



# GESTIÓN DE LA PRIVACIDAD, IDENTIDAD DIGITAL Y REPUTACIÓN ONLINE EN INTERNET

# MÓDULO 6



Almacenamiento y compartición de información en la nube de forma segura



## ÍNDICE

1. Almacenamiento de información en la nube .....	4
1.1 Almacenamiento y compartición de información en la nube de forma segura .....	4
1.2 ¿Qué es el almacenamiento en la nube? .....	5
1.3 ¿Cómo funciona? .....	5
1.4 Ejemplos de usos en la nube .....	6
1.5 Formas de almacenamiento en la nube .....	11
1.6 Buenas prácticas de gestión de documentos en la nube.....	14
1.7 Consejos de seguridad en la nube.....	14
2. Compartir información en la nube .....	17
2.1 Cómo compartir información con Google Drive.....	17
2.2 Pasos a seguir para compartir un documento desde el navegador (versión web).....	18
2.3 Pasos para compartir un documento desde un dispositivo móvil .....	20
2.4 Dejar de compartir un documento .....	26
2.5 Plataformas para compartir archivos pesados.....	27
2.6 Recomendaciones para compartir documentos en la nube de forma segura .....	28

## 1. Almacenamiento de información en la nube

### 1.1 Almacenamiento y compartición de información en la nube de forma segura

El almacenamiento en la nube ha entrado en nuestra vida casi sin percatarnos, hasta el punto de que estamos tan acostumbrados a él que no nos damos cuenta de su existencia.

Con la inclusión de las nuevas tecnologías en nuestra vida, tanto a nivel personal como profesional, tenemos acceso a la información desde distintos tipos de dispositivos: teléfono, tableta, portátil o PC. El hecho de que esta información esté siempre disponible y actualizada se ha convertido en una necesidad para todo el mundo.

El concepto de “nube” apareció a principios de la década de los sesenta, con el desarrollo de Arpanet, que fue una red de computadoras creada por el departamento de defensa de los Estados Unidos como medio de comunicación entre las diferentes instituciones académicas y estatales. Pero fue a finales de la década del 2000 cuando el término “nube” empezó a adquirir popularidad.

En este sentido, se han integrado en nuestra vida de tal forma que muchos de nosotros no seríamos capaces de imaginarnos una vida sin fotos y vídeos en los teléfonos, sin aplicaciones de mensajería instantánea, ni redes sociales. La mayoría de estas aplicaciones que usamos diariamente disponen de una copia de seguridad en la nube por si necesitásemos reinstalarlas en otro dispositivo y de esta forma no perder la información generada o transmitida en cada una de ellas.

Hace unos años, cambiar de teléfono móvil podía resultar una pesadilla solo por el hecho de tener que reinstalar todas las aplicaciones que usábamos y toda la información contenida en estos (contactos, fotos, documentos, etc.). Podía llevarnos días o semanas volver a tener todo lo necesario en nuestro nuevo teléfono. Sin embargo, gracias a los servicios de almacenamiento en la nube, todo este paradigma ha cambiado y nos facilitan la vida a todos en muchos sentidos.

## 1.2 ¿Qué es el almacenamiento en la nube?

Lo que conocemos como almacenamiento en la nube es un lugar en el que guardamos aquellos documentos que queremos compartir entre varios dispositivos o tenerlos a salvo por si ocurre algún problema con nuestros dispositivos. Es decir, nos permiten realizar copias de seguridad de la información en un servidor de una empresa o servicio que estará siempre disponible para que nosotros dispongamos de esa información cuando lo necesitemos.

Al almacenar estos documentos o ficheros en la nube, realmente lo que estamos haciendo es enviar esa información a través de Internet a un servidor web que funcionará 24 horas al día desde cualquier lugar del mundo y es accesible desde distintos tipos de dispositivos.

Un sistema de almacenamiento en la nube es como si pudiésemos acceder a nuestro ordenador, o a ciertas partes de él, desde cualquier lugar y desde distintos dispositivos (otro PC, portátil, tableta, teléfono), sin necesidad de tenerlo encendido todo el tiempo y sin necesidad de preocuparnos por la seguridad y accesibilidad de terceras personas a los datos.



*Ejemplos más conocidos de servicios en la nube*

## 1.3 ¿Cómo funciona?

Actualmente existen sistemas de almacenamiento en la nube gratuitos y otros de pago, en el que los requisitos técnicos exigibles son muy básicos. La información que se puede almacenar en sus servidores está limitada. La mayoría de estos servidores ofrecen un servicio gratuito, con capacidad de almacenamiento más limitada y un servicio *premium* o por suscripciones que nos permiten disponer de un mayor espacio o servicios específicos adicionales y también con opciones y funciones extra.

El funcionamiento de la nube puede cambiar de una aplicación a otra, por ejemplo, no es lo mismo una aplicación que nos guarde una copia de seguridad en la nube,

como es el caso de WhatsApp, que una aplicación que nos permita gestionar y compartir información, como podría ser Google Drive e iCloud.

La nube ofrece varios modelos de servicios a destacar:

- **Platform as a Service (PaaS).** Incluye todo lo necesario para que los desarrolladores creen, ejecuten y gestionen aplicaciones.
- **Infrastructure as a Service (IaaS).** Recursos informáticos que permiten a las personas usuarias construir y administrar su propia infraestructura de tecnología.
- **Software as a Service (SaaS).** Es un modelo de distribución y de licencias que sirve para entregar aplicaciones de *software* mediante Internet.

Los proveedores de servicios en la nube suelen llevar a cabo medidas de seguridad para proteger los datos de todos los clientes usuarios.

## 1.4 Ejemplos de usos en la nube

En el caso de copias de seguridad en la nube, cuando instalamos la aplicación en un móvil nos pregunta si queremos configurar las copias de seguridad y su periodicidad. Si no la configuramos, por defecto vienen configuradas para que se realicen de forma automática a cada X tiempo y siempre que el dispositivo esté conectado a la wifi (para que no consuma datos en el caso de que no se disponga de una tarifa plana de datos). Este es el caso por ejemplo de la aplicación WhatsApp.

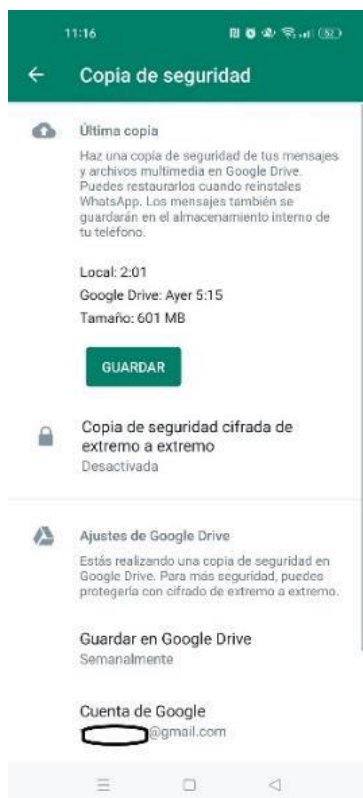
Estas copias de seguridad se pueden configurar para indicar qué tipo de datos queremos guardar en la misma, cada cuánto tiempo queremos realizar las copias y si preferimos que lo haga mediante los datos móviles o la red wifi, así como la periodicidad con la que realizará otra copia de respaldo fuera del dispositivo.

