios de Adobe que están en contacto con contenido del cliente han pasado muchas certificaciones del sector. Para obtener una lista detallada de todas los estándares y las certificaciones de cumplimiento, así como las normativas gubernamentales que cumplen actualmente las soluciones y los productos de Adobe, consulta la lista actual de certificaciones, estándares y normativas. Para obtener información sobre el RGPD, consulta la página sobre preparación para el RGPD.

Este informe técnico describe el enfoque de defensa en profundidad y los procedimientos de seguridad implementados por Adobe para mejorar la seguridad de Adobe Acrobat DC, Acrobat Reader DC, Document Cloud, los servicios de Document Cloud y los datos asociados.

Resumen de Adobe DC con los servicios de Document Cloud

Adobe Acrobat DC combina el último software de escritorio de Acrobat con las funciones premium de la aplicación móvil de Acrobat Reader y los servicios online de Adobe Document Cloud para ayudar a las organizaciones a cumplir con las exigencias de los usuarios finales respecto a la conectividad y la productividad en cualquier dispositivo mientras ayuda a garantizar la seguridad entre dispositivos. Con Adobe Acrobat DC y los servicios de Document Cloud, los clientes pueden convertir su contenido en un documento electrónico que puede compartirse con otros y generar, manipular y transformar con facilidad archivos PDF desde cualquier servicio en la nube, aplicación de escritorio y aplicación móvil de Adobe.

Funciones de seguridad de documentos de Acrobat

Censurar

Adobe Acrobat DC incluye un conjunto de herramientas de censura para ayudar a los clientes a proteger la información delicada o confidencial, incluida la eliminación permanente de tanto texto como imágenes en un documento antes de la distribución. Además, los usuarios pueden buscar y censurar contenido a partir de patrones como, por ejemplo, números de teléfono, números de tarjeta de crédito y direcciones de correo electrónico. La información censurada se elimina completamente del archivo, en lugar de quedar simplemente enmascarada como sucede con otras herramientas o métodos. Con la función de limpieza del documento, los clientes también pueden eliminar la información oculta y los objetos no gráficos como, por ejemplo, los metadatos que pueda haber en el PDF.

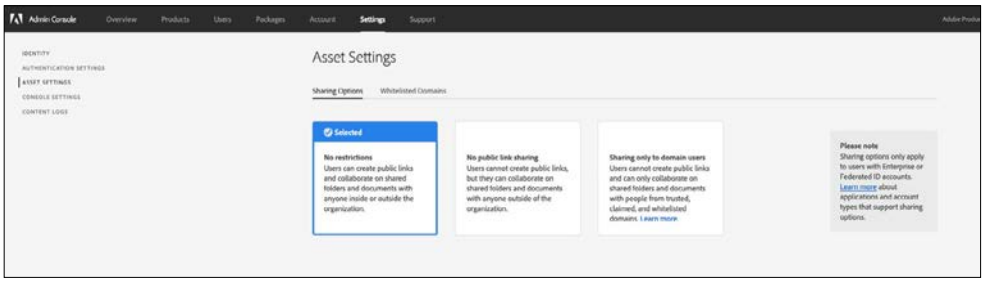
Compartir archivos

Todos los archivos de Document Cloud almacenados en la nube se etiquetan automáticamente como "privado", lo que significa que el contenido solo es visible para el usuario final que lo cargó. Un usuario final debe realizar acciones expresas para compartir ese contenido, o seguirá siendo privado. Todo el uso compartido de contenido de Document Cloud se completa enviando un enlace al contenido de Document Cloud a los destinatarios mediante correo electrónico, mensaje de texto o cualquier otro software para colaboración.

Los usuarios de los servicios de Document Cloud pueden compartir archivos con dos opciones: Solo ver o Revisar. Si el usuario envía el enlace con la restricción Solo ver, el destinatario solo puede ver el contenido como un documento de solo lectura. Por otra parte, si el usuario envía el documento para revisión, el destinatario puede comentar en el documento, pero no puede editarlo ni alterarlo de ninguna otra manera.

Configuración de activos y restricciones para compartir

La configuración de activos da el control a una organización sobre cómo sus empleados comparten los activos fuera de la organización. El administrador de TI puede seleccionar una configuración restrictiva que limita a los empleados el uso de determinadas funciones de uso compartido con Document Cloud, que incluye la restricción del uso compartido basado en invitación a destinatarios en los dominios reivindicados, de confianza y en la lista blanca. Cuando se establece esta política, se evita que los usuarios compartan activos pertenecientes a la organización con usuarios externos que no están en la lista de dominios permitidos.



Configuración de activos en la Admin Console

Microsoft Information Protection (MIP)

Para los clientes que usan Acrobat DC o Acrobat Reader DC para abrir archivos protegidos con las soluciones de Microsoft Information Protection (MIP), incluidas Azure Information Protection (AIP) e Information Protection para Microsoft Office 365, consulta este documento.

Modo protegido en Acrobat Reader DC

Para ayudar a proteger a los clientes de código malintencionado que intenta utilizar el formato PDF para escribir en el sistema de archivos de un ordenador o leerlo, Adobe ofrece una implementación de tecnología de zonas protegidas denominada "Modo protegido", que se introdujo por primera vez en Adobe Reader X.

La zona protegida es un método de seguridad que crea un entorno de ejecución limitado para ejecutar programas con derechos o privilegios reducidos. Estas zonas protegidas protegen los sistemas de los usuarios contra los daños causados por los documentos no fiables que contienen código ejecutable. En el contexto de Acrobat Reader DC, todos los archivos PDF y los procesos que estos invocan se consideran contenido no fiable. Acrobat Reader DC trata a todos los archivos PDF como potencialmente corruptos y limita todo el procesamiento que estos invocan a la zona protegida.

