Google for Education

Más de 40 maneras de usar las ediciones de pago de Google Workspace for Education

goo.gle/use-edu-workspace

Cómo utilizar esta presentación

En esta presentación se recogen algunos casos de los usos más populares que tienes a tu disposición si utilizas alguna de las **ediciones de pago de Google Workspace for Education**. Estas herramientas pueden ayudarte a mejorar **la seguridad de los datos, la eficiencia del personal docente, la implicación del alumnado** y **la colaboración en el centro educativo**, entre otros aspectos.

La presentación está organizada por **funciones**, seguidas de **usos habituales** e **instrucciones** sencillas sobre cómo usar cada una de las funciones. Lee la presentación al completo para ver el amplio abanico de opciones que te ofrecen las ediciones de pago de Google Workspace for Education.

Ediciones de pago de Google Workspace for Education

Disfruta de más opciones, control y flexibilidad para dar respuesta a las necesidades de tu organización con tres ediciones de pago de Google Workspace for Education.

Google Workspace for Education Plus

Incluye Education Standard, Teaching and Learning Upgrade y más funciones exclusivas de Education Plus.

Education Plus ofrece a los alumnos, profesores, responsables educativos y administradores de TI una solución de tecnología educativa **integral** con herramientas fáciles de usar que ofrecen **prestaciones avanzadas de seguridad y estadísticas, así como una experiencia de enseñanza y aprendizaje enriquecida**.

Google Workspace for Education Standard

Incluye herramientas avanzadas de seguridad y estadísticas que ayudan a reducir los riesgos y las amenazas con un mayor nivel de visibilidad y control en todo el entorno de aprendizaje.

Teaching and Learning Upgrade

Las herramientas de enseñanza y aprendizaje mejoradas aumentan la eficacia de la enseñanza al convertir el aprendizaje en un proceso más personalizado. Y esto lo consiguen fomentando tanto la eficiencia en el aula como la posibilidad de enseñar y aprender desde cualquier lugar.

Índice

Funciones avanzadas de seguridad y estadísticas

Panel de control de seguridad

- Volumen de spam
- Compartir archivos externamente
- Aplicaciones de terceros
- Intentos de phishing

Página sobre el estado de seguridad

- Prácticas recomendadas de seguridad
- Recomendaciones para áreas de riesgo

Herramienta de investigación

- Material inadecuado que se comparte
- Archivos compartidos accidentalmente
- Correos de phishing y malware
- Poner freno a agentes perniciosos
- Estadísticas de seguridad más detalladas
- Impedir reuniones no supervisadas

Control y gestión de dominios

- Escanear archivos adjuntos en Gmail para detectar amenazas
- Crear informes y paneles de uso
- Buscar archivos de forma más sencilla
- Organización de documentación interna
- Rellenar automáticamente grupos de departamentos
- Crear audiencias para el sistema interno de archivos compartidos
- Restringir el sistema de archivos compartidos
- Restricciones de las aplicaciones de Workspace
- Gestión del almacenamiento
- Reglamentos en materia de datos
- Bases reguladoras de las becas
- Gestionar dispositivos endpoint
- Gestionar dispositivos Windows
- Configuración personalizada para dispositivos Windows
- Automatización de las actualizaciones de dispositivos Windows
- Uso del cifrado del lado del cliente

Índice

Mejora de las capacidades de enseñanza y aprendizaje

Google Classroom

- Gestión del acceso a los complementos de Classroom
- Incluir contenido interesante en Classroom
- Crear clases a gran escala

Informes de originalidad

- Detectar los plagios con informes de originalidad
- Comprobar la originalidad con ayuda de los trabajos de antiguos alumnos
- Transformar la detección de plagio en oportunidades de aprendizaje

Documentos, Hojas de cálculo y Presentaciones

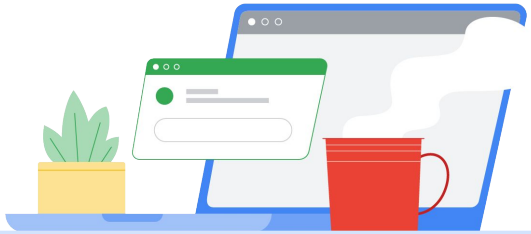
- Aprobar documentos internos

Google Meet

- Grabar reuniones
- Transcribir lo que se ha tratado en clase
- Eliminar la barrera del idioma
- Emitir asambleas y eventos escolares
- Hacer preguntas
- Recopilar comentarios
- Clases en grupos reducidos
- Registrar asistencias

Funciones avanzadas de seguridad y estadísticas

Disfruta de un mayor control en tu dominio gracias a las herramientas de seguridad proactivas que defienden tu organización frente a amenazas, analizan los incidentes de seguridad y protegen los datos de alumnos y profesores.

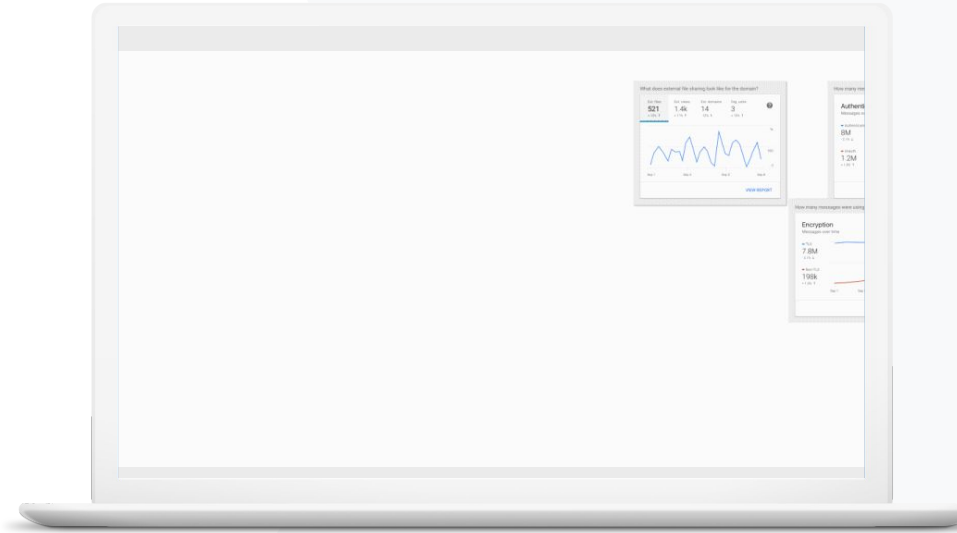


- Panel de control de seguridad
- Página sobre el estado de la seguridad
- Herramienta de investigación
- Control y gestión de dominios

Panel de seguridad

¿Qué es?

