CCN
centro criptológico nacional

CCN-CERT BP/16

RECOMENDACIONES DE SEGURIDAD DE ADOBE ACROBAT READER DC

Marzo 2022

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL,
2.5.4.97=VATES-S2800155J, ou=CENTRO
CRIPTOLOGICO NACIONAL, o=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2022.03.22 13:56:11 +01'00'

Pº de la Castellana 109, 28046 Madrid

Fecha de Edición: marzo de 2022

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

1. INTRODUCCIÓN

Este documento forma parte de la documentación emitida por el Centro Criptológico Nacional cuyo objetivo es el de preservar la seguridad de los sistemas TIC de las Administraciones Públicas.

Para ello, se proporciona un mecanismo de aplicación de medidas de seguridad de forma automatizada y desatendida sobre un *software* de visualización de ficheros PDF, para facilitar la posibilidad de implementar seguridad en los sistemas TIC de forma sencilla y ágil.

2. OBJETO

El propósito de este documento consiste en establecer los procedimientos y utilidades necesarias para implementar y garantizar la seguridad en *Adobe Reader DC* versión continuada.

3. ALCANCE

Este documento establece un procedimiento para mejorar la seguridad y proteger *Adobe Acrobat Reader DC* para mitigar las posibles vulnerabilidades y los riesgos frente a los que pudiera estar expuesto.

Los usuarios de esta guía pueden mejorar la seguridad de esta aplicación a través de la interfaz de usuario y de la configuración del Registro, además de configurar características de este producto para proteger la integridad del contenido PDF.

4. INSTALACIÓN Y BASTIONADO DE *ADOBE READER DC* PISTA CONTINUA EN WINDOWS

El programa *Adobe Reader* está disponible para descargar de manera gratuita desde la página web de Adobe, y permite la visualización e impresión de documentos PDF.

Este manual está diseñado para *Adobe Acrobat Reader DC* Pista Continua, aunque también se puede utilizar para versiones posteriores.

Adobe Reader DC debe tener instaladas las últimas actualizaciones de *software* relacionadas con la seguridad. Para ello, determine el método de actualización (por ejemplo, conexión a un servidor *WSUS*, procedimiento local, actualización automática, etc.).

Para determinar la versión que tenemos instalada, debe hacer *click en Ayuda >> Acerca de Adobe Acrobat Reader DC*. Verifique que tiene aplicada la última actualización de *software*. Si no se aplican las últimas actualizaciones de *software* relacionadas con la seguridad de Adobe, este sería un fallo crítico de seguridad.

4.1. DESCARGAR E INSTALAR ADOBE READER DC PISTA CONTINUA

La descarga del programa debemos realizarla en un equipo conectado a internet.

Antes de realizar la descarga del programa, debemos tener en cuenta los datos que se exponen a continuación.

4.2. VERSIONES

El software de escritorio Acrobat Reader DC está disponible para su implementación tanto con la versión "*clásica*" como con la versión "*continua*".

La versión *"continua"* proporciona herramientas basadas en servicios, así como nuevas características, mejoras de seguridad y plataforma, y correcciones de errores con mayor frecuencia. La cadencia de actualización de la pista continua es más frecuente que la pista clásica.

La versión "*clásica*" es similar al modelo 10.X – 11.X y no proporciona nuevas características en las actualizaciones. Los servicios gratuitos están disponibles, pero opcionales. La cadencia de actualización es trimestral y ofrece mejoras de seguridad y plataforma, así como correcciones de errores.

A continuación, podemos ver el formato genérico para mostrar la versión definitiva de Adobe Reader DC (mayor.menor.menor_menor).

Descripción

Versión	Rango	Notas
mayor	1-255	Los dos últimos dígitos del año de lanzamiento.
menor	1-255	Un número interno que indica cuándo se mueve el código de Trunk a Beta.
menor_menor	1-65535	Los dos primeros dígitos indican la versión: 20 = Continua. 30 Clásica.
4to campo oculto	Changelist number	Solo visible si el usuario hace clic en el número de versión en e cuadro Acerca de.

4.3. REQUISITOS

A continuación, se detallan los requisitos mínimos necesarios del sistema para realizar la implementación del programa Adobe Acrobat Reader DC.

Acrobat Reader DC (32 bits)

- Procesador Intel® o AMD de 1,5 GHz o más rápido
- Windows 11 (64 bits), Windows 10 (32 bits y 64 bits) versión 1809 o posterior, Windows 8, 8.1 (32 bits y 64 bits) *, Windows 7 SP1 (32 bits y 64 bits) o Windows Server - 2008 R2 (64 bits), 2012 (64 bits), 2012 R2 (64 bits) *, 2016 (64 bits) o 2019 (64 bits)
- 2 GB de RAM
- 450 MB de espacio disponible en el disco duro
- Resolución de pantalla de 1024 × 768
- Internet Explorer 11

*Con la *actualización de Windows 2919355* instalada.

Acrobat Reader DC (64 bits)

- Procesador Intel® o AMD de 1,5 GHz o más rápido
- Windows 11 (64 bits), Windows 10 (64 bits) versión 1809 o posterior, Windows Server 2016 (64 bits) o Windows Server 2019 (64 bits)
- 2 GB de RAM

- 900 MB de espacio disponible en el disco duro para inglés
- 1 GB de espacio disponible en el disco duro para otros idiomas
- Resolución de pantalla de 1024 × 768
- Internet Explorer 11

4.4. UBICACIÓN DE LA INSTALACIÓN

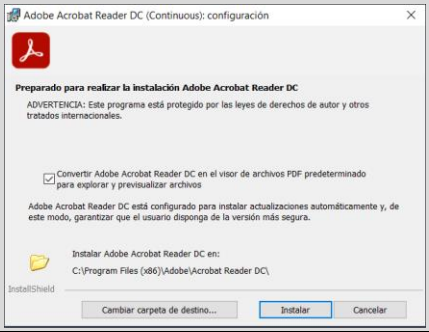
A continuación, se describen las rutas de instalación de *Acrobat Reader DC*:

- Ruta de instalación en Windows(32bits) *C:\Program Files (x86)\Adobe\Acrobat Reader DC*
- Ruta de instalación en Windows(64bits) *C:\Program Files\Adobe\Acrobat Reader DC*
- Ruta de registro *HKCU\Software\Adobe\Acrobat Reader\DC*
- Ruta de datos de la aplicación *%Appdata%\Roaming\Adobe\Acrobat\DC*

Para el seguimiento continuo, todos los servicios son visibles. Los servicios gratuitos de *Adobe Document Cloud* son funcionales de forma predeterminada, y los servicios de pago requieren una actualización o compra.