En términos generales, los pasos a seguir para configurar las copias de seguridad (puede variar de un dispositivo a otro) suelen ser los siguientes:

1. Elegir el almacenamiento que vamos a usar, por ejemplo, Google Drive.
2. Descargar el servicio en caso de no tenerlo en el dispositivo. En este caso sería la aplicación de Google Drive.
3. Configurar la copia de seguridad automática.



4. Establecer la frecuencia con la que se quiere realizar la copia de seguridad. Puede ser días, semanas e incluso meses
5. Ajustar la configuración de seguridad y privacidad según las preferencias.



*Información sobre la copia de seguridad de WhatsApp*



*Opciones para configurar el uso de datos móvil*



### Activar Copia de seguridad cifrada



En caso de disponer un teléfono móvil con sistema Android, el servicio de respaldo por defecto sería Google Drive, ya que lo tenemos vinculado a una cuenta de Gmail, la cual, ofrece multitud de aplicaciones bastante provechosas. Para los móviles iPhone, la copia se realizará en iCloud.

Otra funcionalidad que ofrecen los servicios en la nube, además de guardar nuestras copias de seguridad de forma segura, es crear carpetas, gestionar nuestros documentos o incluso compartirlos con otros usuarios.

### Funcionalidades de Google Drive

#### Tus cosas, a tu manera: funciones de Drive

15 GB de espacio    Guarda cualquier archivo    Comparte como quieras    Seguro y protegido

#### Diseñado para funcionar con Google

Guarda adjuntos de Gmail    Búsqueda avanzada    Google Fotos    Chromebooks





## Trabaja de forma más eficiente con aplicaciones

Documentos, Hojas de Cálculo y Presentaciones

Formularios de Google

Dibujos de Google

Más aplicaciones de Drive

## Llega aún más lejos con Drive

Escanea documentos

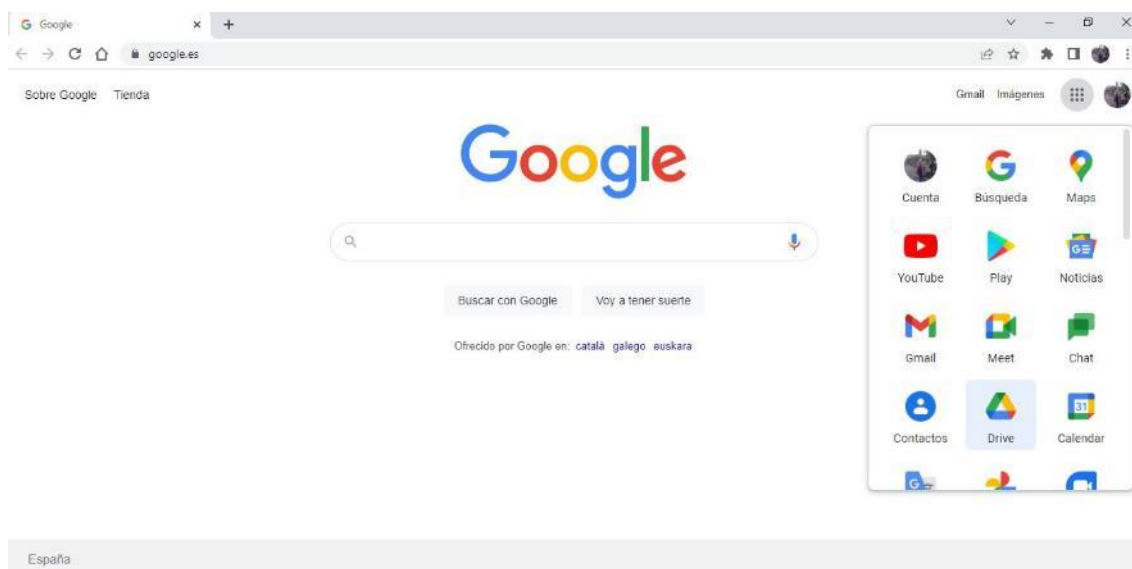
Trabaja sin conexión

Consulta versiones anteriores



### MÁS INFORMACIÓN

Para acceder a Google Drive, simplemente hay que acceder al servicio, bien vía web, como se puede ver en la siguiente captura o iniciando sesión desde: [Ver enlace](#)

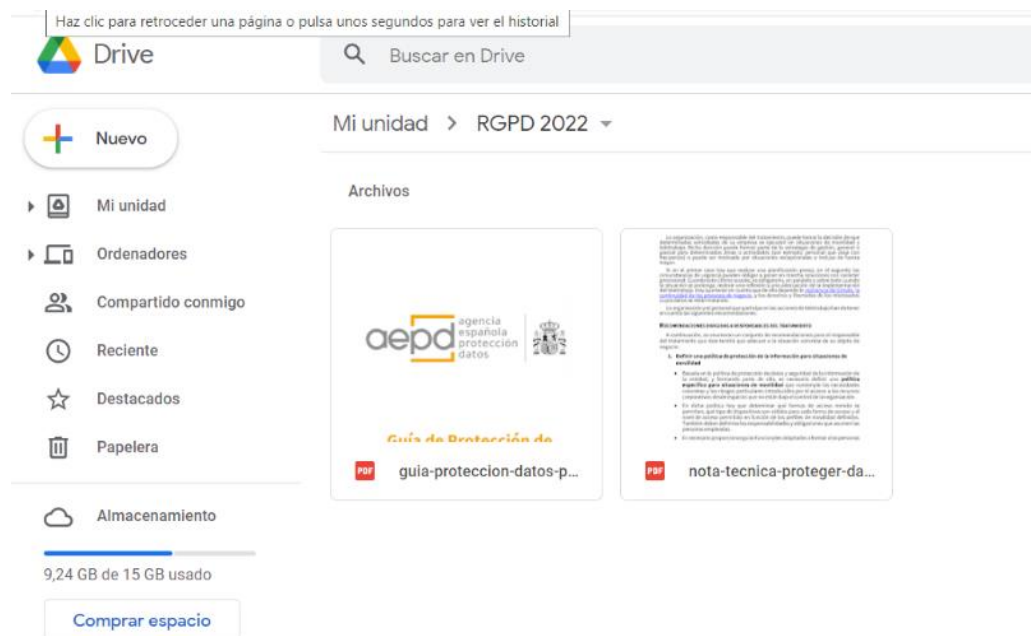


*Acceso a Google Drive desde el portal de Google*

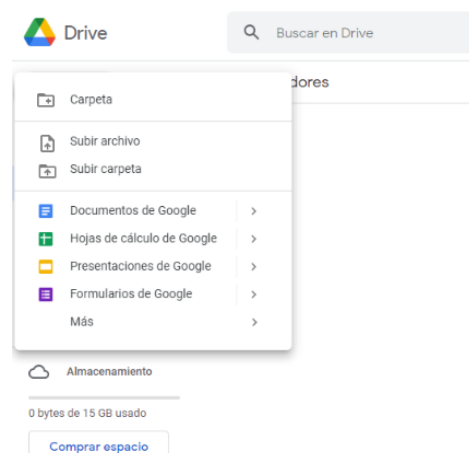
O también a través de la aplicación que podemos instalar en nuestros móviles. En los teléfonos Android, muchas veces esta aplicación ya viene instalada por defecto. El único requisito para usarla es disponer de una cuenta de usuario en Google.

