Resumen de la seguridad de Acrobat DC

La solución de PDF líder en el mundo para crear, editar y gestionar documentos

Índice

Cuando confías la información de tu organización a una aplicación de terceros, la seguridad es fundamental. Adobe lleva más de 20 años de liderazgo en el ámbito de los documentos digitales y, además, creó el estándar para los PDF y las firmas digitales. Cientos de miles de organizaciones han producido miles de millones de PDF en todo el mundo porque confían a diario en el software Adobe Acrobat software y Adobe PDF para preparar, proteger y compartir sus documentos más importantes.

Adobe Acrobat DC con los servicios de Adobe Document Cloud es la solución completa de PDF para el mundo actual conectado mediante dispositivos móviles. Combina el software de escritorio de Acrobat con la aplicación móvil de Adobe Acrobat Reader, mejorada con características móviles prémium y los servicios de Document Cloud, para ayudar a las organizaciones a crear flujos de trabajo de documentos más inteligentes y a satisfacer las demandas de soluciones móviles por parte de los usuarios finales, al tiempo que garantiza la seguridad de los documentos en todos los dispositivos. Con Acrobat DC, siempre estarás al día, ya que podrás acceder a las actualizaciones de seguridad más recientes y a las últimas funciones, que podrás implementar cuando mejor te convenga.

Este documento describe la exhaustiva estrategia de seguridad de Adobe en lo tocante a Acrobat DC (lo que abarca la seguridad de los documentos, las aplicaciones y en la nube) con el fin de facilitarte aún más la protección de tu información y tu experiencia.

Seguridad de documentos

Los autores de los documentos pueden usar el software Acrobat DC para crear documentos PDF y aplicar una infinidad de medidas de seguridad, entre las que se incluye el cifrado, el control de acceso, las firmas de certificación y la eliminación permanente de texto e imágenes mediante herramientas de censura. La cómoda funcionalidad Acciones de Acrobat DC permite definir un conjunto de tareas de seguridad que los usuarios pueden aplicar fácilmente sin necesidad de formación oficial ni herramientas especiales, lo que ayuda a las organizaciones a mantener la privacidad y confidencialidad de la información con mayor facilidad.

Cifrado

Estándares de seguridad admitidos por Acrobat DC:

- estándar de cifrado avanzado (AES) de 256 bits;
- estándares admitidos por el Instituto Europeo de Normas de Telecomunicación (ETSI).

Control de acceso

Comparte documentos con seguridad mediante la aplicación de contraseñas y permisos para controlar el acceso a cualquier documento PDF o para evitar cambios en él, así como para restringir su impresión, copiado o alteración.

Firmas electrónicas y digitales

En Acrobat DC, los usuarios pueden elegir entre dos herramientas distintas para trabajar de forma segura con las firmas: Enviar para firmar y Certificados.

Enviar para firmar permite a los usuarios gestionar de forma integral los procesos de firma 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. Todo el proceso se gestiona de forma segura, y Adobe certifica los documentos y las pistas de

auditoría mediante un sello de garantía que evidencia cualquier intento de manipulación. Enviar para firmar utiliza la tecnología de *Adobe Sign*, una solución de *Adobe Document Cloud*, que está certificada de forma independiente en cumplimiento de los estándares más exigentes en materia de seguridad, incluidos la norma ISO 27001, el informe SOC 2 de tipo 2 y la HIPAA, así como el PCI DSS.

La herramienta Certificados te permite firmar documentos mediante ID digitales basados 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 uno de los métodos más seguros 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 (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 el algoritmo de cifrado AES-256/RSA-4096/SHA-512. La herramienta Certificados también te permite añadir marcas de hora a los documentos y certificarlos con un sello de garantía que evidencia cualquier intento de manipulación.

Para obtener más información sobre las firmas electrónicas y digitales, consulta el informe técnico *Transforma los procesos empresariales mediante firmas electrónicas y digitales*.