Para la versión Acrobat DC Enterprise, durante el proceso de instalación se encuentra marcado por defecto, el establecer Adobe Acrobat Reader DC como el visor de archivos PDF predeterminado.

Nota: Es posible personalizar la ruta donde se realiza la instalación del programa en el proceso de instalación del programa.



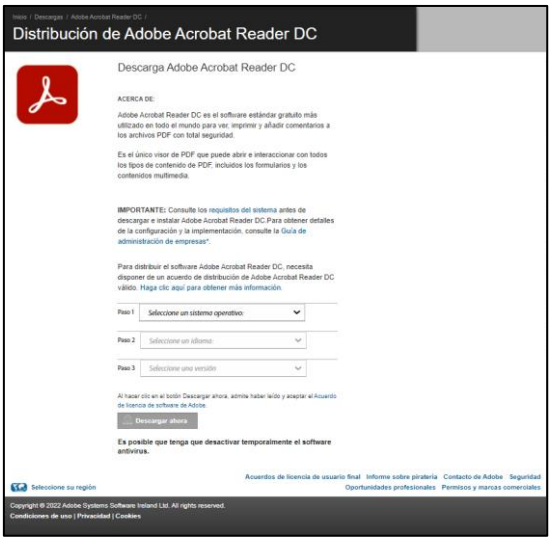
4.5. DESCARGA E INSTALACIÓN DE READER

4.5.1 ACROBAT READER DC (ENTERPRISE)

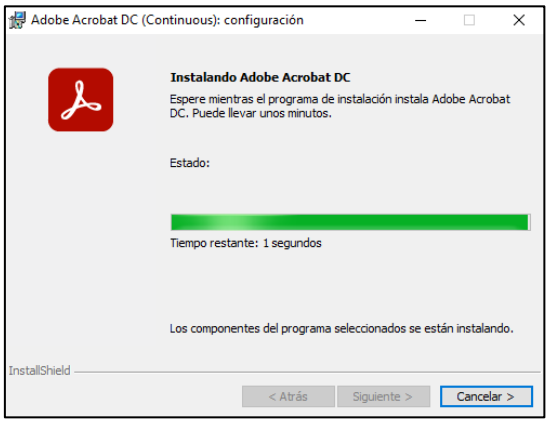
A través de la siguiente URL: https://get.adobe.com/es/reader/enterprise/

Todas las versiones de *Adobe Acrobat Reader DC* disponibles para descarga en este enlace usan el seguimiento continuo.

Descripción
En esta ventana seleccionaremos el sistema operativo en el cual realizaremos la instalación de esta descarga "*Paso 1*", el idioma "*Paso 2*" y por último la versión "*Paso 3*". A continuación, pulsaremos el botón "*Descargar ahora*" para iniciar la descarga del programa. Una vez realizado este paso, haremos doble clic sobre el archivo de instalación y esperaremos hasta que el proceso de instalación haya terminado.



El archivo de instalación que descarguemos será utilizado para instalar o actualizar la versión de Acrobat Reader.



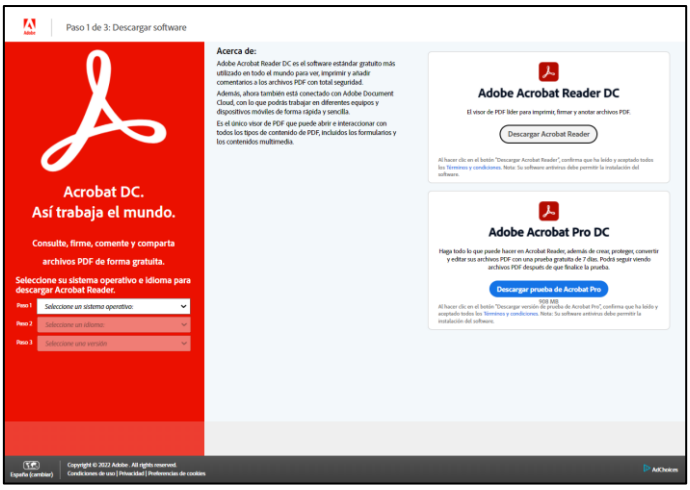
Reinicia el sistema y ya estará listo para poder utilizar el programa.

4.5.2 ACROBAT READER DC (PARTICULARES)

A través de la siguiente URL: https://get.adobe.com/es/reader/

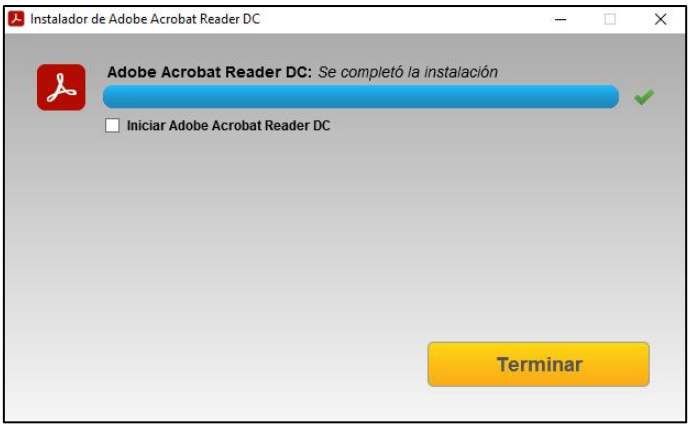
La instalación de Adobe Acrobat Reader DC se realiza directamente en su equipo. Se necesita Internet para completar el proceso de autorización en el primer inicio y cada 30 días con el fin de validar su suscripción.

Descripción
En esta ventana seleccionaremos el sistema operativo en el cual realizaremos la instalación de esta descarga "*Paso 1*", el idioma "*Paso 2*" y por último la versión "*Paso 3*". A continuación, pulsaremos el botón "*Descargar Acrobat Reader*" para iniciar la descarga del archivo de instalación de Adobe Acrobat, llamado "reader[xxx]_install.exe". Una vez realizado este paso, haremos doble clic sobre el archivo de instalación para completar la instalación.



Nota: La instalación de Acrobat Reader DC es un proceso de dos etapas: se descarga el programa de instalación y, a continuación, se instala Reader.

Haga clic en Terminar y reinicie el sistema. Ya estará listo para poder utilizar el programa.



