

## Taller formativo

### Administra la seguridad de tu cuenta de Google

## LICENCIA DE CONTENIDOS

La presente publicación pertenece a Instituto Nacional de Ciberseguridad (INCIBE) y está bajo licencia Reconocimiento-No Comercial-CompartirIgual 4.0 Internacional de Creative Commons. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- **Reconocimiento.** El contenido de esta publicación se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa a INCIBE y su sitio web: <https://www.incibe.es>. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- **Uso No Comercial.** El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.
- **Compartir Igual.** Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuirla bajo esta misma licencia.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.

Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE como titular de los derechos de autor.

*Texto completo de la licencia:*

[https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es\\_ES](https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es_ES)



## ÍNDICE

<b>1. Objeto del documento.....</b>	<b>4</b>
<b>2. Organización y estructura .....</b>	<b>5</b>
<b>3. Objetivo .....</b>	<b>8</b>
<b>4. Metodología y recursos .....</b>	<b>9</b>
<b>5. Contenidos.....</b>	<b>10</b>
5.1. Diapositiva 1. Presentación del taller .....	10
5.2. Diapositiva 2. Índice .....	10
5.3. Diapositiva 3. Introducción al programa formativo .....	10
5.4. Diapositiva 4. Google y sus servicios.....	11
5.5. Diapositiva 5-6. Nuestra cuenta de Google.....	11
5.6. Diapositiva 7. Configuración de las principales opciones de seguridad en nuestra cuenta de Google.....	12
5.7. Diapositiva 8-10. Actividad de seguridad reciente.....	12
5.8. Diapositiva 11. Iniciar sesión en Google .....	13
5.9. Diapositiva 12. Métodos para verificar tu identidad.....	14
5.10. Diapositiva 13-14. Tus dispositivos .....	14
5.11. Diapositiva 15-16. Buscar un dispositivo perdido.....	14
5.12. Diapositiva 17-20. Aplicaciones de terceros con acceso a la cuenta .....	15
5.13. Diapositiva 21. Acceso a aplicaciones poco seguras.....	16
5.14. Diapositiva 22. Iniciar sesión con Google en otros sitios web .....	16
5.15. Diapositiva 23. Gestor de contraseñas .....	17
5.16. Diapositiva 24. Cuentas vinculadas .....	17
5.17. Diapositiva 25. Pagos y suscripciones .....	18
5.18. Diapositiva 26. Métodos de pago .....	18
5.19. Diapositiva 27-30. Experiencia de Google Pay .....	18
5.20. Diapositiva 31. Compras, suscripciones y reservas .....	19
1.1. Diapositiva 32. Cuestionario de evaluación 1.....	19
1.2. Diapositiva 33. Cuestionario de evaluación 2.....	20
1.3. Diapositiva 34. Cuestionario de evaluación 3.....	20
1.4. Diapositiva 35. Cuestionario de evaluación 4.....	20
1.5. Diapositiva 36. Cuestionario de evaluación 5.....	20
5.21. Diapositiva 37. Turno de preguntas y respuestas .....	21
5.22. Diapositiva 38. Final del taller .....	21
<b>ANEXO .....</b>	<b>22</b>
Recursos para ampliar .....	22

## 1. OBJETO DEL DOCUMENTO

---

El presente documento constituye una herramienta didáctica que servirá de apoyo al docente para la planificación del **taller formativo “Mejora la seguridad de tu cuenta de Google”**.

Esta herramienta supone un **instrumento específico de planificación y desarrollo** de cada una de las áreas de las que se compone la acción formativa, y requiere de la labor docente para concretar los distintos elementos curriculares adaptándolos a las características del alumnado.

A lo largo de la guía docente, se profundizará en los **objetivos generales y específicos de la acción formativa, sus contenidos y aquellos materiales y recursos adicionales** que se requieran para la impartición de las competencias recogidas en el taller.

## 2. ORGANIZACIÓN Y ESTRUCTURA

La estructura del taller estará compuesta por 4 puntos clave que profundizarán en la configuración de los aspectos de seguridad de nuestra cuenta de Google. Al final habrá un turno de preguntas para contestar las dudas de los participantes.

La estructura completa del taller formativo es la siguiente:

#	APARTADO	DURACIÓN
1	<b>Introducción del programa formativo</b> Se realizará una presentación más institucional sobre el programa formativo, su objetivo, la metodología utilizada y el temario.	3 min.
2	<b>Google y sus servicios</b> Breve repaso de los diferentes <a href="#">servicios</a> que Google pone a nuestra disposición para poner en contexto a todos los participantes del taller. También, se describirá el <a href="#">Centro de Seguridad de Google</a> , donde analizaremos las principales funciones de privacidad y seguridad de las aplicaciones de Google.	4 min.
3	<b>Nuestra cuenta de Google</b> Introducción al sitio <a href="https://myaccount.google.com">https://myaccount.google.com</a> para un primer acercamiento al <i>site</i> de Google, donde es posible configurar los principales aspectos de privacidad y seguridad relacionados con nuestras cuentas de usuario y la actividad realizada a través de los distintos servicios que ofrece. Es importante conocer cómo acceder a estas configuraciones desde cualquier dispositivo, bien sea accediendo al <i>site</i> específico a través del navegador web, o de las opciones de configuración del propio dispositivo Android (Ajustes > Google > Gestionar tu cuenta de Google).	5 min.
4	<b>Configuración de las principales opciones de seguridad disponibles</b> Analizaremos las principales <a href="#">opciones de seguridad</a> de nuestra cuenta de Google. Veremos aquellas opciones más representativas que afecten a la seguridad de nuestra cuenta, así como la función “Revisar la seguridad” que facilita Google y que es capaz de detectar y resolver los problemas de seguridad más importantes. El objetivo es que comprendamos la importancia de proteger nuestras cuentas y la información personal almacenada en ellas, así como conocer las herramientas que ofrece Google para mejorar nuestra seguridad y que impedirán a terceros acceder y tomar control de nuestro perfil.	4 min.
4.1	<b>Iniciar sesión en Google</b> Dentro de esta sección, podremos acceder a las opciones de configuración de nuestra contraseña, cómo modificarla, cómo <a href="#">utilizar un segundo elemento para iniciar sesión como nuestro dispositivo móvil</a> o cómo activar la verificación en dos pasos. Esta sección es muy útil para blindar nuestra cuenta de posibles ataques que intenten hacerse con el control de la misma.	6 min.

