

ACERODOCS v1.8

Manual de Usuario



acerodocs



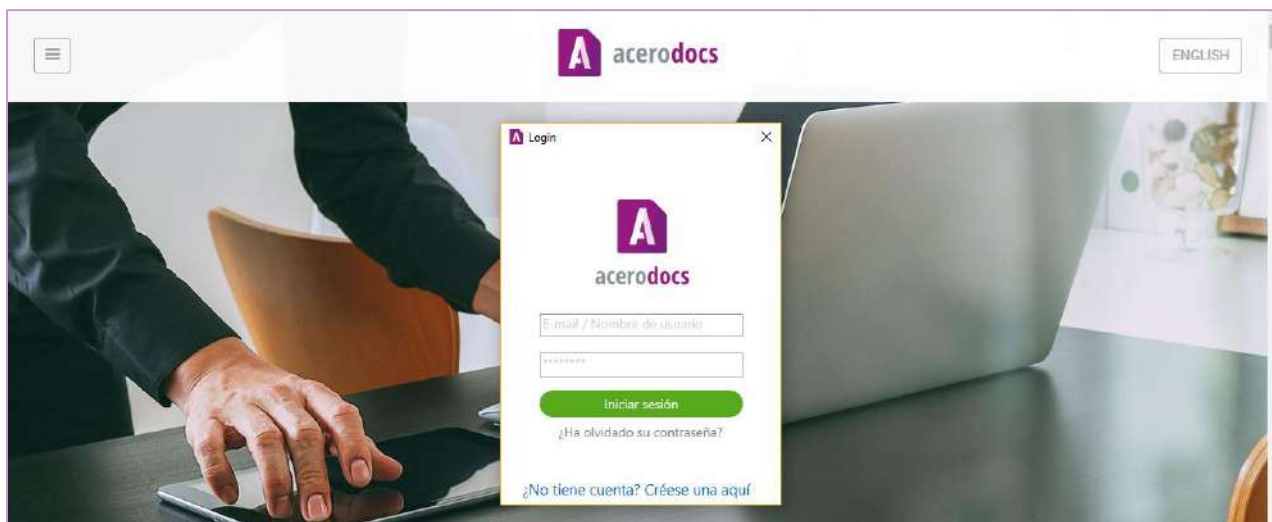
Manual de Uso AceroDocs v1.8

Acerca de este manual

Este manual de usuario está diseñado específicamente para describir en detalle las funciones de la aplicación

Contenido

1. Proteger un documento
2. Panel de control AceroDocs
3. IRM abierto
4. IRM selectivo
5. Proteger carpetas
6. Drag&Drop
7. Vigilancia Dropbox y USB
8. Traductor
9. Papelera
10. Trazabilidad
11. Menú contextual
12. Grupos y jerarquías



¿Qué es AceroDocs?

AceroDocs es una aplicación que le permite proteger sus archivos mediante cifrado (encriptado) y acceder a ellos de forma sencilla desde cualquier ubicación y dispositivo, pero sin que otros tengan acceso. Podrá guardar sus documentos sensibles en la nube (Dropbox, Google Drive, etc.) o en un pendrive de forma segura. Esto es el cifrado tradicional, utilizado para securizar el archive en reposo y en tránsito.

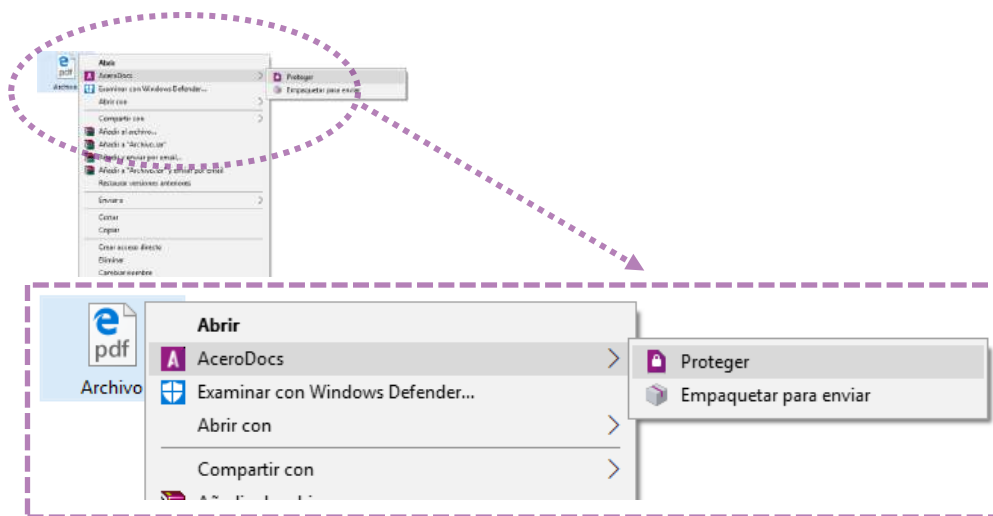
Para los documentos con formato PDF, el cifrado AceroDocs incluye además la funcionalidad de “protección remota” o IRM (Information Rights Management). Podrá enviarlo protegido a uno o varios destinatarios, que lo podrán visualizar (mediante un visor) pero no podrán extraer el archivo original. Cuando ud. lo decida podrá eliminar el acceso y todo el que haya recibido el documento ya no lo podrá visualizar. Esta funcionalidad innovadora permite proteger el documento también en destino: allá donde viaje el documento, este se mantiene encriptado, incluso cuando un receptor lo esté visualizando; esta protección, se mantiene para todas las copias que se hayan hecho del archivo.



1. Proteger un Documento

La forma habitual de proteger un documento es mediante la aplicación AceroDocs instalada en Windows.

1. Antes de nada, asegúrate de haber instalado AceroDocs para escritorio en tu ordenador.
2. Para proteger un archivo solo tienes que hacer clic derecho sobre él, después seleccionar “AceroDocs -> Proteger”.



¡Y listo!

Ya tienes tu archivo protegido por **AceroDocs**



Dependiendo del formato del archivo original, aparecerá el archivo encriptado con uno de estos dos iconos:



Naranja: Archivo con extensión **.acero** →
Protegido con cifrado tradicional

Al hacer **dobles clic** sobre este archivo **extraemos el original**.



Morado: Archivo con extensión **.acerov**

Cifrado con funcionalidad avanzada de **protección remota** que incluye un visor **IRM** para proteger el archivo también en destino.

Aparecerá al cifrar archivos con formato **.PDF**, **.TXT** e imágenes

*Al hacer doble clic sobre este archivo vemos el contenido del archivo original en el visor nativo de **AceroDocs***



Visor nativo AceroDocs

Cifrado en reposo y en tránsito

Con ambos tipos de cifrado podrás guardar tus documentos sensibles en nubes públicas (p.e. Dropbox o Google Drive) o en dispositivos externos (p.e. pendrive USB) con total seguridad. Si lo deseas puedes permitir el acceso a otras personas, identificándolas por su correo electrónico; para acceder al archivo no necesitan tener instalada la aplicación, ni tampoco tener una cuenta en AcerDocs.

Cifrado en destino

Los archivos de color morado tienen la protección adicional del visor IRM, lo que significa que se pueden modificar de forma remota los permisos o incluso eliminar el acceso al documento y sus copias al cabo de un tiempo después incluso de haberlo enviado.

Para acceder a los archivos naranja **.acero** o los morados **.acerov**, el receptor no tener instalada la aplicación, ni tampoco tener una cuenta en AcerDocs, a no ser que el autor del documento lo fuerce.

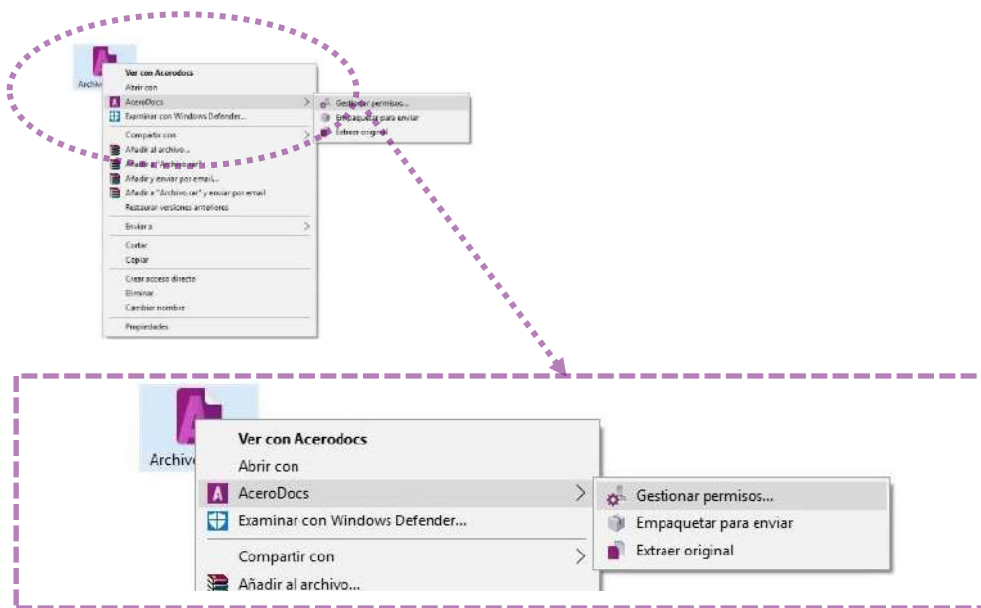
NOTA: un usuario de AceroDocs puede cifrar un archivo con la plataforma web sin necesidad de tener la aplicación instalada, como se verá más adelante.