Si accedemos a través del navegador, una vez logueados con nuestra cuenta de usuario y contraseña, veremos una pantalla con un menú que ofrece varias opciones, entre las que se encuentran 'Mi unidad', donde están todos los archivos que has ido subiendo a la nube y 'Compartido conmigo' que es la opción que te permite ver qué información han compartido otros usuarios contigo. El botón '+ Nuevo' será el que te permitirá subir más información a la nube.

Menú de opciones de Google Drive



Opción '+ Nuevo' para subir nueva información en la nube



## 1.5 Formas de almacenamiento en la nube

Como hemos comentado anteriormente, la gran mayoría de proveedores de servicios en la nube tienen disponibles varios perfiles o servicios que ofrecer a sus clientes, desde un espacio en la nube de forma gratuita, a una serie de servicios a los que pueden suscribirse en función de sus necesidades.

Dependiendo de quién es el propietario de los recursos informáticos, y por tanto el responsable de su seguridad, y a quién vaya dirigido, podemos diferenciar varios tipos de nube por modelo de despliegues.

### ◆ Nube pública

En el caso de la nube pública, los recursos informáticos de los que hacemos uso son propiedad de un proveedor de servicios externos, que pueden resultar de pago o no, en función de su uso. La principal característica de la nube pública es que se comparte con otros usuarios y estos pueden hacer uso de ella. Los servicios que generalmente utilizan los usuarios para hacer sus copias de seguridad son los que se conocen como IaaS (Infraestructura como Servicio) en el que el encargado de proveer los servicios a los usuarios proporciona también el *software*, así como las aplicaciones para poder hacer uso de ellas a través de Internet. Aunque también están los servicios PaaS (Plataforma como Servicio) en el que el proveedor proporciona un entorno en el que el usuario crea y distribuye sus aplicaciones; y los servicios SaaS (*Software* como Servicio) en los que el usuario puede acceder al *software*, que a su vez está alojado en el servidor del proveedor, a través de un navegador.



## ◆ Nube privada

La nube privada es propia de cada empresa o corporación, y es responsabilidad de esta garantizar la seguridad y la recuperación de los datos contenidos en esta.

La nube privada puede alojarse en las instalaciones de la propia empresa, o, por el contrario, contratar con un proveedor de Internet este servicio (servidor virtual).

Pero, en cualquier caso, es responsabilidad de la empresa el mantenimiento tanto del sistema operativo instalado en estos como de las aplicaciones y actualizaciones necesarias para su funcionamiento, por lo que requiere ciertos conocimientos para gestionar correctamente la información contenida en estos espacios (gestión de copias de seguridad, antivirus, cortafuegos, etc.)



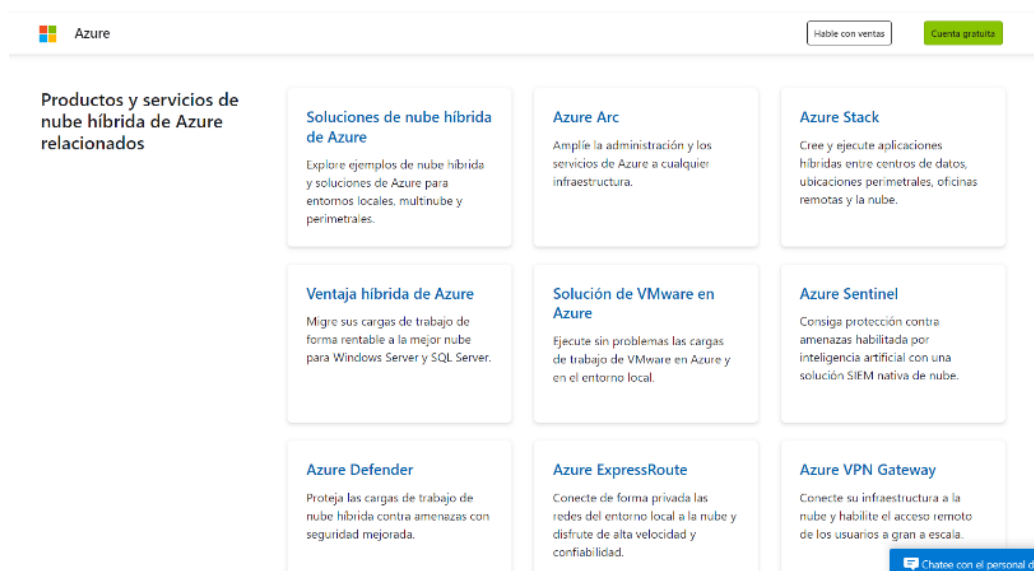
*Principales proveedores de nube privada en Europa*

## ◆ Nube híbrida

Los espacios de nube híbrida se caracterizan por combinar uno o varios servicios de la nube pública y privada, con el objetivo de obtener todos aquellos servicios que se necesitan minimizando los costes económicos.

En lugar de tener que contratar una nube privada con mucho espacio para almacenar la información que necesitemos, podemos optar por ubicar la información pública (poco sensible) en una nube pública, y los datos sobre

estrategias comerciales, investigaciones, CRM, etc. en una nube privada en la que se incluyen sistemas de seguridad avanzados.



*Servicios de nube híbrida ofrecidos por Microsoft Azure*

## ◆ **Nube Multifunción**

Este tipo de nube puede combinar las características de las nubes señaladas anteriormente. Es capaz de llevar a cabo aplicaciones de una nube privada, y, de manera transversal, basarse por ejemplo en una nube pública para su sitio de comercio electrónico.

Este tipo de nube ayuda a favorecer la simplificación y mejorar la gestión en las nuevas tecnologías, puesto que es más efectivo a nivel operativo, y además, promueve la innovación tecnológica.

En ocasiones se confunde con nube híbrida, pero son conceptos totalmente diferentes, que en algunas ocasiones pueden darse conjuntamente.



## **MÁS INFORMACIÓN**

En el siguiente enlace, se pueden ver los diez principales proveedores de nube;

[Ver enlace](#)

## 1.6 Buenas prácticas de gestión de documentos en la nube

Las recomendaciones para gestionar los datos en la nube van a ser muy similares a las que debemos de tener habitualmente con nuestros dispositivos electrónicos. No obstante, en el caso de la nube pública pueden diferir un poco, ya que hay aspectos relativos a la seguridad que dependen directamente del proveedor de servicios, y radican en las medidas de seguridad implementadas en los servidores donde se encuentran almacenados nuestros datos.