El panel de seguridad muestra una vista general de los diferentes informes de seguridad. De forma predeterminada, en el panel de control de cada uno de estos informes se ofrecen datos de los últimos siete días, pero puedes personalizarlos para que muestren los datos de otros periodos, como hoy, ayer, esta semana, la semana pasada, este mes, el mes pasado o días anteriores (hasta 180 días antes).



Casos prácticos

Volumen de spam	Instrucciones paso a paso
Compartir archivos externamente	Instrucciones paso a paso
Aplicaciones de terceros	Instrucciones paso a paso
Intentos de phishing	Instrucciones paso a paso

Quiero controlar el volumen excesivo de correos innecesarios y reducir las amenazas de seguridad en mi centro educativo”.

Volumen de spam

El **panel de control de seguridad** te ofrece una representación visual de la actividad en tu entorno de Google Workspace for Education, que incluye:

- Spam
- Phishing
- Malware
- Archivos adjuntos sospechosos
- Y otros

Instrucciones paso a paso

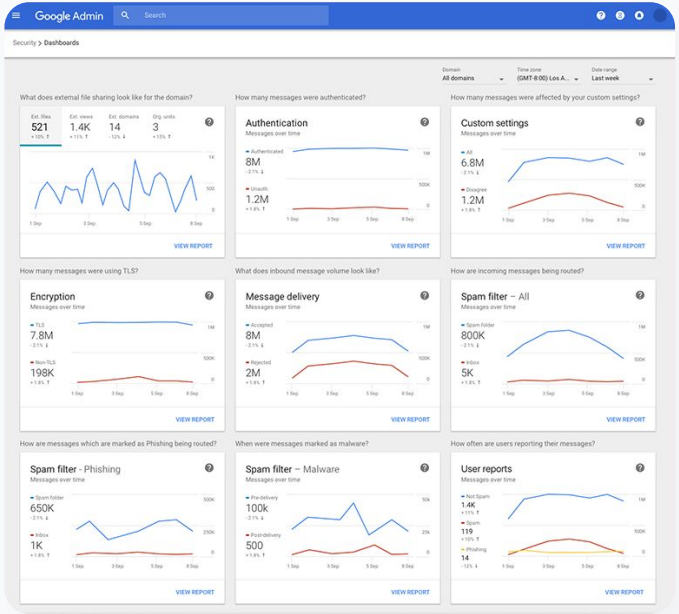
Documentación relacionada del Centro de Ayuda

- Acerca del panel de control de seguridad

Instrucciones: vista general del panel de control

Cómo visualizar el panel de control de seguridad

- Inicia sesión en tu **consola de administración**.
- Haz clic en **Seguridad** > **Panel de control**.
- En el panel de control de seguridad puedes analizar los datos, exportarlos a Hojas de cálculo o a herramientas de terceros, o iniciar una investigación en la herramienta de investigación.



Documentación relacionada del Centro de Ayuda

- Acerca del panel de control de seguridad

Quiero ver la actividad de los archivos compartidos externamente para impedir que los datos sensibles se compartan con terceros”.

Compartir archivos externamente

Con el **informe "Visibilidad de archivos"** del **panel de control de seguridad** puedes consultar métricas de los archivos compartidos externamente en tu dominio, como las siguientes:

- Número de eventos de uso compartido con usuarios ajenos a tu dominio durante un periodo concreto.
- Número de visualizaciones que ha recibido un archivo externo durante un periodo determinado.

Instrucciones paso a paso

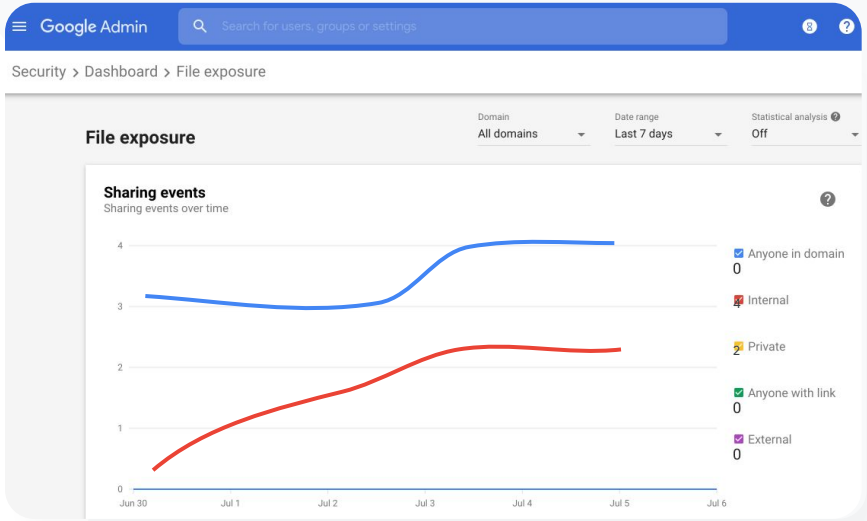
Documentación relacionada del Centro de Ayuda

- Introducción a la página Estado de seguridad

Instrucciones: compartir archivos externamente

Cómo consultar el informe “Visibilidad de archivos”

- Inicia sesión en tu **consola de administración**.
- Haz clic en **Seguridad** > **Panel de control**.
- En la esquina inferior derecha del panel **¿Qué elementos se comparten con usuarios externos al dominio?**, haz clic en **Ver informe**.



Documentación relacionada del Centro de Ayuda

- Acerca del panel de control de seguridad
- Informe "Visibilidad de archivos"

Aplicaciones de terceros

Quiero ver qué aplicaciones de terceros tienen acceso a los datos de mi dominio".

Con el **informe "Actividad de Autenticación OAuth"** del **panel de control de seguridad** puedes monitorizar qué aplicaciones de terceros están conectadas a tu dominio y a qué datos tienen acceso.

- OAuth permite que servicios de terceros accedan a la información de las cuentas de los usuarios sin exponer sus contraseñas. También puedes limitar qué aplicaciones de terceros tienen acceso.
- Usa el panel de actividad de Autenticación OAuth para monitorizar la actividad de autenticación por aplicación, permiso o usuario, así como para actualizar los permisos de autenticación.