4.6. APLICAR VALORES DE SEGURIDAD

A continuación, se describe paso a paso cómo añadir los archivos .admx y .adml, y los valores de seguridad para bastionar Adobe Reader DC en un equipo Windows.

4.6.1 CLIENTE WINDOWS

En este ejemplo, se parte de la suposición de que, en el equipo, en el que se van a ejecutar los scripts, se ha instalado el sistema operativo Windows y el programa Adobe Reader DC.

	Descripción
1.	Inicie sesión con un usuario que tenga privilegios de administrador y que sea miembro del grupo “Usuarios de Shell” en la máquina donde se desea ejecutar los scripts.
2.	Copie los ficheros y carpetas que acompañan a esta guía al directorio "C:\Scripts" del equipo.
3.	Asegúrese de que al menos los siguientes ficheros hayan sido copiados al directorio “C:\Scripts”: – *GP Report* – *GPOs* – *PolicyDefinitions* – *Scripts_local*
4.	A continuación, vaya a la carpeta “C:\Scripts\Scripts_local” y ejecute como administrador (Opción ejecutar como administrador) el fichero “Import ADMX - Install GPO.bat”.
5.	Las Plantillas administrativas estarán añadidas correctamente e importados los valores GPO.
6.	Cuando finalice la ejecución pulse de nuevo una tecla para cerrar la ventana
7.	Reinicie el sistema.

Nota: La importación de la configuración de la directiva de grupo local desde la copia de seguridad de GPO incluida en la carpeta Scripts se realiza con la herramienta gratuita LGPO.exe que es una utilidad de línea de comandos para automatizar la administración de la directiva de grupo local y forma parte del kit de herramientas de cumplimiento de seguridad de Microsoft. URL de descarga: *https://www.microsoft.com/download/details.aspx?id=55319*

4.6.2 WNDOWS SERVER, COMO CREAR Y ADMINISTRAR EL ALMACEN CENTRAL PARA PLANTILLAS ADMINISTRATIVAS DE DIRECTIVAS DE GRUPO.

A continuación, se describe cómo usar los archivos .admx y .adml para crear y administrar la configuración de directiva basada en el Registro en Windows. Además de cómo se usa el almacén central para almacenar y replicar los archivos de directivas de grupo de Adobe Reader DC, que acompañan a esta guía, en un entorno de dominio.

El almacén Central

Para beneficiarse de las ventajas de los archivos .admx, debe crear un almacén Central en la carpeta SYSVOL en un controlador de dominio. El almacén Central es una ubicación de archivo que está protegida por las herramientas de directiva de grupo. Las herramientas de directiva de grupo utilizan cualesquiera archivos .admx que se encuentran en el almacén Central. Más tarde, los archivos que se encuentran en el almacén Central se replican en todos los controladores de dominio en el dominio.

Para crear un almacén Central para archivos .admx y .adml, cree una carpeta denominada PolicyDefinitions en la ubicación siguiente:

\\FQDN\SYSVOL\FQDN\policies

Nota: FQDN es un nombre de dominio completo.

Por ejemplo, para crear un almacén Central para el dominio contoso.com, cree una carpeta PolicyDefinitions en la ubicación siguiente:

\\contoso.com\SYSVOL\contoso.com\policies

Copie todos los archivos de la carpeta PolicyDefinitions, que acompañan a esta guía, en la carpeta PolicyDefinitions del controlador de dominio. La carpeta PolicyDefinitions, que acompaña a esta guía, almacena los archivos .admx y .adml para el idioma español (es-ES).

Ahora si abrimos una GPMC y editamos una política ya existente, veremos que en las plantillas administrativas ya nos aparece el nuevo tipo de template que hemos habilitado con el directorio PolicyDefinitions y además en nuestro idioma.

En la carpeta GPO de esta guía encontraremos una copia de seguridad de GPO con la configuración de seguridad.

4.7. VALORES DE REGISTRO

A continuación, se detallan las modificaciones de seguridad ejecutadas a nivel de registro en el proceso de refuerzo de seguridad establecido en el punto “4.6 APLICAR VALORES DE SEGURIDAD”.

Adobe Reader DC debe evitar la apertura de archivos que no sean PDF o FDF

Los archivos adjuntos representan un riesgo potencial de seguridad porque pueden contener contenido malicioso, abrir otros archivos peligrosos o iniciar aplicaciones.

Los archivos con extensión .bin, .exe, .bat, etc. serán reconocidos como amenazas.

Esta función evita que los usuarios abran o inicien tipos de archivos que no sean PDF o FDF y deshabilita la opción de menú.

El valor de “*iFileAttachmentPerms*” debe estar establecido en "1" y el tipo configurado como “*REG_DWORD*”.

Comprobación:

Ruta GUI: Edición> Preferencias> Administrador de confianza> En la sección 'Adjuntos de archivo PDF'> Verificar “Permitir la apertura de archivos no PDF con aplicaciones externas” debe mostrar la casilla de verificación desactivada y en gris (bloqueada).

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown" /v "iFileAttachmentPerms”
```

Adobe Reader DC debe bloquear contenido Flash.

Adobe Reader y Acrobat dejaron de enviarse con un reproductor Flash dedicado en la versión 9.5.1. Desde entonces, la representación de contenido Flash en un PDF requiere que Flash Player ya se encuentre en la máquina del usuario.

Esta estrategia simplifica las implementaciones de Acrobat y Reader al reducir la cantidad de futuras actualizaciones necesarias en caso de que surja un problema de seguridad.

El contenido Flash se puede incrustar en PDF y podría utilizarse para instalar software malintencionado en un equipo de usuario.

El valor de “*bEnableFlash*” debe estar establecido en "0" y el tipo configurado como “REG_DWORD”.

Comprobación:

```
REG QUERY
“HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown” /v “bEnableFlash”
```

Adobe Reader DC debe deshabilitar todo acceso de servicio a Document Cloud Services

De forma predeterminada, los servicios en línea de Adobe están estrechamente integrados en Adobe Reader DC.

Con la integración de *Adobe Document Cloud*, deshabilitar esta función evita el riesgo de vectores de ataque adicionales.

Dentro de Adobe Reader DC, los recursos de Adobe Cloud requieren una suscripción de pago por cada servicio.

El valor de “*bToggleAdobeDocumentServices*” debe estar establecido en "1" y el tipo configurado como “REG_DWORD”.

Comprobación:

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown\cServices" /v
"bToggleAdobeDocumentServices"
```

Nota: El nombre de la clave "*cServices*" no se crea de forma predeterminada en la instalación de Adobe Reader DC y debe crearse.