## 1.7 Consejos de seguridad en la nube

<b>Definir contraseñas seguras</b>	La mayoría de los sistemas ya nos están exigiendo que las contraseñas de acceso a sus servicios estén formadas por letras, números, caracteres especiales, contengan al menos 8 dígitos y una mayúscula. Con todos estos requisitos se pretende que, en caso de pérdida del dispositivo, el acceso a la información se dificulte.
<b>No guardar las contraseñas de acceso en los propios dispositivos</b>	En caso de pérdida o robo, cualquier persona podría acceder a la información, o incluso borrar dicha información.
<b>Cifrar los datos antes de subirlos a un servicio en la nube</b>	Especialmente si son de carácter personal o sensibles. De esta forma, si el servicio sufre algún acceso autorizado en sus sistemas, tu información no se verá expuesta al estar cifrada. Existen múltiples herramientas que te permite realizar esta acción.



<b>Seleccionar la información que se almacena en la nube</b>	<p>Cuando almacenamos documentos en la nube, tenemos que tener la certeza de que se van a cumplir todos los protocolos para que dicha información no caiga en manos no deseadas, y en caso de que no se pueda garantizar, almacenarlas en otros lugares más seguros.</p> <p>También debemos tener en cuenta las normativas legales que podamos encontrar al respecto, como es el caso de la Protección de datos (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales)</p>
<b>Administrar el control de acceso a los datos</b>	<p>Debido a que se puede acceder a la nube desde múltiples dispositivos, debe de gestionarse correctamente qué dispositivos pueden acceder a la información y en qué momento.</p>
<b>Copias de seguridad de respaldo</b>	<p>En muchas ocasiones usamos la nube para realizar copias de seguridad de nuestros dispositivos o aplicaciones, pero si no contamos con copias de seguridad adicionales, corremos el riesgo de perder toda la información si alguien accede a ella o el proveedor que nos la suministra deja de prestar servicio de forma temporal o definitiva.</p>
<b>Revisar condiciones de uso y políticas de privacidad</b>	<p>Debemos revisar las condiciones de uso, responsabilidades y políticas de privacidad que asume nuestro proveedor de servicios, con la finalidad de conocer qué limitaciones o garantías nos ofrece su servicio y poder seleccionar el proveedor que más garantía nos dé.</p>
<b>Instalar antivirus en todos los dispositivos</b>	<p>Desde los que se acceda al servicio en la nube. De esta forma podremos tener la información más controlada y evitar el robo y/o destrucción de dicha información por terceras personas debido a una infección por <i>malware</i>.</p>

<b>Uso de <i>software</i> original actualizado</b>	<p>En ocasiones, las aplicaciones no actualizadas pueden generar fallos de seguridad que permiten que se acceda a nuestros dispositivos, y desde ahí a la documentación ubicada en la nube si no se ha protegido suficientemente. Es importante asegurarse de que tenemos instalada la aplicación oficial que presta el servicio en la nube y que esta está actualizada.</p>
<b>Autenticación multifactor avanzada (MFA)</b>	<p>Usa métodos de autenticidad muy avanzados para reforzar la seguridad de las cuentas de los usuarios. Si un atacante quisiera acceder a la cuenta de un usuario, además de la contraseña, necesitaría otro factor que solo el dueño de la misma posee.</p> <p><a href="https://www.incibe.es/ciudadania/tematicas/contrasenas-seguras/autenticacion-de-dos-factores">https://www.incibe.es/ciudadania/tematicas/contrasenas-seguras/autenticacion-de-dos-factores</a></p>

## 2. Compartir información en la nube

Debido a los tiempos en los que vivimos, en los que las nuevas tecnologías y la digitalización de documentos se ha hecho imprescindible, es habitual que tengamos que compartir documentos con otras personas y no siempre es viable la opción de enviarlos por email, como se ha venido haciendo hasta ahora. Normalmente, los servidores de correo electrónico, con el fin de poder ofrecer un mayor servicio a todos sus usuarios limita el tamaño de los archivos que podemos enviar.

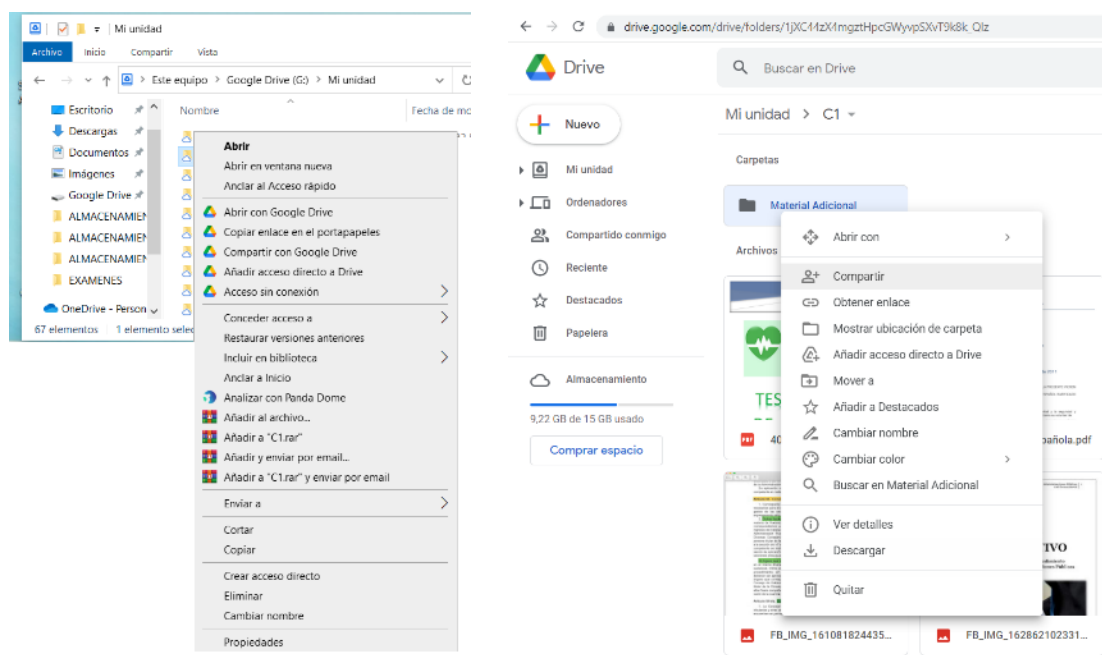
En ocasiones, simplemente con el uso de herramientas de optimización de archivo conseguimos reducir su tamaño para poder enviarlo por email, pero en otras ocasiones no es posible, con lo que es necesario recurrir a la nube para compartir dichos archivos con otros usuarios. En este caso, es muy importante configurar los permisos que queremos otorgarle a dicho usuario sobre los mismos para evitar pérdidas, robos o accesos indebidos al resto de documentación que tengamos alojada en la nube. Una solución podría ser crear una carpeta específica para compartir con el usuario y dar acceso solo a esa carpeta de todas las que tenemos creadas en la nube que estemos utilizando.