4.2	<b>Actividad de seguridad reciente</b> Veremos en detalle esta función que nos permite a los usuarios <a href="#">monitorizar la actividad reciente</a> relacionada con nuestra cuenta de Google. Es especialmente útil para identificar actividad sospechosa, como dispositivos desconocidos desde los que se haya iniciado sesión.	5 min.
4.3	<b>Métodos para verificar tu identidad</b> Descubriremos como configurar un número de teléfono y un correo electrónico alternativo desde el que Google podrá comprobar nuestra identidad o contactar con nosotros (SMS o email) en el caso de que se detecte una actividad sospechosa en nuestra cuenta. Por ejemplo, si alguien descubre tu nombre de usuario y tu contraseña, este paso ayuda a impedir que realicen acciones sensibles en la cuenta.	4 min.
4.4	<b>Tus dispositivos</b> Analizaremos este apartado donde se recoge toda la información necesaria para <a href="#">gestionar los dispositivos</a> donde hemos iniciado sesión con nuestra cuenta de Google. No solo nos permitirá cerrar sesión en algún dispositivo, sino que nos proporcionará más detalles sobre el inicio de sesión: sistema operativo del dispositivo, lugar, hora, etc. Además, sus funciones nos permitirán encontrar un dispositivo perdido en caso de robo o pérdida, siempre y cuando tengamos la sesión abierta con nuestra cuenta, y tengamos activados los permisos de geolocalización.	4 min.
4.5	<b>Aplicaciones de terceros con acceso a la cuenta</b> Aprenderemos cómo obtener un <a href="#">histórico de todas las aplicaciones y servicios web a las que hemos concedido permisos</a> para acceder a algunos datos de nuestra cuenta de Google. Desde sus opciones de configuración podremos: <ul style="list-style-type: none"> <li>• Retirar el acceso a nuestra cuenta de Google.</li> <li>• Ver detalles sobre la aplicación.</li> <li>• Denunciarla.</li> <li>• Comprobar los permisos de acceso.</li> </ul> Todas ellas categorizadas en función de su origen (aplicación de terceros, de Google o sitios web).	5 min.
4.6	<b>Pagos y suscripciones</b> Repasaremos esta sección destinada a gestionar <a href="#">nuestros datos de pagos, transacciones y suscripciones</a> . Desde aquí, podremos comprobar y gestionar los métodos de pago que tenemos asociados a nuestra cuenta, así como consultar las transacciones y actividad dentro de Google Pay, la aplicación para pagos online de Google. Al mismo tiempo, dispondremos de un histórico de todas nuestras compras, suscripciones y reservas que podremos gestionar en cualquier momento.	5 min.

	Es fundamental que revisemos este apartado de vez en cuando para comprobar que no haya movimientos bancarios sospechosos y revisar la información bancaria que hemos compartido con Google.	
5	<b>Turno de preguntas.</b> Sesión final que recogerá las preguntas y comentarios de los participantes del taller.	5 min.

### 3. OBJETIVO

---

Este taller tiene como objetivo principal **proporcionar a los alumnos las instrucciones necesarias para gestionar las principales opciones de seguridad disponibles dentro de la configuración de sus cuentas de Google**. Dado el enfoque teórico-práctico, así como el nivel de profundidad de sus contenidos, el recurso va dirigido a un colectivo de usuarios con conocimientos muy básicos sobre tecnología y seguridad.

A lo largo del taller, se ofrecerá a los alumnos recursos de ampliación en forma de enlaces de la OSI, con el fin de expandir sus competencias y satisfacer su curiosidad. Del mismo modo, servirán al docente para enriquecer los contenidos del taller.



## 4. METODOLOGÍA Y RECURSOS

---

La metodología empleada en el desarrollo de este recurso es de **carácter teórico-práctico, visual y buscando la participación activa del alumnado** durante la impartición del taller:

- **Teórico-práctica:** Los contenidos teóricos vendrán acompañados en todo momento de ejemplos reales que aterricen la teoría. A través de casos reales y actividades, el alumnado pondrá en práctica la información transmitida a través del recurso.
- **Visual:** Las imágenes técnicas y decorativas abundarán a lo largo de todo el Webinar para apoyar el contenido y ayudar al usuario a visualizar las diferentes pantallas/interfaces.
- **Participación activa:** El alumnado tendrá un papel fundamental en los Webinars, pues no se limitarán a escuchar. Los contenidos están preparados para que se pongan en práctica desde el comienzo, en cada uno de los dispositivos del alumnado.

Además, se busca enriquecer la experiencia formativa a través de las dudas y comentarios que se expongan durante su desarrollo.

El taller cuenta con diferentes **recursos** al servicio del docente para la impartición:

- **Presentación en Power-Point.** Se trata de una presentación con comentarios en texto para apoyar al docente, y los contenidos a compartir con el alumnado.
- **Enlaces para ampliar.** Servirán para afianzar los contenidos desarrollados mediante ejemplos y contenidos para ampliar, con los que enriquecer la acción formativa.