Adobe Reader DC debe habilitar la Seguridad mejorada en una aplicación independiente.

Los archivos PDF han evolucionado de páginas estáticas a documentos complejos con características tales como formularios interactivos, contenido multimedia, secuencias de comandos y otras capacidades.

Estas características hacen que los archivos PDF sean vulnerables a scripts maliciosos o acciones que pueden dañar el sistema o robar datos.

La función de seguridad mejorada protege al sistema contra estas amenazas al bloquear o permitir selectivamente acciones para ubicaciones y archivos de confianza.

La seguridad mejorada determina si un PDF se ve dentro de una aplicación independiente. Una amenaza para los usuarios de Adobe Reader DC es abrir un archivo PDF que contenga contenido ejecutable malicioso.

La seguridad mejorada "endurece" la aplicación contra acciones de riesgo como evitar el acceso a varios dominios, prohibir la inyección de datos y secuencias de comandos, bloquear el acceso de la secuencia a *XObjects*, la impresión silenciosa y la ejecución de JavaScript de alto privilegio.

El valor de "*bEnhancedSecurityStandalone*" debe estar establecido en "1" y el tipo configurado como "REG_DWORD".

Comprobación:

Ruta GUI: Edición> Preferencias> Seguridad (mejorada)> En la sección 'Seguridad mejorada'> La casilla de verificación 'Habilitar seguridad mejorada' está marcada y desactivada (bloqueada).

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown" /v "bEnhancedSecurityStandalone"
```

Adobe Reader DC debe desactivar los conectores web de terceros.

Cuando los conectores web de terceros están deshabilitados, impide la configuración del acceso de Adobe Reader DC a servicios de terceros para el almacenamiento de archivos.

El valor de "*bToggleWebConnectors*" debe estar establecido en "1" y el tipo configurado como "*REG_DWORD*".

Comprobación *:*

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown\cServices" /v
"bToggleWebConnectors"
```

Nota: El nombre de la clave "*cServices*" no se crea de forma predeterminada en la instalación de Adobe Reader DC y debe crearse.

Adobe Reader DC debe desactivar la sincronización de nube.

De forma predeterminada, los servicios en línea de Adobe están estrechamente integrados en Adobe Reader DC.

Cuando la sincronización de *Adobe Cloud* está deshabilitada, evita la sincronización de las preferencias de escritorio en los dispositivos en los que el usuario ha iniciado sesión con un ID de Adobe (incluidos los teléfonos).

El valor de "*bTogglePrefsSync*" debe estar establecido en "1" y el tipo configurado como "*REG_DWORD*".

Comprobación:

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown\cServices" /v "bTogglePrefsSync"
```

Nota: El nombre de la clave "*cServices*" no se crea de forma predeterminada en la instalación de Adobe Reader DC y debe crearse.

Adobe Reader DC debe habilitar el modo FIPS.

El uso de algoritmos de cifrado débiles o no probados socava los propósitos de utilizar el cifrado para proteger los datos.

La aplicación debe implementar módulos criptográficos que cumplan con los estándares más altos aprobados por entidades, ya que esto garantiza que se hayan probado y validado.

El valor de "*bFIPSMode*" debe estar establecido en "1" y el tipo configurado como "*REG_DWORD*".

Comprobación:

```
REG QUERY "HKEY_CURRENT_USER\Software\Adobe\Acrobat
Reader\DC\AVGeneral" /v "bFIPSMode"
```

Adobe Reader DC debe deshabilitar el acceso a Webmail.

Cuando Webmail está deshabilitado, el usuario no puede configurar una cuenta de correo web para enviar un documento PDF abierto como un archivo adjunto.

Los usuarios deben tener la capacidad de enviar documentos como archivos adjuntos de Microsoft Outlook.

La diferencia es que Outlook debe ser configurado por el administrador en la máquina local.

El valor de "*bDisableWebmail*" debe estar establecido en "1" y el tipo configurado como "*REG_DWORD*".

Comprobación:

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown\cWebmailProfiles" /v
"bDisableWebmail"
```

Nota: El nombre de la clave "*cWebmailProfiles*" no se crea de forma predeterminada en la instalación de Adobe Reader DC y debe crearse.

Adobe Reader DC debe deshabilitar la capacidad de elevar (trust) documentos certificados como una ubicación privilegiada.

Las ubicaciones privilegiadas permiten al usuario confiar de forma selectiva en los archivos, carpetas y hosts para omitir algunas restricciones de seguridad, como la seguridad mejorada y la vista protegida.

De forma predeterminada, el usuario puede crear ubicaciones privilegiadas a través de la GUI.

La desactivación de documentos certificados desactiva y bloquea la capacidad del usuario final para elevar documentos certificados como una ubicación privilegiada.

El valor de "*bEnableCertificateBasedTrust*" debe estar establecido en "0" y el tipo configurado como "*REG_DWORD*".

Comprobación:

Ruta GUI: Edición> Preferencias> Seguridad (Mejorada)> En la sección 'Ubicación privilegiada', verifique que la opción 'Confiar automáticamente en los documentos con una certificación válida' esté desactivada y en gris (bloqueada).

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown" /v
"bEnableCertificateBasedTrust"
```

Adobe Reader DC debe bloquear los sitios web.

Hacer clic en cualquier enlace a Internet representa un riesgo de seguridad potencial.

Los sitios web malintencionados pueden transferir contenido dañino o recopilar datos en silencio.

Los documentos de Acrobat Reader pueden conectarse a sitios web que pueden representar una amenaza potencial para los sistemas y esa funcionalidad debe estar bloqueada.

Sin embargo, los flujos de trabajo de documentos PDF de confianza pueden beneficiarse al aprovechar el acceso legítimo a sitios web con un riesgo mínimo.

Por lo tanto, puede aprobar el acceso a sitios web y aceptar el riesgo si el acceso proporciona un beneficio y es un sitio confiable o el riesgo asociado con el acceso al sitio se ha mitigado.

El valor de "*iURLPerms*" debe estar establecido en "1" y el tipo configurado como "*REG_DWORD*".

Comprobación:

Ruta GUI: Edición> Preferencias> Administrador de confianza> En la sección "Acceso a Internet desde archivos PDF fuera del explorador web"> Seleccione la opción "Cambiar configuración"> En "Los archivos PDF pueden conectar con sitios Web para compartir u obtener información" sección> Verificar el botón de opción "Bloquear el acceso de los archivos PDF a todos los sitios Web" está seleccionado y desactivado (bloqueado).

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown\cDefaultLaunchURLPerms" /v
"iURLPerms"
```

Adobe Reader DC debe habilitar el modo protegido.

