Adobe Document Cloud

Adobe

DOCUMENTO TÉCNICO

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

# Índice de contenidos

# Seguridad de Adobe

En Adobe, somos conscientes de la importancia que tiene la seguridad de tus experiencias digitales. Las prácticas de seguridad están profundamente integradas en nuestros procesos de operaciones, desarrollo de software interno y herramientas. Nuestros equipos multifuncionales siguen estas prácticas estrictamente a fin de evitar, detectar y responder ante los incidentes de forma oportuna. Además, nos mantenemos al día de las últimas amenazas y vulnerabilidades gracias a nuestra colaboración con partners, investigadores líderes, instituciones de investigación sobre seguridad y otras organizaciones del sector; e incorporamos con frecuencia técnicas de seguridad avanzadas en los productos y servicios que ofrecemos.

En este informe técnico se describen el enfoque de defensa en profundidad y los procedimientos de seguridad que implementa Adobe para reforzar la seguridad de Adobe Acrobat con los servicios de Document Cloud, así como los datos asociados.

# Resumen de Acrobat con los servicios de Document Cloud

Acrobat con los servicios de Document Cloud es una solución de PDF completa para el actual mundo multidispositivo conectado. El uso combinado del software de ordenador de Acrobat y la aplicación móvil de Adobe Acrobat Reader (mejorada con funciones móviles prémium) con los servicios de Document Cloud permite a las organizaciones crear flujos de trabajo de documentos más inteligentes y satisfacer las demandas de soluciones móviles por parte de los/as usuarios/as finales, al tiempo que garantiza la seguridad de los documentos en todos los dispositivos.

Con Acrobat con los servicios de Document Cloud, se puede convertir prácticamente cualquier contenido en un documento electrónico que se puede compartir con otras personas. Asimismo, se puede automatizar fácilmente la generación, manipulación y transformación de archivos en PDF desde cualquier servicio en la nube de Acrobat, aplicación para ordenador o aplicación móvil.

# Experiencias de usuario/a de Acrobat

Los/as clientes pueden usar los servicios de Document Cloud en una amplia variedad de experiencias de usuario/a de Acrobat:

- Acrobat Pro: aplicación para usuarios/as de ordenador portátil y de sobremesa
- Acrobat online: aplicación web incluida en los navegadores compatibles de ordenadores y dispositivos móviles, como Chrome, Microsoft Edge, Firefox y Safari
- Cliente móvil de Acrobat Reader: aplicación para descargar de forma gratuita desde la App Store de Apple o Google Play destinada a usuarios/as de dispositivos móviles y tabletas

Además, Adobe ha integrado Acrobat en varias herramientas de productividad de Microsoft. Sin embargo, la función de almacenamiento de documentos de estas integraciones difiere de la versión independiente de Acrobat. En la sección "Integraciones con Microsoft de Acrobat", se detalla la información sobre seguridad de cada integración.

# Servicios de Document Cloud

Estos son algunos servicios de Adobe Document Cloud:

- Enviar PDF: enviar un archivo PDF a un/a destinatario/a usando un cliente de correo electrónico
- Organizar PDF: insertar, eliminar, reorganizar o rotar las páginas de un PDF
- Crear PDF: convertir documentos de Word, Excel y PowerPoint, así como imágenes y fotografías, en archivos PDF
- Exportar PDF: convertir archivos PDF en archivos editables de Microsoft Word, Excel, PowerPoint o RTF
- Editar PDF: editar PDF existentes desde un dispositivo móvil o portátil
- Combinar PDF: combinar varios archivos en un solo PDF y agrupar paquetes de documentos desde cualquier parte
- Rellenar y firmar: cumplimentar un formulario y firmarlo
- Adobe Scan: recopilar y convertir cualquier archivo en un PDF de gran calidad y con función de búsqueda
- Adobe Acrobat Sign: preparar y enviar documentos para solicitar su firma electrónica con fiabilidad desde cualquier dispositivo moderno, desde firmas simples hasta firmas digitales en la nube.

Adobe añade continuamente nuevas ofertas a los servicios de Document Cloud. En Adobe.com, puedes obtener una lista actualizada de todos los servicios de Document Cloud.

# Funciones de seguridad de Acrobat Document

## Censura

Los servicios de Adobe Document Cloud incluyen una serie de herramientas de censura para que los/as clientes protejan la información confidencial o privada, como la eliminación permanente de texto e imágenes gráficas en un documento antes de su distribución. Además, los/as usuarios/as 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 seleccionada se elimina por completo del archivo, en lugar de quedar simplemente enmascarada como sucede con otras herramientas o métodos. Con la función de limpieza del documento, los/as clientes también pueden eliminar la información oculta y los objetos no gráficos como, por ejemplo, los metadatos que pueda haber en el PDF.