Verdadera censura

Acrobat DC ofrece un conjunto de herramientas de censura que te ayuda a proteger la información delicada o confidencial. Puedes eliminar de forma permanente tanto texto como imágenes gráficas de un documento antes de distribuirlo. Puedes incluso buscar y censurar a partir de patrones como, por ejemplo, números de teléfono, números de tarjeta de crédito y direcciones de correo electrónico. La información que selecciones se eliminará completamente del archivo, en lugar de quedar simplemente enmascarada como sucede con otras herramientas o métodos.

Con la función Esterilizar documento, puedes eliminar la información oculta y los objetos no gráficos como, por ejemplo, los metadatos que pueda haber en el PDF.

Seguridad de aplicaciones

Las funciones de seguridad mejoradas de Acrobat DC aumentan la protección contra los ataques que intentan aprovechar el formato de archivo PDF para instalar malware en tu sistema o extraer datos confidenciales de tu ordenador.

En Adobe, las prácticas de seguridad están profundamente integradas en nuestra cultura, así como en nuestros procesos de desarrollo de software y de diseño. Acrobat DC y Acrobat Reader se diseñan siguiendo prácticas de seguridad estándares del sector (para la gestión de accesos, la confidencialidad de los datos y la integridad de los documentos) con el fin de proteger tus documentos, datos e información personal.

Ingeniería segura

Las aplicaciones de Adobe DC se diseñan siguiendo el proceso de ciclo de vida seguro de los productos (SPLC, Secure Product Lifecycle) de Adobe, que incluye varios centenares de estrictas actividades de seguridad que comprenden las prácticas de desarrollo de software, los procesos y las herramientas. El SPLC de Adobe se integra en varias etapas del ciclo de vida del producto Acrobat DC, desde el diseño y el desarrollo hasta el control de calidad, las pruebas y la implementación. Para obtener más información sobre los procesos de seguridad, el compromiso con la comunidad y el SPLC de Adobe, consulta *www.adobe.com/es/security*.

Modo protegido de Adobe Acrobat Reader DC

Para protegerte, así como a tu organización, del código malintencionado que intenta utilizar el formato PDF para escribir o leer el sistema de archivos de un ordenador, Adobe desarrolla una implementación vanguardista de la tecnología de zonas protegidas denominada "Modo protegido", que se introdujo por primera vez en Adobe Reader X.

En Acrobat Reader DC, el modo protegido amplía la protección contra los atacantes que tratan de instalar malware en tu ordenador con el fin de impedir también que ningún individuo malintencionado pueda acceder a los datos confidenciales y a la propiedad intelectual de tu ordenador o red corporativa y extraerlos.

El modo protegido está activado de forma predeterminada cada vez que inicias Acrobat Reader DC. Este modo limita el nivel de acceso permitido al programa, lo que protege a los sistemas que ejecutan el sistema operativo 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. Ahora, el modo protegido de Reader (en Windows 8.1 y versiones posteriores) se puede ejecutar en un AppContainer. Más información sobre AppContainer: *https://msdn.microsoft.com/en-us/library/windows/desktop/mt595898(v=vs.85).aspx* (en inglés).

Además, dentro del esfuerzo continuo de la empresa por integrar la seguridad en varias fases del ciclo de vida de los productos a través del proceso de SPLC, Adobe realiza revisiones periódicas del código existente y lo refuerza cuando es preciso, lo que aumenta aún más la seguridad de las aplicaciones y de tus datos cuando utilizas los productos de Adobe.

Modo protegido de Acrobat DC

¿Qué son las zonas protegidas?