## 5. CONTENIDOS

---

A continuación, se muestra el contenido del taller ordenado en diapositivas para facilitar la tarea al docente.

### 5.1. Diapositiva 1. Presentación del taller

Presentación del taller “Administra la seguridad de tu cuenta de Google”. Debe mencionarse la labor de INCIBE y el teléfono de ayuda 017.

Este taller ha sido elaborado en colaboración con Google para dar a conocer las opciones de configuración de nuestras cuentas de usuario. Además, se han desarrollado otros recursos complementarios que se irán publicando en la web de la OSI, como otro taller que abordará las configuraciones de privacidad de la cuenta, tres vídeos prácticos que mostrarán las opciones de seguridad y privacidad más relevantes en servicios como Chrome, Búsqueda, Asistente y Android y finalmente una guía completa para la configuración de nuestra cuenta y otros servicios de Google.

### 5.2. Diapositiva 2. Índice

Presentación del índice de contenidos del taller:

1. Introducción del programa formativo.
2. Google y sus servicios
3. Nuestra cuenta de Google.
4. Configuración de las principales opciones de seguridad en nuestra cuenta de Google.

Para más información sobre los contenidos, consultar el apartado 2 de la guía del docente, donde se detallan cada uno de los apartados junto a su explicación.

### 5.3. Diapositiva 3. Introducción al programa formativo

Tener una cuenta de Google supone tener acceso a una gran variedad de servicios y plataformas desde las que poder disfrutar de todas las ventajas que nos ofrece esta empresa.

Es probable que conozcamos varios de estos servicios pero **¿sabemos cómo configurar correctamente [nuestra cuenta de Google](#)?**

Estas opciones nos permitirán **proteger nuestra seguridad**, es decir, **aplicar medidas y configuraciones para controlar el acceso a nuestra cuenta y proteger la información almacenada en los distintos servicios de Google**. Este punto es fundamental, ya que a ninguno nos gustaría que un desconocido tuviese acceso a nuestra cuenta y a todos los datos que tenemos, como nuestro historial de búsquedas y credenciales de otros servicios ¿verdad?

Con este taller queremos proporcionar las instrucciones y conocimientos necesarios para una correcta gestión de las principales opciones de seguridad disponibles dentro de la configuración de nuestra cuenta de Google.

Google pone a nuestra disposición el [Centro de Seguridad de Google](#), donde publican varias guías con las principales opciones de privacidad de las que disponemos los usuarios para todos y cada uno de sus servicios. Esta herramienta nos resultará muy útil y un

complemento perfecto para este taller, donde ofreceremos recursos de ampliación y consejos relacionados con la ciberseguridad.

## 5.4. Diapositiva 4. Google y sus servicios

Google nació de la mente de dos programadores, Larry Page y Sergey Brin, que tenían el objetivo de crear un buscador eficaz para Internet.

Con el tiempo, la idea original acabó **convirtiéndose en el motor de búsqueda más conocido por todos los usuarios y a su alrededor, se crearon una multitud de servicios y aplicaciones.**

Consulta más información sobre el origen e historia de la empresa en: [De un garaje al Googleplex.](#)

Algunos de los servicios que probablemente todos conozcamos y que forman parte del [universo Google](#) son los siguientes:

- Google Chrome: un navegador con el que entrar a Internet.
- YouTube: la plataforma desde la que ver o crear vídeos de la comunidad.
- Gmail: un gestor de correo electrónico conocido por todos.
- Android: el sistema operativo más popular entre dispositivos móviles.
- Drive: la plataforma para el almacenamiento de archivos en la nube.
- Google Pay: la plataforma desde la que podremos realizar pagos con nuestro *smartphone* y gestionar nuestras tarjetas y carteras virtuales.
- Y muchos más.

**Todos ellos pueden ser controlados a través de una única cuenta** desde la que podemos configurar permisos, modificar nuestra información personal y gestionar lo que compartimos con todas estas aplicaciones y otros usuarios. El centro de seguridad de Google nos ayudará en esta labor, pero también podemos gestionar todos los aspectos de privacidad y seguridad desde las opciones de configuración de la propia cuenta.

## 5.5. Diapositiva 5-6. Nuestra cuenta de Google

Nuestra cuenta de Google es el **puesto de control desde donde podemos gestionar todas las opciones de configuración tanto a nivel de privacidad como de seguridad de la cuenta**, así como de los distintos servicios que tengamos vinculados a ella.

Podemos acceder a dichas configuraciones desde cualquier servicio o aplicación de Google haciendo clic sobre nuestra foto de perfil y seleccionando [Gestionar tu cuenta de Google.](#)

A continuación, vamos a desglosar las diferentes opciones y funciones que podemos encontrar en nuestro menú inicial:

- **Inicio:** desde aquí podremos acceder a un vistazo global del estado de nuestra cuenta de Google y a las funciones más importantes que podemos gestionar a través del resto de apartados del menú.
- **Información personal:** contiene todos los datos personales que utilizamos como identificativos en los servicios de Google (nombre, fecha de nacimiento, datos de contacto...). Podremos modificarlos y gestionar qué compartimos con terceros ("Sobre mí").