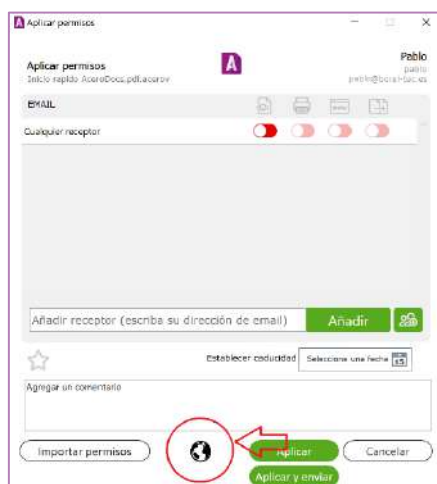
2. Panel de control (dashboard) de AceroDocs

Se pueden gestionar los permisos directamente en Windows clicando sobre un archivo, o buscándolo en la lista de archivos en el dashboard web.

1. Una vez hayas cifrado un archivo con soporte de protección remota, haz clic derecho sobre el icono morado del archivo cifrado generado y selecciona “AceroDocs -> Gestionar permisos”.



2. Aparecerá una ventana nativa de gestión de permisos sobre ese archivo en particular. Clicando sobre el icono del globo del mundo aparece el dashboard web con ese archivo desplegado dentro de la lista de todos los archivos gestionados.





3. IRM Abierto:

Enviar un archivo “.acerov” con protección remota

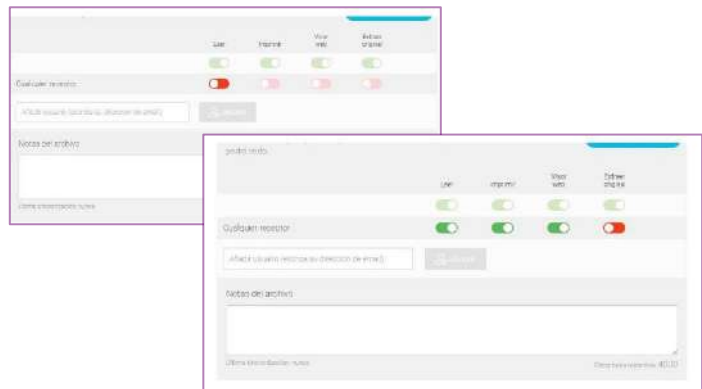
Quien lo reciba podrá tener acceso a tu documento incluso si no tiene cuenta AceroDocs

Para los documentos con soporte de visor IRM (PDF, TXT e imágenes), el cifrado AceroDocs incluye la funcionalidad de “protección remota” o IRM (Information Rights Management). De esta forma podrás enviarlo protegido a uno o varios destinatarios que lo podrán visualizar (mediante un visor) pero no podrán extraer el archivo original. Cuando tú lo decidas podrás eliminar el acceso y todo el que haya recibido el documento ya no lo podrá visualizar.

Los tipos de archivo con soporte de visor IRM son PDF, TXT e imágenes. Los archivos ofimáticos como MS Office se pueden convertir directamente a PDF al cifrarlos para darles soporte IRM, con la posibilidad de incrustar el archivo editable original dentro del archivo cifrado.

La modalidad IRM abierto no requiere autenticación por parte del receptor.

1. En el Panel de Control, selecciona “Cualquier receptor” bajo el nombre del archivo. Al hacer clic sobre el botón, cambiará de color rojo a verde.

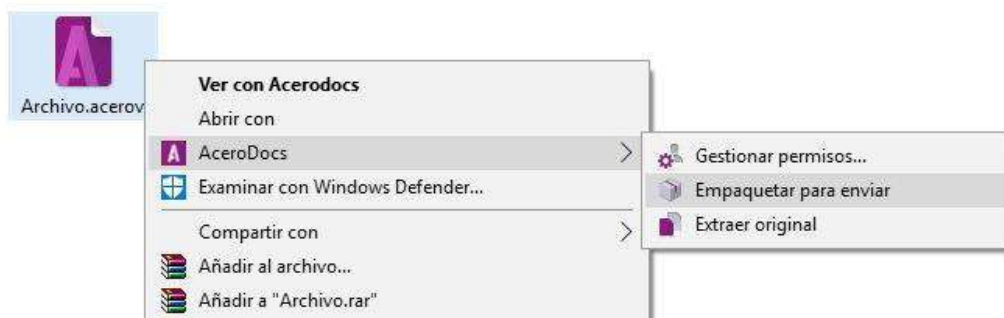


Si ahora envías el documento protegido .acerov a otra persona, lo podrá abrir con la aplicación o mediante nuestro visor web en www.acerodocs.com/go.



Tu receptor también puede abrirlo simplemente haciendo doble clic. ¡Incluso aunque él no tenga instalado AceroDocs

Solo tienes que hacer clic derecho sobre el archivo protegido .aceroV y seleccionar “AceroDocs -> Empaquetar para enviar”.

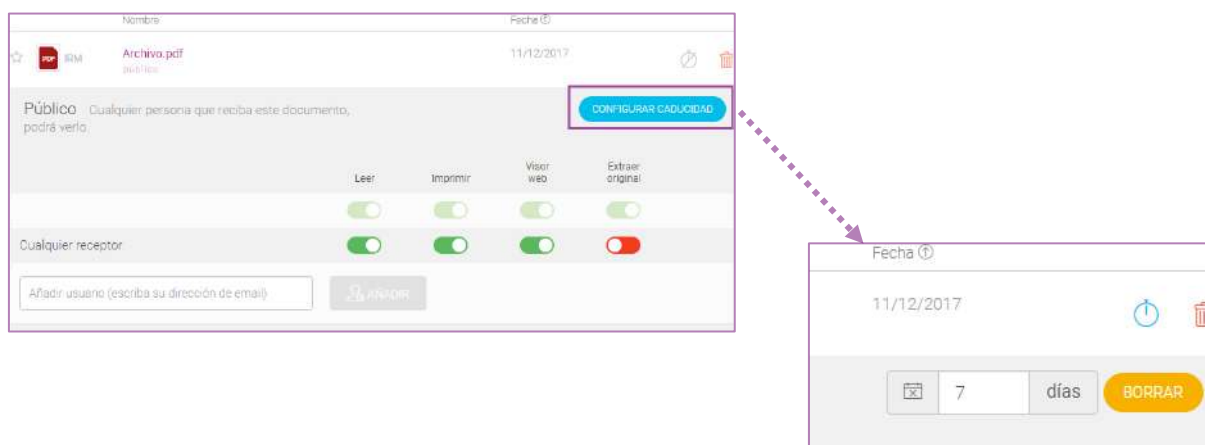


Se creará un archivo html (o .zip si son varios archivos) con el documento cifrado en su contenido. Este archivo podrás enviarlo de la forma que quieras (por e-mail, con un pendrive USB, etc.)

Este archivo detectará si tu receptor tiene la aplicación instalada, en cuyo caso se le abrirá con el visor nativo. En caso contrario, se le abrirá automáticamente con un visor web.

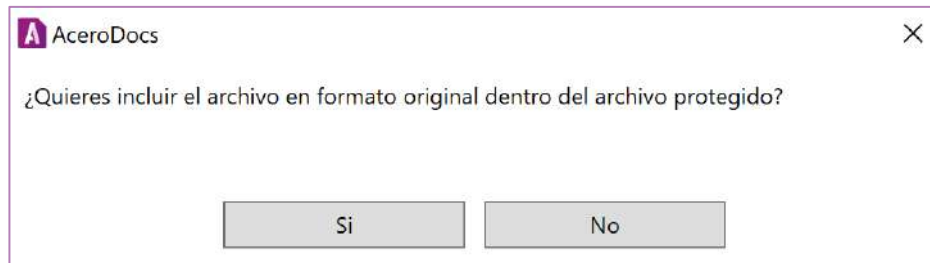
Tus receptores lo podrán visualizar siempre y cuando mantengas el permiso activado. Cuando lo desactives desde el Panel de Control se perderá el acceso al documento, así como a todas sus copias. Si lo prefieres, también puedes poner un tiempo de caducidad al archivo antes de enviarlo.

¿Cómo? Solo tienes que hacer clic en Configurar caducidad y podrás otorgar a los receptores el tiempo que quieras para que accedan al archivo.

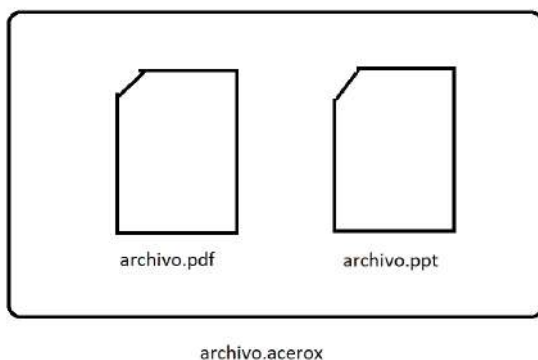


Los formatos de archivos ofimáticos que no tengan soporte a IRM se pueden pasar a PDF al cifrarlos con la opción clic derecho --> AceroDocs --> pasar a PDF y proteger.

Aparecerá el siguiente mensaje:



Si se elige "Sí" se creará un fichero protegido con extensión .acerox con soporte de visor IRM que incluirá archivo original así como el archivo convertido a PDF. De esta forma un receptor con permiso solo de visualización verá el PDF en el visor, pero el que tenga permiso de extracción extraerá el editable original.





4. IRM Selectivo

Antes de enviar un documento, podrás seleccionar de antemano quién podrá visualizarlo.