Una amenaza para los usuarios de Adobe Reader DC es abrir un archivo PDF que contenga contenido ejecutable malicioso.

El *sandboxing* es una técnica para crear un entorno de ejecución aislado, que permite ejecutar programas que no son de confianza.

En el contexto de Adobe Reader, un "programa no confiable" es cualquier PDF y los procesos que invoca.

Cuando el *sandboxing* está habilitado, Reader asume que todos los archivos PDF son potencialmente maliciosos y limita cualquier procesamiento invocándolo en este.

Este aislamiento de los archivos PDF reduce el riesgo de fallos de seguridad en áreas fuera del *sandbox*.

El valor de "*bProtectedMode*" debe estar establecido en "1" y el tipo configurado como "*REG_DWORD*".

Comprobación:

Ruta GUI: Edición>Preferencias> Seguridad (Mejorada)> Protecciones de la zona de pruebas> Activar el modo protegido al iniciar.

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown" /v "bProtectedMode"
```

Adobe Reader DC debe habilitar la vista protegida.

Esencialmente es un modo de solo lectura. Esta función se basa en la tecnología *sandbox*.

En Reader, la Vista protegida solo se admite cuando el "Modo protegido" está habilitado. Si una clave de registro *HKCU o HKLM Protected Mode* se establece en 0 (apagado), la Vista protegida no se puede habilitar.

El valor de "*iProtectedView*" debe estar establecido en "2" y el tipo configurado como "*REG_DWORD*".

Comprobación:

Ruta GUI: Edición> Preferencias> Seguridad (Mejorada)> Vista protegida (Todos los archivos).

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown" /v "iProtectedView"
```

Adobe Reader DC debe habilitar la Seguridad mejorada en un navegador.

Los archivos PDF han evolucionado de páginas estáticas a documentos complejos con características tales como formularios interactivos, contenido multimedia, secuencias de comandos y otras capacidades.

La seguridad mejorada bloquea comportamientos específicos como: inyección de datos, inyección de scripts, impresión silenciosa, enlaces web (si no están permitidos por la configuración de *Trust Manager*), acceso entre dominios y acceso a flujos externos.

El valor de "*bEnhancedSecurityInBrowser*" debe estar establecido en "1" y el tipo configurado como "*REG_DWORD*".

Comprobación:

Ruta GUI: Edición> Preferencias> Seguridad (mejorada)> Seguridad mejorada > Activar seguridad mejorada.

```
REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown" /v "bEnhancedSecurityInBrowser"
```

Adobe Reader DC debe bloquear el acceso a sitios web desconocidos.

Debido a que el acceso a Internet es un riesgo de seguridad potencial, hacer clic en cualquier enlace de sitio web desconocido a Internet representa un riesgo de seguridad potencial. Los sitios web maliciosos pueden transferir contenido dañino o recopilar datos en silencio.

El valor de "*iUnknownURLPerms*" debe estar establecido en "3" y el tipo configurado como "REG_DWORD".

Comprobación:

Ruta GUI: Edición> Preferencias> Administrador de confianza> Acceso a internet desde Archivos PDF fuera del explorador Web> Cambiar configuración> Bloquear el acceso de los archivos PDF a todos los sitios Web.

```
REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cDefaultLaunchURLPerms" /v "iUnknownURLPerms"
```

Adobe Reader DC debe deshabilitar Online SharePoint Access.

Desactiva las características de integración de SharePoint y Office 365.

Controla la capacidad de la aplicación para detectar que un archivo proviene de un servidor de *SharePoint*. Deshabilita la solicitud de extracción y elimina los elementos del menú específicos de SharePoint.

El valor de "*bDisableSharePointFeatures*" debe estar establecido en "1" y el tipo configurado como "*REG_DWORD*".

Comprobación:

```
REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cSharePoint" /v "bDisableSharePointFeatures"
```

Nota: El nombre de la clave "*cSharePoint*" no se crea de forma predeterminada en la instalación de Adobe Reader DC y debe crearse.

Adobe Reader DC debe deshabilitar la capacidad de elevar las confianzas de IE a ubicaciones privilegiadas.

Las ubicaciones privilegiadas permiten al usuario confiar de forma selectiva en los archivos, carpetas y hosts para evitar algunas restricciones de seguridad, como la seguridad mejorada y la vista protegida.

Al deshabilitar la confianza de IE en ubicaciones privilegiadas, se deshabilita y bloquea la capacidad del usuario final para tratar los sitios de confianza de IE como una ubicación privilegiada.

El valor de "*bDisableTrustedSites*" debe estar establecido en "1" y el tipo configurado como "*REG_DWORD*".

Comprobación:

Ruta GUI: Edición> Preferencias> Seguridad (mejorada)> Ubicaciones privilegiadas > Agregar host. Esta opción debe estar en gris desactivada.

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown" /v "bDisableTrustedSites"
```

Adobe Reader DC debe deshabilitar la capacidad de agregar archivos y carpetas de confianza.

Deshabilita carpetas y archivos de confianza y evita que los usuarios especifiquen una ubicación privilegiada para los directorios.

El valor de "*bDisableTrustedFolders*" debe estar establecido en "1" y el tipo configurado como "*REG_DWORD*".

Comprobación:

Ruta GUI: Edición > Preferencias> Seguridad (mejorada)> Ubicaciones privilegiadas > Agregar ruta de carpeta. Esta opción debe estar en gris desactivada.

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown" /v "bDisableTrustedFolders"
```

Adobe Reader DC debe deshabilitar la capacidad de especificar ubicaciones privilegiadas basadas en host.

Deshabilita y bloquea la capacidad de especificar ubicaciones privilegiadas basadas en host.

El valor de "*bDisableOSTrustedSites*" debe estar establecido en "1" y el tipo configurado como "REG_*DWORD*".

Comprobación:

Ruta GUI: Edición > Preferencias> Seguridad (mejorada)> Ubicaciones privilegiadas > Confiar automáticamente en sitios de las zonas de seguridad de mi Win OS. Esta opción debe estar desactivada.