Instrucciones paso a paso

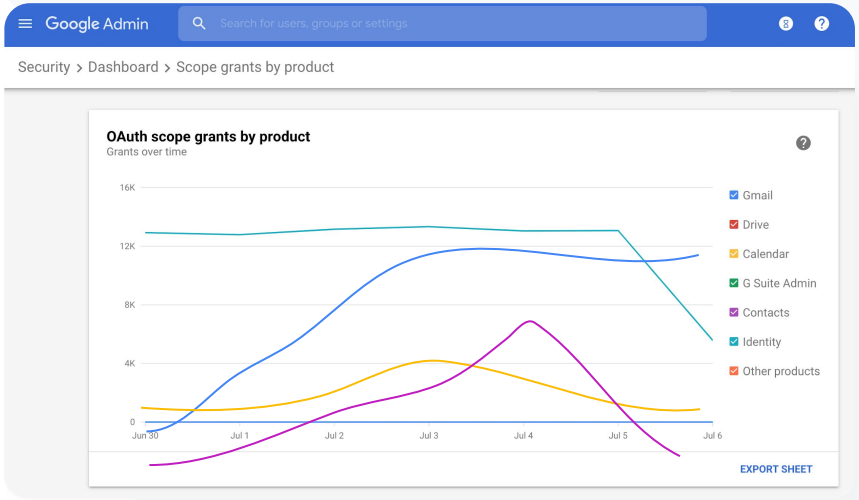
Documentación relacionada del Centro de Ayuda

- Informe "Actividad de Autenticación OAuth"

Instrucciones: aplicaciones de terceros

Cómo consultar el informe “Actividad de Autenticación OAuth”

- Inicia sesión en tu **consola de administración**.
- Haz clic en **Seguridad** > **Panel de control**.
- En la parte inferior, haz clic en **Ver informe**.
- Puedes ver la actividad de Autenticación OAuth por producto (aplicación), permiso o usuario.
- Para filtrar la información, haz clic en **Aplicación**, **Permiso** o **Usuario**.
- Para crear una hoja de cálculo con los datos del informe, haz clic en **Exportar hoja**.



Documentación relacionada del Centro de Ayuda

- Informe "Actividad de Autenticación OAuth"

“Algunos usuarios han denunciado un intento de phishing.
Quiero averiguar cuándo se recibió el correo de phishing, cómo era exactamente ese correo y a qué riesgos estuvieron expuestos los usuarios”.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Cómo marcan los usuarios sus correos electrónicos
- Informe "Clasificaciones de los usuarios"

Intentos de phishing

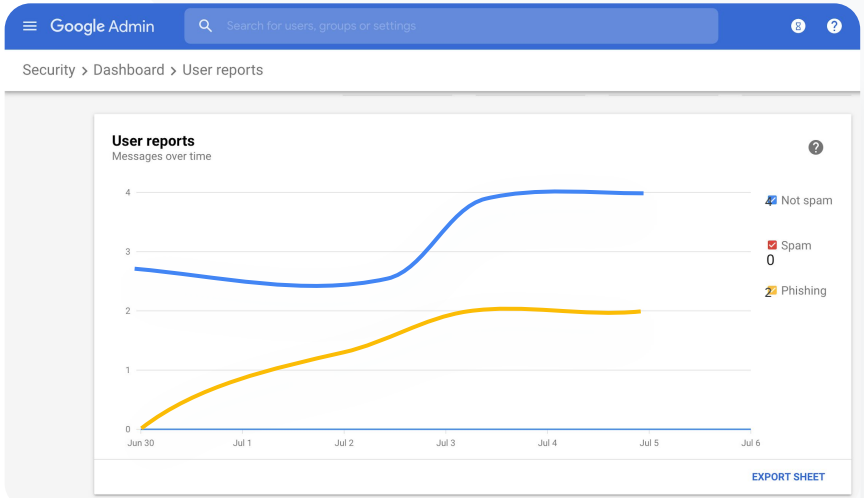
En el **panel Clasificaciones de los usuarios** del **panel de control de seguridad** puedes ver los mensajes que se han marcado como phishing o spam durante un periodo determinado. Por ejemplo, puedes consultar los detalles de los correos marcados como phishing (sus destinatarios, el número de veces que se abrieron, etc.).

- En el informe "Clasificaciones de los usuarios" puedes ver cómo tus usuarios marcan los mensajes (spam, no spam o phishing) y consultar los datos de periodos determinados.
- Puedes personalizar el gráfico para que solo se muestren detalles de determinados tipos de mensajes; por ejemplo, mensajes que se han enviado interna o externamente, en un periodo concreto, etc.

Instrucciones: intentos de phishing

Cómo usar el panel “Clasificaciones de los usuarios”

- Inicia sesión en tu **consola de administración**.
- Haz clic en **Seguridad** > **Panel de control**.
- En la esquina inferior derecha del **panel Clasificaciones de los usuarios**, haz clic en **Ver informe**.



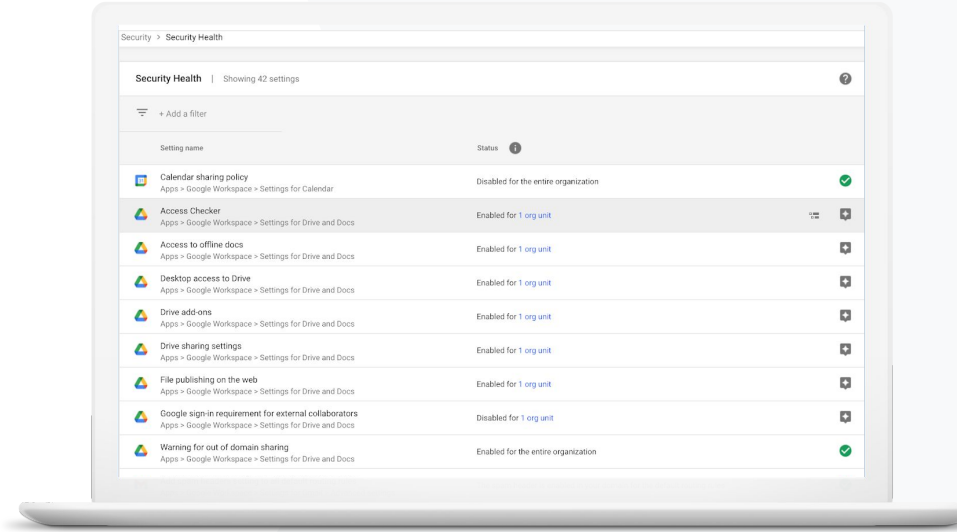
Documentación relacionada del Centro de Ayuda

- Acerca del panel de control de seguridad
- Informe "Visibilidad de archivos"

Estado de seguridad

¿Qué es?