Una de las nubes más usadas en la actualidad es Google Drive, principalmente porque todos los dispositivos Android necesitan una cuenta de Gmail para su configuración y funcionamiento, y la misma lleva asociado un espacio en la nube para hacer copia de seguridad del dispositivo, de su cuenta de correo, o de las carpetas que consideremos oportunas. Es por ello, que nos basaremos en este servicio de alojamiento para basar nuestra explicación.

No obstante, hay otros muchos servicios en la nube que son muy útiles y que se pueden utilizar como son iCloud, recomendado para usuarios con dispositivos de Apple o Dropbox para cualquier usuario en general.

### 2.1 Cómo compartir información con Google Drive

La forma de compartir información con otros usuarios desde Google Drive puede diferir un poco, dependiendo de si se realiza desde su versión web, o desde su versión de escritorio.



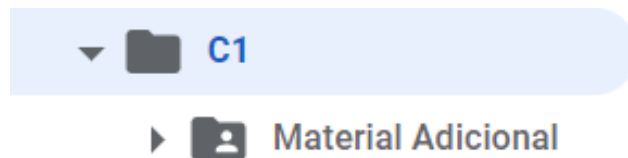
*Opción de compartir desde la versión de escritorio y acceso web*

## 2.2 Pasos a seguir para compartir un documento desde el navegador (versión web)

1. Acceder al servicio desde el enlace: [Ver enlace](#).
2. Loguearse con el usuario y contraseña correspondiente.
3. Localizar el documento o carpeta a compartir, si aún no está subido a la nube hay que hacer clic en el botón "+nuevo", posteriormente "subir archivo".
4. Botón derecho, en el desplegable, dar a la opción de "compartir".
5. Añadir la dirección de correo de las personas con las que queremos compartir los documentos.
6. Seleccionamos el tipo de permisos que vamos a asignar: 'Lector', 'Comentador' o 'Editor'.
7. Opción de notificar por email mediante una casilla el documento que se ha compartido, teniendo la opción a su vez de escribir un mensaje personalizado en el cuadro proporcionado, así como el enlace a los mismos.

## 8. Compartir.

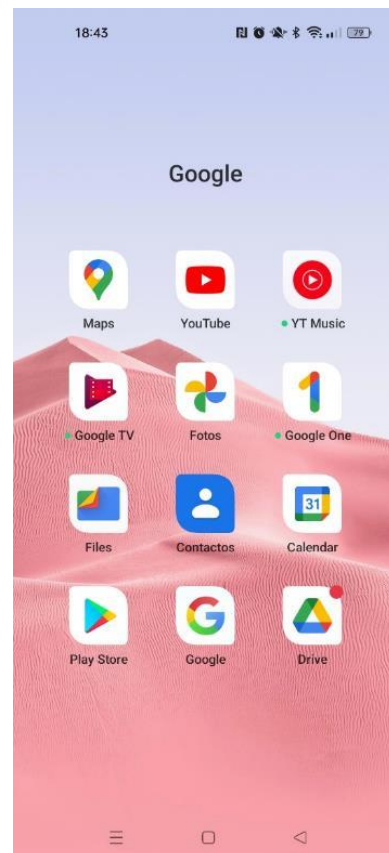
Cuando compartimos una carpeta con otro usuario, aparece un icono con forma de persona dentro de la carpeta, eso quiere decir que está compartida con otros usuarios.



En el caso de tratarse de un documento, el icono aparece al final del nombre del documento.

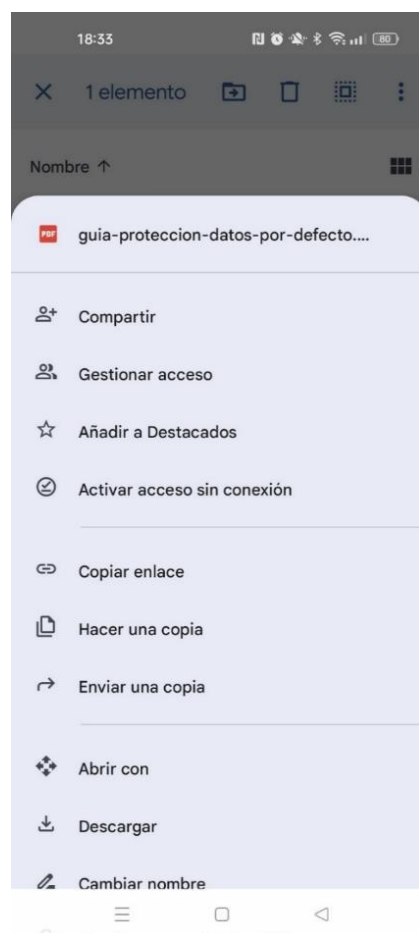
Si queremos acceder a la nube de Google directamente desde el móvil, buscaremos en nuestro dispositivo la aplicación de Google Drive (actualmente, suelen estar agrupadas todas las aplicaciones de Google).