El modo protegido de Acrobat Reader DC ayuda a defenderse contra los atacantes que intentan instalar malware en un sistema informático, por lo que apoya los esfuerzos de las organizaciones para evitar que agentes malintencionados accedan y extraigan datos confidenciales y propiedad intelectual de sus redes. El modo protegido está activado de forma predeterminada cada vez que un usuario inicia Acrobat Reader DC y limita el nivel de acceso permitido al programa, lo que protege a los sistemas que ejecutan Microsoft Windows de los archivos PDF malintencionados que puedan intentar escribir en el sistema de archivos del ordenador o leerlo, eliminar archivos o modificar de cualquier otro modo la información del sistema.

El modo protegido en Windows 8 y versiones posteriores también puede ejecutarse en un AppContainer de Windows, que proporciona un entorno de protección aún más sólido a los clientes que activen el modo protegido.

Vista protegida en Acrobat DC

De forma similar al modo protegido de Acrobat Reader DC, la vista protegida consiste en la implementación de una tecnología de zonas protegidas para el sofisticado conjunto de funciones de este programa. En Acrobat DC, Adobe amplía la funcionalidad del modo protegido para ir más allá del bloqueo de los ataques basados en escritura que tratan de ejecutar código malintencionado en un ordenador a través del formato de archivo PDF, para también ofrecer protección contra los ataques basados en lectura que intentan robar datos confidenciales o propiedad intelectual a través de archivos PDF.

Al igual que el modo protegido, la vista protegida limita la ejecución de los programas no fiables (por ejemplo, cualquier archivo PDF y los proceso que este invoque) a una zona protegida y limitada con el fin de evitar que el código malintencionado utilice el formato PDF para escribir o leer en el sistema de archivos del ordenador. La vista protegida presupone que todos los archivos PDF son potencialmente malintencionados y limita el procesamiento a la zona protegida, a menos que el usuario indique específicamente que un archivo es de confianza.

La vista protegida es compatible en ambas circunstancias en las que los usuarios abren documentos en PDF: desde la aplicación independiente de Acrobat DC y desde un navegador. En Windows 8 y versiones posteriores, la vista protegida se ejecuta siempre en un AppContainer. Esto proporciona un entorno de protección aún más sólido a los clientes que activen la vista protegida.

Cuando un usuario abre un archivo no fiable dentro de la vista protegida, Acrobat DC muestra una barra de mensajes en la parte superior de la ventana de visualización. La barra de mensajes indica que el archivo no es fiable y recuerda al usuario que está en la vista protegida, lo que desactiva muchas de las funciones de Acrobat DC y limita la interacción del usuario con el archivo. Básicamente, el archivo está en modo de "solo lectura", y la vista protegida se defiende frente a que el contenido que incorpora o que está incrustado en él altere el sistema.

Para confiar en el archivo y activar todas las funciones de Acrobat DC, el usuario puede hacer clic en el botón Activar todas las funciones de la barra de mensajes. Esta acción cierra la vista protegida y proporciona una confianza permanente en el archivo añadiéndolo a la lista de ubicaciones privilegiadas de Acrobat. Cada vez que se vuelva a abrir un archivo PDF de confianza, se desactivarán las restricciones de la vista protegida.

Arquitectura de los servicios de Document Cloud

Los servicios de Adobe Document Cloud incluyen:

- **Organizar PDF**: inserta, eliminar, reorganiza o rota las páginas en un PDF.
- **Crear PDF**: convierte documentos de Word, Excel y PowerPoint, e imágenes y fotografías en archivos PDF.
- **Exportar PDF**: convierte con facilidad archivos PDF en archivos editables de Microsoft Word, Excel, PowerPoint o RTF.
- **Editar PDF**: edita con facilidad PDF existentes desde tu dispositivo móvil o portátil.
- **Combinar PDF**: combina varios archivos en un solo PDF y agrupa paquetes de documentos de cualquier parte.
- **Send & Track**: envía, realiza el seguimiento y confirma la entrega de documentos.
- **Adobe Scan**: recopila y convierte cualquier archivo en un PDF de gran calidad en el que puedes realizar búsquedas.
- **Adobe Sign**: prepara y envía documentos para añadir firmas electrónicas seguras, legales y de confianza en cualquier dispositivo.

Seguridad de los servicios de Document Cloud

Gestión de identidades y derechos

Los administradores de TI otorgan derechos a los usuarios finales para acceder a los servicios de Adobe Document Cloud mediante licencias de usuarios designados en la Admin Console de Adobe. Acrobat Document Cloud es compatible con tres (3) tipos distintos de licencias de usuarios designados:

- **Adobe ID**: para cuentas alojadas en Adobe y gestionadas por usuarios cuya creación, propiedad y control recaen en los propios usuarios. Las cuentas de Adobe ID solo disponen de acceso a los servicios de Acrobat Document Cloud si un administrador de TI activa el acceso.
- **Enterprise ID**: es una opción alojada por Adobe y gestionada por la empresa para cuentas que son creadas y controladas por administradores de TI desde la organización empresarial del cliente. La organización posee y gestiona las cuentas del usuario y todos los activos asociados.
- **Federated ID**: una cuenta gestionada por la empresa en la que el sistema de gestión de identidades de inicio de sesión único (SSO) del cliente es el que proporciona todos los perfiles de identidad que la infraestructura de TI del cliente crea, posee y controla. Adobe se integra con la mayoría de los proveedores de identidades compatibles con SAML 2.0.

La mayoría de las organizaciones empresariales utilizan Enterprise ID o Federated ID para sus empleados, contratistas y autónomos siempre que la dirección de correo electrónico se encuentre dentro del dominio de la empresa, porque les permite mantener el control de los derechos y del contenido generado por el usuario almacenados en nombre de ese ID. Para obtener más información acerca de cada tipo de identidad, consulta el sitio web de atención al cliente de Adobe.

El almacenamiento de contraseña tanto de Adobe ID como de Enterprise ID aprovecha el algoritmo hash SHA-256 en combinación con sales de contraseña y un gran número de iteraciones hash. Adobe monitoriza de forma continua las cuentas alojadas por Adobe en busca de actividades anómalas o poco habituales de la cuenta, y evalúa esta información para contribuir a mitigar rápidamente las amenazas para la seguridad. Para las cuentas Federated ID, Adobe no gestiona las contraseñas de los usuarios. Para obtener más información, consulta el Resumen sobre la seguridad de los servicios de gestión de identidades de Adobe.