La página sobre el estado de seguridad incluye una completa vista general de la estrategia de seguridad de tu entorno de Google Workspace y te permite comparar tus configuraciones con las recomendaciones de Google para proteger tu organización de forma proactiva.



Casos prácticos

Prácticas recomendadas de seguridad	Instrucciones paso a paso
Recomendaciones para áreas de riesgo	Instrucciones paso a paso

“Me gustaría saber dónde puedo encontrar prácticas recomendadas o sugerencias sobre cómo configurar políticas de seguridad”.

Prácticas recomendadas de seguridad

Abre la página Estado de seguridad para consultar las prácticas recomendadas sobre las políticas de seguridad:

- Recomendaciones para áreas de riesgo potenciales en tu dominio
- Recomendaciones sobre la configuración óptima para aumentar la eficacia de las medidas de seguridad
- Enlaces directos a la configuración
- Información adicional y artículos de ayuda

Instrucciones paso a paso

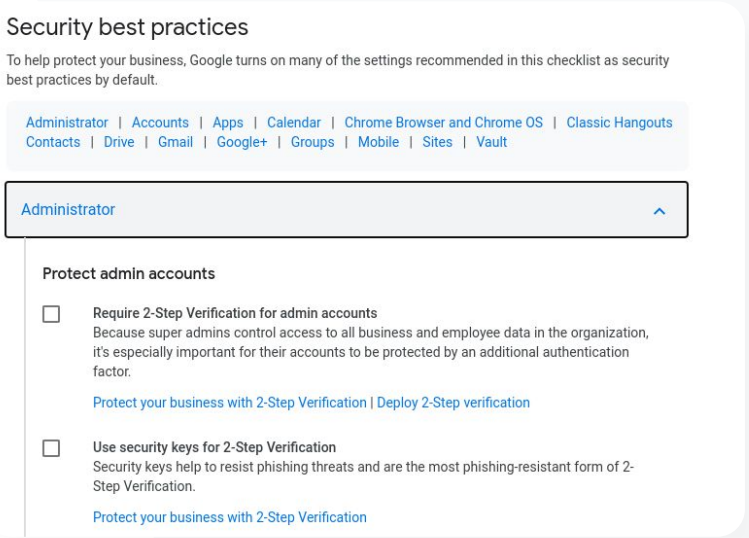
Documentación relacionada del Centro de Ayuda

- Introducción a la página Estado de seguridad

Instrucciones: lista de comprobación de prácticas recomendadas de seguridad

Para proteger tu organización, Google habilita de manera predeterminada muchos de los ajustes recomendados en la lista de comprobación, que forman parte de las prácticas recomendadas en materia de seguridad. Te aconsejamos que prestes especial atención a las que se detallan abajo.

- **Administrador:** proteger cuentas de administrador
- **Cuentas:** ayudar a prevenir y solucionar problemas de vulneración de cuentas
- **Aplicaciones:** revisar el acceso de terceros a los servicios principales
- **Calendar:** limitar el uso compartido de calendarios con usuarios externos
- **Drive:** limitar el uso compartido y la colaboración con usuarios externos al dominio
- **Gmail:** configurar la autenticación y la infraestructura
- **Vault:** controlar, auditar y proteger cuentas de Vault



Documentación relacionada del Centro de Ayuda

- Supervisar el estado de la configuración de seguridad

Quiero poder ver de un vistazo los ajustes de seguridad de mi dominio y recibir recomendaciones útiles para proteger las posibles áreas de riesgo”.

Recomendaciones para áreas de riesgo

En la página **Estado de seguridad** puedes consultar tu configuración de seguridad y ver los cambios recomendados. En esta página puedes:

- Identificar rápidamente las áreas de tu dominio en posible riesgo
- Recibir recomendaciones sobre la configuración óptima para aumentar la eficacia de las medidas de seguridad
- Leer información adicional y artículos de ayuda sobre las recomendaciones

Instrucciones paso a paso

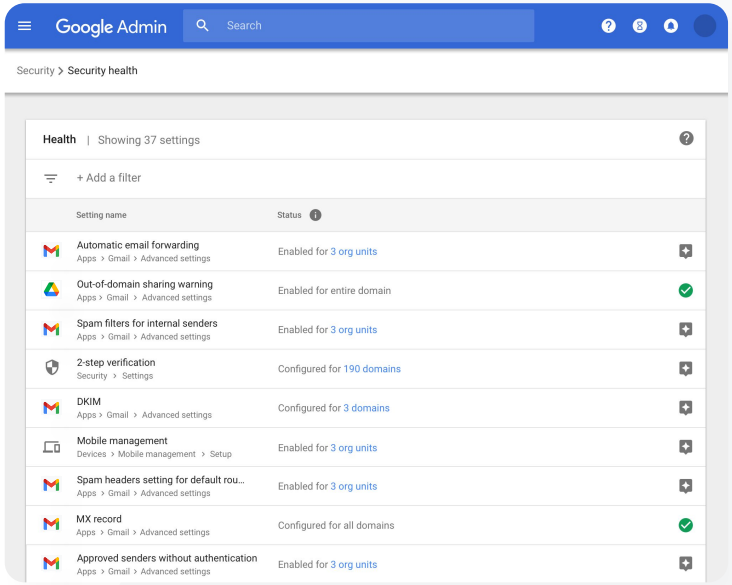
Documentación relacionada del Centro de Ayuda

- Introducción a la página Estado de seguridad

Instrucciones: recomendaciones de seguridad

Cómo ver las recomendaciones

- Inicia sesión en tu **consola de administración**.
- Haz clic en **Seguridad** > **Estado de seguridad**.
- Consulta la configuración de estado en la columna de la derecha.
  - Una marca de verificación verde indica que la configuración es segura
  - Un icono gris indica que hay una recomendación para ese ajuste (haz clic en el icono para ver detalles e instrucciones)