## Uso compartido de archivos

Los archivos de Document Cloud almacenados en la nube se etiquetan automáticamente como "Privado", lo que significa que solo el/la usuario/a final que lo cargó puede visualizarlos. El/la usuario/a final debe realizar acciones expresas para compartir ese contenido o seguirá siendo privado. El uso compartido de contenido de Document Cloud se lleva a cabo mediante el envío a cada destinatario/a de un enlace al contenido de Document Cloud.

Los/as usuarios/as de los servicios de Document Cloud tienen dos opciones para compartir los archivos: Solo ver o Revisar. Si el/la usuario/a envía el enlace con la restricción Solo ver, el/la destinatario/a solo puede ver el contenido como un documento de solo lectura. Por otra parte, si el/la usuario/a envía el documento para revisión, el/la destinatario/a puede comentar en el documento, pero no puede editarlo ni alterarlo de ninguna otra manera. Los enlaces pueden enviarse a sus destinatarios/as mediante correo electrónico, mensaje de texto o cualquier otro software de colaboración.

## Configuración de activos y restricciones de uso compartido

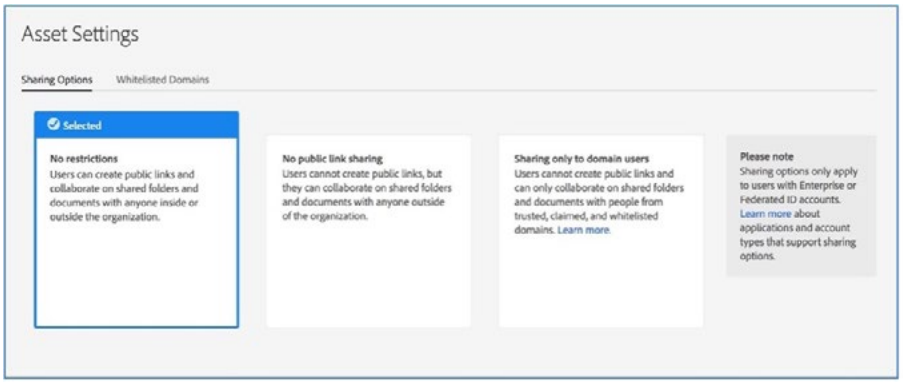


Figura 1: Configuración de los activos de los servicios de Document Cloud

También pueden aplicarse restricciones de uso compartido al contenido almacenado en Document Cloud mediante la función Configuración de activos de la Adobe Admin Console. Esta función permite a los departamentos informáticos de las empresas desactivar el uso compartido de enlaces públicos, así como imponer la colaboración en DC solo en el dominio reclamado por la empresa y en cualquier otro incluido en la lista de dominios permitidos. Si se establecen restricciones de uso compartido, quien reciba el contenido tendrá que iniciar sesión. Además, si el modo "Uso compartido solo con usuarios de dominios" está activado, las personas solo podrán compartir contenido con otros/as usuarios/as de su organización o de otros dominios de confianza; y el uso compartido externo quedará completamente desactivado.

## Microsoft Purview Information Protection

Microsoft Purview Information Protection (MPIP) es una solución de gestión de derechos de Microsoft. Los/as usuarios/as de Azure Information Protection y otras soluciones de Microsoft Purview Information Protection pueden usar Acrobat o Acrobat Reader para leer contenido etiquetado y protegido. Las versiones más recientes para ordenador de Acrobat Pro/Standard (versión 22.003.20258 y posteriores) ahora permiten aplicar y editar de forma nativa etiquetas y directivas de sensibilidad de Information Protection en los PDF, sin necesidad de plug-in ni de instalar nada por separado.

## Modo protegido

Para proteger a los/as clientes del código malintencionado que intenta utilizar el formato PDF para escribir o leer el sistema de archivos de un ordenador, Adobe ofrece una implementación vanguardista de la tecnología de zonas protegidas denominada Modo protegido.

En Acrobat Reader, el Modo protegido amplía la protección contra atacantes que tratan de instalar malware en el sistema de un ordenador con el fin de impedir también que ninguna persona malintencionada pueda acceder a los datos confidenciales y a la propiedad intelectual de la red corporativa y extraerlos. El modo protegido se activa de forma predeterminada cada vez que un/a usuario/a inicia Acrobat Reader 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, leerlo, eliminar archivos o modificar de cualquier otro modo la información del sistema.

El Modo protegido de Acrobat Reader (en Windows 8.1 y versiones posteriores) se puede ejecutar de forma aislada en un AppContainer.