- **Datos y personalización:** podremos personalizar nuestra experiencia e interacción con Google. Desde la información que se almacena sobre nuestra actividad online, hasta el uso de ésta. **Lo veremos en profundidad a lo largo del presente taller.**
- **Seguridad:** Aquí podremos configurar todos los mecanismos de protección de Google para proteger el acceso y la autenticación o recuperar nuestra cuenta. Se configuran aspectos como los siguientes: cómo activar la verificación en dos pasos, el uso de contraseñas robustas, métodos para verificar tu identidad, dispositivos desde los que se ha iniciado sesión, cómo buscar un dispositivo perdido, etc. Más información en: [Herramientas y sugerencias para que te mantengas seguro en línea.](#)
- **Contactos e información compartida:** desde este apartado podremos organizar tus contactos, bloquearlos y gestionar la información que guardas sobre ellos. Del mismo modo, gestionaremos lo que ellos ven sobre nosotros, como nuestra ubicación o **información personal** (Sobre mí).
- **Pagos y suscripciones:** Si hemos realizado alguna vez un pago dentro de los servicios de Google, podremos disponer de un histórico. Desde los métodos de pago asociados, hasta compras, suscripciones y reservas realizadas.
- **Información general:** en caso de tener alguna duda sobre los mecanismos de seguridad o privacidad, o si queremos mantenernos al día con las últimas novedades de nuestra cuenta Google, desde aquí podremos informarnos.

## 5.6. Diapositiva 7. Configuración de las principales opciones de seguridad en nuestra cuenta de Google

Las opciones con las que configurar la seguridad de nuestra cuenta se encuentran dentro del apartado [Seguridad](#), localizado en el menú lateral.

Si hacemos clic, veremos distintos bloques que se corresponden con las distintas **configuraciones y recomendaciones de seguridad que Google** pone a nuestra disposición para **proteger mejor nuestra información**.

En las siguientes diapositivas nos adentraremos en cada una de ellas para analizar sus funciones y cuál sería la configuración más segura.

Finalmente, antes de entrar en detalles, es necesario mencionar la utilidad del primero de estos bloques, denominado [Revisión de seguridad](#). Esta función analizará y nos alertará de aquellas vulnerabilidades en la seguridad de nuestra cuenta que requieren de supervisión. Otra de sus ventajas es que nos guiará por cada una de ellas para que llevemos a cabo las modificaciones necesarias.

Ahora sí, conozcamos en profundidad **cómo funciona la configuración de nuestra seguridad**.

## 5.7. Diapositiva 8-10. Actividad de seguridad reciente

Cada vez que realizamos un cambio en nuestra cuenta o un inicio de sesión en un nuevo dispositivo, un registro de dicha actividad se almacena en nuestra cuenta.

Esta información la podemos encontrar dentro del bloque [Actividad de seguridad reciente](#) y nos aporta mucha información:

- **Nos permite revisar toda la actividad relacionada con la seguridad de nuestra cuenta**, desde cambios en la contraseña o en la información de recuperación de la

cuenta, hasta inicios de sesión realizados y si ha habido solicitudes de descarga de nuestros datos (copia de seguridad).

De este modo, siempre estaremos al tanto de cualquier cambio importante que afecte a los parámetros de seguridad.

- **Podremos comprobar en todo momento si parte de esta actividad es sospechosa.** Por ejemplo, ¿has notado algún inicio de sesión en un dispositivo desconocido o un cambio en tu cuenta?

Cuando hagamos clic sobre cualquier actividad que Google considere sospechosa, podremos visualizar una “alerta de seguridad crítica” en forma de etiqueta, y nos preguntará si hemos sido nosotros o por el contrario, se trata de un tercero.

- **Finalmente, nos sirven como herramienta para combatir el [phishing](#),** ya que si a nuestro correo nos llegase cualquier notificación de una actividad sospechosa o alerta de seguridad, podríamos dirigirnos manualmente a este apartado y comprobarlo nosotros mismos, sin hacer clic sobre ningún enlace sospechoso.

**Recomendación:** la seguridad de nuestra cuenta puede verse vulnerada por diversos factores. En ocasiones, puede ser un ataque a nuestras contraseñas o a raíz de un engaño basado en la [ingeniería social](#). Los mecanismos de protección de Google nos alertarán siempre que detecten un inicio de sesión desde un dispositivo o navegador nuevo y desconocido para que lo comprobemos y llevemos a cabo las acciones preventivas necesarias, como un cambio de contraseña, revisar desde donde se han conectado, etc. Sin embargo, si no realizamos ninguna comprobación, nos exponemos al robo de nuestra cuenta y los datos contenidos en ella.

Cualquier actividad que veamos destacada, deberemos de prestarle unos minutos de nuestro tiempo para comprobar que hemos sido nosotros los autores y así, evitar sustos, como la modificación de nuestros datos o información de recuperación de la cuenta, pagos sin nuestro consentimiento, etc.

## 5.8. Diapositiva 11. Iniciar sesión en Google

¿Qué métodos utilizas para proteger el inicio de sesión de tu cuenta de Google? En este bloque encontrarás algunas herramientas con las que añadir una capa extra de seguridad a la cuenta. Veámoslas:

- **[Contraseña](#):** el requisito mínimo para proteger tu cuenta. Desde aquí podremos comprobar la última vez que actualizamos la contraseña y cambiarla. Es importante hacerlo cada cierto tiempo (3 meses aprox.)
- **[Usar tu teléfono para iniciar sesión](#):** nos permitirá utilizar nuestro teléfono móvil en lugar de la contraseña. Necesitaremos seleccionar nuestro dispositivo personal y asegurarnos de que disponemos de un bloqueo de pantalla. Una notificación nos llegará al móvil y, tras pulsar Sí, podremos acceder a nuestra cuenta.
- **[Verificación en dos pasos](#):** esta función añade una capa adicional de seguridad al requerirnos un código de verificación cada vez que queramos iniciar sesión en nuestra cuenta. Primero deberemos elegir el dispositivo donde queremos recibir el código y luego, tras recibirlo por SMS, introducirlo para poder iniciar sesión.