*Aplicaciones de Google disponibles desde el móvil*

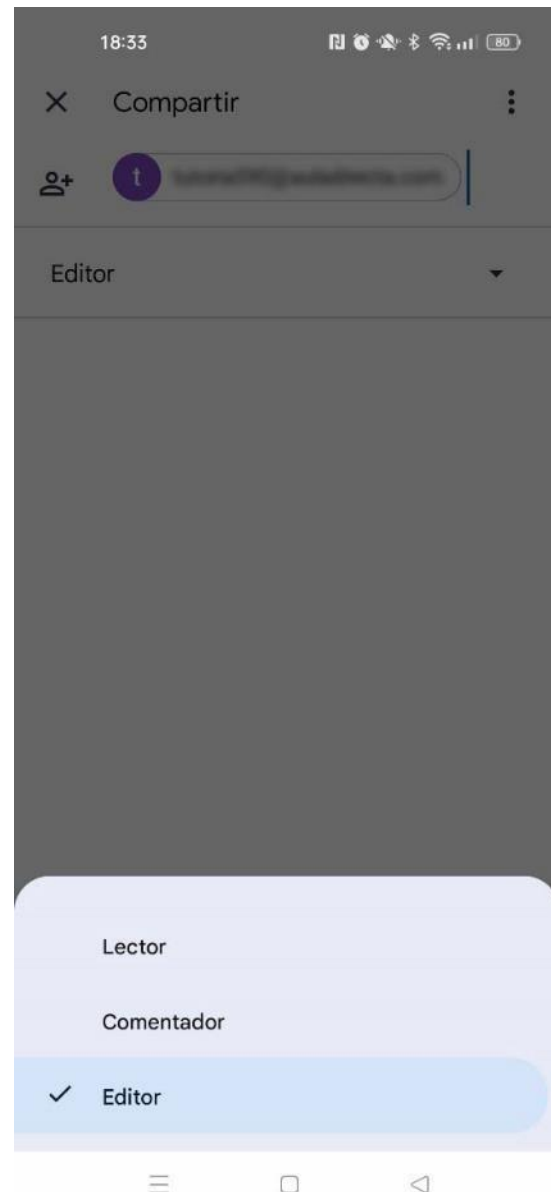


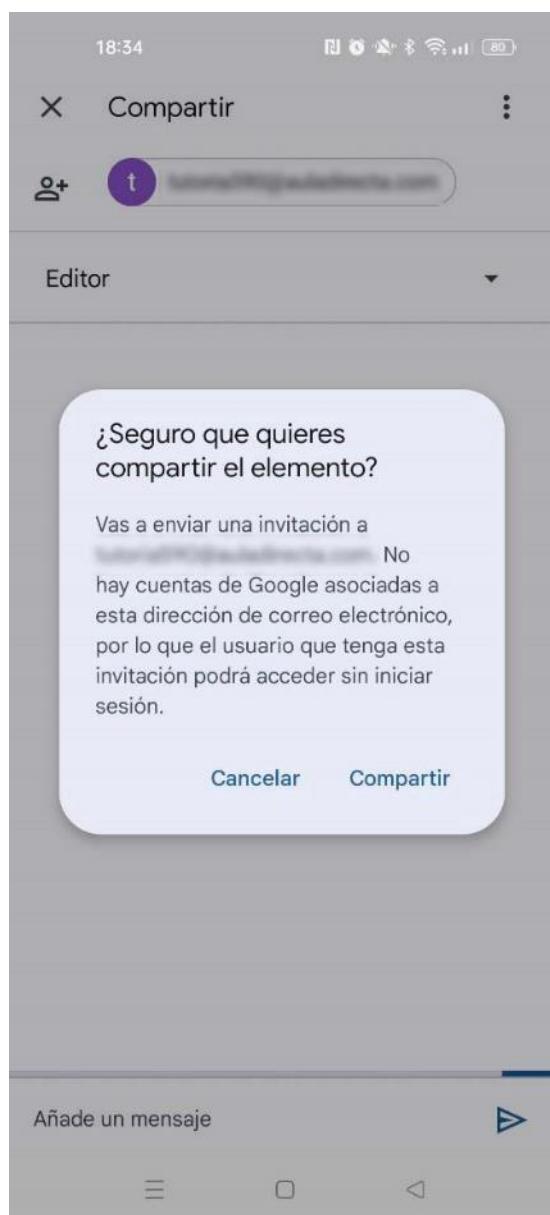
## 2.3 Pasos para compartir un documento desde un dispositivo móvil

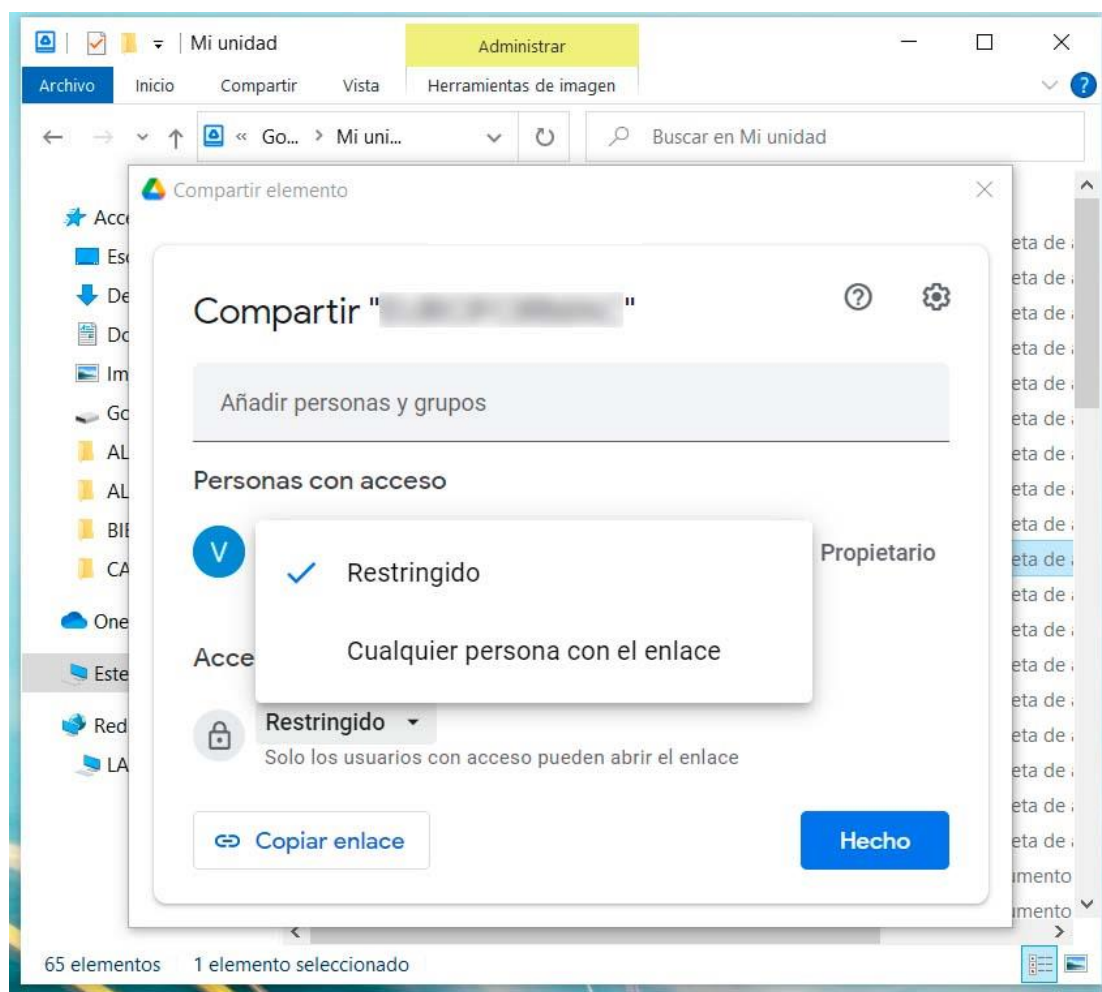
1. Accedemos a Google Drive.
2. Buscamos el archivo que queremos compartir.
3. A través de las opciones (situadas en la parte superior derecha), pulsamos sobre el icono 'Compartir', de igual forma, se puede dejar presionado el documento a compartir, abriendo de este modo también todas las opciones.
4. Indicamos el email del usuario con el que queremos compartir dicho documento.
5. Indicamos qué tipo de permisos le vamos a dar para compartir dicho documento. (si es solo de lectura, si va a poder modificar algo, etc.)
6. Confirmamos que queremos compartir el documento con este usuario.
7. Y finalmente, aparecerá el icono de que se está compartiendo con otro usuario.