## Vista protegida

El uso de zonas protegidas es un método de seguridad muy respetado que crea un entorno de ejecución limitado para ejecutar programas con pocos derechos o privilegios. Estas zonas protegen los sistemas de los/as usuarios/as contra los daños causados por los documentos no fiables que contienen código ejecutable. En el contexto de Acrobat Reader, todos los archivos PDF y los procesos que estos invocan se consideran no fiables. Reader trata todos los archivos PDF como potencialmente corruptos y limita todo el procesamiento que estos invocan a las zonas protegidas. De forma similar al Modo protegido de Acrobat Reader, la Vista protegida consiste en la implementación de una tecnología de zonas protegidas para el sofisticado conjunto de funciones de este programa.

En Acrobat, Adobe amplía la funcionalidad de la Vista protegida para ir más allá del bloqueo de los ataques basados en escritura que tratan de ejecutar código malintencionado en el sistema de un ordenador a través del formato de archivo PDF, con el fin de proteger también 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 pueden ser malintencionados y limita el procesamiento a la zona protegida, a menos que el/la usuario/a indique específicamente que un archivo es de confianza.

La Vista protegida es compatible en ambas circunstancias en las que los/as usuarios/as abren documentos PDF: desde la aplicación independiente de Acrobat 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/as clientes que activen la Vista protegida. Cuando un/a usuario/a abre un archivo potencialmente malintencionado dentro de la Vista protegida, Acrobat muestra una barra amarilla 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/la usuario/a que está en la Vista protegida, lo que desactiva muchas de las funciones de Acrobat y limita la interacción del/la usuario/a con el archivo. Básicamente, el archivo pasa a modo de "solo lectura", y la Vista protegida impide que el contenido malintencionado que incorpora o que está incrustado en él altere el sistema.

Para confiar en el archivo y activar todas las funciones de Acrobat, el/la usuario/a puede hacer clic en el botón "Activar todas las funciones" de la barra amarilla 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.

# Seguridad de los servicios de Adobe Document Cloud

## Autenticación de usuarios/as

Las personas con rol de administrador otorgan derechos a los/as usuarios/as finales para acceder a los servicios de Adobe Document Cloud mediante licencias de usuarios/as designados/as en la Adobe Admin Console. Acrobat con los servicios de Document Cloud es compatible con cuatro (4) tipos distintos de licencias de usuarios/as designados/as: Adobe ID, Business ID, Enterprise ID y Federated ID. Para obtener más información sobre estos tipos de identidades y los servicios de gestión de identidades de Adobe, consulta Resumen sobre la seguridad de los servicios de identidades de Adobe.

## Almacenamiento de documentos y contenido generado por el/la usuario/a

Los servicios de Adobe Document Cloud aprovechan el almacenamiento multiinquilino. Los documentos y el contenido generado por el/la usuario/a se almacenan de forma redundante en varios centros de datos y en distintos 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 replica de forma sincronizada y automática en otras instalaciones de centros de datos de la región del/la cliente, de manera que la integridad de los datos se mantendrá aunque se pierdan en dos ubicaciones.

Por lo general, el contenido generado por usuarios/as y los documentos subidos a Document Cloud se almacenan en el centro de datos regional correspondiente al código de país asociado al/la usuario/a que carga los datos, independientemente del tipo de identidad:

- En el caso de los/as usuarios/as con un código de país de Norteamérica, Centroamérica o Sudamérica, el lugar de almacenamiento se encuentra en Virginia (Estados Unidos).
- En el caso de los/as usuarios/as con un código de país de Europa o de África, el lugar de almacenamiento se encuentra en Dublín (Irlanda).
- En el caso de los/as usuarios/as con un código de país de Asia-Pacífico o de Oriente Medio, el lugar de almacenamiento se encuentra en Tokio (Japón).

Las personas con rol de administrador pueden asignar almacenamiento en la nube individual para las cuentas Enterprise ID y Federated ID a través de la Adobe Admin Console de Adobe, pero no tienen acceso directo a ningún archivo dentro del almacenamiento de servicios de Document Cloud del/la usuario/a final. Sin embargo, las personas con rol de administrador pueden asumir la propiedad de la cuenta del/la usuario/a y denegar el acceso a esta. La eliminación de estos tipos de cuentas con un almacenamiento de servicios compartidos existente impide el acceso del/la usuario/a final a los datos del almacenamiento en la nube, y los datos de dicho/a usuario/a se eliminarán al cabo de 90 días.