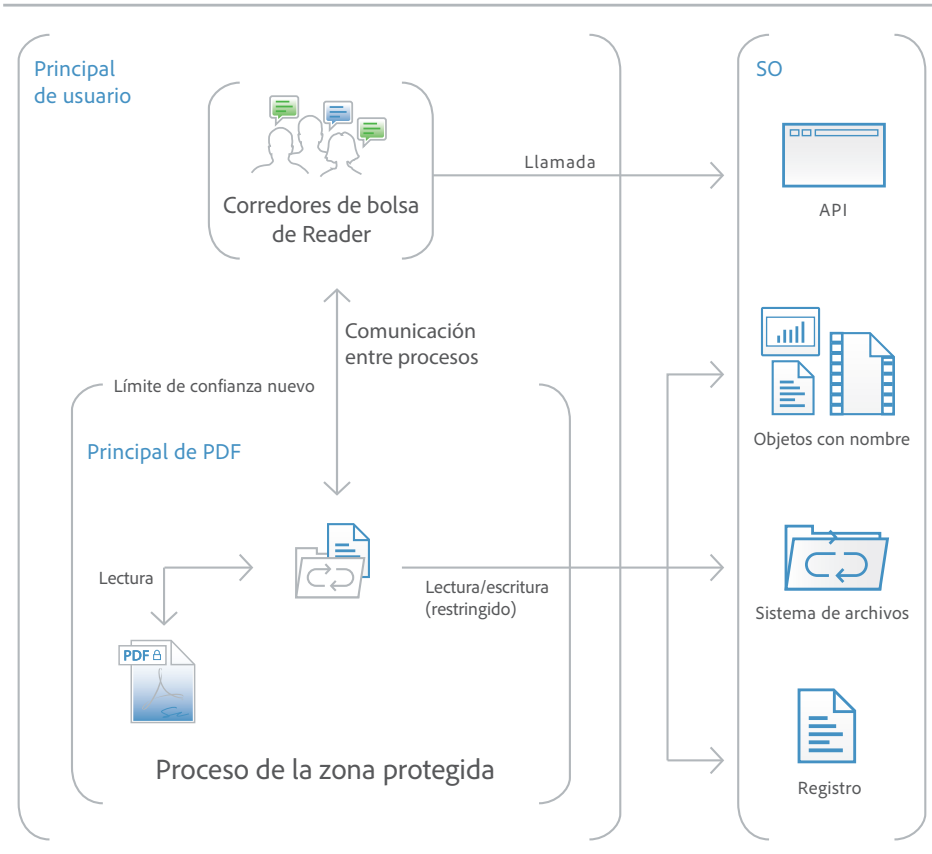
El uso de zonas protegidas es un método muy respetado entre los profesionales de la seguridad que crea un entorno de ejecución limitado para ejecutar programas con pocos derechos o privilegios. Estas zonas protegidas protegen los sistemas de los usuarios contra los daños causados por los documentos no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

De forma similar al de Acrobat Reader DC, el modo protegido de Acrobat DC 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 tu ordenador a través del formato de archivo PDF, con el fin de proteger también contra los ataques basados en lectura que intentan robar tus datos confidenciales o tu propiedad intelectual a través de archivos PDF.

Al igual que el modo protegido de Acrobat Reader DC, el de Acrobat DC 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 de tu ordenador.

El modo protegido presupone que todos los archivos PDF son potencialmente malintencionados y limita el procesamiento a la zona protegida, a menos que indiques específicamente que un archivo es de confianza. El modo protegido 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, el modo protegido se ejecuta siempre en un AppContainer. Esto proporciona un entorno de protección aún más sólido a los clientes que activen el modo protegido.

Cuando abres un archivo potencialmente malintencionado dentro del modo protegido, Acrobat DC muestra una barra amarilla de mensajes en la parte superior de la ventana de visualización. Esta barra indica que el archivo no es fiable y te recuerda que estás en el modo protegido, 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 el modo protegido impide que el contenido malintencionado que incorpora o que está incrustado en él altere tu sistema. Para confiar en el archivo y activar todas las funciones de Acrobat DC, puedes hacer clic en el botón Activar todas las funciones de la barra amarilla de mensajes. Esta acción cierra el modo protegido y proporciona una confianza permanente en el archivo añadiéndolo a la lista de ubicaciones privilegiadas de Acrobat. Cada vez que vuelvas a abrir un archivo PDF de confianza, se desactivarán las restricciones del modo protegido.