*Configuración de seguridad para 'Compartir'*

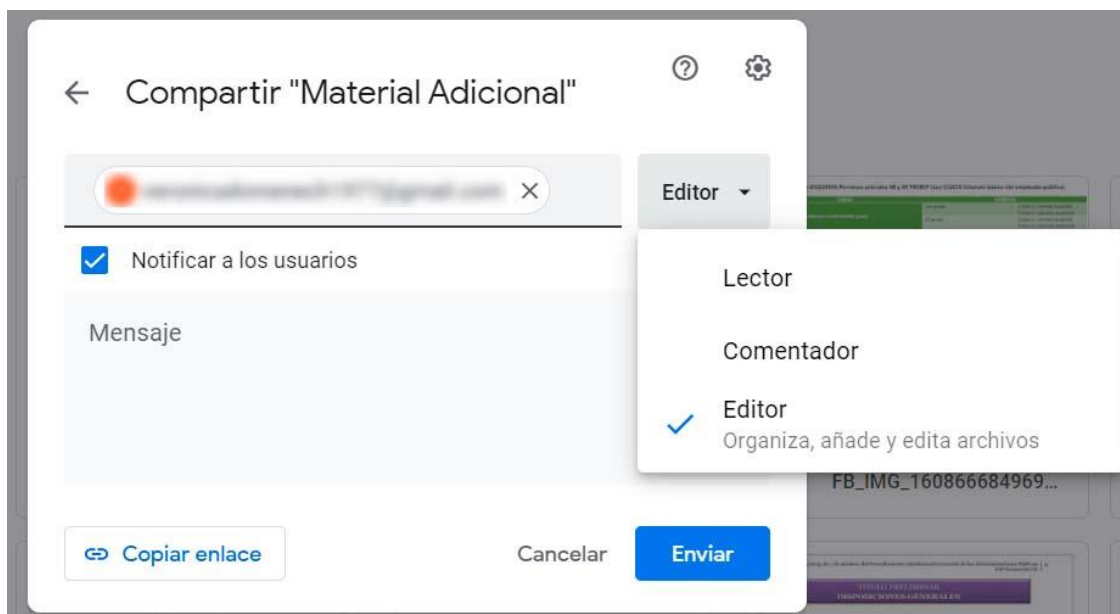
Para compartir cualquier documento que tengamos en la nube, solo tenemos que añadir las personas o grupos con los que queremos compartir la documentación, y configurar el acceso.

Dependiendo del tipo de documentación de que se trate, podemos permitir que todos los usuarios a los que les enviemos el enlace accedan a la información, o uno o varios usuarios específicos. Si, por ejemplo, tenemos nuestro CV en la nube, podemos permitir que todos los usuarios a los que les hagamos llegar nuestro enlace puedan acceder a él, ya que no existe información sensible que pueda hacerse pública.

Si, por el contrario, lo que estamos compartiendo son fotos de un viaje que hemos realizado con unos amigos, es preferible que solo aquellas personas que aparezcan en las fotos puedan acceder a las mismas, ya que en caso contrario estaríamos violando su privacidad, haciendo públicas sus fotos sin su consentimiento.

Por tanto, se pueden establecer diferentes niveles de permisos para controlar quién puede acceder al contenido y qué acciones puede ejecutar en el mismo.

La importancia de la seguridad en la nube radica principalmente en controlar qué personas pueden acceder a la documentación compartida y en qué momento.

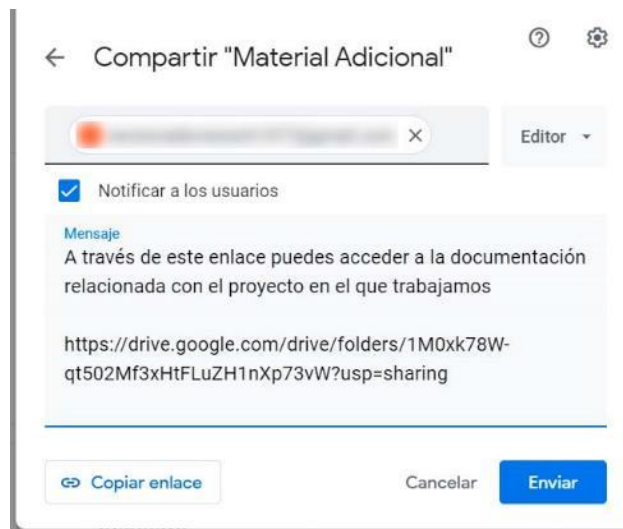


*Permisos para compartir*

Para compartir documentos con otro usuario solo tenemos que indicar su correo electrónico y el tipo de permisos que tiene sobre los documentos:

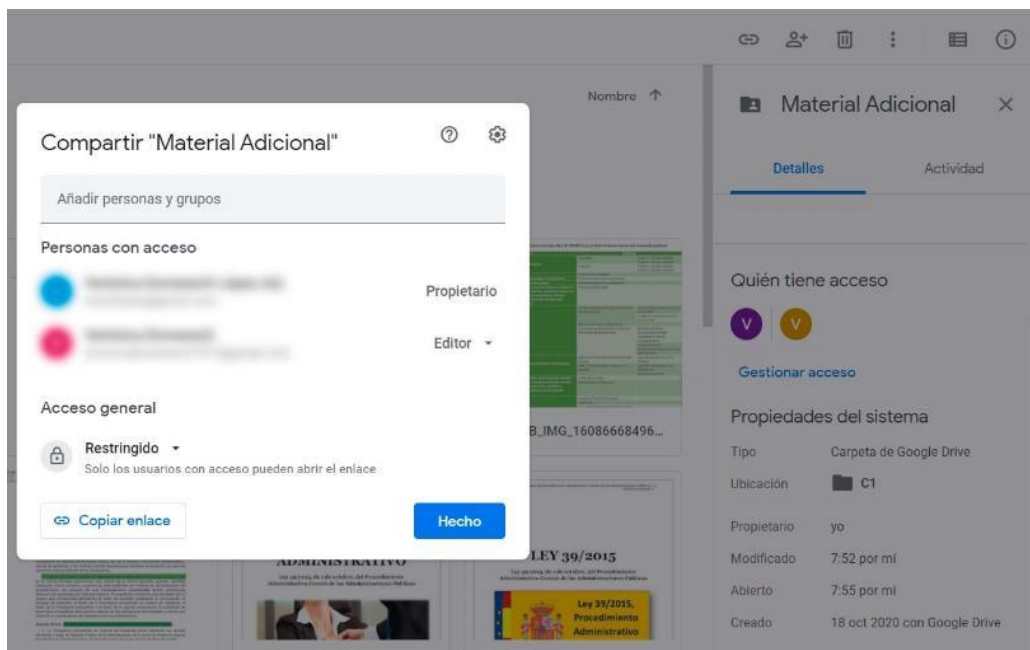
- **Lector:** la persona invitada solo podrá realizar lecturas del documento. No podrá editarlo ni insertar comentarios. Opción bastante práctica para usuarios que sólo quieren mostrar un contenido sin que se pueda modificar nada.
- **Comentador:** la persona invitada puede hacer lectura del documento y además realizar comentarios. Facilita la comunicación entre las personas invitadas ya que todos pueden ver lo comentarios realizados, volviéndose una opción útil en proyectos y trabajos que requieren revisión.
- **Editor** (organiza, añade y edita): la persona invitada con este permiso puede leer, comentar y editar los archivos que se encuentren en esa carpeta compartida. Fomentando de este modo la comunicación en “tiempo real”.