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown" /v "bDisableOSTrustedSites"
```

Adobe Reader DC debe desactivar la capacidad de cambiar el controlador predeterminado.

Deshabilita la capacidad de cambiar el controlador especifico predeterminado (visor PDF).

El valor de "*bDisablePDFHandlerSwitching*" debe estar establecido en "1" y el tipo configurado como "REG_*DWORD*".

Comprobación:

Ruta GUI: Edición > Preferencias> General> Seleccionar como controlador de PDF predeterminado. Esta opción debe estar en gris desactivada.

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown" /v "bDisablePDFHandlerSwitching"
```

Adobe Reader DC debe deshabilitar el complemento de envío y seguimiento de Adobe para *Outlook*.

Cuando está habilitado, aparece un botón de Enviar y seguimiento de Adobe en Outlook al redactar un correo electrónico.

Permite enviar archivos grandes como enlaces públicos a través de *Outlook*.

Los archivos adjuntos se cargan en *Adobe Document Cloud* y los enlaces públicos, a los archivos, se insertan en el cuerpo del correo electrónico.

Los destinatarios pueden hacer clic en el enlace para obtener una vista previa del archivo en una ventana del navegador y pueden descargar el archivo si es necesario.

El valor de "*bAdobeSendPluginToggle*" debe estar establecido en "1" y el tipo configurado como "*REG_DWORD*".

Comprobación:

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown\cServices" /v
"bAdobeSendPluginToggle"
```

Nota: El nombre de la clave "*cCloud*" no se crea de forma predeterminada en la instalación de Adobe Reader DC y debe crearse.

Adobe Reader DC debe deshabilitar Adobe Send for Signature (Adobe Sign).

Desactiva *Adobe Send for Signature* (*Adobe Sign*).

El servicio de firma de *Adobe Document* Cloud permite a los usuarios enviar documentos en línea para firmarlos y firmar desde cualquier lugar o dispositivo.

Los documentos firmados se almacenan en la nube de Adobe.

El servicio de firma *de* Adobe *Document Cloud* funciona bajo suscripción.

Cuando Adobe *Send for Signature* está deshabilitado, los usuarios no podrán utilizar la función de firma de *Adobe Document Cloud*.

El valor de "*bToggleAdobeSign*" debe estar establecido en "1" y el tipo configurado como "REG_DWORD".

Comprobación:

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown\cServices" /v "bToggleAdobeSign"
```

Nota: El nombre de la clave "*cCloud*" no se crea de forma predeterminada en la instalación de Adobe Reader DC y debe crearse.

Adobe Reader DC debe deshabilitar la instalación de reparación de Adobe.

Cuando la Instalación de reparación está deshabilitada, el usuario no tiene la opción (Menú de Ayuda) o funcional para reparar una instalación de Adobe Reader DC.

El valor de "*DisableMaintenance*" debe estar establecido en "1" y el tipo configurado como "*REG_DWORD*".

Comprobación:

Ruta GUI: Ayuda> Reparar instalación de. Esta opción debe estar en gris desactivada.

Para 32 bits:

```
REG QUERY "HKEY_LOCAL_MACHINE\Software\Adobe\Acrobat
Reader\DC\Installer" /v "DisableMaintenance"
```

Para 64 bits:

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Wow6432Node\Adobe\Acrobat
Reader\DC\Installer" /v "DisableMaintenance"
```

Adobe Reader DC debe deshabilitar la carga periódica de certificados de Adobe.

Especifica si los certificados de confianza se pueden descargar periódicamente de Adobe.

El valor de "*bLoadSettingsFromURL*" debe estar establecido en "0" y el tipo configurado como "REG_DWORD".

Comprobación:

Ruta GUI: Edición> Preferencias> Administrador de confianza> Actualizaciones automáticas de Adobe *Approved Trust List* (*AATL*)> Cargar los certificados de confianza de un servidor de AATL de Adobe. La casilla no debe estar marcada.

```
REG QUERY "HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\Security\cDigSig\cAdobeDownload" /v "bLoadSettingsFromURL"
```

Nota: Los nombres de clave "*cDigSig*" y "*cAdobeDownload*" no se crean de forma predeterminada en la instalación de Adobe Reader DC y deben crearse.

Adobe Reader DC debe deshabilitar la carga periódica de certificados europeos.

Especifica si los certificados de confianza se pueden descargar periódicamente de Adobe.

El valor de "*bLoadSettingsFromURL*" debe estar establecido en "0" y el tipo configurado como "REG_DWORD".

Comprobación:

Ruta GUI: Edición > Preferencias> Administrador de confianza> Actualizaciones automáticas de *European* Lists (EUTL)> Cargar los certificados de confianza de un servidor de EUTL de Adobe. La casilla no debe estar marcada.

```
REG QUERY "HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\Security\cDigSig\cEUTLDownload" /v "bLoadSettingsFromURL"
```

Nota: Los nombres de clave "*cDigSig*" y "*cEUTLDownload*" no se crean de forma predeterminada en la instalación de Adobe Reader DC y deben crearse.

Adobe Reader DC debe desactivar Acrobat Upsell.

Para los productos DC, deshabilita los mensajes que animan al usuario a actualizar el producto. Por ejemplo, los usuarios de Reader pueden comprar herramientas y funciones adicionales.

El valor de "*bLoadSettingsFromURL*" debe estar establecido en "1" y el tipo configurado como "REG_*DWORD*".

Comprobación:

```
REG QUERY
"HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown" /v "bAcroSuppressUpsell"
```

Adobe Reader DC debe desactivar la pantalla de bienvenida de Adobe.

Desactiva la pantalla de bienvenida al iniciar la aplicación.

El valor de "*bShowWelcomeScreen*" debe estar establecido en "0" y el tipo configurado como "*REG_DWORD*".

Comprobación:

Ruta GUI: Edición > Preferencias> General> Inicio de la aplicación> Mostrar pantalla de bienvenida. La casilla no debe estar marcada.