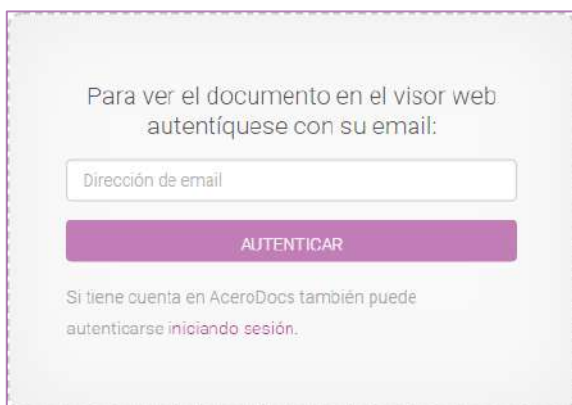
Si alguien que no está en la lista lo recibe, no podrá abrirlo.

Gracias al IRM selectivo, podrás gestionar de manera individual los permisos de los archivos.

El receptor podrá acceder al archivo mediante un visor tras autenticarse con su email. Sin embargo, si ya tiene AceroDocs solo tiene que iniciar sesión.

Permisos:

- Leer: la persona podrá visualizarlo con un visor.
- Imprimir: la persona podrá imprimir el archivo en papel con una impresora física. No podrá imprimir en PDF con una impresora virtual.
- Visor web: el receptor del archivo, al soltarlo a través del Drag&Drop o www.acerodocs.com/go, se le solicita autenticar su email. Se le enviará un enlace de confirmación y tras confirmarlo, se le autoriza poder visualizarlo en el visor web.



www.acerodocs.com/go



[Drag&Drop](#)

- Extraer original: permite al receptor extraer el documento original ya sea un receptor fiable, sea que solo deseemos encriptar el documento en tránsito o si el documento se encuentra en un repositorio en la nube.

Panel de control selectivo:



El icono morado situado a la derecha del correo indica que el receptor al que le has dado permisos es usuario AceroDocs.

NOTA: El receptor no necesita tener una cuenta en AceroDocs para abrir un documento, basta con que demuestre que tiene acceso a su email. Esto es válido para el visor nativo y para el visor web.

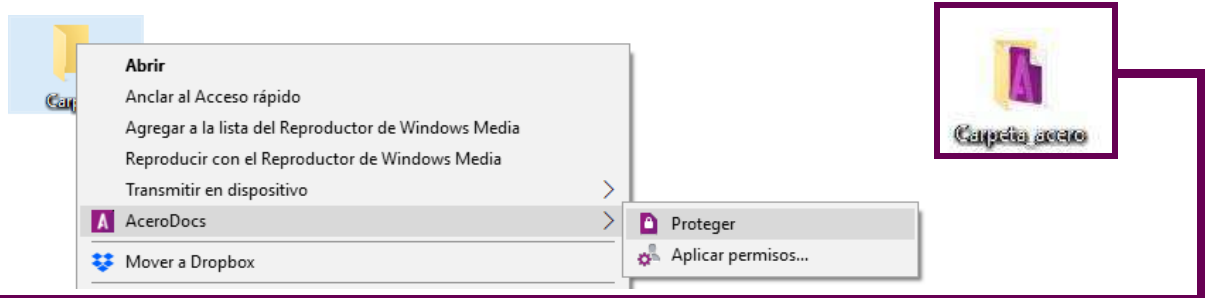


5. Proteger carpetas

Protege los archivos dentro de carpetas y subcarpetas para uso privado, y en caso de que quieras compartirlos permite aplicarles permisos de acceso.

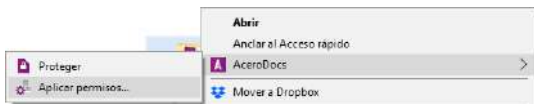
¿Cómo se protegen las carpetas?

Haz clic derecho en la carpeta que desees proteger y selecciona AceroDocs > Proteger.



Después, elige la ubicación de tu carpeta protegida con el mismo nombre seguido de `_acero`.

¿Cómo se aplican los permisos en masa?

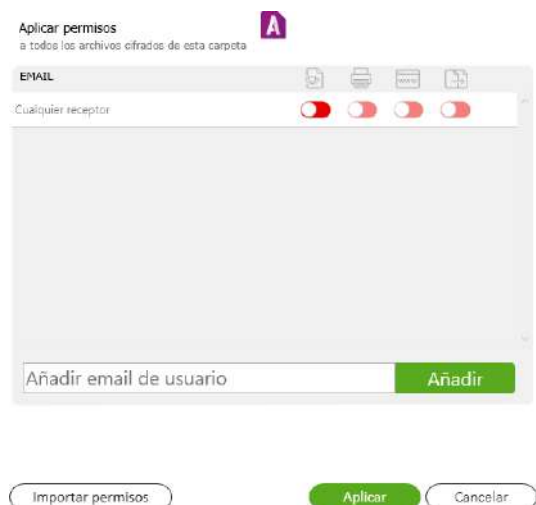


Haz clic derecho en la carpeta protegida y selecciona AceroDocs > Aplicar permisos

Aplicaremos en masa los permisos a los archivos que se encuentran en la carpeta, independientemente de los que tuviera antes. Ahora podrás añadir tantos usuarios como quieras y gestionar individualmente sus permisos.

Ojo: si importamos permisos de un fichero AceroDocs, se sobre-escriben los permisos con los de ese fichero en lugar de los que hayamos configurado.

Puedes aplicar permisos en serie importando los permisos directamente de un archivo `.acero` concreto.



NOTA: Si dentro de la carpeta hay archivos que no estén protegidos y archivos que sí, los permisos solo se aplicarán a los archivos protegidos.

NOTA: Si dentro de la carpeta a cifrar hay archivos .acero, (sin visor IRM) aparecerá el siguiente mensaje:

 Los archivos .acero (sin visor IRM) tendrán permiso de extracción si tienen permiso de lectura. [Modificar](#)

Esto significa que el receptor autorizado a ver podrá extraer los ficheros naranjas .acero. Se puede modificar este comportamiento para que se les aplique directamente el permiso de "Extraer original", para ello hay que clicar en "Modificar". La desventaja de hacer esto es que el receptor autorizado a visualizar el resto de archivos (.acero) no podrán siquiera visualizar los .acero.

Los archivos .acero (sin visor IRM):

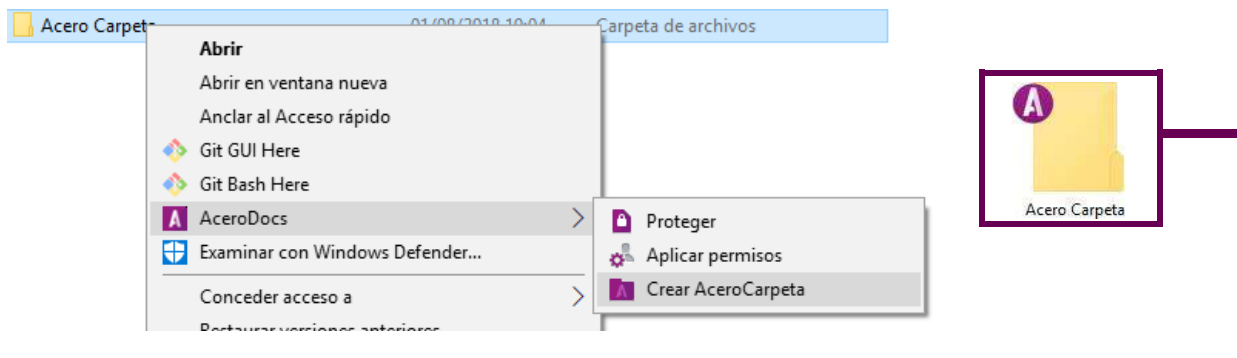
- Se les aplicará el permiso de "Extraer original"
- Tendrán permiso de extracción si tienen permiso de lectura.

AceroCarpetas

Las AceroCarpeta son carpetas de cifrado automático. Cualquier archivo que se guarde dentro será cifrado con los permisos asociados de la carpeta (si es el caso).

¿Cómo puedo proteger todos los archivos que muevo a una carpeta?

Haz clic derecho en la carpeta que desees convertir en AceroCarpeta y selecciona AceroDocs > Crear AceroCarpeta.

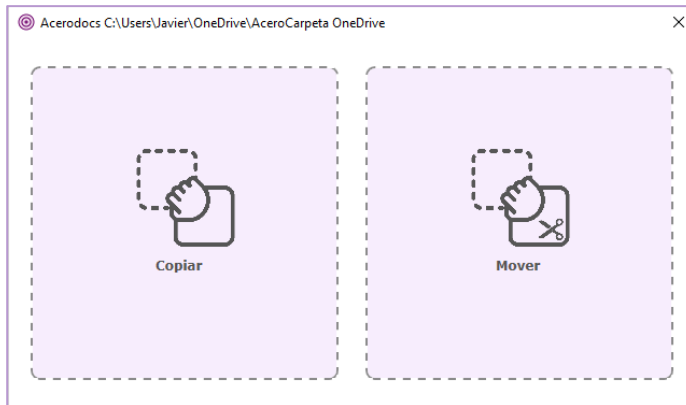


Al hacer esto, se creará la AceroCarpeta, una carpeta que se encarga de proteger todos los archivos que arrastres dentro. Si lo haces sobre una carpeta que tiene archivos, se protegerán todos los que contenga.

¿Y si se trata de una carpeta de un servicio en la nube (Google Drive, Dropbox, etc)?