En esta opción, también se nos permite enviar un email al usuario informándole que se ha compartido un documento con él, e indicar el enlace al mismo.



*Configurar notificaciones*

Si pulsamos sobre la carpeta que acabamos de compartir, podemos obtener información sobre la carpeta compartida, personas con acceso, así como el tipo de acceso, es decir, si puede acceder cualquier persona que reciba el enlace o solo aquellas que están autorizadas.



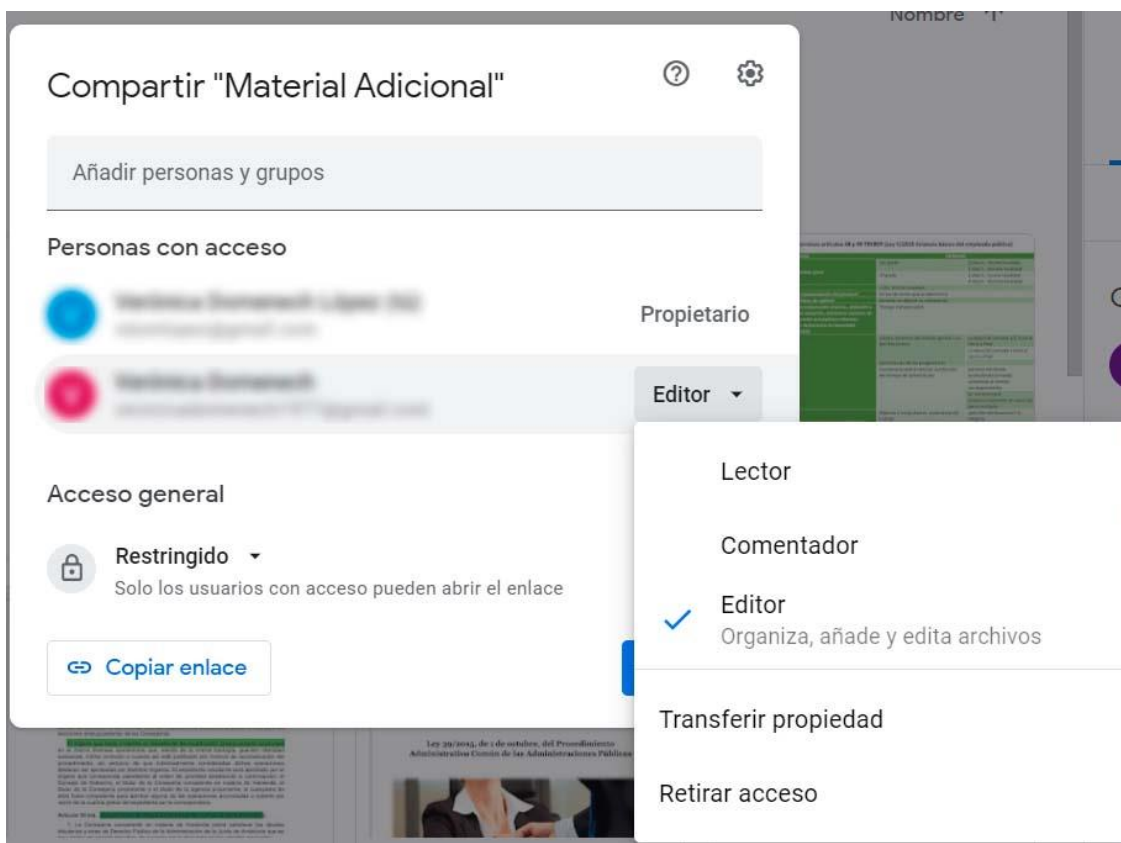
*Usuarios con los que se comparte una carpeta*

X PRESUPUESTOS.xlsx

Si activamos esta última opción es muy importante tener la máxima confianza en las personas invitadas, ya que los cambios que se pueden realizar en el documento compartido es constante, sin ningún tipo de restricción. Si lo que queremos es tener el control del documento en cuestión, esta opción no es la más recomendada.

## 2.4 Dejar de compartir un documento

En el momento que nos interese dejar de compartir los archivos con ciertas personas, podemos dejar de hacerlo.



Dejar de compartir un documento



Los pasos para dejar de compartir una carpeta o documento son los siguientes:

1. Localizamos la carpeta o el documento dentro de nuestra unidad.
2. Opción 'Compartir'.
3. Buscamos el usuario con el que queremos dejar de compartir el documento.
4. Pulsamos 'Retirar acceso'. De esta forma, el usuario deja de tener acceso al mismo.
5. Una vez retirado el acceso, hay que hacer clic en "guardar cambios", o "listo".
6. Por último, verifica en el documento que no se encuentra la persona o personas que se acaba de eliminar.

Debemos tener en cuenta que, si el usuario se ha descargado el documento en su ordenador, seguirá teniéndolo, lo que no podrá es acceder a las actualizaciones que se realicen sobre él en la nube.

## 2.5 Plataformas para compartir archivos pesados

Como ya hemos comentado previamente, existen otras plataformas para compartir documentos muy útiles e interesantes para los usuarios. Mencionamos algunas de ellas; We transfer, Dropbox, Google Drive, iCloud Drive, One Drive, Filestage



## 2.6 Recomendaciones para compartir documentos en la nube de forma segura

Las recomendaciones a la hora de compartir documentos en la nube son similares a las que debemos de tener en cuenta siempre que usamos nuestros ordenadores, pero con la característica añadida de que debemos revisar periódicamente qué compartimos y con qué usuarios.

- Evaluar y elegir plataformas de almacenamiento seguras.
- Utilizar contraseñas de acceso seguras, que se cambiarán periódicamente y no se revelarán a terceras personas. Activar el sistema de doble autenticación en el servicio, siempre que esté disponible, para añadir una capa extra de seguridad a la cuenta de usuario.
- Utilizar dispositivos con *software* original, actualizados y con antivirus instalados.
- Compartir solo los documentos necesarios con usuarios que conozcamos.
- Revisar periódicamente las carpetas y/o documentos que compartimos y sus permisos.
- No subir información sensible a la nube a la que puedan acceder otros usuarios.
- Si es necesario compartir información sensible, será necesario cifrar dicha información para evitar que terceras personas puedan acceder a ella.
- Realizar copias de seguridad en dispositivos externos periódicamente para garantizar su disponibilidad en todo momento, incluso sin conexión a Internet.