Las personas con rol de administrador también pueden usar la Admin Console para asignar almacenamiento a cuentas de Adobe ID. Aunque no pueden controlar las cuentas de Adobe ID, pueden eliminarlas quitando de las cuentas de los/as usuarios/as finales la cuota de almacenamiento concedida de la empresa, así como el acceso a servicios y aplicaciones, lo que provoca que los datos también se borren al cabo de 90 días.

## Cifrado de datos

De manera predeterminada, los documentos y el contenido generado por el/la usuario/a de los servicios de Document Cloud se cifran en tránsito con el cifrado HTTPS TLS 1.2. El contenido de los servicios de Document Cloud se cifra en reposo con claves de seguridad simétricas AES de 256 bits exclusivas para cada cliente y el dominio que haya reclamado. Estos métodos de cifrado se aplican tanto al almacenamiento de documentos permanente como al temporal.

## Claves de cifrado exclusivas

Además de las capacidades de cifrado estándar integradas, las personas con rol de administrador pueden añadir una capa adicional de control y seguridad a los documentos en reposo mediante una clave de cifrado exclusiva para algunos o todos los dominios de la organización del/la cliente. Después, el contenido de los servicios de Document Cloud se puede cifrar en reposo utilizando esa clave de cifrado exclusiva, que, en caso de que resulte necesario, se puede denegar desde la Admin Console. Si se deniega la clave, los/as usuarios/as finales no podrán acceder al contenido cifrado con esta, y se impedirá la carga y descarga de contenido hasta que la clave de cifrado vuelva a activarse.

*Nota: Solo los archivos de Adobe Document Cloud pueden cifrarse con la clave de cifrado exclusiva; los metadatos no pueden cifrarse usando dicha clave.*

Dispones de más información sobre la gestión del cifrado mediante clave exclusiva en Adobe.com.

## Firmas electrónicas y digitales

Con los servicios de Document Cloud, los/as usuarios/as pueden emplear distintas herramientas para trabajar con las firmas como, por ejemplo, las siguientes:

- **Herramienta Rellenar y firmar**: permite abrir un PDF, rellenar los campos de formulario y firmar el documento de forma electrónica.
- **Herramienta Certificados**: permite firmar los documentos mediante una firma electrónica que cuenta con el respaldo de un certificado digital, vinculado criptográficamente al campo de la firma. Cada certificado digital (o ID digital) identifica de forma inequívoca al firmante y lo emite un proveedor de servicios de confianza (TSP) o una autoridad de certificación enumerada en la lista de confianza aprobada por Adobe (Adobe Approved Trust List, AATL) y las listas de confianza de la Unión Europea (European Union Trusted Lists, EUTL). Con la herramienta Certificados, se pueden añadir marcas de hora a los documentos y certificarlos con un sello de garantía.

# Integraciones con Microsoft de Acrobat

Adobe se ha asociado con Microsoft para crear integraciones con sus principales herramientas de productividad, de modo que se puede acceder a Acrobat con los servicios de Document Cloud de manera nativa desde las siguientes soluciones:

- Microsoft SharePoint y OneDrive
- Microsoft Teams
- Microsoft Word, Excel y PowerPoint (solo la creación y protección de archivos PDF)

Con cada una de estas integraciones, Adobe crea solo una copia temporal del documento PDF y no recopila ninguna información del/la cliente ni información de identificación personal del/la usuario/a.

## Acrobat para SharePoint y OneDrive

Acrobat para SharePoint y OneDrive concede a los/as usuarios/as acceso a flujos de trabajo de PDF en Microsoft 365, y les permite visualizar, crear y modificar archivos PDF en la nube.

Con esta versión integrada de Acrobat, los documentos se almacenan en la ubicación original de SharePoint o OneDrive. Acciones tales como la visualización, la creación de comentarios y la búsqueda se producen en el equipo del/la usuario/a. Cuando esta persona realiza algún cambio en su documento, este se vuelve a almacenar en su cuenta de SharePoint o OneDrive.

Si el/la usuario/a crea, organiza, combina o exporta un documento, este se envía a los servidores de Adobe Document Cloud de la región correspondiente al código de país de dicha persona para el procesamiento transitorio y se elimina en un plazo de 24 horas. El documento permanece cifrado tanto en tránsito como en reposo durante este proceso (consulta la sección "Cifrado de datos"). El documento modificado se guarda de nuevo en la cuenta de SharePoint o OneDrive del/la usuario/a.

Accede a Adobe.com para obtener información más específica sobre la funcionalidad de Acrobat para SharePoint y OneDrive.

## Acrobat para Microsoft Teams

Acrobat para Microsoft Teams concede a los/as usuarios/as acceso a flujos de trabajo de PDF en Microsoft Teams, y les permite visualizar, crear y modificar archivos PDF en la nube. Los/as clientes pueden utilizar Acrobat para Microsoft Teams como pestaña personal, pestaña de bot, acción de mensaje o extensión de mensajes.