Documentación relacionada del Centro de Ayuda

- Introducción a la página Estado de seguridad

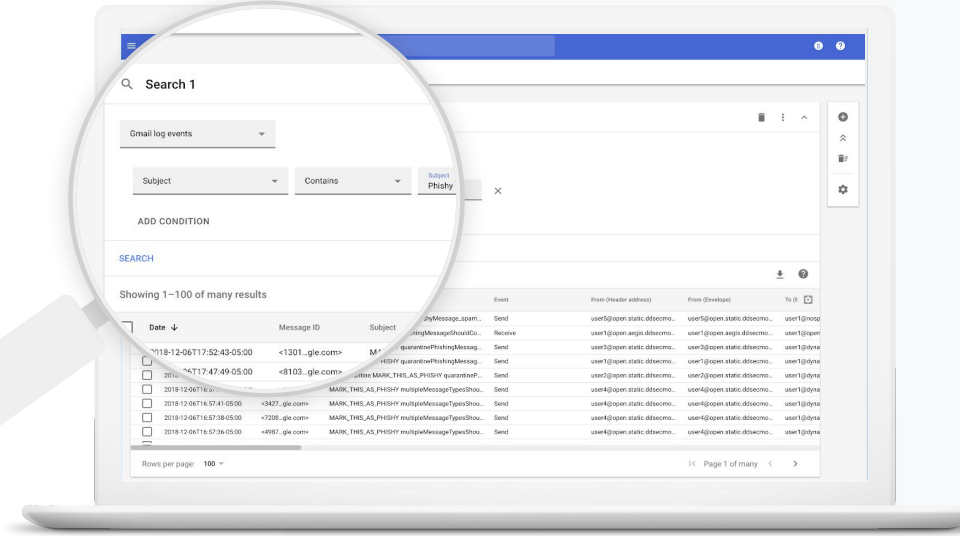
Herramienta de investigación

¿Qué es?

Usa la herramienta de investigación para identificar, clasificar y abordar problemas de seguridad y de privacidad en tu dominio.

Casos prácticos

Material inadecuado que se comparte	Instrucciones paso a paso
Archivos compartidos accidentalmente	Instrucciones paso a paso
Clasificación de correos	Instrucciones paso a paso
Correos de phishing y malware	Instrucciones paso a paso
Poner freno a agentes perniciosos	Instrucciones paso a paso
Estadísticas de seguridad más detalladas	Instrucciones paso a paso
Impedir reuniones no supervisadas	Instrucciones paso a paso



“Sé que se está compartiendo un archivo con material inadecuado. Quiero saber quién lo creó, cuándo lo hizo, quiénes lo compartieron y con quién, quién lo modificó y cómo eliminarlo”.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Condiciones de los eventos de registro de Google Drive
- Acciones con los eventos de registro de Drive

Material inadecuado que se comparte

Los eventos de registro de Drive de la **herramienta de investigación** pueden servirte para encontrar, monitorizar, aislar o eliminar archivos no deseados en tu dominio. Accede a los datos de eventos de registro de Drive para hacer lo siguiente:

- Buscar documentos por nombre, actor, propietario, etc.
- Tomar medidas cambiando los permisos del archivo o eliminándolo
- Buscar el contenido que los usuarios crean en Google Workspace y el contenido que suben a Drive
- Consultar toda la información del registro relacionada con ese documento
  - Fecha de creación
  - A quién pertenece, quién lo ha visto y quién lo ha modificado
  - Fecha en que se compartió

Se ha compartido accidentalmente un archivo con un grupo que NO debería tener acceso a él.

Quiero que esos usuarios dejen de tener acceso al archivo".

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Hacer búsquedas en la herramienta de investigación
- Tomar medidas en función de los resultados de búsqueda

Archivos compartidos accidentalmente

Los eventos de registro de Drive de la **herramienta de investigación** permiten hacer un seguimiento de los problemas con los archivos compartidos y resolverlos. Accede a los datos de eventos de registro de Drive para hacer lo siguiente:

- Buscar documentos por nombre, actor, propietario, etc.
- Consultar toda la información del registro relacionada con el documento, como quién lo ha visto o cuándo se ha compartido
- Tomar medidas cambiando los permisos e inhabilitando las funciones de descarga, impresión y copia

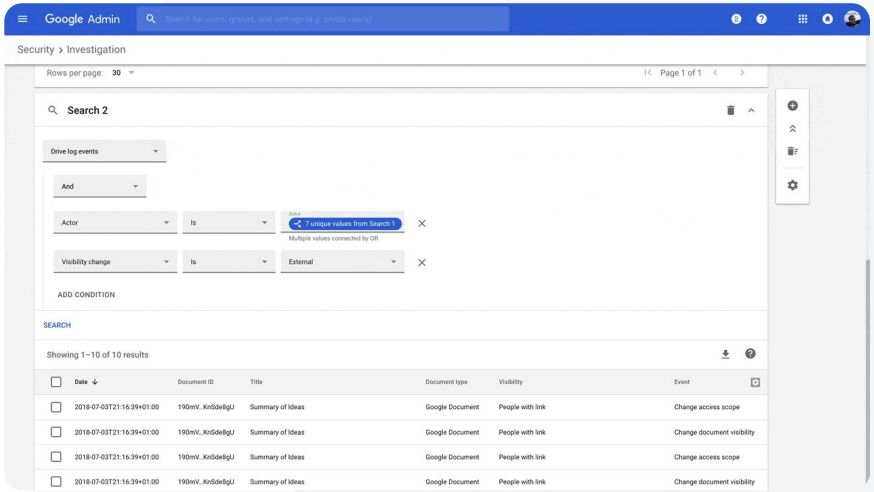
Instrucciones: eventos de registro de Drive

Cómo investigar los eventos de registro de Drive

- Inicia sesión en tu **consola de administración**.
- Haz clic en **Seguridad** > **Herramienta de investigación**.
- Selecciona **Eventos de registro de Drive**.
- Haz clic en **Añadir condición** > **Buscar**.

Cómo tomar medidas

- Selecciona los archivos pertinentes en los resultados de búsqueda.
- Haz clic en **Acciones** > **Auditar permisos de archivos** para abrir la página Permisos.
- Haz clic en **Personas** para ver quién tiene acceso.
- Haz clic en **Enlaces** para ver o modificar las opciones para compartir mediante enlace de los archivos seleccionados.
- Haz clic en **Cambios pendientes** para revisar los cambios antes de guardarlos.