Ejecución de JavaScript

Acrobat DC ofrece unos controles sofisticados y detallados mediante listas blancas y negras para la ejecución de JavaScript en una gran variedad de entornos como, por ejemplo, Microsoft Windows y Macintosh. El marco de trabajo de listas blancas de JavaScript de Adobe permite usar JavaScript de forma selectiva en archivos PDF, sitios o hosts específicos, o en documentos firmados con un certificado de confianza. Además, el marco de trabajo de listas negras de JavaScript de Adobe permite utilizar JavaScript dentro de los flujos de trabajo empresariales, al tiempo que se protege a los usuarios y los sistemas de los ataques que tienen como objetivo llamadas API específicas de JavaScript. Al añadir una llamada API específica de JavaScript a la lista negra, puedes impedir que se ejecute sin desactivar JavaScript por completo. También puedes evitar que los usuarios anulen tu decisión de bloquear una llamada API específica de JavaScript, lo que contribuirá a proteger a toda tu empresa del código malintencionado.

Configuración de varios dominios

Marco de trabajo de listas blancas

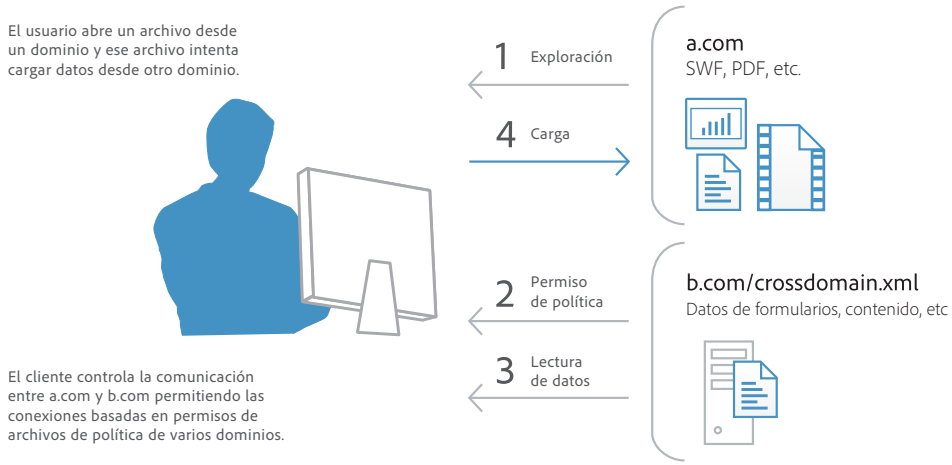
Puedes activar selectivamente JavaScript para los flujos de trabajo de confianza poniendo documentos en listas blancas mediante ubicaciones privilegiadas, que permiten conceder confianza basada en zonas de seguridad de Microsoft Windows, documentos certificados o añadiendo a ellas archivos, carpetas o hosts concretos.

De manera predeterminada, Acrobat DC desactiva el acceso no restringido a varios dominios en los clientes de Windows y Mac OS X, lo que evita que los intrusos exploten los archivos PDF sofisticados para acceder a los recursos de otro dominio.

Al aprovechar la compatibilidad integrada con los archivos de política de varios dominios basados en el servidor, permitirás que Acrobat DC y Acrobat Reader DC gestionen los datos de varios dominios. Este archivo de política interdominio (un documento XML) está alojado en un dominio remoto, lo que permite acceder al dominio fuente y que Acrobat DC o Acrobat Reader DC continúen la transacción.

Es conveniente activar la compatibilidad con varios dominios de Adobe en las siguientes situaciones:

- Si necesitas un acceso selectivo a varios dominios y deseas aprovechar otras funciones como, por ejemplo, el reconocimiento basado en certificados digitales.
- Si deseas gestionar de forma centralizada los permisos de acceso a varios dominios desde una sola ubicación basada en el servidor.
- Si tienes que implementar flujos de trabajo que incluyen solicitudes de datos de varios dominios para devolver datos de formularios, solicitudes de SOAP, referencias a transmisiones de contenido multimedia y solicitudes HTTP de .NET.