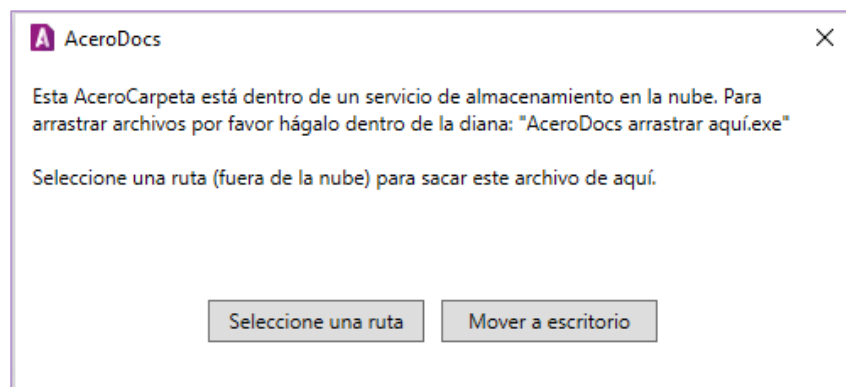
Tras crear una AceroCarpeta, dentro veremos:  AceroDocs arrastre aquí

Al arrastrar un archivo o hacer doble clic sobre la diana, se nos abrirá un menú donde debemos subir nuestros archivos para proteger antes de que se suba una copia en la nube.



Copia el fichero sobre la ventana o arrastra el fichero sobre la ventana. Entonces, se protegerá en la carpeta en la nube y se subirá el fichero protegido.

NOTA: También puedes arrastras el archivo directamente sobre el icono de la diana para protegerlo.



Ojo: Para evitar que los archivos suban a la nube en claro, si arrastras el fichero sin usar la diana AceroDocs no te dejará, apareciendo un mensaje para sacar el archivo. De esta forma aseguramos que los archivos suban siempre encriptados a la nube.

i Antes de mover una AceroCarpeta debes deshabilitarla.

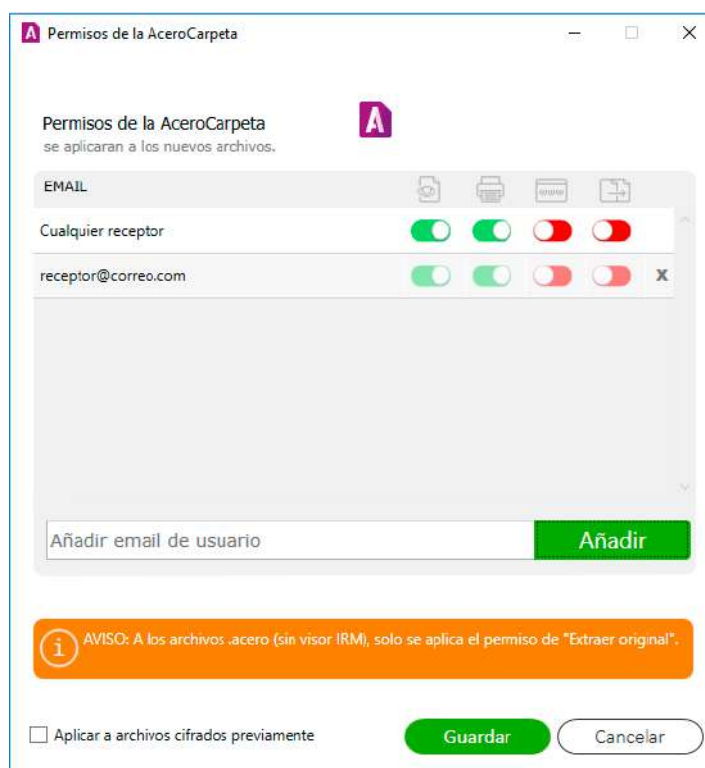
Haz clic derecho en la AceroCarpeta y selecciona AceroDocs > Deshabilitar AceroCarpeta.



¿Cómo puedo gestionar los permisos de los ficheros de mi AceroCarpeta?

Haz clic derecho en la AceroCarpeta y selecciona AceroDocs > Gestionar permisos.

Verás entonces el siguiente panel de permisos.



Cualquier archivo que coloquemos dentro de nuestra AceroCarpeta, herederá los permisos definidos en este panel, donde definimos los usuarios que pueden acceder y gestionar individualmente sus permisos.

Si marcamos el check Aplicar a archivos cifrados previamente, los archivos que ya existen en la carpeta tendrán los nuevos permisos así como el control de usuarios.

Aplicar a archivos cifrados previamente

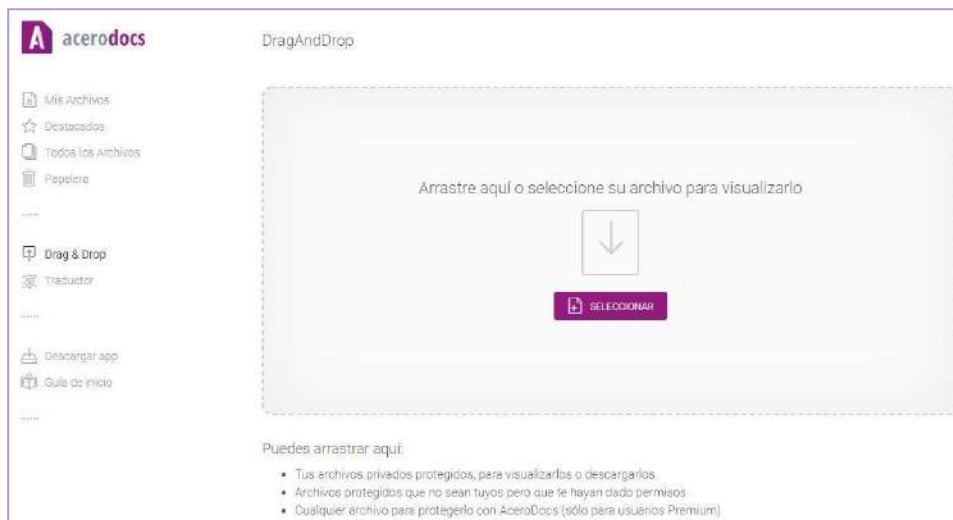


6. Drag&Drop

Los usuarios pueden visualizar y descifrar los archivos en el panel de control. Además, la versión Premium de AceroDocs también les otorga la posibilidad de proteger los archivos en Drag&Drop

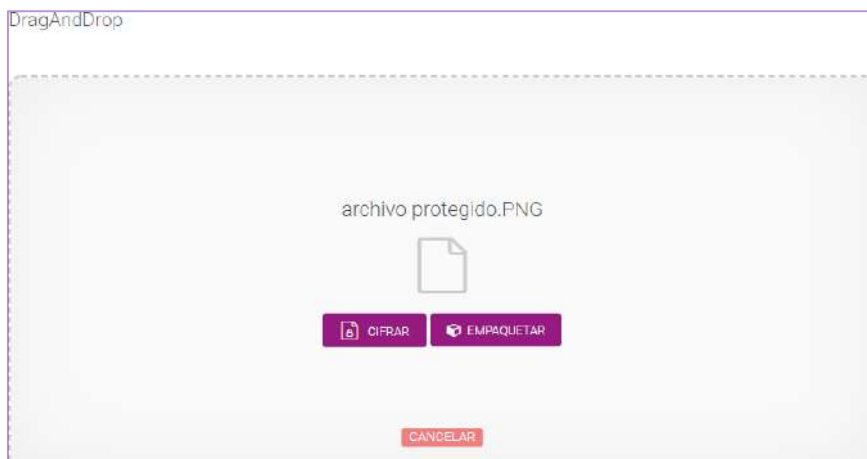
Drag&Drop en el panel de control:

Permite visualizar y descifrar tus archivos privados y los ajenos que te hayan dado permiso arrastrándolos a la zona marcada o seleccionándolos al hacer clic en Seleccionar.



Cifrar archivos y empaquetar archivos en el panel de control:

Si deseas cifrar un archivo sin instalar la aplicación, tan solo tienes que arrastrar el mismo sobre la zona marcada o seleccionándolo al hacer clic en Seleccionar. Entonces tendrás que seleccionar si cifrar o empaquetar.



Una vez seleccionado la opción deseada, puedes gestionar los permisos del mismo.



Drag&Drop en la web funcional:

En la web funcional de AceroDocs, la opción Drag&Drop permite sólo descifrar. Tan solo arrastra el archivo protegido al cuadrado indicado y así podrás visualizarlo.



www.acerodocs.com



www.acerodocs.com/go/



7. Vigilancia Dropbox y USB

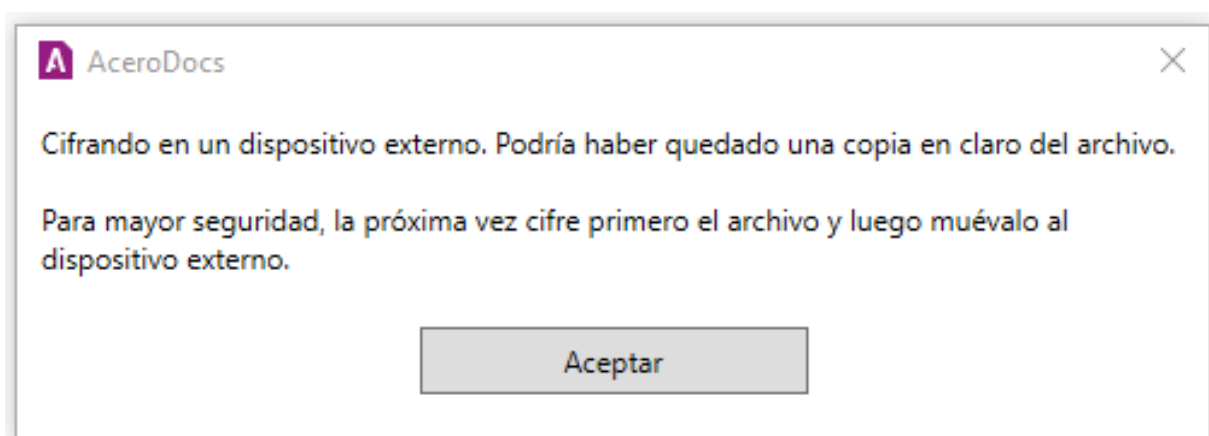
El archivo debe ser cifrado antes de moverlo a un dispositivo externo (pendrive, disco externo, etc.) o a una carpeta sincronizada con nubes públicas (Dropbox, Google Drive, etc) para garantizar su seguridad.