Documentación relacionada del Centro de Ayuda

- Hacer búsquedas en la herramienta de investigación
- Tomar medidas en función de los resultados de búsqueda

“Alguien envió un correo que NO debería haberse enviado. Queremos saber a quién se lo envió, si los destinatarios lo abrieron y si respondieron, y queremos eliminar ese correo. También queremos ver el contenido de ese mensaje”.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Condiciones de los registros de Gmail y de los mensajes de Gmail
- Acciones con mensajes de Gmail y eventos de registro de Gmail
- Pasos para poder ver el contenido de un correo

Clasificación de correos

Los **registros de Gmail** de la **herramienta de investigación** pueden ayudarte a identificar y tomar medidas respecto a los correos peligrosos o inadecuados dentro de tu dominio. Accede a los registros de Gmail para hacer lo siguiente:

- Buscar correos por asunto, ID de mensaje, archivo adjunto, remitente, etc.
- Ver los detalles del mensaje, como el autor, el destinatario y las veces que se ha abierto y reenviado
- Tomar medidas en función de los resultados de búsqueda; por ejemplo, en cuanto a los mensajes de Gmail, puedes eliminarlos, restaurarlos, marcarlos como spam o como phishing, enviarlos a la bandeja de entrada o ponerlos en cuarentena

Correos de phishing y malware

“Se ha enviado un correo de phishing y malware a los usuarios. Queremos saber si han hecho clic en el enlace del correo o si han descargado el archivo adjunto, ya que esto podría poner en riesgo la seguridad de los usuarios y de nuestro dominio”.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Condiciones de los registros de Gmail y de los mensajes de Gmail
- Acciones con mensajes de Gmail y eventos de registro de Gmail
- Pasos para poder ver el contenido de un correo
- Consultar los informes de VirusTotal

La **herramienta de investigación**, y los **registros de Gmail** en particular, pueden ayudarte a identificar y aislar los correos maliciosos que se reciban en tu dominio. Accede a los registros de Gmail para hacer lo siguiente:

- Buscar mensajes de correo por contenido concreto, incluidos los archivos adjuntos
- Ver información sobre correos concretos, como sus destinatarios o las veces que se han abierto
- Ver los mensajes y la conversación para determinar si son maliciosos
- Analizar archivos adjuntos de correos para consultar el contexto detallado de las amenazas y los datos de reputación con informes de VirusTotal
- Tomar medidas (por ejemplo, marcar los mensajes como spam o como phishing, enviarlos a una bandeja de entrada concreta, ponerlos en cuarentena o eliminarlos)

Herramienta de investigación | Herramientas de seguridad y estadísticas

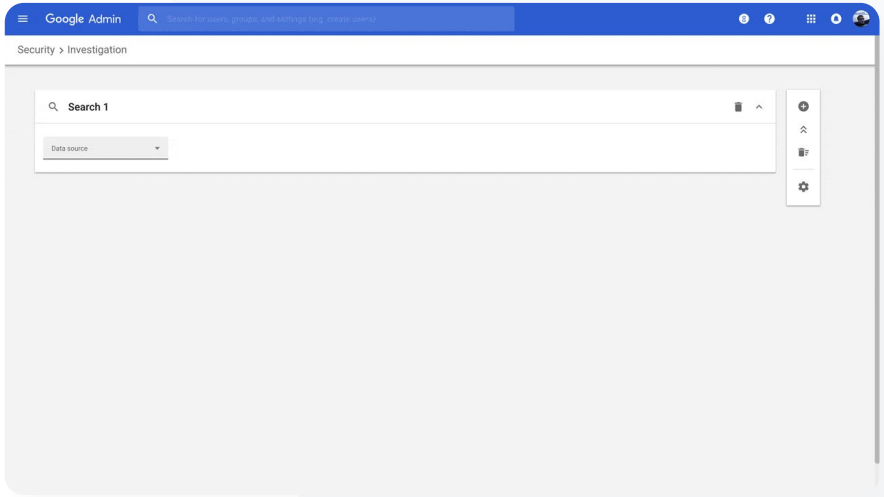
Instrucciones: registros de Gmail

Cómo investigar los registros de Gmail

- Inicia sesión en tu **consola de administración**.
- Haz clic en **Seguridad** > **Herramienta de investigación**.
- Selecciona **Eventos de registro de Gmail** O **Mensajes de Gmail**.
- Haz clic en **Añadir condición** > **Buscar**.

Cómo tomar medidas

- Selecciona los archivos pertinentes en los resultados de búsqueda.
- Haz clic en **Acciones**.
- Selecciona **Eliminar mensaje (De la bandeja de entrada del propietario)**.
- Para confirmar la acción, en la parte inferior de la página, haz clic en Ver.
- En la columna **Resultado** puedes ver el estado de la acción.



Documentación relacionada del Centro de Ayuda

- Condiciones de los registros de Gmail y de los mensajes de Gmail
- Acciones con mensajes de Gmail y eventos de registro de Gmail
- Pasos para poder ver el contenido de un correo

“Un agente pernicioso se dedica a atacar constantemente a usuarios destacados de mi dominio mientras yo trato inútilmente de detenerlo.

¿Qué puedo hacer para pararle los pies?”

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Buscar e investigar eventos de registro de usuarios
- Crear reglas de actividad con la herramienta de investigación

Poner freno a agentes perniciosos

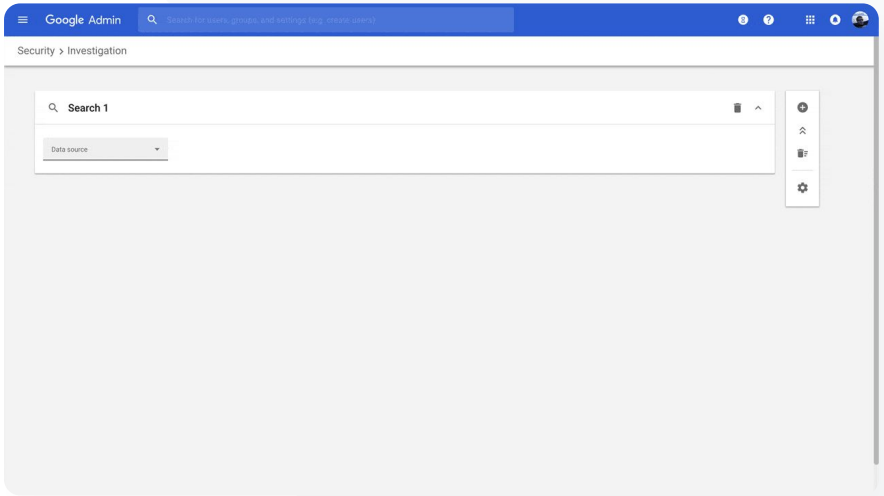
El **registro de usuarios** de la **herramienta de investigación** puede ayudarte a:

- Identificar e investigar los intentos de hackear cuentas de usuarios de tu organización
- Monitorizar qué métodos de verificación en dos pasos usan los usuarios de tu organización
- Obtener más información sobre los intentos fallidos de iniciar sesión realizados por los usuarios de tu organización
- Crear reglas de actividad con la herramienta de investigación: bloquear automáticamente los mensajes y otras actividades maliciosas de personas concretas
- Proteger a usuarios destacados con el Programa de Protección Avanzada
- Restaurar o suspender usuarios

Instrucciones: poner freno a agentes perniciosos

Cómo investigar un evento de registro de usuario

- Inicia sesión en tu **consola de administración**.
- Haz clic en **Seguridad** > **Herramienta de investigación**.
- Selecciona **Eventos de registro de usuarios**.
- Haz clic en **Añadir condición** > **Buscar**.