Firmas electrónicas y digitales

Con los servicios de Document Cloud, los usuarios pueden elegir entre dos herramientas distintas para trabajar de forma segura con las firmas:

- **Herramienta rellenar y firmar**: con tecnología de Adobe Sign, permite a los usuarios gestionar de forma integral los procesos de firma diseñados para que cumplan las leyes de firma electrónica de los Estados Unidos, la Unión Europea y la mayoría de las naciones industrializadas de todo el mundo. Esta herramienta permite solicitar firmas a otras personas, realizar el seguimiento del proceso de firma y archivar automáticamente los documentos firmados y las pistas de auditoría. Se aplican medidas de seguridad a todo el proceso y Adobe certifica los documentos y las pistas de auditoría mediante un sello de garantía que evidencia cualquier intento de manipulación.
- **Herramienta Certificados**: permite a los usuarios firmar documentos mediante firmas digitales basadas en certificados emitidos por entidades de confianza que prestan este servicio y que están registradas en la lista Adobe Approved Trust List (AATL) o en las listas de confianza de la Unión Europea (EUTL, European Union Trusted Lists). Firmar con un ID de certificado emitido por una autoridad de certificados externa es un método que se reconoce generalmente como seguro para firmar documentos de forma electrónica. El ID está vinculado exclusivamente al firmante y solo puede identificarlo a él. El certificado del firmante se vincula criptográficamente al documento durante el proceso de firma mediante una clave privada exclusiva del firmante.

  Acrobat DC valida la firma del firmante (así como la autenticidad del documento firmado) conectándose automáticamente con la autoridad emisora del certificado para su verificación. Este tipo de firma cumple los estándares de firma electrónica de PDF, incluidos el PDF Advanced Electronic Signature (PAdES), partes 2, 3 y 4; así como el uso de criptografía e infraestructuras de clave pública (PKI, Public Key Infrastructure) por parte del Joint Interoperability Test Command (JITC) del Departamento de Defensa de EE. UU. con AES-256, RSA-4096, SHA-512 y RSA-PSS. La herramienta Certificados también permite a los usuarios añadir marcas de hora a los documentos y certificarlos con un sello de garantía que evidencia cualquier intento de manipulación.

El seguimiento no está disponible en dispositivos móviles.

Para obtener más información sobre Adobe Sign y sus funciones de seguridad, consulta el resumen de características técnicas de Adobe Sign.

Almacenamiento en la nube de los servicios de Document Cloud

Aunque los administradores asignan almacenamiento en la nube individual para las cuentas Enterprise ID y Federated ID a través de la Admin Console de Adobe, no tienen acceso directo a ningún archivo dentro del almacenamiento de servicios de Document Cloud del usuario. La eliminación de una cuenta Enterprise ID o Federated ID con un almacenamiento de servicios compartidos existente impide el acceso del usuario final a los datos del almacenamiento en la nube, y los datos de dicho usuario se eliminarán tras 90 días.

Los administradores también pueden usar la Admin Console para asignar almacenamiento a cuentas de Adobe ID. Aunque no pueden borrar cuentas de Adobe ID, los administradores pueden revocar tanto la cuota de almacenamiento concedida de la empresa como el acceso a servicios y aplicaciones. Los datos asociados a esas cuentas se borrarán en tras 90 días.

Los servicios de Adobe Document Cloud aprovechan el almacenamiento en multipropiedad. El contenido del cliente se procesa mediante una instancia de Amazon Elastic Compute Cloud (Amazon EC2) y se almacena en una combinación de depósitos Amazon Simple Storage Services (Amazon S3) y mediante una instancia de MongoDB en un Amazon Elastic Block Store (Amazon EBS). El contenido se almacena en depósitos Amazon S3 y los metadatos relativos al contenido se almacenan en Amazon EBS mediante MongoDB; y todo ello está protegido por roles de gestión de accesos e identidades (IAM) dentro de la región Amazon Web Services (AWS).

Los activos de soporte y los metadatos que se almacenan en Amazon EBS están cifrados con cifrado AES de 256 bits mediante algoritmos criptográficos aprobados por los Federal Information Processing Standards (FIPS) 140-2 coherentes con las recomendaciones del National Institute of Standards and Technology (NIST) 800-57.

Los datos se almacenan de forma redundante en varios centros de datos y en varios dispositivos en cada centro de datos. Todo el tráfico de red se somete a cálculos de sumas de comprobación y verificación de datos sistemáticos para evitar fallos y garantizar la integridad. Por último, el contenido almacenado se repica de forma sincronizada y automática a otras instalaciones de centros de datos en la región del cliente de manera que la integridad de los datos se mantendrá incluso aunque ocurra una pérdida de datos en dos ubicaciones.

Para obtener más información acerca de los servicios de Amazon subyacentes, consulta:

- MongoDB
- Amazon S3
- Servicio Key Management Service (KMS) de AWS
- Servicio Amazon EC2

Clave de cifrado exclusiva

De forma predeterminada, el contenido y los activos almacenados en Amazon S3 se cifran con claves de seguridad simétricas AES de 256 bits exclusivas para cada cliente y para el dominio reclamado por cada cliente. Si los administradores desean añadir una capa adicional de control y seguridad para alguno o todos los dominios de su organización, pueden usar una clave de cifrado exclusiva que está gestionada por KMS de AWS y rota automáticamente anualmente.

Los administradores también pueden revocar esta clave de cifrado exclusiva a través de la Admin Console, que hará que todos los datos cifrados con esa clave sean inaccesibles para los usuarios finales, y evitará la carga y descarga de contenido hasta que la clave de cifrado vuelva a activarse.

Nota: Aunque los archivos de Adobe Document Cloud pueden cifrarse con la clave de cifrado exclusiva, los metadatos no pueden cifrarse usando la clave.