Cualquier PDF que se comparta en un canal o chat de Microsoft Teams se almacena en el OneDrive o SharePoint del/la usuario/a de forma predeterminada. Sin embargo, si se comparte un PDF y varias personas colaboran en él (por ejemplo, añadiendo comentarios) en Acrobat para Microsoft Teams, el documento se envía a los servidores de Adobe Document Cloud de la región correspondiente al código de país del/la usuario/a para el procesamiento transitorio y se elimina en un plazo de 24 horas. El documento permanece cifrado tanto en tránsito como en reposo durante este proceso (consulta la sección "Cifrado de datos"). El documento modificado se guarda de nuevo en la ubicación original.

Si la persona con rol de administrador del/la cliente desactiva los servicios de Document Cloud, los/as usuarios/as finales podrán previsualizar y comentar sus propios documentos, pero no podrán colaborar con otras personas mediante las funciones de compartir comentarios.

Dispones de más información sobre la funcionalidad concreta de Acrobat que se ofrece en la integración para Microsoft Teams en Adobe.com.

## Acrobat para Word, Excel y PowerPoint

El complemento Crear PDF permite convertir fácilmente un documento de Microsoft 365 en un archivo PDF de gran calidad, así como guardarlo en OneDrive o descargarlo en un disco duro personal. También se pueden proteger los documentos PDF añadiendo una contraseña para evitar el acceso no autorizado.

# Resumen del programa de seguridad de Adobe

El programa de seguridad integrada de Adobe se compone de cinco (5) centros de excelencia, que reproducen y perfeccionan constantemente los métodos de detección y prevención de riesgos haciendo uso de las tecnologías emergentes y más recientes, como la automatización, la inteligencia artificial y el aprendizaje automático.


Figura 2: Los cinco centros de excelencia en seguridad

Los centros de excelencia del programa de seguridad de Adobe son los siguientes:

- **Seguridad de las aplicaciones**: se centra en la seguridad de nuestros códigos de producto, lleva a cabo investigaciones sobre amenazas e implementa programas de recompensas por errores (“bug bount”).
- **Seguridad operativa**: contribuye a controlar y proteger nuestros sistemas, redes y sistemas de producción en la nube.
- **Seguridad empresarial**: está enfocado en proteger los accesos y la autenticación en el entorno empresarial de Adobe.
- **Cumplimiento normativo**: supervisa nuestro modelo de control de la seguridad, los programas de auditoría y de cumplimiento normativo, y los análisis de riesgos.
- **Respuesta ante incidentes**: incluye nuestro centro de operaciones de seguridad y respuesta ante amenazas, disponible las 24 horas del día, los 7 días de la semana.

Como ejemplo de nuestro compromiso con la seguridad de nuestros productos y servicios, los centros de excelencia informan a la oficina del director de Seguridad (CSO) de Adobe, quien coordina todos los esfuerzos de seguridad actuales y desarrolla la visión de la evolución de la seguridad en Adobe en el futuro.

# La organización de seguridad de Adobe

La organización de seguridad de Adobe, basada en una plataforma de toma de decisiones transparente, responsable y fundamentada, aúna la amplia variedad de servicios de seguridad en un modelo de control de la seguridad. El director de Seguridad (CSO) de Adobe colabora con la directora de Informática (CIO) y la de Privacidad (CPO) para garantizar la coordinación en la estrategia y las operaciones de seguridad.

Además de los centros de excelencia descritos anteriormente, Adobe incluye miembros de los equipos de asuntos legales, privacidad, marketing y RR. PP. en la organización de seguridad para garantizar la transparencia y responsabilidad en todas las decisiones relacionadas con la seguridad.