**Recomendación:** la mayoría de cuentas que terminan siendo robadas son por una mala gestión de su seguridad. Ya sean de Google, redes sociales o de cualquier servicio, si no

se protegen con una contraseña robusta y otros mecanismos de seguridad, es muy probable que su seguridad acabe vulnerada en algún momento.

Por esta razón, debemos asegurarnos de utilizar una contraseña robusta y diferente a la que utilicemos para acceder a cualquier otro servicio online. Y por supuesto, actualizarla cada cierto tiempo (3-6 meses dependiendo de la información que contengan).

Además, es fundamental que vinculemos otros mecanismos de autenticación, como son la verificación en dos pasos con nuestro dispositivo móvil o el uso del mismo para iniciar sesión, de modo que involucremos otro dispositivo en el proceso de inicio de sesión.

## 5.9. Diapositiva 12. Métodos para verificar tu identidad

En este bloque se nos muestran distintas opciones mediante las cuales Google puede tratar de comprobar nuestra identidad cuando detecte alguna actividad sospechosa.

Tanto el [teléfono](#), como el [correo electrónico de recuperación](#) que indiquemos nos servirán para recibir notificaciones de Google en caso de cualquier actividad inusual y para recuperar nuestra cuenta por un bloqueo accidental o no recordar nuestra contraseña, por ejemplo.

**Recomendación:** perder nuestra cuenta a manos de un tercero, o simplemente olvidarnos de la contraseña y no ser capaz de recuperarla puede suponer un problema serio, por ejemplo, perder información privada almacenada en nuestros servicios al no poder acceder a ellos o ser víctimas de una suplantación de identidad al no poder recuperar el control de la misma.

Para evitar este tipo de situaciones, podemos configurar ambos mecanismos de verificación (móvil y correo electrónico) desde el menú de opciones de nuestra cuenta de Google, dentro de los métodos para verificar nuestra identidad.

## 5.10. Diapositiva 13-14. Tus dispositivos

**¿Somos conscientes de todos los dispositivos donde hemos iniciado sesión con nuestra cuenta de Google?**

Cuando hacemos clic en [Gestionar dispositivos](#), veremos una lista desde la que podremos obtener más detalles sobre este asunto, como la fecha y ubicación desde donde se inició la sesión en un momento dado o los navegadores utilizados. Y, por supuesto, si hacemos clic en los tres puntos junto al dispositivo, podremos cerrar la sesión en aquellos que ya no utilizemos o nos resulten desconocidos.

**Recomendación:** además de nuestros dispositivos habituales, en ocasiones revisamos nuestro correo o hacemos búsquedas desde otros dispositivos con la sesión abierta. Este tipo de prácticas hay que hacerlas con cuidado, ya que corremos el riesgo de dejar nuestra sesión abierta por descuido, a merced de cualquiera.

Para evitarlo, es recomendable que revisemos este apartado cada cierto tiempo, y revisemos en cuantos dispositivos hemos iniciado sesión. Así, podremos cerrarla en aquellos dispositivos desconocidos o que hace tiempo que no utilizamos e identificar posibles inicios de sesión no deseados o que dejamos abiertos por error.

## 5.11. Diapositiva 15-16. Buscar un dispositivo perdido



Otra función muy interesante que encontraremos en **Tus dispositivos** es la de [Buscar un dispositivo perdido](#).

Tras seleccionarla, y hacer clic sobre uno cualquiera de la lista, veremos su ubicación o la red a la que está conectado entre otros datos, y podremos llevar a cabo las siguientes acciones:

- **Reproducir sonido:** nos ayudará a localizar el dispositivo perdido, aunque esté en modo silencio.
- **Bloquear dispositivo:** Si nos han robado el dispositivo o no podemos encontrarlo, esta opción lo bloqueará y cerrará la sesión de nuestra cuenta para evitar que terceros puedan acceder a él y a su información.
- **Borrar datos del dispositivo:** eliminará definitivamente todos los datos del teléfono. En el caso de encontrarlo después de haberlo hecho, necesitaremos utilizar la contraseña de Google para volver a utilizarlo.

**Recomendación:** en ocasiones, podremos extraviar alguno de nuestros dispositivos. En estos casos, podremos recurrir a la función de Reproducir sonido para tratar de localizarlo. Sin embargo, en el peor de los casos el dispositivo puede no aparecer o haber sido robado y nuestra privacidad y seguridad estar en peligro.

En estos casos, lo más recomendable es que nos aseguremos de bloquearlo y, para mayor seguridad, borremos toda la información almacenada en él desde la opción Borrar datos del dispositivo. De este modo, aunque consiguieran acceso, nuestra información seguiría estando a salvo al no estar disponible.

## 5.12. Diapositiva 17-20. Aplicaciones de terceros con acceso a la cuenta

Cuando instalamos una aplicación en nuestro dispositivo, a la vez estamos concediéndole ciertos permisos con los que podrá acceder a algunos aspectos datos de nuestra cuenta de Google.

Desde este apartado podremos gestionar, no solo las aplicaciones instaladas y los permisos otorgados sino también los que hemos concedido a otros servicios. Para ello, deberemos hacer clic en [Gestionar el acceso](#), donde veremos varias listas de aplicaciones y servicios:

- **Aplicaciones de terceros con acceso a la cuenta:** aquí se muestran todas las apps que tenemos instaladas en cualquiera de nuestros dispositivos donde hayamos iniciado sesión. Si hacemos clic en alguna de ellas, veremos:
  - La información a la que tiene acceso y los permisos otorgados.
  - Su página dentro de Google Play.
  - Cuando se instaló y se le concedieron los permisos.
  - Y, en casos de sospecha, podemos retirarle el acceso a estos permisos y denunciarla.
- **Iniciar sesión con Google:** se trata de los sitios web y servicios online donde nos hemos registrado con nuestra cuenta de Google. Y, al igual que con las aplicaciones, si hacemos clic sobre ellos veremos:
  - Los permisos que tienen y la información a la que tienen acceso.
  - La página web principal y cuándo se concedieron estos permisos.
  - Y, en caso de sospecha, también podemos retirarle el acceso.