Para obtener más información sobre la administración del cifrado con una clave exclusiva, consulta estas páginas de ayuda de Adobe:

- Administración del cifrado
- Preguntas frecuentes sobre claves de cifrado exclusivas

Amazon Web Services

Como se ha mencionado con anterioridad, todos los componentes de los servicios de Adobe Document Cloud se alojan en AWS, incluidos Amazon EC2 y Amazon S3, en Estados Unidos. Amazon EC2 es un servicio web que proporciona una capacidad informática ampliable automáticamente en la nube, lo que simplifica la informática a escala web. Amazon S3 se reconoce generalmente como una infraestructura de almacenamiento de datos de gran fiabilidad para el almacenamiento y la recuperación de cualquier cantidad de datos.

La plataforma AWS proporciona servicios de acuerdo con las prácticas estándar del sector y se somete con frecuencia a auditorias y certificaciones reconocidas en el sector. Puedes encontrar información más detallada acerca de AWS y los controles de seguridad de Amazon en el sitio web de seguridad en la nube de AWS.

Responsabilidades operativas de AWS y Adobe

AWS opera, gestiona y controla los componentes desde la capa de virtualización del hipervisor hasta la seguridad física de las instalaciones en las que operan los servicios de Adobe Document Cloud. A su vez, Adobe asume la responsabilidad y la gestión del sistema operativo invitado (incluidos actualizaciones y parches de seguridad) y el software de aplicaciones, así como la configuración del firewall del grupo de seguridad proporcionado por AWS.

AWS también opera la infraestructura de nube utilizada por Adobe para proporcionar una variedad de recursos informáticos básicos, incluido el procesamiento y el almacenamiento. La infraestructura de AWS incluye instalaciones, red y hardware, así como el software operativo (por ejemplo, el SO invitado, el software de virtualización, etc.), que admite el aprovisionamiento y el uso de estos recursos. Amazon diseña y gestiona AWS de acuerdo con las prácticas estándar del sector, así como una variedad de estándares de cumplimiento normativo.

Gestión segura

Adobe utiliza Secure Shell (SSH) y Secure Sockets Layer (SSL) para las conexiones de gestión con el fin de administrar la infraestructura de AWS.

Ubicación geográfica de los datos de los clientes en la red de AWS

Todo el contenido generado por el usuario que está cargado a Document Cloud se almacena en los centros de datos regionales US-East (Virginia) de AWS. Se hace una copia de seguridad del contenido dentro de cada centro de datos y en otros centros de datos dentro de la región, para la redundancia y el equilibrio de la carga.

Ubicación geográfica de los datos de identidad en la red de AWS

Los datos de identidad se almacenan en centros de datos de multirregión y con equilibrio de carga ubicados en Virginia (US-East), Oregón (US-West), Irlanda (EU-West) and Singapur (AP-Southeast). Los datos de identidad se replican en todos los centros de datos. Adobe cumple con la legislación aplicable en relación con las transferencias de datos transfronterizas, como se describe con más detalle en https://www.adobe.com/es/privacy/eudatatransfers.html.

Aislamiento de los datos de los clientes y segregación de los clientes

AWS utiliza sólidas capacidades de control y seguridad de aislamiento del inquilino. Como entorno multiinquilino y virtualizado, AWS implementa procesos de gestión de la seguridad y otros controles de seguridad designados para aislar a cada cliente de los demás clientes de AWS. Adobe utiliza la gestión de accesos e identidades (IAM) de AWS para restringir más el acceso a instancias de proceso y almacenamiento.

Arquitectura de red segura

AWS utiliza dispositivos de red, incluidos firewall y otros dispositivos limitadores, para monitorizar y controlar las comunicaciones en el límite externo de la red y en los límites internos clave dentro de la red. Estos dispositivos limitadores hacen uso de conjuntos de reglas, listas de control de acceso (ACL) y configuraciones para reforzar el flujo de información a servicios de sistemas de información específicos. Las ACL o políticas de flujo de tráfico existen en cada interfaz gestionada para administrar y reforzar el flujo de tráfico.

Amazon Information Security aprueba las políticas ACL y las incluye automáticamente en cada interfaz gestionada mediante la herramienta ACL-Manage de AWS, lo que contribuye a garantizar que estas interfaces gestionadas refuercen las ACL más actualizadas.

Monitorización y protección de la red

AWS emplea una variedad de sistemas de monitorización automatizados para proporcionar un elevado nivel de rendimiento del servicio y disponibilidad. Las herramientas de monitorización contribuyen a detectar actividades poco habituales o no autorizadas y las condiciones en los puntos de comunicación de acceso y salida. La red AWS proporciona protección significativa frente a problemas de seguridad de red tradicionales:

- Ataques de denegación de servicio distribuido (DDoS)
- Ataques de Man-in-the-middle (MITM)
- Falsificación de IP
- Análisis de puertos
- Visualización de paquetes por parte de otros inquilinos

Para obtener más información acerca de la monitorización y protección de la red, consulta el sitio web de seguridad en la nube de AWS.

Detección de intrusos

Adobe monitoriza activamente los servicios de Adobe Document Cloud a través de sistemas de detección de intrusos estándares del sector (IDS) y sistemas de prevención de intrusos (IPS).

Registro

Adobe realiza registros en el lado del servidor de la actividad del cliente en los servicios de Adobe Document Cloud para diagnosticar interrupciones del servicio, problemas de los clientes específicos y errores de los que se haya informado. Los registros solo almacenan Adobe ID para ayudar a diagnosticar problemas de los clientes específicos y no contienen combinaciones de nombres de usuario y contraseñas. Solo pueden acceder a los registros los miembros del personal de asistencia técnica de Adobe autorizados, ingenieros principales y algunos desarrolladores con el fin de diagnosticar problemas concretos que puedan surgir.

Monitorización del servicio

AWS monitoriza equipos y sistemas eléctricos, mecánicos y de apoyo a la vida para ayudar a la identificación inmediata de cualquier problema de servicio. Con el fin de mantener la operatividad continua de los equipos, los servicios AWS realizan un mantenimiento preventivo continuo.