Cuando borramos un archivo de un USB, éste deja de estar ante nuestros ojos. Sin embargo, los datos siguen ahí, sólo que el espacio en donde estaba almacenado queda marcado como libre y a medida que más lo uses, y más archivos e información guardes, será mucho más difícil recuperar lo eliminado; pero no imposible.

AceroDocs recomienda siempre proteger el archivo en una carpeta local antes de moverlo a un USB.

En el caso de plataformas de sincronización en la nube como Google Drive o Dropbox el problema es más grave, porque tras subir el archivo, queda una copia en claro en la nube, independientemente de que el fichero en claro se elimine y dejemos solo el cifrado.

Al proteger un archivo con AceroDocs en cualquiera de los supuestos mencionados (un archivo en un dispositivo externo o dentro de una plataforma en la nube), AceroDocs lo detectará y aparecerá un mensaje de este estilo:



Antes de proceder a cifrar el archivo, el mensaje te recordará que la acción no es totalmente segura.



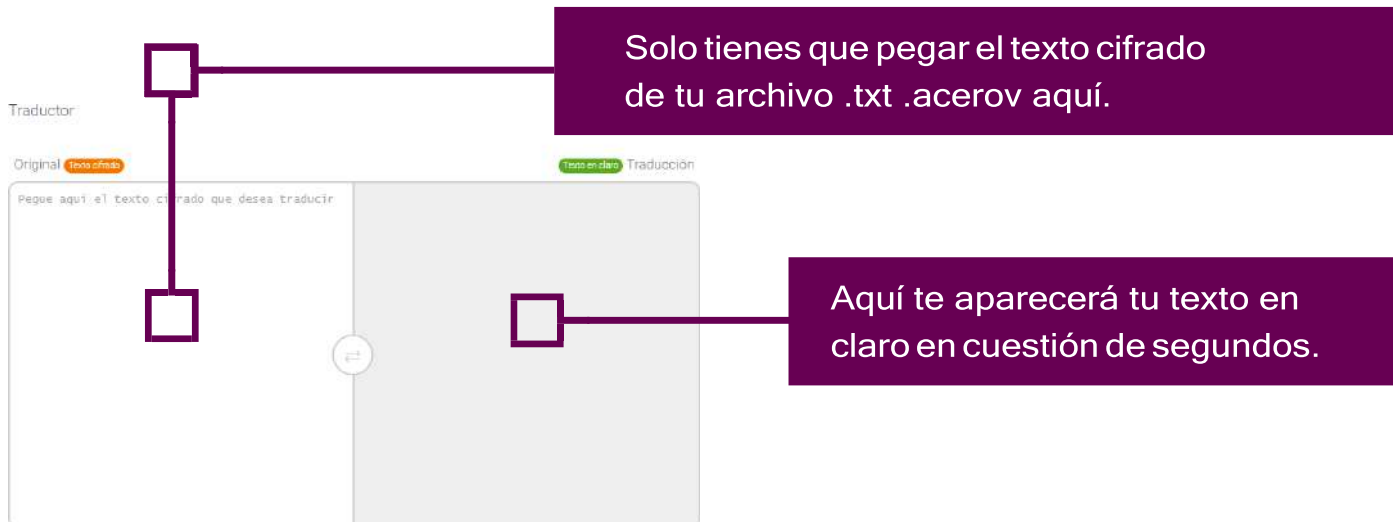
8. Traductor

AceroDocs también aporta la función de traductor.

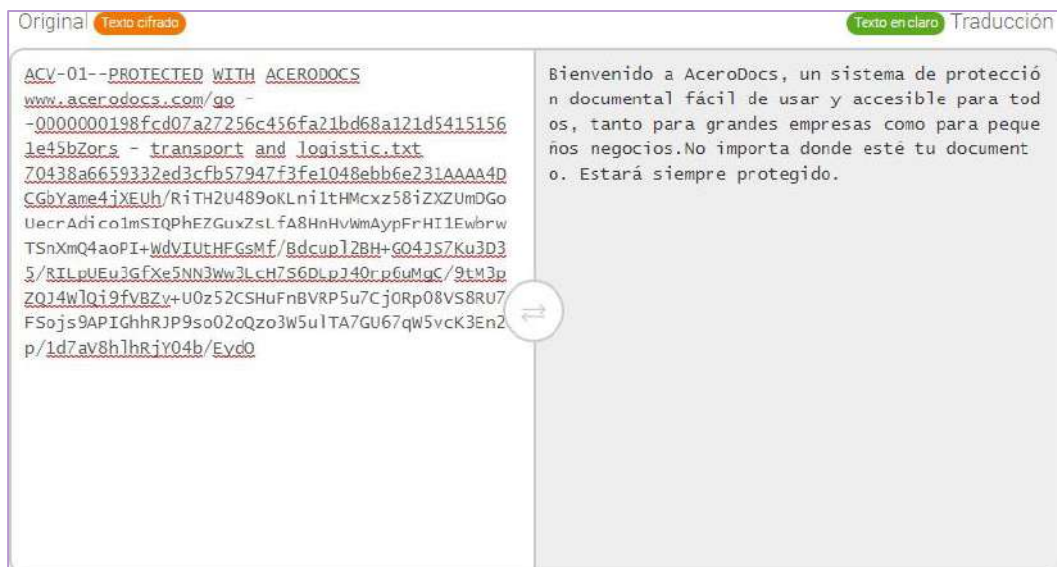
Lo puedes encontrar en la barra situada a la izquierda del panel de control.

El texto cifrado se puede ver abriendo cualquier archivo .txt .aceroV con un editor de texto plano (ej. Notepad de Windows).

Además, cuando se protege un archivo .txt, por defecto queda el texto cifrado en el portapapeles (clipboard).



Ejemplo:



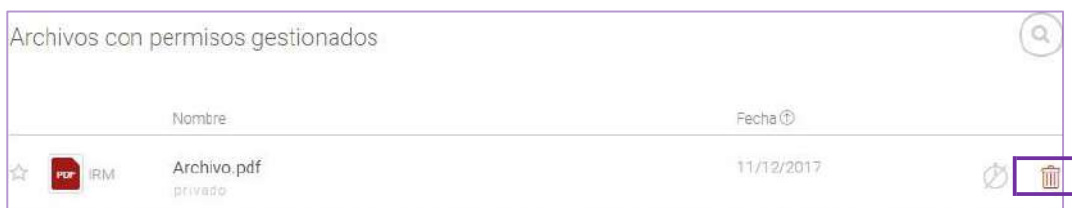


9. Papelera

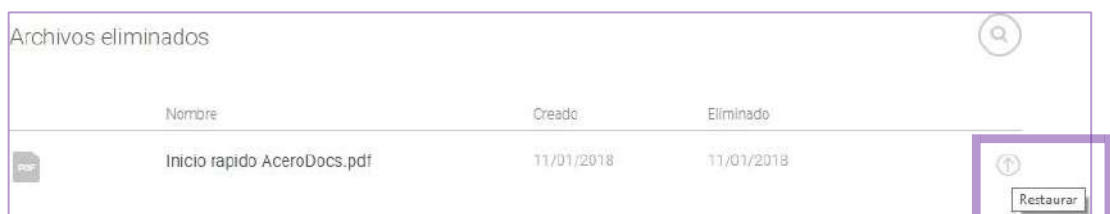
Se pueden mover a "Papelera" los archivos en el dashboard de AceroDocs.

Lo podrás encontrar en la barra situada a la izquierda del panel de control.

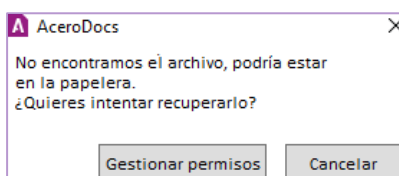
Al eliminar el archivo haciendo clic en el icono de la papelera del panel de control situado a la derecha del archivo, éste se mueve a "Papelera".



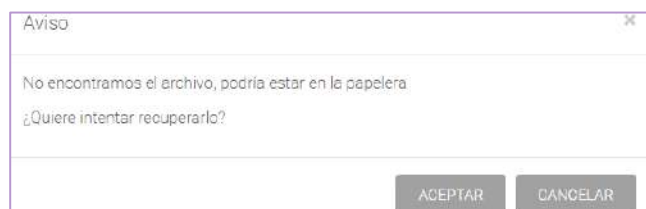
Al moverlo o eliminarlo el archivo queda inaccesible incluso para el propietario, pero éste lo podrá recuperar haciendo clic en el icono de la flecha hacia arriba de la derecha del archivo en la "Papelera".



Una vez enviado el documento a la papelera, nadie podrá abrir el documento ni sus copias excepto el propietario. Si intentas abrirlo saltará el siguiente mensaje informativo:



En tu ordenador



En el panel de control de AceroDocs

Al hacer clic en aceptar o gestionar permisos, podrás recuperar el archivo y éste se volverá a mover al dashboard de AceroDocs.



10. Trazabilidad

Haz seguimiento de quién, cuándo y dónde se hacen acciones con tus documentos.

Muy útil para acción comercial y confirmación de entrega (no repudio).