- **Aplicaciones de Google:** son las apps y servicios de Google que hemos instalado en nuestros dispositivos. Las opciones a las que tenemos acceso cuando hacemos clic en ellas son las mismas que en los casos anteriores.

**Recomendación:** cuando descargamos una aplicación en nuestros dispositivos móviles debemos aceptar una serie de permisos para que funcione correctamente. Lamentablemente algunas apps pueden tratar de aprovecharse de esos permisos para obtener control sobre nuestro dispositivo o acceder a información personal, como contactos, fotografías, conversaciones, etc. de manera no justificada. A través de [Google Play Protect](#) puedes proteger tu dispositivo contra aplicaciones dañinas. Esta herramienta verifica las aplicaciones una vez instaladas, y analiza tu dispositivo de forma periódica.

La seguridad de nuestra cuenta también depende del tiempo que dediquemos a revisar lo que hemos instalado en nuestros dispositivos y los permisos que hemos dado. Por eso es importante dedicar unos minutos a revisar este apartado y gestionar las apps instaladas para evitar convertirnos en víctimas de alguna app maliciosa.

### 5.13. Diapositiva 21. Acceso a aplicaciones poco seguras

En ocasiones, los usuarios descargamos aplicaciones desde sitios no oficiales, lo que puede suponer un riesgo para nuestra seguridad. Por ello, Google cuenta con la opción para [permitir o bloquear las aplicaciones y/o dispositivos que puedan vulnerar nuestra cuenta](#).

**Recomendación:** algunos dispositivos y/o aplicaciones utilizan sistemas de inicio de sesión poco seguro o requieren permisos abusivos que pueden poner en peligro la seguridad de nuestro dispositivo. Los usuarios debemos ser precavidos a la hora de descargar aplicaciones desde otras fuentes no fiables, ya que, que si una aplicación o un sitio no cumplen con los estándares de seguridad, Google podría bloquear a cualquier persona que intente iniciar sesión en su cuenta.

Cómo medida de protección adicional, la función de bloquear el acceso a aplicaciones poco seguras impedirá la instalación y, por lo tanto, el acceso a nuestra información de este tipo de aplicaciones. Las aplicaciones menos seguras pueden facilitar que los ciberdelincuentes accedan a nuestra cuenta, por lo que bloquear los inicios de sesión desde estas aplicaciones ayuda a mantener tu cuenta segura.

Por otro lado, si queremos probar alguna app en desarrollo, o estamos convencidos de que es segura aunque provenga de otra fuente distinta a Google Play, podremos activarla e instalarla en nuestro dispositivo, aunque siempre bajo nuestra responsabilidad.

### 5.14. Diapositiva 22. Iniciar sesión con Google en otros sitios web

Desde este bloque podemos acceder a las opciones que ya hemos visto sobre los [sitios web y servicios donde hemos utilizado nuestra cuenta de Google para iniciar sesión](#).

Pero también podemos acceder a otras opciones, como el **gestor de contraseñas** o las **cuentas de terceros vinculadas**. A continuación veremos más en detalle estas dos últimas opciones.



## 5.15. Diapositiva 23. Gestor de contraseñas

Cuando utilizamos el navegador Google Chrome e iniciamos sesión en alguna web o servicio, nos preguntará si queremos guardar las credenciales para autorellenarlas la próxima vez que accedamos.

Para poder gestionarlas, Google pone a nuestra disposición su propio [Gestor de contraseñas](#), una forma segura de proteger todas tus cuentas online, donde nos encontraremos con varias opciones:

- **Revisión de contraseñas:** revisará las credenciales que tengamos almacenadas y serán cotejadas con las que hayan sido expuestas en alguna fuga de información de datos de terceros para que las cambiemos de inmediato en caso de ser así. También nos informará de claves repetidas o poco seguras.
- **Sitios web y aplicaciones:** es una lista con todas las credenciales que hemos almacenado. Cuando hagamos clic en cualquiera de ellas, podremos modificarlas (cambiar contraseña), comprobar el usuario y la clave almacenada, así como eliminar la cuenta.

**Recomendación:** nuestras contraseñas son uno de los objetivos principales de los ciberdelincuentes. Además, los usuarios no solemos prestarles la suficiente atención y cometemos varios errores relacionados con ellas, como utilizar claves poco seguras, usar la misma en diferentes cuentas y servicios online y no cambiarlas. Guardar nuestras credenciales en el navegador, puede conllevar el riesgo de que acaben en malas manos si por ejemplo, el navegador es utilizado por varias personas (equipo familiar, ordenadores públicos, etc.).

Las defensas automatizadas de Google protegen nuestras contraseñas guardadas de forma ininterrumpida, avisando de si un sitio donde tengamos una contraseña guardada ha sido vulnerado. Además, aunque un atacante consiga nuestra contraseña, la gran mayoría de los intentos sospechosos de acceso a tu cuenta de Google se bloquearán. Todas las contraseñas que guardemos siguen siendo privadas, solo se utilizarán para ayudarnos a iniciar sesión más fácilmente y para mantener la seguridad de nuestras cuentas.

En el caso de mantener todas nuestras credenciales almacenadas en nuestra cuenta de Google, podremos utilizar el gestor de contraseñas. Pero asegurándonos de que nuestra cuenta dispone de todas las medidas de seguridad que Google pone a nuestra disposición, como las que hemos mencionado.