Almacenamiento y copia de seguridad de datos

Adobe almacena todos los datos de servicios de Adobe Document Cloud en Amazon S3, lo que proporciona una infraestructura de almacenamiento con una gran durabilidad. Para contribuir a proporcionar durabilidad, las operaciones PUT y COPY de Amazon S3 almacenan los datos de los clientes de forma sincronizada en diferentes instalaciones y almacenan objetos de forma redundante en varios dispositivos en diferentes instalaciones en una región Amazon S3.

Amazon S3 calcula sumas de comprobación en todo el tráfico de red para detectar errores en paquetes de datos en el momento de almacenar o recuperar los datos. La replicación de datos para los objetos de datos de Amazon S3 se produce dentro del conglomerado regional en el que están almacenados los datos y no se replican en los conglomerados de centros de datos de otras regiones.

Los metadatos se replican tomando instantáneas de los volúmenes de Amazon EBS y se almacenan como en Amazon S3. Para obtener información detallada acerca de la seguridad de AWS, consulta el sitio web de seguridad en la nube de AWS.

Gestión de cambios

AWS autoriza, registra, prueba, aprueba y documenta cambios de rutina, emergencia y configuración en la infraestructura de AWS existente de acuerdo con los estándares del sector para sistemas similares. Amazon planifica actualizaciones de AWS para minimizar cualquier impacto en el cliente. AWS se comunica con los clientes por correo electrónico o mediante el panel AWS Service Health Dashboard cuando se prevé que el uso del servicio se va a ver perjudicado. Adobe también mantiene un estado del sistema Adobe para Adobe Document Cloud.

Gestión de parches

AWS conserva la responsabilidad de los sistemas de parches que mantienen la entrega de los servicios AWS, como el hipervisor y los servicios de red. Adobe es responsable de parchear los sistemas operativos (SO), el software y las aplicaciones que se ejecutan en AWS. Cuando se requieren parches, Adobe proporciona una nueva instancia endurecida con anterioridad del SO y la aplicación en lugar de un parche real.

Controles de entorno y físicos de AWS

Los controles de entorno y físicos se indican específicamente en los informes SOC de tipo 1 y SOC de tipo 2. La siguiente sección indica algunos de los controles y medidas de seguridad en funcionamiento en los centros de datos de AWS en todo el mundo. Para obtener información más detallada acerca de la seguridad de AWS, consulta el sitio web de seguridad en la nube de AWS.

Seguridad en una instalación física

Los centros de datos de AWS emplean enfoques arquitecturales y de ingeniería estándares en el sector. Los centros de datos AWS se alojan en instalaciones no definidas, y Amazon controla el acceso físico al perímetro y a los puntos de acceso al edificio mediante personal de seguridad profesional, videovigilancia, sistemas de detección de intrusión y otros medios electrónicos. El personal autorizado debe pasar una autenticación de dos factores un mínimo de dos veces para acceder a plantas de centros de datos. Es necesario que todos los visitantes y contratistas presenten una identificación y que inicien sesión, así como que vayan acompañados de personal autorizado en todo momento.

AWS únicamente proporciona acceso a centros de datos y a información a empleados y contratistas que dispongan de una necesidad empresarial legítima de obtener dichos privilegios. Cuando un empleado deja de tener la necesidad empresarial de estos privilegios, su acceso se revoca de inmediato, aunque continúe siendo empleado de Amazon o AWS. Todo el acceso físico a los centros de datos por parte de empleados de AWS se registra y se audita de forma periódica.

Prevención de incendios

AWS instala equipos de prevención y detección de incendios automáticos en todos los centros de datos de AWS. El sistema de detección de incendios emplea sensores de detección de humo en todos los entornos de centro de datos, espacios de infraestructuras mecánicas y eléctricas, salas de refrigeración y salas de equipos de generadores. Estas áreas están protegidas por sistemas de preacción con doble interconexión de tubería mojada o sistemas de aspersión gaseosa.

Entorno controlado

AWS hace uso de un sistema de control de climatización para mantener una temperatura de funcionamiento constante para servidores y demás hardware, con el fin de evitar el sobrecalentamiento y reducir la posibilidad de que se produzcan interrupciones del servicio. Los centros de datos de AWS mantienen las condiciones atmosféricas en niveles óptimos. Los sistemas y el personal de AWS monitorizan y controlan la temperatura y la humedad en niveles adecuados.

Alimentación de apoyo

Los sistemas de alimentación eléctricos de los centros de datos de AWS están diseñados para ser totalmente redundantes y sostenibles sin tener ningún impacto en las operaciones las 24 horas del día, los 7 días de la semana. Las unidades de sistema de alimentación ininterrumpida (UPS) proporcionan una alimentación de reserva en caso de un fallo eléctrico para cargas vitales en las instalaciones. Los centros de datos utilizan generadores para proporcionar alimentación de reserva en toda la instalación.

Recuperación frente a desastres

Los centros de datos de AWS ofrecen una gran disponibilidad, y toleran fallos de hardware y del sistema con un mínimo impacto. Todos los centros de datos, construidos en varias regiones globales, permanecen online de manera ininterrumpida los 365 días del año para atender a los clientes; ningún centro de datos está "inactivo". En caso de fallo, los procesos automatizados alejan el tráfico de datos del cliente de la zona afectada.

Las aplicaciones principales se implantan en una configuración N+1, de modo que, en caso de un error en el centro de datos, hay suficiente capacidad para permitir que el tráfico sea equilibrado en los sitios restantes. Para obtener más información acerca de los protocolos de recuperación frente a desastres de AWS, consulta el sitio web de seguridad en la nube de AWS.

Gestión del riesgo y la vulnerabilidad de Adobe

Adobe se esfuerza por garantizar que nuestra gestión de riesgos y vulnerabilidades, nuestra respuesta ante incidentes, nuestra mitigación y nuestro proceso de resolución es ágil y preciso. Monitorizamos continuamente el panorama de amenazas, compartimos conocimiento con expertos sobre seguridad de todo el mundo, resolvemos incidentes rápidamente cuando ocurren y devolvemos esta información a nuestros equipos de desarrollo para lograr los niveles más altos de seguridad para todos los productos y servicios de Adobe.