Alertas de seguridad fáciles de utilizar

Además de los procesos de respuesta ante incidentes y las alertas de seguridad de Adobe, Acrobat DC implementa un método de alertas de seguridad fáciles de utilizar por medio de la barra amarilla de mensajes. Si se activa la seguridad mejorada y no se ha configurado el archivo PDF como ubicación privilegiada o fiable, la barra amarilla de mensajes aparecerá cuando el archivo intente ejecutar una acción potencialmente peligrosa como, por ejemplo:

- invocar el acceso a varios dominios;
- ejecutar JavaScript con privilegios;
- invocar URL ejecutadas por JavaScript;
- llamar una API de JavaScript de la lista negra;
- insertar datos;
- insertar secuencias de comandos;
- reproducir contenido multimedia heredado incrustado.

En Acrobat DC y Reader DC, la barra amarilla de mensajes aparece en la parte superior del documento con el mensaje de advertencia o de error. El usuario puede elegir entre confiar en el documento una vez o siempre. Al seleccionar "siempre", el documento se añadirá a la lista de documentos con privilegios de la aplicación.

El botón Opciones permite a los usuarios definir la confianza sobre la marcha, una vez o siempre. También puedes preconfigurar la confianza de los archivos, las carpetas y los hosts de toda la empresa para que la barra amarilla de mensajes no vuelva a aparecer en los flujos de trabajo empresariales de confianza.

Seguridad en la nube

En Adobe supervisamos y mejoramos constantemente nuestros servicios, sistemas y procesos en la nube para ayudar a los clientes a satisfacer las demandas y los retos cada vez mayores que plantean la salvaguarda y protección de los datos. Los servicios de Document Cloud, incluidos Adobe Sign y los servicios de PDF que utiliza Acrobat DC, están diseñados para contribuir a garantizar la confidencialidad, integridad y disponibilidad de tus documentos. Los servicios de Document Cloud cumplen la norma ISO 27001, el PCI DSS y el informe SOC 2 de tipo 2, así como muchos otros estándares, certificaciones, estándares y normativas específicos del sector. Para obtener más información sobre nuestra estrategia de seguridad en la nube consulta el documento *Adobe Document Cloud Security Overview* (Resumen de la seguridad de Adobe Document Cloud).

Seguridad del centro de datos

En la actualidad, el centro de datos de Document Cloud que aloja los servicios de PDF y el almacenamiento de archivos reside en un centro de datos de nivel 4 del American National Standards Institute (ANSI) gestionado por nuestro proveedor de servicios en la nube de confianza, Amazon Web Services (AWS). AWS mantiene controles muy estrictos del acceso al centro de datos, la tolerancia a errores, los controles medioambientales y la seguridad. Solo los empleados aprobados y autorizados por Adobe, los empleados del proveedor de servicios en la nube y los contratistas con una relación comercial legítima y documentada pueden acceder a este centro protegido de Virginia (EE. UU.). Para obtener más información sobre la seguridad del centro de datos de AWS, consulta *https://aws.amazon.com/es/security/*.

Cifrado de datos y privacidad

Los productos y servicios de Adobe, incluidos los servicios de Document Cloud, están diseñados pensando en la privacidad. Document Cloud cifra los documentos y los activos en reposo mediante el estándar de cifrado avanzado (AES) de 256 bits del National Institute of Standards and Technology (NIST) y es compatible con el protocolo de transferencia de hipertexto (HTTP, Hypertext Transfer Protocol) dentro de una conexión cifrada mediante seguridad en la capa de transporte (TLS, Transport Layer Security) para garantizar que todos los datos en tránsito también reciban una protección adecuada.

Los empleados y los proveedores de confianza de Document Cloud acceden a los datos de los clientes únicamente para realizar algunas funciones empresariales y de asistencia técnica concretas, o por imperativo legal. Adobe no permite a ningún gobierno acceder de forma directa o sistemática a los datos que almacenamos de los clientes. Para obtener más información sobre las políticas de privacidad de Adobe, consulta *www.adobe.com/es/privacy*.

Integración con las arquitecturas de los sistemas operativos

Seguridad siempre activa

Para proporcionar una mayor defensa contra los ataques que intentan controlar los sistemas de escritorio o dañar la memoria, Acrobat DC aprovecha las protecciones de seguridad integradas y siempre activas de los sistemas operativos Windows y Mac OS X.