## 5.16. Diapositiva 24. Cuentas vinculadas

En ocasiones, cuando nos registramos en un servicio o web es posible utilizar nuestra cuenta de Google para hacerlo. En estos casos, lo que hacemos es utilizar la [cuenta de Google como medio de autenticación con la web](#) y, a cambio, la web puede tener acceso a determinados datos de nuestra cuenta. Antes de que se compartan los datos, podrás decidir si Google otorgará acceso a tu cuenta de terceros.

En este apartado podemos gestionar las cuentas que hemos creado utilizando este sistema y desvincularlas. Esta acción eliminará nuestra cuenta y dejaremos de compartir información con el servicio en cuestión.

**Recomendación:** utilizar nuestra cuenta de Google para que acceda y autentique nuestra identidad en otros servicios es una función muy cómoda para evitar crearnos una cuenta

nueva cada vez que nos registremos en un servicio online. Al hacerlo tenemos la opción de decidir si parte de nuestra información es compartida con estos servicios y viceversa.

Si estamos seguros de que queremos hacerlo, y que el servicio es fiable y de confianza, no supone ningún problema. Eso sí, es fundamental que previamente hayamos llevado a cabo todas las configuraciones de seguridad de nuestra cuenta para asegurarnos de no estar compartiendo más información de la necesaria.

## 5.17. Diapositiva 25. Pagos y suscripciones

Toda la información recogida en nuestra cuenta de Google sobre los métodos de pago utilizados y el histórico de pagos realizados desde nuestra cuenta y otros servicios de Google se encuentra en este apartado.

Vamos a verlo detenidamente a continuación.

## 5.18. Diapositiva 26. Métodos de pago

Cuando queremos realizar un pago haciendo uso del servicio de Google Pay tendremos que configurar un [método de pago](#) en nuestra cuenta, como una tarjeta bancaria o un servicio de plataforma de pago como PayPal. Datos que se sincronizarán con nuestro móvil, para realizar [pagos a través de nuestro smartphone](#).

Cuando seleccionemos **Gestionar métodos de pago**, accederemos al menú desde donde **añadir, eliminar o editar los métodos de pago** almacenados. Es un proceso sencillo, sólo hay que seguir las indicaciones que facilita Google para ello.

**Recomendación:** guardar la información de nuestras tarjetas bancarias dentro de nuestra cuenta de Google y utilizarlas para realizar pagos online es una función muy útil y cómoda. Google Pay envía un número de cuenta virtual al comerciante, por lo que nuestra información de pago siempre permanece segura y privada. En cualquier caso, si es posible, se recomienda configurar tarjetas virtuales o recargables que muchos bancos proporcionan para utilizarlas a través de este tipo de servicios.

## 5.19. Diapositiva 27-30. Experiencia de Google Pay

Cada vez que utilizamos la aplicación de Google Pay, realizamos una compra online o ingresamos un nuevo método de pago, se crea un registro dentro de nuestra cuenta. Esta información puede ser analizada por Google para personalizar nuestra experiencia, recomendándonos productos acorde a nuestros intereses, por ejemplo.

Si hacemos clic en **Gestionar experiencia**, accederemos a las opciones de configuración de **Gestiona tu experiencia de Google Pay**:

- **Personalización en Google Pay:** al activarlo, permitiremos a Google analizar los datos que guardamos (transacciones, tarjetas, ubicación desde donde compramos...) para ofrecernos una experiencia más personalizada. En el modo desactivado seguirán almacenándose, pero Google no utilizará esa información.  
Dentro, podremos acceder al registro de transacciones y pagos realizados, gestionar los métodos de pago y realizar ajustes de configuración dentro de la aplicación de Google Pay.
- **Perfil de pagos:** esta opción nos llevará de vuelta a los métodos de pago almacenados en nuestra cuenta. El apartado que hemos detallado en la diapositiva anterior.

- **Transacciones y actividad de pagos:** desde aquí podremos observar un resumen de nuestras últimas transacciones con Google Pay, pudiendo eliminar todo el registro o, mediante el desplegable, aplicar un filtro para eliminar solo la actividad del último mes, por ejemplo.

**Recomendación:** como en muchas otras funciones de Google, toda la información almacenada y recogida sirve para ofrecernos una experiencia más personalizada y siempre, podremos configurarla según nuestras necesidades. Si nos gusta recibir ofertas, anuncios y promociones adaptadas a nuestros hábitos como consumidor de la mano de Google, es probable que nos interese activar la opción de Personalización en Google Pay. Si por el contrario no queremos que esta información sea utilizada para una experiencia personalizada, simplemente tendremos que desactivarla. Siempre dispondremos de la posibilidad de elegir qué información compartir con Google de cara a personalizar nuestra experiencia. Google nunca compartirá con terceros nuestra información personal y siempre la protegerá con las tecnologías más avanzadas.

## 5.20. Diapositiva 31. Compras, suscripciones y reservas

Ya hemos comentado previamente que Google guarda un registro de toda nuestra actividad vinculada a nuestros pagos y actividades relacionadas con Google Pay. Desde estos tres bloques podremos acceder al registro de todas nuestras compras, suscripciones y reservas realizadas desde nuestra cuenta.

Al hacer clic en cualquiera de los enlaces de **Gestionar compra**, **Gestionar suscripciones** o **Gestionar reservas** podremos revisar cuando fue realizada, qué método de pago se utilizó, el precio, etc.

**Recomendación:** al igual que ocurre con los inicios de sesión y la actividad sospechosa, el registro de nuestra actividad de Google Pay puede servirnos para alertarnos sobre movimientos bancarios realizados sin nuestro consentimiento. Puede que estemos registrados a una suscripción de la que no seamos conscientes, o que se hayan realizado pequeños pagos a lo largo de un periodo de tiempo determinado del que tampoco seamos conscientes.