Pruebas de penetración

Adobe aprueba la realización de pruebas de penetración y colabora con empresas líderes de seguridad de terceros para realizarlas, con el objetivo de descubrir posibles vulnerabilidades de seguridad y mejorar la seguridad general de los productos y los servicios de Adobe. Tras la recepción del informe proporcionado por el tercero, Adobe documenta estas vulnerabilidades, evalúa la gravedad y la prioridad, y crea una estrategia de mitigación o un plan de corrección. Adobe realiza una prueba de penetración completa anualmente y análisis de vulnerabilidad mensualmente.

Internamente, el equipo de seguridad de Adobe Document Cloud realiza una evaluación de riesgos de todos los componentes y servicios de Document Cloud trimestralmente y antes de cada lanzamiento. El equipo de seguridad de Document Cloud colabora con los líderes de desarrollo y operaciones técnicas para ayudar a garantizar que todas las vulnerabilidades de alto riesgo se han mitigado antes de cada lanzamiento. Para obtener más información sobre los procedimientos de pruebas de penetración, consulta el resumen de ingeniería segura de Adobe.

Notificación y respuesta ante incidentes

Las nuevas vulnerabilidades y amenazas evolucionan día a día y Adobe intenta reaccionar y mitigar las nuevas amenazas descubiertas. Además de suscribirse a las listas de anuncios de vulnerabilidades extendidas entre el sector, incluidos el Equipo de Respuesta ante Emergencias Informáticas de los Estados Unidos (US-CERT, del inglés "United States Computer Emergency Readiness Team"), Bugtraq y SANS, Adobe se suscribe a las listas de alerta de seguridad más recientes emitidas por los principales proveedores de seguridad.

Para obtener más información acerca del proceso de notificación y respuesta ante incidentes de Adobe, consulta el resumen de respuesta ante incidentes de Adobe.

Análisis forense

Para las investigaciones de incidentes, el equipo de Document Cloud se adhiere a un proceso de análisis forense de Adobe que incluye la captura de imágenes completas o descarga de la memoria de una o varias máquinas afectadas, recogida segura de pruebas y grabación de la cadena de vigilancia.

La organización de seguridad de Adobe

Como parte de nuestro compromiso con la seguridad de nuestros productos y servicios, Adobe coordina todos los esfuerzos de seguridad con el director de seguridad (CSO). La oficina del CSO coordina todas las iniciativas de seguridad de productos y servicios, y la implantación del ciclo de vida seguro de los productos (SPLC) de Adobe.

El CSO también gestiona el equipo de ingeniería de software de seguridad de Adobe (ASSET), un equipo central dedicado de expertos en seguridad que actúan como consultores para los equipos de operaciones y productos clave de Adobe, incluido el equipo de Adobe Document Cloud. Los investigadores de ASSET trabajan con equipos de productos y operaciones individuales de Adobe para lograr el nivel de seguridad adecuado para productos y servicios, y asesorar a estos equipos en relación con las prácticas de seguridad, y así lograr unos procesos claros y repetibles para el desarrollo, la implantación, las operaciones y la respuesta ante incidentes.

Organización de seguridad de Adobe

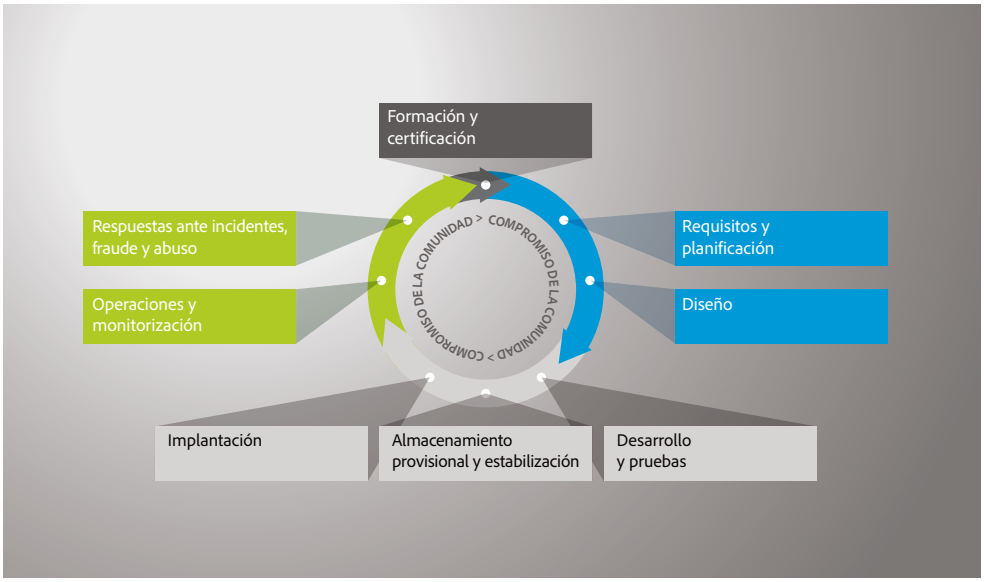
Desarrollo de productos seguros de Adobe

Al igual que con otras organizaciones de servicios y productos clave de Adobe, la organización de Adobe Document Cloud utiliza el proceso SPLC de Adobe. El proceso SPLC de Adobe, un conjunto riguroso de varios cientos de actividades de seguridad concretas que abarcan prácticas de desarrollo de software, procesos y herramientas, está integrado en varias fases del ciclo de vida del producto, desde el diseño hasta el desarrollo pasando por la garantía de calidad, las pruebas y la implantación. Los investigadores de seguridad de ASSET proporcionan una guía de SPLC específica para cada producto clave o servicio basado en una evaluación de los posibles problemas de seguridad. En combinación con el compromiso continuo de la comunidad, Adobe SPLC evoluciona para mantenerse al día a medida que se producen cambios en la tecnología, las prácticas de seguridad y el panorama de las amenazas.