```
REG QUERY
"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown\cWelcomeScreen" /v
"bShowWelcomeScreen"
```

Nota: El nombre de la clave "`cWelcomeScreen`" no se crea de forma predeterminada en la instalación de Adobe Reader DC y debe crearse.

Adobe Reader DC debe deshabilitar tanto las actualizaciones de los componentes del complemento web del producto como todos los servicios.

De forma predeterminada, los servicios en línea de Adobe están perfectamente integrados en Adobe Reader DC.

Al desactivar las actualizaciones de servicio, se desactivan las actualizaciones de los componentes del complemento web del producto y todos los servicios sin excepción, incluida cualquier pantalla de inicio de sesión en línea.

El valor de "*bUpdater*" debe estar establecido en "0" y el tipo configurado como "*REG_DWORD*".

Comprobación:

```
REG QUERY
"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown\cServices" /v "bUpdater"
```

Nota: El nombre de la clave "`cServices`" no se crea de forma predeterminada en la instalación de Adobe Reader DC y debe crearse.

Adobe Reader DC debe desactivar las actualizaciones del producto.

Deshabilita las actualizaciones del producto.

El valor de "*bUpdater*" debe estar establecido en "0" y el tipo configurado como "*REG_DWORD*".

Comprobación:

```
REG QUERY
"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat
Reader\DC\FeatureLockDown" /v "bUpdater"
```

Valores de registro adicionales.

- **Opciones del reproductor**
  Apple ya no proporciona actualizaciones de seguridad para QuickTime heredado para software de Windows, por lo que este software es vulnerable a la explotación. Por lo tanto, para proteger Reader, Adobe también ha eliminado la compatibilidad con QuickTime en Windows. Reader DC ahora usa el reproductor de vídeo integrado de Windows para reproducir vídeos heredados de QuickTime, que son los vídeos insertados en los documentos PDF creados con Acrobat 9 y versiones anteriores. Si esta opción no está seleccionada y QuickTime Player no está disponible, Windows utiliza su reproductor integrado.

  Ruta GUI: Edición> Preferencias> Multimedia (heredado)> en "Opciones del reproductor" verificar que en "No utilizar QuickTime Player para elementos multimedia" la casilla está marcada.

- **JavaScript**
  Permite ajustar el comportamiento de la aplicación de manera que JavaScript se ejecute en el nivel de seguridad deseado. Esto permite limitar el acceso de la aplicación a las API JavaScript y aísla los flujos de trabajo que no requieren API JavaScript.

  Desactive esta opción para deshabilitar JavaScript completamente o restringir JavaScript mediante API.

  Ruta GUI: Edición> Preferencias> JavaScript> en "JavaScript" verificar que en "Activar Javascript para Acrobat" la casilla está desmarcada.

- **Documentos en la lista de archivos recientes**
  La lista de archivos recientes proporciona accesos directos a tus archivos abiertos recientemente. Esto es una falta de privacidad si compartes el dispositivo con alguien.

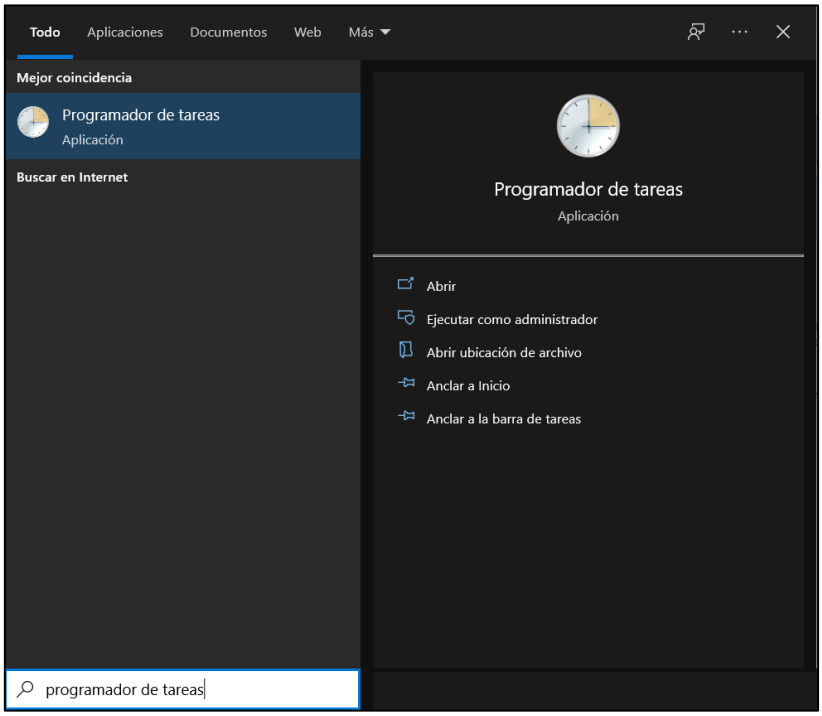
  Si reducimos a cero esta opción, se deshabilita la lista recientes.

Ruta GUI: Edición> Preferencias> Documentos> en “Configuración de apertura” verificar que “Documentos en la lista de archivos recientes:” esta en cero (0).

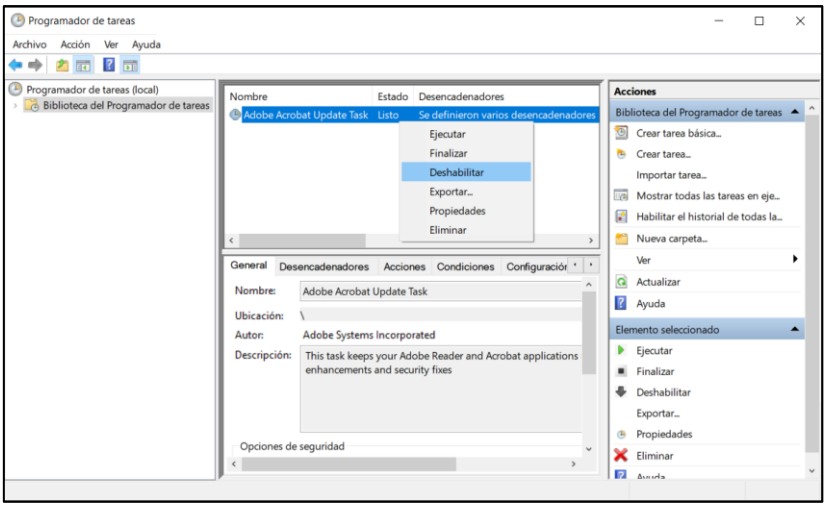
4.8. DESHABILITAR LA TAREA DE ACTUALIZACIÓN DE ADOBE ACROBAT

El primer paso para deshabilitar la actualización automática en Adobe Reader es deshabilitar la 'Tarea de actualización de Adobe Acrobat' en el Programador de tareas. Para ello:

- En el cuadro de búsqueda, escriba: programador de tareas
- Abrir el Programador de tareas y Ejecutar como administrador



- Haga clic en Biblioteca de programación de tareas a la izquierda y, a continuación, en el panel derecho, haga clic con el botón derecho en la tarea de actualización de Adobe Acrobat y seleccionar Deshabilitar.



4.9. DESHABILITAR SERVICIO "*ADOBEARMSERVICE*"

A continuación, se describe paso a paso cómo realizar la configuración del servicio "*AdobeARMservice*" en un equipo Windows independiente.

En este ejemplo, se parte de la suposición de que, en el equipo, en el que se va a deshabilitar dicha funcionalidad, se ha instalado el sistema operativo Windows y el programa Adobe Reader DC.

Nota: Para los equipos clientes unidos a dominio se recomienda deshabilitar el servicio "*AdobeARMservice*" mediante directivas de grupo establecidas en el dominio.

	Descripción
1.	Inicie sesión con un usuario que tenga privilegios de administrador y que sea miembro del grupo "Usuarios de *shell*" en la máquina donde se desea desactivar "*AdobeARMservice*".
2.	Copie los ficheros y carpetas que acompañan a esta guía al directorio "C:\Scripts" del equipo.
3.	Asegúrese de que al menos los siguientes ficheros hayan sido copiados al directorio "C:\Scripts\Scripts_local": – AdobeARMservice.bat – AdobeARMservice.inf