Para asegurarnos de que nuestra cuenta sigue siendo segura, es recomendable que, cada vez que realicemos un pago a través de la aplicación o periódicamente, revisemos el registro de nuestra actividad para asegurarnos de que no haya ninguna transacción sospechosa. Y, en caso de detectarla, deberemos ponernos en contacto con nuestro banco para cancelar dicha transacción, cambiar la contraseña de nuestra cuenta de Google, revisar los métodos de pago y, finalmente, llevar a cabo todas las configuraciones de seguridad que hemos visto a lo largo de este taller.

## 1.1. Diapositiva 32. Cuestionario de evaluación 1

1. Para proteger aún más la seguridad de nuestra cuenta, podemos añadir la necesidad de incluir un código de verificación cada vez que iniciemos sesión. Esta función se conoce como:

- a) Verificación en dos pasos.
- b) Contraseña doble.
- c) Código de recuperación.

Feedback: La respuesta correcta es la a) Verificación en dos pasos. Esta función añade una capa adicional de seguridad al requerirnos un código de verificación cada vez que queramos iniciar sesión en nuestra cuenta. Primero deberemos elegir el dispositivo donde queremos recibir el código y luego, tras recibirlo por SMS, introducirlo para poder iniciar sesión.

## 1.2. Diapositiva 33. Cuestionario de evaluación 2

2. En el caso de perder nuestro dispositivo, disponemos de la opción Buscar mi dispositivo. ¿Qué funciones nos ofrece este servicio?

- a) Emitir un sonido para localizarlo.
- b) Bloquear nuestro dispositivo.
- c) Ambas opciones son correctas.

Feedback: La respuesta correcta es la c) Ambas opciones son correctas. Además de estas opciones para localizar o proteger la información almacenada, podremos borrar todos los datos de nuestro dispositivo para evitar que caiga en malas manos.

## 1.3. Diapositiva 34. Cuestionario de evaluación 3

3. Si queremos comprobar los permisos que hemos concedido a una aplicación que hayamos instalado en nuestro dispositivo, deberemos acceder a:

- a) Acceso a aplicaciones poco seguras.
- b) Aplicaciones de terceros con acceso a la cuenta.
- c) Cuentas vinculadas.

Feedback: La respuesta correcta es la b) Aplicaciones de terceros con acceso a la cuenta. Desde este apartado podremos acceder a mucha información sobre la aplicación, como los permisos concedidos y la información que compartimos con ella, la fecha en la que la instalamos, así como la página de la tienda o la función de eliminar los permisos concedidos.

## 1.4. Diapositiva 35. Cuestionario de evaluación 4

4. Activar la personalización de la experiencia en Google Pay significa que:

- a) Google podrá compartir nuestros datos con terceros para ofrecernos publicidad personalizada.
- b) Google podrá analizar nuestros datos para ofrecernos ofertas acorde a nuestra actividad, pudiendo el usuario gestionar la configuración de privacidad.
- c) Google almacenará, pero no utilizará la información referente a nuestras compras.

Feedback: La respuesta correcta es la b) Google podrá analizar nuestros datos para ofrecernos ofertas acorde a nuestra actividad. Si desactivamos esta opción, Google podrá almacenar dicha información pero no la analizará ni hará uso de ella, y mucho menos la compartirá con terceros.

## 1.5. Diapositiva 36. Cuestionario de evaluación 5

5. En el caso de que realicemos pagos con nuestro dispositivo móvil o a través de los servicios de Google, lo más recomendable es:

- a) Almacenar todos los datos de nuestras tarjetas y cuentas bancarias.
- b) Almacenar los datos de una tarjeta virtual.
- c) Almacenar los datos de una de nuestras tarjetas de crédito.

Feedback: La respuesta correcta es la b) Almacenar los datos de una tarjeta virtual. Lo más recomendable es que utilicemos los datos de alguna tarjeta virtual para realizar nuestras compras y minimizar posibles riesgos. Google siempre mantiene nuestros datos privados, y solo facilita un número de cuenta virtual al comerciante en lugar de la tarjeta real, siendo segura siempre nuestra información de pago.

## **5.21. Diapositiva 37. Turno de preguntas y respuestas**

Espacio destinado a resolver las dudas de los participantes del taller y profundizar en aquellos puntos que hayan generado inquietudes.

## **5.22. Diapositiva 38. Final del taller**

¡Gracias por vuestra atención!

## ANEXO

---

### RECURSOS PARA AMPLIAR

Se recomienda la lectura de la siguiente selección de recursos complementarios, por parte del docente:

Recursos de Google:

- [Centro de Seguridad de Google](#)
- [Acceso a tu cuenta de Google.](#)
- [Centro de seguridad y familias de Google.](#)
- [Cómo ayuda Google Pay a mantener tus datos privados.](#)
- [Revisar la actividad relacionada con la seguridad.](#)
- [Iniciar sesión con el teléfono.](#)
- [Google: Verificación en dos pasos.](#)
- [Ver los dispositivos que han usado tu cuenta.](#)
- [Aplicaciones poco seguras y la cuenta de Google.](#)
- [Crear una contraseña segura y proteger mejor la cuenta.](#)

Recursos de la OSI:

- [Guía para aprender a identificar fraudes online](#)
- [Guía de privacidad y seguridad en Internet](#)
- [Guía de ciberataques](#)
- [Guía para configurar el router wifi](#)
- [Los ciberdelincuentes, ¿quiénes son?](#)
- [¡Contraseñas seguras!](#)
- [Ingeniería social: que no te engañen](#)
- [Juegos de mesa sobre ciberseguridad](#)