Ciclo de vida seguro de los productos de Adobe

Las actividades del SPLC de Adobe incluyen, en función del componente concreto de Adobe Document Cloud, algunas o todas las siguientes mejores prácticas recomendadas, procesos y herramientas:

- Formación y certificación de seguridad para equipos de producto
- Análisis del panorama de amenazas, el riesgo y el estado del producto
- Directrices, reglas y análisis de codificación segura
- Planificación de servicios, herramientas de seguridad y métodos de pruebas que guían al equipo de seguridad de Adobe Document Cloud para contribuir a hacer frente a los 10 riesgos de seguridad de aplicaciones web más graves de Open Web Application Security Project (OWASP) y a los 25 errores de software más peligrosos de CWE/SANS
- Revisión de la arquitectura de seguridad y pruebas de penetración
- Revisiones de códigos fuente para contribuir a eliminar los defectos conocidos que podrían provocar vulnerabilidades
- Validación de contenido generado por el usuario
- Análisis de redes y aplicaciones
- Revisión de preparación completa, planes de respuesta y lanzamiento de materiales de formación de desarrolladores



Ciclo de vida seguro de los productos de Adobe

Programa de certificación de seguridad de software de Adobe

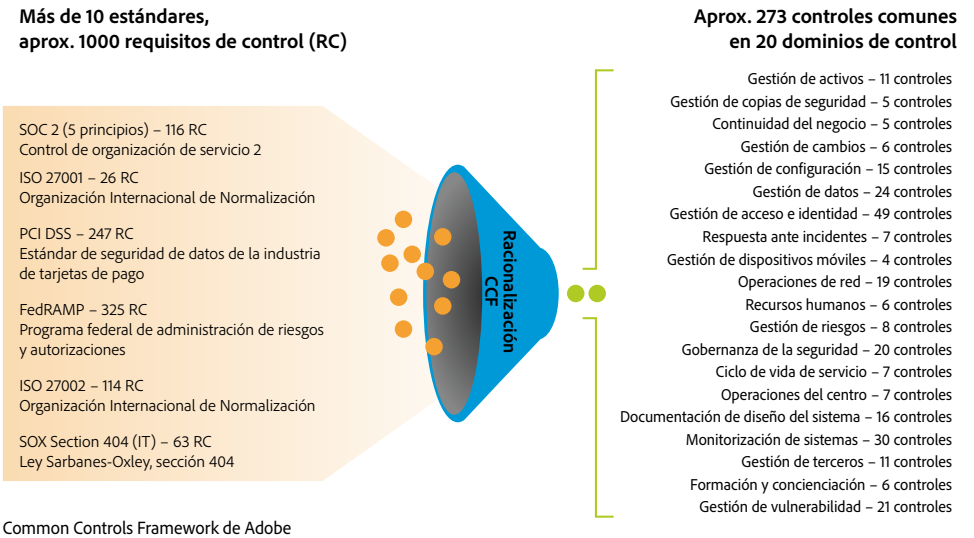
Como parte de Adobe SPLC, Adobe lleva a cabo programas de formación de seguridad continua entre los equipos de desarrollo para mejorar el conocimiento de la seguridad en toda la empresa y mejorar la seguridad general de nuestros productos y servicios. Los empleados que participan en el programa Adobe Software Security Certification Program obtienen diferentes niveles de certificación mediante la realización de proyectos de seguridad. Para obtener más información sobre las prácticas de seguridad de nuestros productos, consulta el resumen de ingeniería segura de Adobe.

Para obtener más información sobre el programa de certificación de seguridad de software de Adobe, consulta el informe técnico sobre cultura de la seguridad de Adobe.

Cumplimiento normativo de los servicios de Document Cloud

El marco Common Controls Framework (CCF) de Adobe es un conjunto de actividades de seguridad y controles de cumplimiento normativo que se implementan dentro de nuestros equipos de operaciones de productos, así como en varias partes de nuestros equipos de aplicaciones e infraestructura.

Cuando creó el CCF, Adobe analizó los criterios de las certificaciones de seguridad más habituales para los negocios basados en la nube y racionalizó los más de 1000 requisitos hasta llegar a los controles específicos de Adobe que mapean aproximadamente una docena de estándares del sector.



Common Controls Framework de Adobe

Normativas actuales y cumplimiento normativo de los servicios Adobe Document Cloud

El SOC 2 es un conjunto de principios de seguridad que definen controles de prácticas líderes en relación con la seguridad, la confidencialidad y la privacidad. Los servicios de Adobe Document Cloud cumplen con el SOC 2 de tipo 2 (seguridad y disponibilidad).

La ISO 27001 es un conjunto de estándares adoptados globalmente que definen requisitos de seguridad estrictos y ofrecen un enfoque sistemático a la gestión de la confidencialidad, la integridad y la disponibilidad de la información del cliente. Los servicios de Adobe Document Cloud cumplen con la ISO 27001:2013.

El Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS, del inglés "Payment Card Industry Data Security Standard") es un estándar de seguridad para información patentado para organizaciones que gestionan información de tarjetas de pago, como números de tarjetas de crédito. Ser un proveedor de servicios que cumple con el PCI DSS permite a Adobe ayudar a los clientes a cumplir los requisitos de la PCI acerca de la gestión segura de datos personales identificables asociados con el titular de la tarjeta.

La ley Gramm-Leach-Bliley Act (GLBA, del inglés "Gramm-Leach-Bliley Act") requiere que las instituciones financieras protejan los datos personales de sus clientes. Los servicios de Adobe Document Cloud cumplen con la GLBA, lo que significa que permiten a nuestros clientes financieros que cumplan los requisitos GLBA para el uso de proveedores de servicios.

El Programa federal de administración de riesgos y autorizaciones (FedRAMP, del inglés "Federal Risk and Authorization Management Program") es un programa gubernamental que ofrece un enfoque estandarizado a la evaluación de la seguridad, la autorización y la monitorización continua de los productos y los servicios de la nube. Los servicios de Adobe Document Cloud están adaptados a FedRAMP, lo que significa que permiten a nuestros clientes cumplir con los requisitos del FedRAMP.