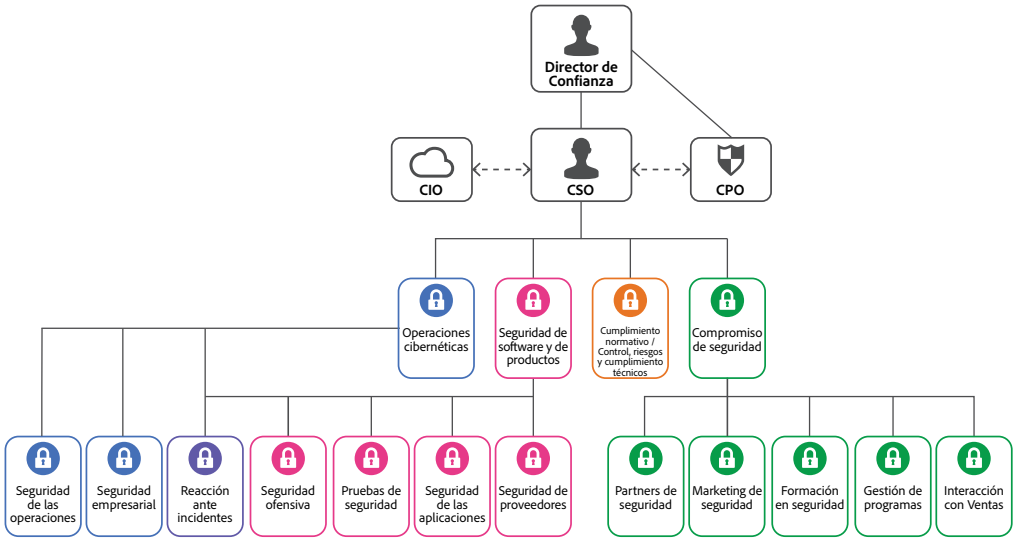


Figura 3: La organización de seguridad de Adobe

Como parte de la cultura de seguridad de toda la empresa, todo el personal de Adobe debe llevar a cabo nuestra formación en concienciación e información sobre seguridad, que debe realizarse y volverse a certificar cada año. Todo esto contribuye a garantizar que cada miembro del personal contribuya a la protección de los activos corporativos de Adobe, así como de los datos de nuestra clientela y nuestro personal. En el momento de la contratación, se inscribe de manera automática a nuestros empleados técnicos, incluidos los equipos de ingeniería y operaciones técnicas, en un programa de formación exhaustivo "al estilo de las artes marciales" adaptado a cada función. Para obtener más información sobre nuestra cultura de seguridad y nuestros programas de formación, consulta el informe técnico sobre la cultura de la seguridad de Adobe.

# Ciclo de vida seguro de los productos de Adobe

El ciclo de vida seguro de los productos de Adobe (SPLC), que está integrado en varias fases del ciclo de vida de los productos, desde su diseño y desarrollo hasta la garantía de calidad, prueba e implementación, es la base de toda la seguridad de Adobe. El SPLC de Adobe (un conjunto riguroso de varios cientos de actividades de seguridad específicas que abarcan herramientas, procesos y prácticas de desarrollo de software) define procesos claros y repetibles para ayudar a nuestros equipos de desarrollo a integrar la seguridad en nuestros productos y servicios, así como a evolucionar continuamente para incorporar las prácticas recomendadas más recientes del sector.

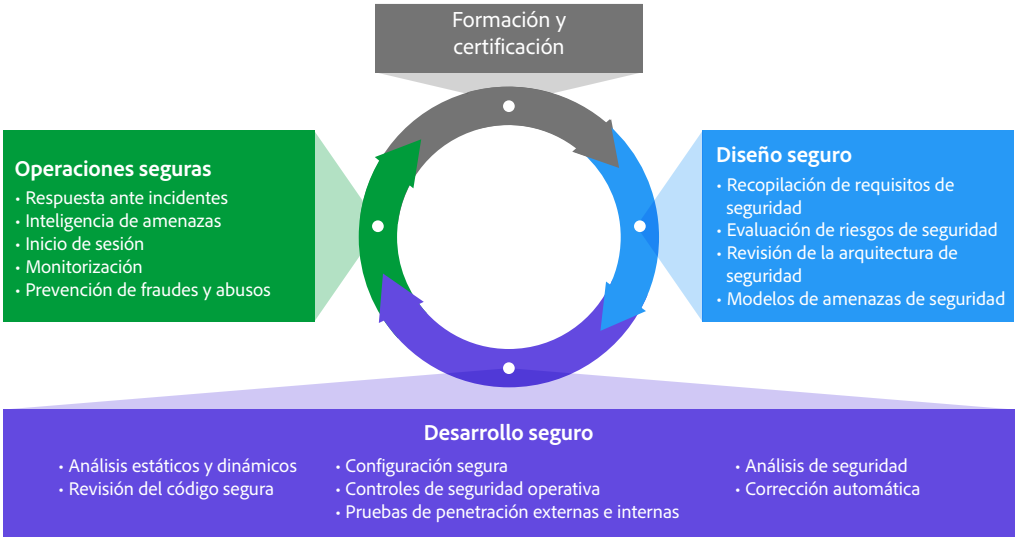


Figura 4: Ciclo de vida seguro de los productos de Adobe

Adobe tiene publicado un estándar de ciclo de vida seguro de los productos que puedes revisar previa solicitud. Puedes obtener más información sobre los componentes del SPLC de Adobe en Resumen sobre la seguridad de las aplicaciones de Adobe.