4.	A continuación, vaya a la carpeta "C:\Scripts\Scripts_local" y ejecute como administrador (Opción Ejecutar como administrador) el fichero "*AdobeARMservice.bat*".
5.	Deberá volver a introducir las credenciales de usuario con privilegios de administrador.
6.	En la ventana emergente pulse una tecla para comenzar la ejecución del script. Cuando finalice la ejecución pulse de nuevo una tecla para cerrar la ventana.
7.	El servicio "*AdobeARMservice*" se ha desactivado correctamente.

5. LISTA DE COMPROBACIÓN (*ASSESSMENT*)

Criticidad	Verificación
Alta	Adobe Reader DC debe tener instaladas las últimas actualizaciones de software relacionadas con la seguridad.
Media	Adobe Reader DC debe deshabilitar el servicio de actualizaciones "*AdobeARMservice*"
Media	Adobe Reader DC debe evitar la apertura de archivos que no sean PDF o FDF.
Media	Adobe Reader DC debe bloquear el contenido de Flash.
Media	Adobe Reader DC debe deshabilitar todo acceso de servicio a *Document Cloud* Services.
Media	Adobe Reader DC debe habilitar la Seguridad mejorada en una aplicación independiente.
Media	Adobe Reader DC debe desactivar los conectores web de terceros.
Media	Adobe Reader DC debe desactivar la sincronización de nube.
Media	Adobe Reader DC debe habilitar el modo FIPS.
Media	Adobe Reader DC debe deshabilitar el acceso a *webmail*.
Media	Adobe Reader DC debe deshabilitar la capacidad de elevar (fideicomiso) documentos certificados como una ubicación privilegiada.
Media	Adobe Reader DC debe bloquear los sitios web.
Media	Adobe Reader DC debe habilitar la Vista protegida.
Media	Adobe Reader DC debe habilitar el modo protegido.
Media	Adobe Reader DC debe habilitar la Seguridad mejorada en un navegador.
Media	Adobe Reader DC debe bloquear el acceso a sitios web desconocidos.
Media	Adobe Reader DC debe deshabilitar *Online SharePoint Access.*
Media	Adobe Reader DC debe deshabilitar la capacidad de elevar las confianzas de IE a ubicaciones privilegiadas.
Media	Adobe Reader DC debe deshabilitar la capacidad de agregar archivos y carpetas de confianza.
Media	Adobe Reader DC debe deshabilitar la capacidad de especificar ubicaciones privilegiadas basadas en host.
Baja	Adobe Reader DC debe desactivar la capacidad de cambiar el controlador predeterminado.
Baja	Adobe Reader DC debe deshabilitar el complemento de envío y seguimiento de Adobe para Outlook.
Baja	Adobe Reader DC debe deshabilitar *Adobe Send for Signature.*

Criticidad	Verificación
Baja	Adobe Reader DC debe deshabilitar la instalación de reparación de Adobe.
Baja	Adobe Reader DC debe deshabilitar la carga periódica de certificados de Adobe.
Baja	Adobe Reader DC debe deshabilitar la carga periódica de certificados europeos.
Baja	Adobe Reader DC debe desactivar Acrobat *Upsell*.
Baja	Adobe Reader DC debe desactivar la pantalla de bienvenida de Adobe.
Baja	Adobe Reader DC debe desactivar las actualizaciones de servicio.

6. DECÁLOGO DE RECOMENDACIONES

	Decálogo de seguridad para Acrobat Reader DC
1	**Utilizar siempre la versión más actualizada de Adobe.**
2	**Se aconseja revisar cualquier función relativa a la seguridad del software, puesto que proporciona una mayor defensa contra los ataques.**
3	**Se recomienda bloquear la interfaz de usuario para que el usuario final no pueda modificar los ajustes.**
4	**Se recomienda realizar una limpieza de metadatos cuando los archivos pdf sean de acceso público.**
5	**Se recomienda utilizar Adobe Reader DC tan solo para la apertura de archivos que sean PDF o FDF.**
6	**Se recomienda utilizar un certificado digital para firmar documentos PDF y así garantizar la autoría ante posibles manipulaciones o modificaciones por parte de terceras personas.**
7	**Se recomienda no utilizar *plugins* de terceros.**
8	**Se recomienda bloquear vínculos a internet en archivos PDF.**
9	**Se recomienda habilitar el modo y la vista protegida.**
10	**Se recomienda bloquear cualquier tipo de conexión a Internet desde archivos PDF.**

ANEXO: SCRIPTS DE CONFIGURACIONES SEGURAS

Para facilitar la aplicación del refuerzo de seguridad sobre Acrobat Reader DC, se incluyen al presente documento una carpeta de scripts la cual contiene los ficheros necesarios para el bastionado del programa.

El propósito de los scripts es la ejecución de estos de manera automática, mitigando en la medida de lo posible fallos ocasionados a la hora de bastionar un sistema o programa específico.

A continuación, se detalla los ficheros o carpetas incluidos en la carpeta "**Scripts**".

- GP Report
  - Adobe Reader DC Continuo - equipo.htm
  - Adobe Reader DC Continuo - usuario.htm
- GPOs
  - {5FDCB222-F465-4C7C-864B-E5EE4E8BFA09}
  - {CD465C95-EA48-4901-A8F1-41A65B64ECFA}
- PolicyDefinitions
  - es-ES
    - AcrobatReaderDC.adml
  - AcrobatReaderDC.admx
- Scripts_local
  - Tools
    - LGPO.exe
  - Import ADMX - Install GPO.bat
  - Import ADMX - Install GPO.ps1
  - AdobeARMservice.bat
  - AdobeARMservice.ps1