La Ley de derechos educativos y privacidad familiar (FERPA, del inglés "Family Educational Rights and Privacy Act") de EE. UU. está diseñada para mantener la confidencialidad de la información del directorio y los registros de educación de los estudiantes de EE. UU. De acuerdo con las directrices de la FERPA, Adobe puede acordar contractualmente actuar como "funcionario escolar" en lo relativo a la gestión de los datos regulados de estudiantes, lo que permite a nuestros clientes en educación cumplir con los requisitos de la FERPA.

El estándar SAFE-BioPharma describe los requisitos para la confianza en la identidad estandarizada tanto para la autenticación de identidad como para la firma digital. Adobe Document Cloud tiene la certificación de cumplimiento con el estándar de identificación digital de SAFE-BioPharma. Adobe Acrobat DC cumple con SAFE-BioPharma y es seguro para el uso en los flujos de trabajo de SAFE-BioPharma. Además, los servicios de Adobe Document Cloud y Adobe Sign cumplen con el SOC 2 de tipo 2.

Para obtener más información acerca de la posición de cumplimiento normativo actual de Adobe Sign, consulta el resumen de características técnicas de Adobe Sign.

En última instancia, los clientes son los responsables de garantizar el cumplimiento de sus obligaciones legales y de asegurarse de que nuestras soluciones satisfacen sus necesidades de cumplimiento normativo y están protegidas de una manera adecuada.

Empleados de Adobe

Adobe tiene empleados y oficinas en todo el mundo e implementa los siguientes procesos y procedimientos en toda la empresa para protegerla frente a amenazas de seguridad.

Acceso de los empleados a los datos de los clientes

Adobe mantiene entornos de desarrollo y producción segmentados para Adobe Document Cloud, y utiliza controles técnicos para limitar la red y el acceso al nivel de aplicación a los sistemas de producción activos. Los empleados tienen autorizaciones específicas para acceder a los sistemas de producción y desarrollo, y los empleados sin un propósito empresarial legítimo tienen restringido el acceso a estos sistemas.

Revisión de antecedentes

Adobe obtiene informes de revisión de antecedentes con fines de contratación. La naturaleza específica y la finalidad del informe que Adobe suele buscar incluye consultas relacionadas con la formación académica, el historial laboral, los registros judiciales, incluidos antecedentes de condenas penales; y referencias obtenidas de colaboradores profesionales y conocidos personales, todo ello según lo permitido por la ley. Estos requisitos de revisión de antecedentes se aplican a empleados regulares de nueva contratación en EE. UU., incluidos los que vayan a administrar sistemas o tener acceso a la información del cliente. Los nuevos empleados contratados mediante agencias de trabajo temporal de EE. UU. están sujetos a requisitos de revisión de antecedentes a través de la agencia de trabajo temporal correspondiente, en cumplimiento con las directrices de comprobación de antecedentes de Adobe. Fuera de los Estados Unidos, Adobe lleva a cabo revisiones de antecedentes en el caso de algunos nuevos empleados de acuerdo con la política de revisión de antecedentes de Adobe y las leyes aplicables locales.

Rescisión del contrato de un empleado

Cuando un empleado abandona Adobe, su superior le envía un formulario de salida de empleados. Una vez aprobado, Adobe People Resources inicia un flujo de correos electrónicos para informar a las partes implicadas relevantes que lleven a cabo acciones específicas hasta el último día de trabajo del empleado. En caso de que Adobe despida a un empleado, Adobe People Resources envía un aviso por correo electrónico similar a las partes implicadas relevantes en el que incluye la fecha y la hora de la rescisión del contrato del empleado.

A continuación, Adobe Corporate Security planifica las siguientes acciones para contribuir a garantizar que, tras la conclusión del último día de trabajo del empleado, este no pueda seguir accediendo a las oficinas y los archivos confidenciales de Adobe:

- Retirada del acceso al correo electrónico
- Eliminación del acceso al VPN remoto
- Invalidación del distintivo de las oficinas y el centro de datos
- Eliminación del acceso a la red

Bajo solicitud, los responsables pueden pedir a los miembros de seguridad del edificio que acompañen al empleado mientras abandona la oficina o el edificio de Adobe.

Seguridad de las instalaciones

Todas las ubicaciones de oficinas empresariales de Adobe cuentan con guardas en las instalaciones que las protegen 24 horas al día 7 días a la semana. Los empleados de Adobe cuentan con una tarjeta distintivo de ID que es, además, una llave para acceder a los edificios. Los visitantes acceden por la entrada principal, registran su entrada y su salida con el recepcionista, muestran un distintivo de ID de visitante y van acompañados de un empleado. Adobe mantiene todos los equipos de servidores, máquinas de desarrollo, sistemas telefónicos, servidores de archivos y correo, y demás sistemas sensibles bloqueados en todo momento en salas de servidores de entorno controlado a las que solo pueden acceder los miembros del personal autorizados.

Protección frente a virus

Adobe escanea todos los correos empresariales de entrada y salida para detectar amenazas de programas dañinos conocidos.

Confidencialidad de los datos de los clientes

Adobe siempre trata los datos de todos los clientes como confidenciales. Adobe no utiliza ni comparte la información recopilada en nombre de un cliente excepto si se le ha autorizado para ello en un contrato con el cliente en cuestión y según lo establecido en las condiciones de uso de Adobe y la política de privacidad de Adobe.

Conclusión

El enfoque proactivo de Adobe con respecto a la seguridad y los estrictos procedimientos descritos en este documento contribuyen a proteger la seguridad de Adobe Acrobat DC, Acrobat Reader DC y los servicios de Document Cloud, y tus datos confidenciales. En Adobe, nos tomamos la seguridad de tu experiencia digital muy en serio. Monitorizamos continuamente el panorama de amenazas en evolución para adelantarse a las actividades malintencionadas y ayudar a garantizar la seguridad de los datos de nuestros clientes.

Para obtener más información, visita el centro de confianza de Adobe.

Adobe

Adobe Inc.
345 Park Avenue
San Jose, CA 95110-2704 EE. UU.
www.adobe.com
www.adobe.com/es
www.adobe.com/la

5/19