# Seguridad de las aplicaciones de Adobe

En Adobe, el desarrollo de las aplicaciones con una "seguridad de serie" parte de la pila de seguridad de las aplicaciones de Adobe. Esta pila combina procesos claros y repetirles basados en una investigación y una experiencia consolidadas con la automatización, que permiten garantizar la aplicación coherente de los controles de seguridad; por lo que contribuye a la mejora de la eficiencia del desarrollo y la minimización del riesgo de que se cometan errores de seguridad. Mediante el uso de bloques de codificación seguros, probados y preaprobados, que eliminan la necesidad de codificar desde cero los patrones y bloques más utilizados, los desarrolladores pueden centrarse en su área de especialización con la tranquilidad de saber que su código es seguro. La Pila de seguridad de las aplicaciones de Adobe, junto con las pruebas, las herramientas especializadas y las supervisión, ayuda a los desarrolladores de software a crear un código seguro de serie.

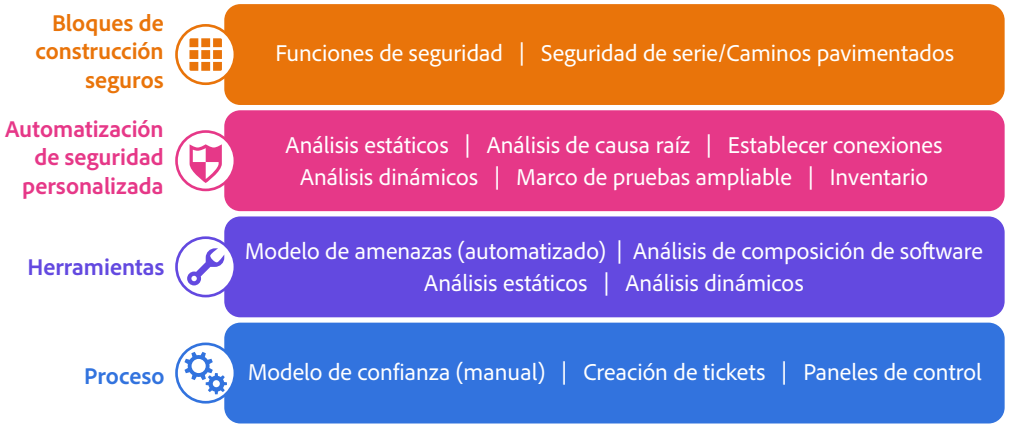


Figura 5: Pila de seguridad de las aplicaciones de Adobe

Adobe también tiene varios estándares publicados sobre la seguridad de las aplicaciones, incluidos los destinados a trabajos específicos para el uso de la infraestructura de la nube pública. Puedes revisar estos estándares previa solicitud. Para obtener más información sobre la seguridad de las aplicaciones de Adobe, consulta el Resumen sobre la seguridad de las aplicaciones de Adobe.

# Seguridad operativa de Adobe

Para garantizar que todos los productos y servicios de Adobe se diseñaran desde su concepción teniendo en cuenta las prácticas recomendadas en materia de seguridad, el equipo de seguridad operativa creó la pila de seguridad operativa de Adobe. Se trata de un conjunto consolidado de herramientas que ayudan a los ingenieros y desarrolladores de productos a mejorar su enfoque de seguridad y reducir los riesgos tanto para Adobe como para sus clientes. Además, contribuye a garantizar la conformidad con los marcos de cumplimiento, privacidad y otros marcos de control.

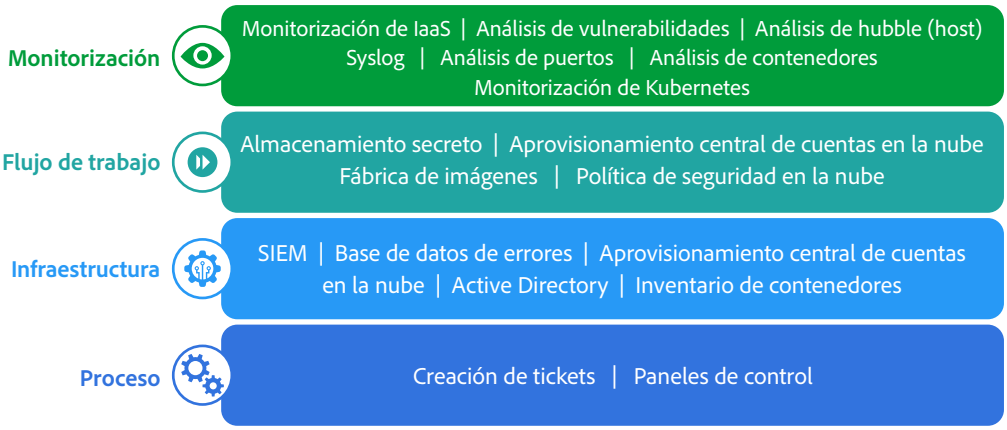


Figura 6: La pila de seguridad operativa de Adobe

Adobe tiene publicados varios estándares sobre sus operaciones en la nube en curso que puedes consultar previa solicitud. Para obtener una descripción detallada de la pila de seguridad operativa de Adobe y las herramientas concretas usadas en Adobe, consulta la información general sobre la seguridad operativa de Adobe.