Cómo restaurar o suspender usuarios

- En los resultados de búsqueda, selecciona a un usuario o a varios.
- Haz clic en el menú desplegable **Acciones**.
- Haz clic en **Restaurar usuario** o en **Suspender usuario**.

Cómo ver los detalles de un usuario concreto

- En la página de resultados de búsqueda, selecciona solo un usuario.
- En el menú desplegable ACCIONES, haz clic en **Ver detalles**.

Documentación relacionada del Centro de Ayuda

- Buscar e investigar eventos de registro de usuarios

Uno de los profesores ha marcado como sospechoso un archivo adjunto de Gmail.

¿Hay alguna forma de que el departamento de TI pueda determinar si el archivo representa una amenaza para la seguridad?”

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Hacer búsquedas en la herramienta de investigación
- Consultar los informes de VirusTotal desde la herramienta de investigación

Obtener estadísticas de seguridad más detalladas

Los informes de VirusTotal amplían la información obtenida a través de los resultados de investigaciones de seguridad. Aportan un resumen completo que permite revisar la seguridad de un dominio, archivo adjunto, dirección IP o URL concretos a partir de datos de crowdsourcing.

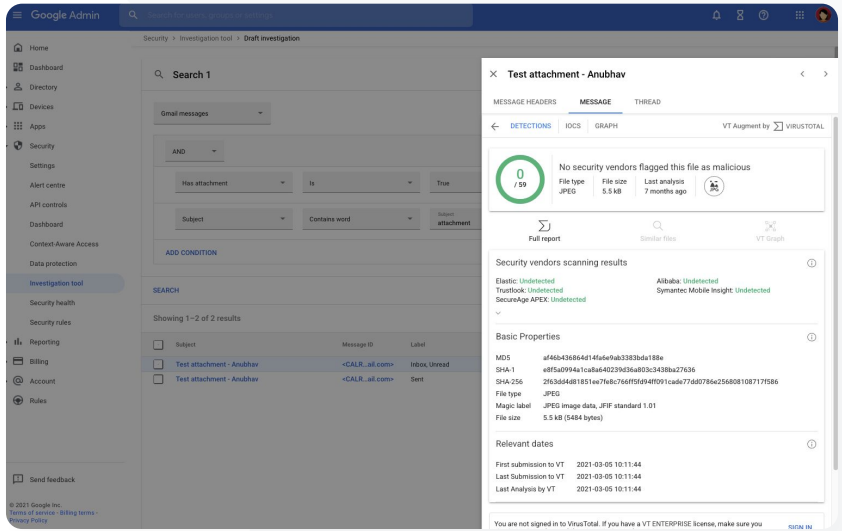
- Obtener más estadísticas de seguridad relacionadas con eventos de registro de Gmail y Chrome
- Analizar archivos, URLs, dominios y direcciones IP sospechosos
- Acceder a información obtenida mediante crowdsourcing sobre los motivos por los que un archivo adjunto o un sitio web pueden considerarse peligrosos
- Obtener ayuda a la hora de tomar decisiones sobre los problemas de seguridad

Herramienta de investigación | Herramientas de seguridad y estadísticas

Instrucciones: obtener estadísticas de seguridad más detalladas

Cómo ver los informes de VirusTotal relacionados con Gmail

- Inicia sesión en tu **consola de administración.**
- Haz clic en **Seguridad** > **Centro de seguridad** > **Herramienta de investigación.**
- Selecciona **Mensajes de Gmail.**
- Haz clic en **Añadir condición** > **Con archivo adjunto.**
- En los resultados de búsqueda, haz clic en el enlace **ID de mensaje** o **Asunto.**
- En el panel lateral, haz clic en la pestaña **Mensaje** o **Conversación.**
- Selecciona **Ver informe de VirusTotal.**



Los administradores también pueden consultar los informes de VirusTotal relacionados con Chrome. Para ello, solo tienen que seguir las instrucciones de arriba y seleccionar **Eventos de registro de Chrome** en la herramienta de investigación.

Documentación relacionada del Centro de Ayuda

- Consultar los informes de VirusTotal desde la herramienta de investigación

“Los alumnos se quedan en las llamadas de Google Meet una vez que la clase ha finalizado. Necesito que las llamadas de Meet finalicen para todos los participantes y evitar interrupciones durante las sesiones de aprendizaje”.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Utilizar la herramienta de investigación para terminar reuniones

Impedir las reuniones virtuales no supervisadas

Los administradores de Google Workspace pueden usar la acción **Terminar la reunión para todo el mundo** de la herramienta de investigación para quitar a todos los usuarios de una reunión de la organización. En las llamadas de Google Meet individuales, los anfitriones de las reuniones también pueden encargarse de hacerlo.

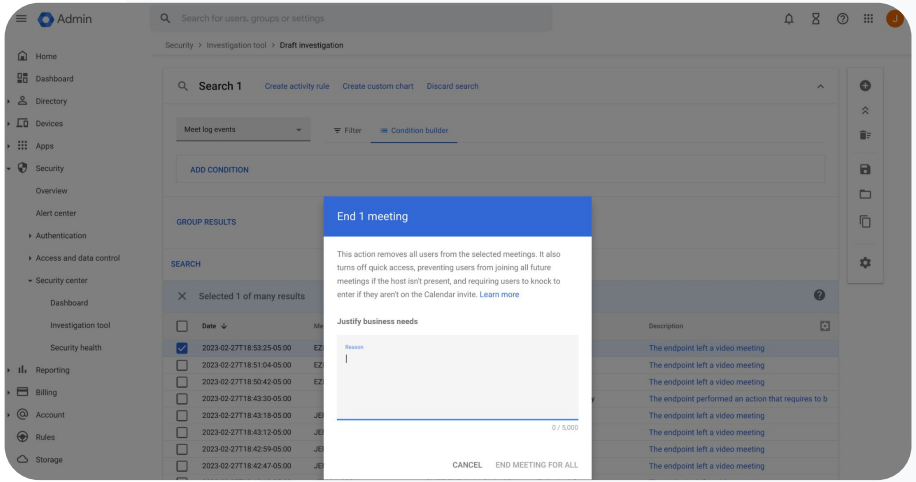
- La reunión terminará para todos los usuarios, incluidos los que estén en grupos de trabajo asociados a ella.
- Se impide que los usuarios asistan a futuras instancias de esa reunión sin que el anfitrión esté presente.