La prevención de ejecución de datos (DEP, Data Execution Prevention) limita el almacenamiento de datos o de código peligroso en las ubicaciones de la memoria configuradas como protegidas por el sistema operativo Windows. Apple ofrece una protección similar para Mac OS X Lion, que incluye una DEP en la pila y otra basada en montones de memoria, y la amplía a las aplicaciones de 32 y 64 bits, lo que hace que todas las aplicaciones sean más resistentes a los ataques.

La selección aleatoria del diseño del espacio de direcciones (ASLR, Address space layout randomization) oculta las ubicaciones de los archivos de memoria y páginas de los componentes del sistema, lo que dificulta que los intrusos encuentren y ataquen estos componentes. Tanto Windows como Mac OS X Lion utilizan la ASLR. En Mac OS X Lion, la ASLR se amplía a las aplicaciones de 32 y 64 bits.

Configuración de nivel de registro y archivos plist

Acrobat DC te brinda una amplia gama de herramientas para gestionar los ajustes de seguridad, incluidas las preferencias del nivel de registro (Windows) y de los archivos plist (Mac OS). Con estos ajustes, puedes configurar los clientes antes y después de la implementación para hacer lo siguiente:

- activar o desactivar la seguridad mejorada;
- activar o desactivar las ubicaciones con privilegios;
- especificar las ubicaciones con privilegios predefinidas;
- bloquear algunas funciones y desactivar la interfaz de usuario de la aplicación para que los usuarios finales no puedan modificar los ajustes;
- desactivar, activar o configurar prácticamente cualquier función relativa a la seguridad.

Una implementación y una administración más sencillas

Refuerzo de la seguridad del software

Las mejoras de seguridad como el modo protegido son solo un ejemplo de las cuantiosas inversiones en ingeniería que Adobe ha realizado para reforzar a Acrobat DC contra las amenazas. Al reforzar el software contra los ataques, Adobe puede reducir o incluso eliminar la necesidad de las actualizaciones de seguridad fuera de banda y reducir la urgencia de lanzar actualizaciones programadas de forma periódica. Todo esto aumenta la flexibilidad operativa y disminuye los costes totales de propiedad, sobre todo en entornos de gran envergadura con exigentes requisitos de controles de seguridad.

Compatibilidad con Citrix y la virtualización de aplicaciones

Gracias a la asistencia técnica con licencia de usuario designada para Citrix XenApp, Citrix XenDesktop, VMware Horizon y Microsoft App-V, puedes permitir que tus usuarios accedan con seguridad de forma remota a la funcionalidad de Acrobat que necesitan.

Compatibilidad con soluciones de administración de movilidad empresarial (EMM, Enterprise mobility management)

Adobe se compromete a ayudar a los clientes empresariales en su objetivo de satisfacer la demanda de soluciones de productividad empresarial móviles y de, al mismo tiempo, salvaguardar la seguridad y el cumplimiento normativo de la empresa. Las aplicaciones móviles de Acrobat Reader y Adobe Sign son compatibles con la plataforma de EMM Android for Work; y Adobe Acrobat Reader para Microsoft Intune está disponible tanto para iOS como para Android. Acrobat Reader también es compatible con la plataforma AppConfig. Más información sobre los *recursos de TI*.

Compatibilidad con objetos de directivas de grupo de Windows Server y Active Directory de Microsoft

Los objetos de directivas de grupo de Windows y Active Directory de Microsoft te permiten automatizar la gestión unidireccional de sistemas informáticos. Adobe ha incorporado la compatibilidad con plantillas del Centro de administración de Active Directory de Microsoft para directivas de grupo en Acrobat DC, lo que te permite instalar software bajo demanda y reparar las aplicaciones automáticamente. Si necesitas configurar las aplicaciones en mayor detalle tras la implementación, puedes usar estas plantillas para propagar los parámetros requeridos por toda la organización.