Tras recibir el fichero, el receptor actuará sobre el mismo permitiéndonos saber:

- Fecha y hora de la acción
- Acción realizada: impresión, visor web, extracción de original, intento de impresión
- Plataforma: aplicación de escritorio, uso del visor web, aplicación móvil
- Sistema operativo empleado
- Navegador utilizado en acción visor web

Para el caso de archivos protegidos con IRM abierto, los receptores que no sean usuarios de AceroDocs aparecerán como anónimos. Con la protección IRM selectiva en cambio, todos los receptores estarán identificados por su correo electrónico.

Para acceder a esta información es importante saber que existen dos vistas y que el proceso puede tardar unos segundos al hacer clic sobre el icono :



Vista resumida:

Aparece al hacer clic sobre el check de color verde y muestra los 10 últimos eventos.

Contamos con la siguiente información general de manera resumida:

- Visualizaciones: plataforma, sistema operativo y navegador
- Acceso de usuarios registrados
- Acceso de usuarios anónimos
- Impresiones
- Extracciones
- Fecha y hora de la acción

Trazabilidad Acciones sobre el fichero encriptado realizadas por otros usuarios.

Resumen

- Visualizaciones: Usuarios conocidos
- Extracciones: Accesos anónimos
- Impresiones: Acciones de usuarios

Fecha	Hora	Usuario	Acción	Plataforma
09-04-2018	14:24	empresas@herrera.com	Impresión	Escritorio
09-04-2018	11:47	manue20@yahoo.es	Extracción	Web
09-04-2018	11:17	Anónimo	Visualización	Dashboard Web

VER INFORME COMPLETO

Vista ampliada:

Estando en la vista resumida, podemos acceder a la vista ampliada al hacer clic en el botón ver informe completo. Aparecerá más información:

- Dirección IP de acceso
- Geolocalización (si ha sido posible obtener la información)

acerodocs
Informe Detallado de Trazabilidad

Información del Fichero
Fichero: Genérica: Inbound Marketing E&G-GH.pdf Fecha de Cifrado: 27-03-2018

Trazabilidad
EXPORTAR A EXCEL

Resumen

- Visualizaciones: 6
- Usuarios conocidos: 1
- Extracciones: 1
- Accesos anónimos: 1
- Impresiones: 0
- Acciones de usuarios: 6

Fecha	Hora	Usuario	Acción	Plataforma	Dirección IP
09-04-2018	14:24	empresas@herrera.com	Visualización	Escritorio	2.154.85.6
09-04-2018	13:14	manuel20@yahoo.es	Extracción	Web	2.154.85.6
09-04-2018	11:52	Anónimo	Acceso	Dashboard Web	2.154.85.6

©2018 | AceroDocs v1.3

Notificaciones por email:

Para el caso de los archivos que tengan una estrella en el dashboard, se enviará una notificación por email al autor cuando un receptor abra el documento. Esta notificación solo ocurre en la primera apertura.



11. Menú preferencias

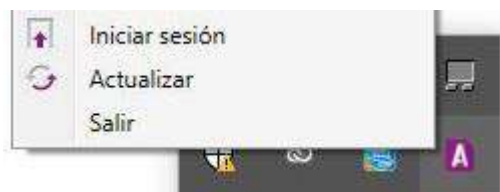
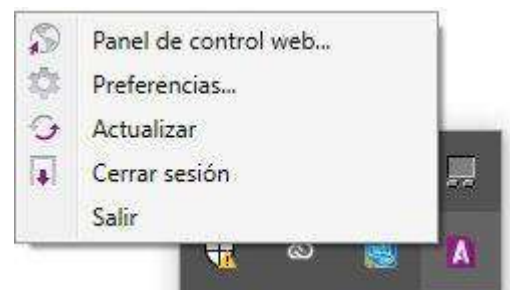
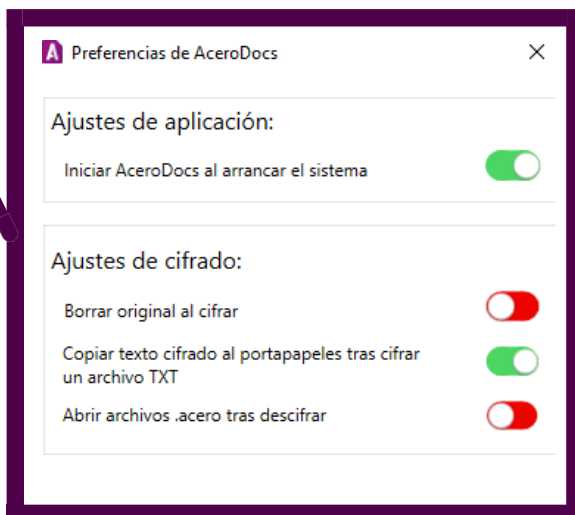
El menú preferencias es la ventana que aparece cuando hacemos clic con el botón secundario del ratón sobre el icono AceroDocs de la barra de tareas.

Barra de herramientas

Este menú aparece cuando haces clic con el botón derecho sobre el símbolo de AceroDocs en la barra de herramientas.

Las opciones que permite estando conectado son:

- Panel de control web. Conduce hacia el panel de control en el que gestionamos los permisos de nuestros documentos.
- Preferencias. Nos permite realizar los siguientes ajustes en nuestra configuración: arrancar aplicación al arrancar el sistema operativo, borrar archivo original al cifrar, copiar texto cifrado al portapapeles al cifrar un archivo TXT y abrir archivos .acero tras descifrar.
- Actualizar. Permite a los usuarios actualizar AceroDocs a la última versión disponible.
- Cerrar sesión.
- Salir.



Las opciones que permite sin estar conectado son:

- **Actualizar.** Permite a los usuarios actualizar **AceroDocs** a la última versión disponible.
- **Iniciar sesión.**
- **Salir.**



12. Grupos y Jerarquías

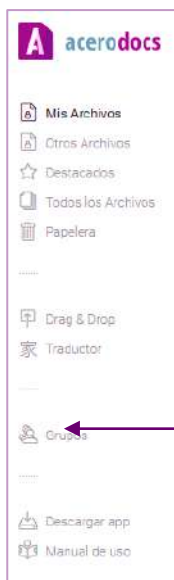
Grupos:

Esta funcionalidad está activa para los usuarios Premium y Enterprise, tanto en el usuario “admin” como en los usuarios “hijos”. El objetivo es poder gestionar listas de usuarios “receptores” de documentos de manera masiva, aplicando los mismos permisos sobre la interacción con documentos a todos los integrantes del grupo.

La funcionalidad permite:

- Crear y gestionar grupos de receptores.
- Importar listas de receptores desde archivos .csv
- Combinar usuarios con otros grupos.
- Nombrar y describir los grupos creados.

Crear un grupo:



En el menú de la columna izquierda del Dashboard se encuentra la pestaña que lleva a la gestión de grupos.

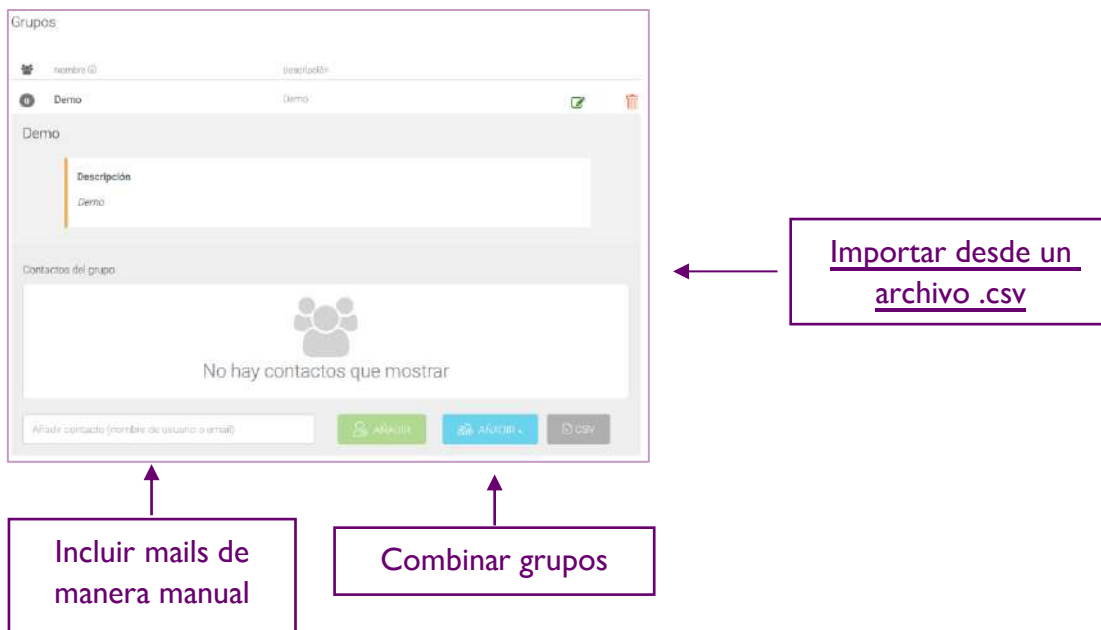
Una vez accedido al apartado, se podrán crear grupos. Para eso será suficiente con digitar el nombre que se quiere dar al grupo y, opcional, incluir una descripción del mismo, antes de presionar el botón de creación de grupo:



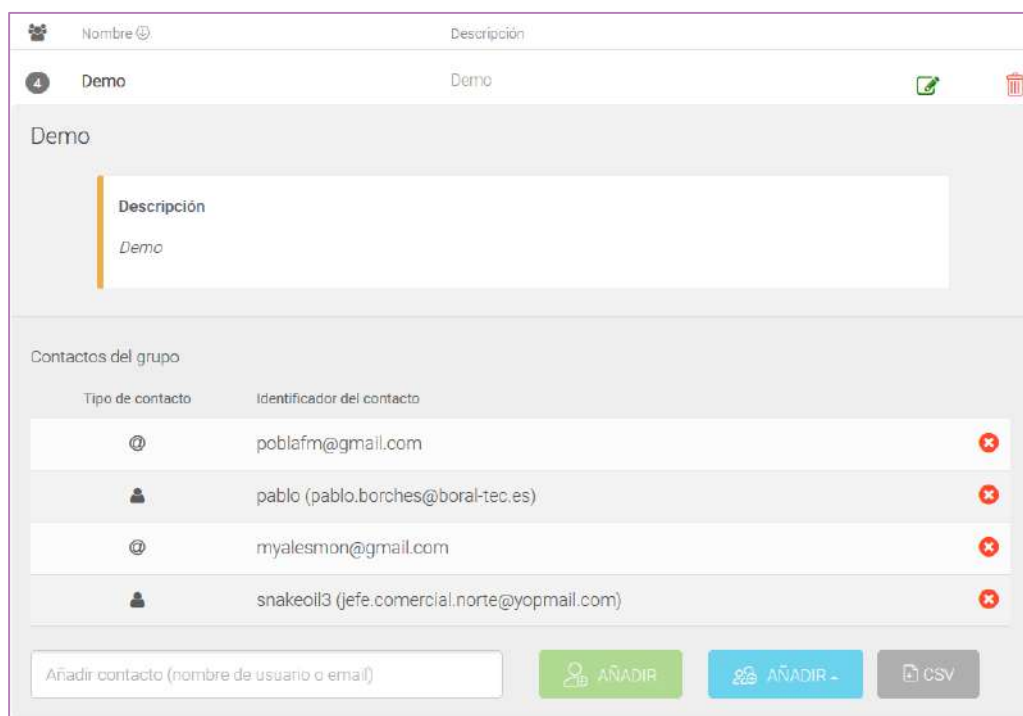
Nombre del grupo

Botón de creación

Una vez creado el grupo podremos incluir usuarios:



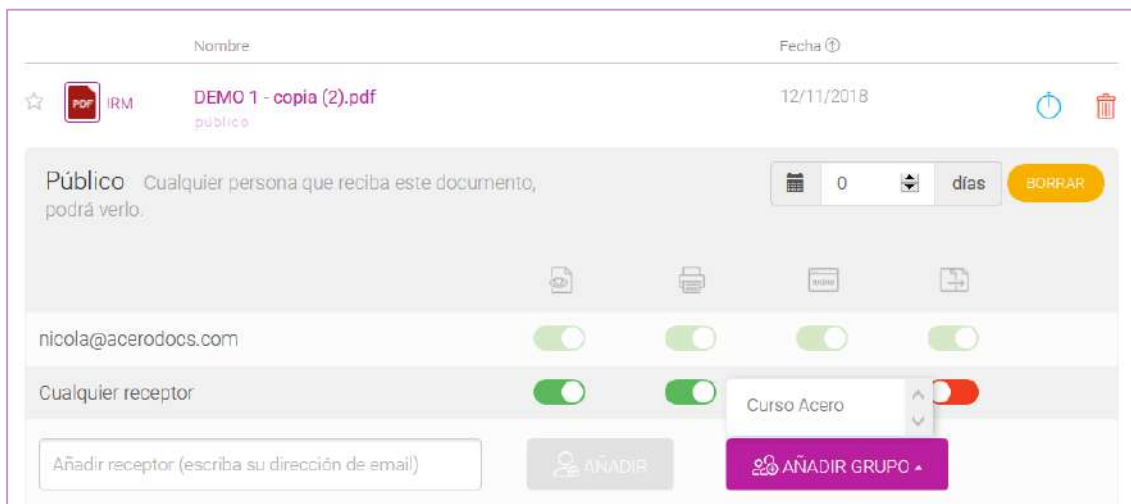
Los usuarios incluidos se verán de la siguiente manera:



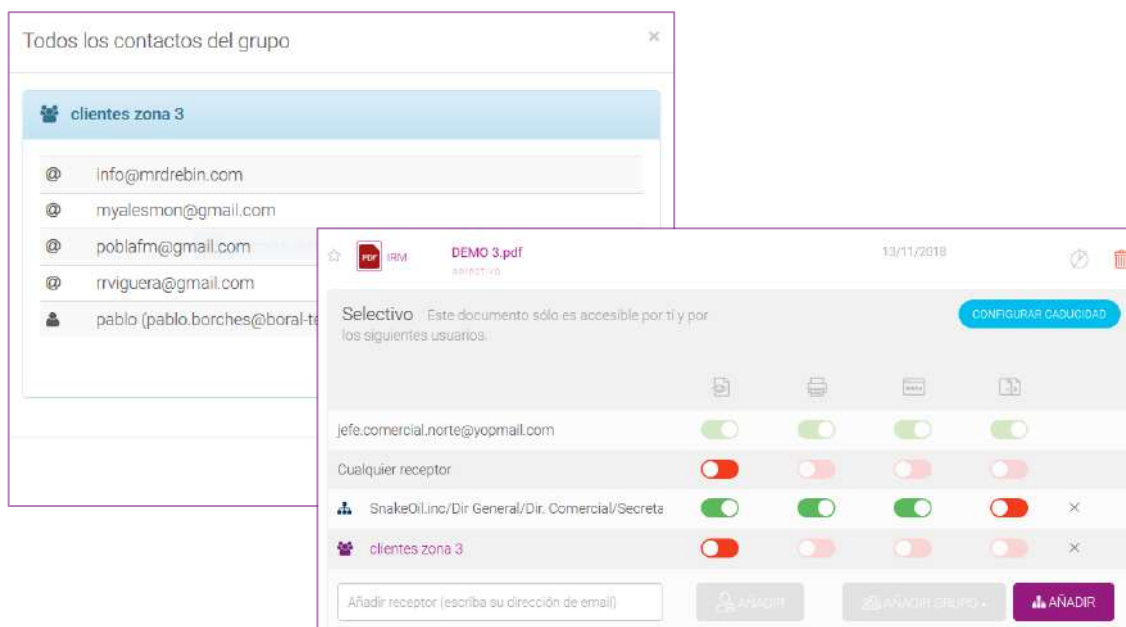
Una vez incluidos los usuarios, podremos detectar si:

1. Tienen cuenta en AceroDocs 👤
2. No tienen cuenta activa @

Una vez creado el grupo, desde la administración de los documentos cifrados (página principal del Dashboard), podrán ser asociados a los documentos o definidos en la gestión de permisos de las AceroCarpetas.



Los usuarios que accedan a la gestión de permisos sobre un documento, por haber sido habilitados por políticas y ser parte de una jerarquía corporativa, podrán consultar los integrantes del grupo que está asignado a los documentos:

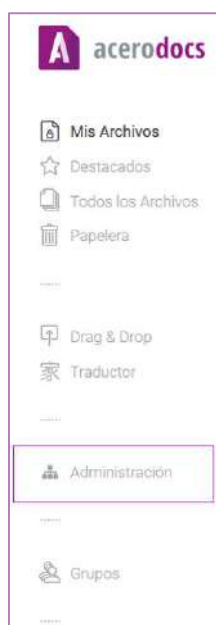


Jerarquías:

Esta funcionalidad está activa solo para la cuenta principal (Administrador) en la versión “Enterprise” que se entrega a los clientes como cuenta principal.

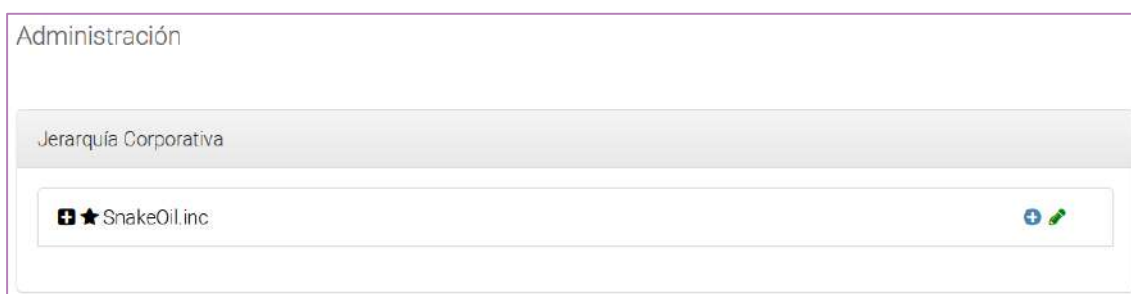
La funcionalidad permite:

- Crear nodos jerárquicos.
- Incluir y gestionar los usuarios emisores de documentos.
- Vincular los usuarios emisores a los nodos jerárquicos correspondientes.
- Relacionar los documentos emitidos por los usuarios incluidos en la jerarquía con el nodo principal por defecto.
- Asignar permisos de gestión de documentos a varios nodos jerárquicos.



En el Dashboard de la cuenta “Admin”, en la versión “Enterprise”, esta funcionalidad se ubica en la columna izquierda bajo el nombre de “Administración”.