# Seguridad empresarial de Adobe

Además de proteger nuestros productos y servicios, así como nuestras operaciones de alojamiento en la nube, en Adobe utilizamos una serie de controles de seguridad internos para garantizar la seguridad de nuestros sistemas y redes, nuestras ubicaciones físicas corporativas, y los datos de nuestros empleados y clientes.

Para obtener más información sobre nuestros controles de seguridad empresarial y los estándares que hemos desarrollado para estos controles, consulta Resumen sobre seguridad empresarial de Adobe.

# Cumplimiento normativo de Adobe

Todos nuestros productos y servicios se adhieren al marco Common Controls Framework (CCF) de Adobe, 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. En la medida de lo posible, Adobe aprovecha innovadores procesos de automatización para alertar a los equipos de posibles casos de incumplimiento normativo, además de para garantizar una mitigación y un reajuste rápidos.

Los productos y servicios de Adobe cumplen los estándares legales aplicables o pueden utilizarse de una forma que permite a los/as clientes cumplir las obligaciones legales relacionadas con el uso de proveedores de servicio. Los/as clientes mantienen el control de sus documentos, datos y flujos de trabajo, y pueden elegir la forma que estimen oportuna de cumplir con las normativas locales y regionales, como el Reglamento General de Protección de Datos (RGPD) de la UE.

Asimismo, Adobe cuenta con una formación en cumplimiento normativo y con los estándares relacionados, que disponibles para su consulta previa solicitud. Para obtener más información sobre el CCF de Adobe y las certificaciones principales, consulta la lista de normativas de cumplimiento, certificaciones y estándares de Adobe.

# Respuesta ante incidentes

En Adobe, nos esforzamos por garantizar que nuestra gestión de riesgos y vulnerabilidades, respuesta ante incidentes, mitigación y proceso de resolución sean ágiles y precisos. Monitorizamos continuamente el panorama de las amenazas, compartimos conocimientos con profesionales de la seguridad de todo el mundo, resolvemos incidentes de forma rápida cuando ocurren, y devolvemos esta información a nuestros equipos de desarrollo para lograr los niveles más altos de seguridad en todos los productos y servicios de Adobe.

También mantenemos estándares internos para la gestión de vulnerabilidades y la respuesta ante incidentes, que puedes revisar previa solicitud. Para obtener información más detallada sobre el proceso de notificación y respuesta ante incidentes de Adobe, consulta el Resumen sobre la respuesta ante incidentes de Adobe.

# Continuidad empresarial y recuperación frente a desastres

El programa Continuidad empresarial y recuperación frente a desastres de Adobe (BCDR, por sus siglas en inglés) se compone del Plan de continuidad empresarial (BCP) y Planes de recuperación frente a desastres (DR) específicos de productos, que contribuyen a garantizar la disponibilidad y entrega continuas de los productos y servicios de Adobe. Nuestro programa BCDR, que cuenta con la certificación ISO 22301, mejora nuestra capacidad de responder ante el impacto de las interrupciones imprevistas, mitigarlo y recuperarnos de él. Puedes obtener más información en el Resumen sobre el programa de continuidad empresarial y recuperación frente a desastres de Adobe.

# Conclusión

El enfoque proactivo con respecto a la seguridad y los estrictos procedimientos descritos en este documento contribuyen a proteger la seguridad de Acrobat con los servicios de Document Cloud, así como tus datos confidenciales. En Adobe, nos tomamos muy en serio la seguridad de los datos de tu experiencia digital, por lo que monitorizamos continuamente la evolución del panorama de amenazas a fin de adelantarnos a las actividades malintencionadas y garantizar la seguridad de los datos de nuestros/as clientes.

Para obtener más información sobre la seguridad de Adobe, ve al Centro de confianza de Adobe.

La información de este documento está sujeta a modificaciones sin previo aviso. Para obtener más información acerca de las soluciones, los controles y las opciones de licencia de Adobe, ponte en contacto con tu representante de ventas de Adobe.

Adobe



8/23