Compatibilidad con Microsoft SCCM y SCUP

Con Acrobat DC, puedes importar y publicar de forma eficiente las actualizaciones a través de Microsoft System Center Configuration Manager (SCCM) para tener la certeza de que los sistemas de escritorio Windows que gestionas están siempre al día con las actualizaciones y los parches de seguridad más recientes.

La compatibilidad con los catálogos de Microsoft System Center Updates Publisher (SCUP) te permite automatizar las actualizaciones del software Acrobat DC en toda tu organización, así como agilizar las implementaciones de software iniciales. Con SCUP, podrás importar automáticamente cualquier actualización que publique Adobe en cuanto esté disponible, lo que te facilitará y racionalizará la actualización de las implementaciones de Acrobat DC. La integración con SCCM y SCUP contribuye a reducir los costes totales de propiedad de tu software de Adobe, ya que te permite implementar parches en toda la organización con mayor rapidez y facilidad.

Compatibilidad con el instalador de paquetes de Apple y Apple Remote Desktop

Adobe ha implementado en Acrobat DC el instalador de paquetes estándar de Apple proporcionado por Mac OS X en lugar del instalador patentado de Adobe. Esto simplifica la implementación del software Acrobat en los sistemas de escritorio Macintosh de la empresa, ya que ahora puedes utilizar el software de gestión Apple Remote Desktop para gestionar tanto la implementación inicial del software como las actualizaciones y los parches posteriores desde una ubicación centralizada.

Parches y actualizaciones acumulativos y periódicos

Para ayudarte a mantener el software actualizado, Adobe publica de forma proactiva actualizaciones periódicas que contienen mejoras de funciones y correcciones de seguridad. Adobe proporciona todos los parches fuera del ciclo que sean necesarios para que puedas reaccionar con rapidez ante los ataques de día cero. Adobe aprovecha al máximo los parches acumulativos para reducir el esfuerzo y el coste necesario para mantener los sistemas actualizados. Asimismo, antes de publicarlos, Adobe somete a los parches de seguridad a pruebas agresivas con el fin de garantizar la compatibilidad con las instalaciones y los flujos de trabajo existentes.

La fecha de todas y cada una de las actualizaciones programadas se anuncia previamente en el blog del equipo de respuesta a incidentes de seguridad de los productos (PSIRT, Product Security Incident Response Team) de Adobe en *blogs.adobe.com/psirt*.

Para consultar los boletines de seguridad y las recomendaciones más recientes sobre los productos de Adobe, visita *www.adobe.com/es/support/security*. Para obtener información en mayor detalle sobre los productos de Adobe y las funciones de seguridad, visita la biblioteca de seguridad de Adobe en *www.adobe.com/go/learn_acr_appsecurity_en*.

Adobe Customization Wizard y Enterprise Toolkit

Adobe proporciona las siguientes herramientas para ofrecerte un mayor control de las implementaciones en toda tu empresa:

- **Adobe Customization Wizard**: Utilidad descargable de forma gratuita que te permite personalizar el instalador de Acrobat y configurar las funciones de las aplicaciones antes de la implementación.
- **Adobe Enterprise Toolkit (ETK) para Acrobat y Windows**: Aplicación personalizable que se actualiza automáticamente y contiene el recurso Adobe Preference Reference. Adobe ETK también incluye una lista en continua ampliación de recursos interesantes para los administradores empresariales.

Más información sobre estas herramientas en *Recursos de TI*.

Conclusión

Con Acrobat DC, Adobe aumenta la seguridad de los documentos PDF y tus datos hasta alcanzar niveles nunca vistos. Desde una seguridad ampliada de las aplicaciones destinada a aumentar la protección contra el robo de datos confidenciales y propiedad intelectual corporativos, así como a impedir la instalación de malware peligroso en tus ordenadores, hasta la integración con otras herramientas que facilitan más que nunca la administración de las implementaciones a escala de toda la empresa, Acrobat DC ofrece mayores niveles de seguridad con unos costes totales de propiedad menores que cualquier versión anterior de Acrobat DC.

Para obtener más información

Detalles de la solución:
www.adobe.com/es/security

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704 USA
www.adobe.com
www.adobe.com/es
www.adobe.com/la

7/17