Seleccionando la pestaña, se accederá al gestor de jerarquías:



En el gestor, podrán darse de alta/baja y editar los nodos que sean necesarios a través de la funcionalidad

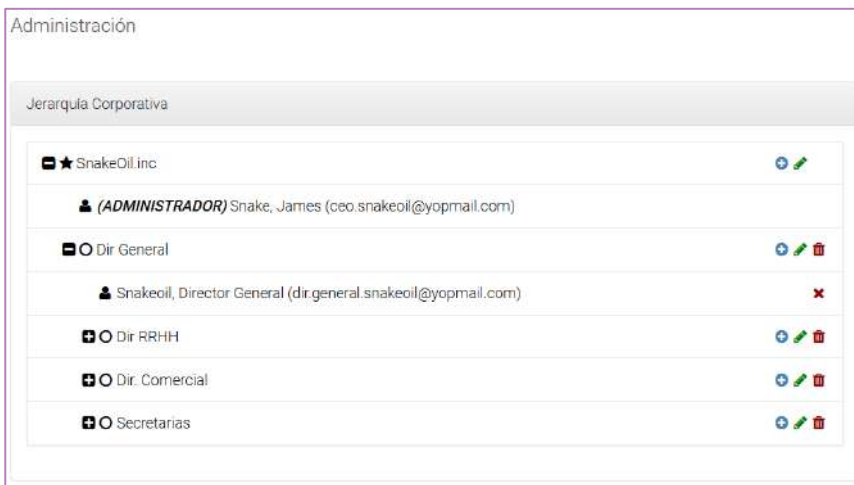


Al seleccionar la opción saldrá una ventana emergente en la que tendrán que nombrar el nodo.



A dialog box titled "Nuevo Elemento" with a close button (X) in the top right corner. It contains a text input field with the placeholder text "Nombre". Below the input field are two buttons: "ACEPTAR" (green) and "CANCELAR" (red).

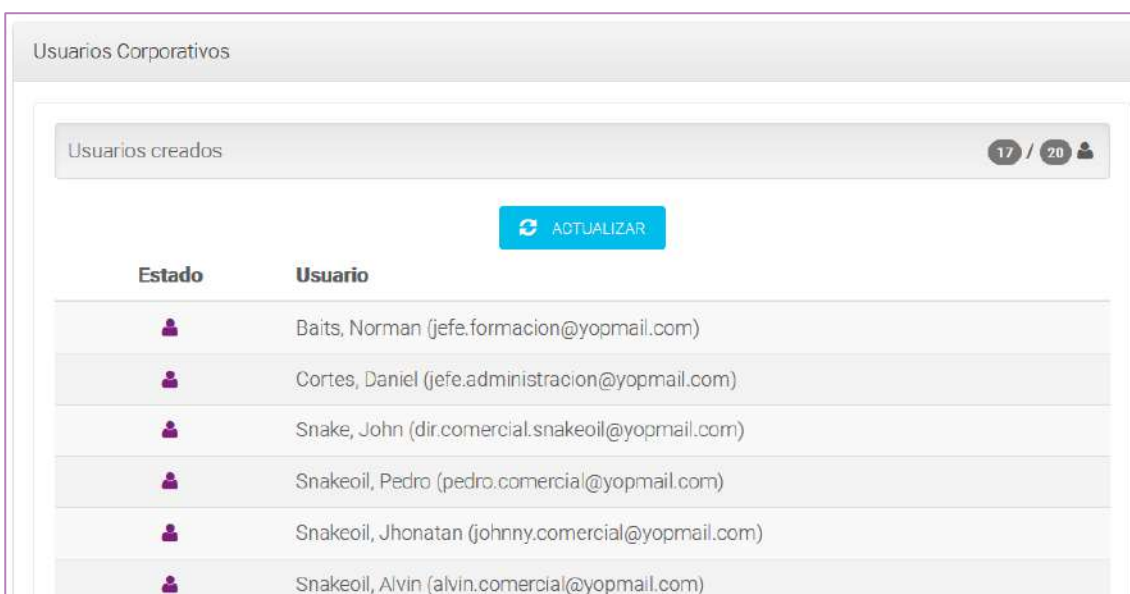
Podrán crearse tantos nodos y sub nodos como quiera el cliente.



The "Administración" section displays a "Jerarquía Corporativa" tree. The root node is "SnakeOil.inc" (marked as ADMINSTRADOR). Below it are several sub-nodes: "Dir General", "Dir RRHH", "Dir Comercial", and "Secretarias". Each node has a plus icon for adding and a trash icon for deleting. The "Dir General" node is currently selected.

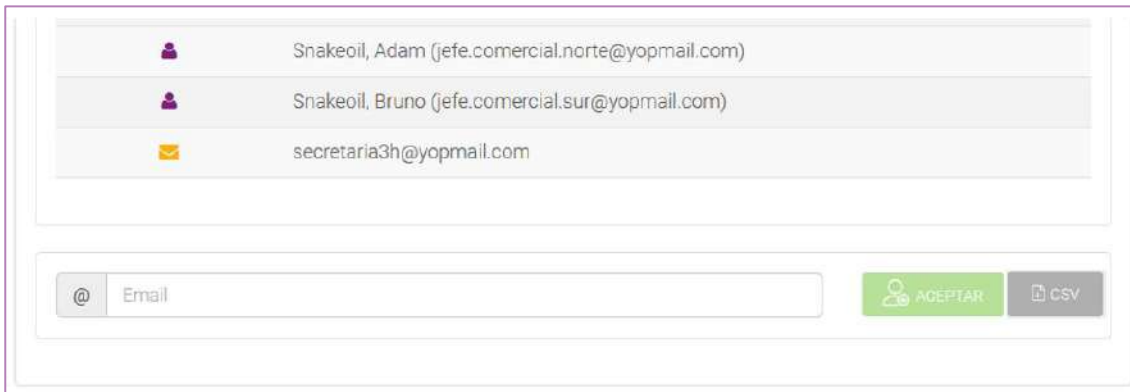
En el recuadro debajo de “Jerarquía Corporativa”, se encuentra el recuadro de “Usuarios Corporativos”. En este recuadro la primera línea indica cuantos usuarios se han creado versus el total de usuarios disponibles por el paquete de licencias adquirido.

A continuación aparece la lista de usuarios que ya crearon sus credenciales y los que han sido invitados, pero aún no han gestionado su credencial.



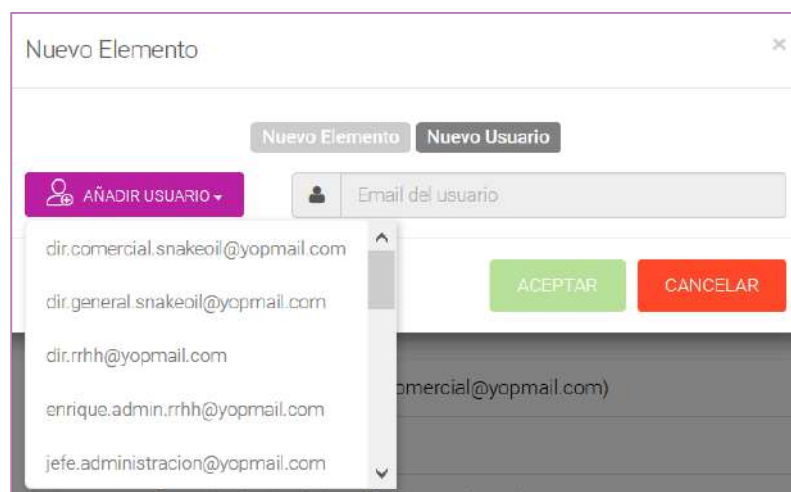
The "Usuarios Corporativos" section shows a summary bar at the top indicating "Usuarios creados" with a count of 17 / 20. Below this is a blue "ACTUALIZAR" button. A table lists the created users:

Estado	Usuario
	Baits, Norman (jefe.formacion@yopmail.com)
	Cortes, Daniel (jefe.administracion@yopmail.com)
	Snake, John (dir.comercial.snakeoil@yopmail.com)
	Snakeoil, Pedro (pedro.comercial@yopmail.com)
	Snakeoil, Jhonatan (johnny.comercial@yopmail.com)
	Snakeoil, Alvin (alvin.comercial@yopmail.com)

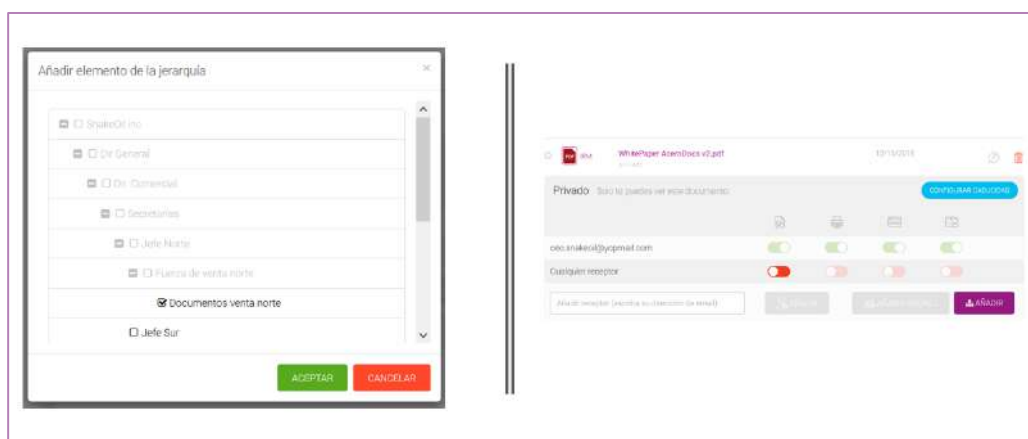


Para invitar usuarios pueden incluir un correo electrónico o importar varios desde un .csv . Los usuarios “invitados” son responsables de generar sus credenciales.

Una vez los invitados hayan generado sus credenciales aparecerá un icono morado encabezando la línea donde están ubicados, éstos podrán ser asociados a los nodos jerárquicos correspondientes, haciendo clic en este icono colocado en el nodo jerárquico correspondiente:



Los documentos emitidos por un usuario tendrán por defecto un único propietario: el nodo jerárquico principal de la empresa. Adicionalmente, de forma manual o según política de empresa, se podrá delegar la posibilidad de gestión de permisos sobre un documento a otros nodos jerárquicos y a los usuarios que vayan asociados a los mismos:





¡Qué disfrutes de AceroDocs!