Herramienta de investigación | Herramientas de seguridad y estadísticas

Instrucciones: impedir las reuniones virtuales no supervisadas

Cómo usar la herramienta de investigación para finalizar una reunión para todos los usuarios

- Inicia sesión en tu **consola de administración**.
- Haz clic en **Seguridad** > **Centro de seguridad** > **Herramienta de investigación**.
- Selecciona **Eventos de registro de Meet**.
- Haz clic en **Buscar**. En los resultados de búsqueda, verás una lista de eventos de registro de Meet.
- Marca las casillas de las reuniones que quieras terminar para todos los usuarios.
- Selecciona **Acciones**.
- Haz clic en **Terminar la reunión para todo el mundo**.



Documentación relacionada del Centro de Ayuda

- Utilizar la herramienta de investigación para terminar reuniones

Control y gestión de dominios

Los administradores tienen acceso a las herramientas avanzadas de Google Workspace para gestionar los datos de su organización, definir controles, monitorizar el uso y contribuir al cumplimiento de los estándares educativos.

Casos prácticos

- Escanear archivos adjuntos de Gmail para detectar amenazas — Instrucciones paso a paso
- Crear informes y paneles de uso — Instrucciones paso a paso
- Buscar archivos de forma más sencilla — Instrucciones paso a paso
- Organización de documentos internos — Instrucciones paso a paso
- Rellenar automáticamente grupos de departamentos — Instrucciones paso a paso
- Crear audiencias para el sistema interno de archivos compartidos — Instrucciones paso a paso
- Restringir el sistema de archivos compartidos — Instrucciones paso a paso
- Restricciones de las aplicaciones de Workspace — Instrucciones paso a paso
- Gestión del almacenamiento — Instrucciones paso a paso
- Reglamentos en materia de datos — Instrucciones paso a paso
- Bases reguladoras de las becas — Instrucciones paso a paso
- Gestionar dispositivos endpoint — Instrucciones paso a paso
- Gestionar dispositivos Windows — Instrucciones paso a paso
- Configuración personalizada para dispositivos Windows — Instrucciones paso a paso
- Automatización de las actualizaciones de dispositivos Windows — Instrucciones paso a paso
- Uso del cifrado del lado del cliente — Instrucciones paso a paso

“Cómo puedo proteger mejor mi dominio contra un ataque de día cero y malware de rescate?”

Escanear archivos adjuntos de Gmail para buscar amenazas

Los archivos adjuntos pueden incluir software malicioso. Para identificar estas amenazas, Gmail puede escanear o ejecutar los archivos adjuntos en el entorno aislado de seguridad. Los archivos adjuntos que se identifiquen como amenazas se envían a la carpeta de Spam.

- Detecta malware “ejecutándolo” virtualmente en un entorno de seguridad y analiza los efectos secundarios para determinar el comportamiento malicioso.
- Escanea archivos Microsoft Word, PowerPoint, PDF, Zip y más.
- Permite escanear todo el dominio, o crear reglas según unas condiciones específicas como el remitente, el dominio y más.

Instrucciones paso a paso

Documentación importante del Centro de Ayuda

- Configurar normas para detectar archivos adjuntos dañinos

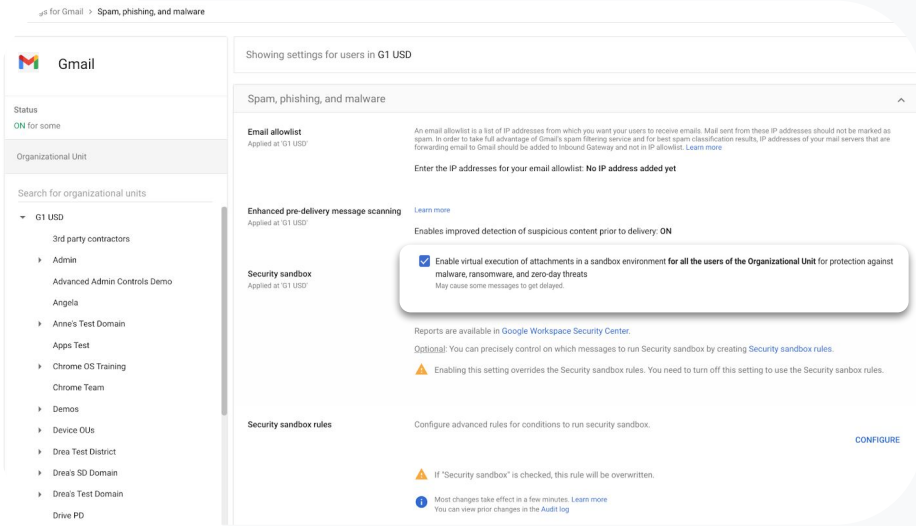
Instrucciones: escanear archivos Gmail para detectar amenazas

Cómo funciona

Los archivos adjuntos a un correo electrónico se “detonan” en un entorno aislado de seguridad en cuestión de minutos antes de mandar el correo, lo cual aporta una capa más de seguridad.

Cómo escanear todos los archivos adjuntos en el entorno aislado de seguridad

- Inicia sesión en tu **consola de administración.**
- Haz click en **Menú** > **Aplicaciones** > **Google Workspace** > **Gmail** > **Spam, Phishing y Software malicioso.**
- Selecciona una unidad organizativa o aplica la configuración en tu dominio.
- Ve al **entorno aislado de seguridad** en **Spam, Phishing y Software malicioso.**
- Marca la casilla **Permitir ejecutar los archivos virtualmente en un entorno aislado de seguridad.**
- Haz clic en **Guardar.**



Documentación relacionada del Centro de Ayuda

- Configurar normas para detectar archivos adjuntos dañinos

“¿Cómo puedo obtener información sobre el uso de Classroom en mi dominio?”

Crear informes y paneles de uso

Con la función de **exportación a BigQuery y la plantilla de Looker Studio**, los administradores pueden usar los registros de actividad de Classroom para crear paneles de control e informes personalizados con herramientas de analíticas, como Looker Studio, y colaboradores de visualización de terceros integrados en BigQuery.

- Exporta datos del registro de Classroom de la consola de administración a BigQuery y a Looker Studio.
- Consulta informes de uso y adopción rápidamente en todo tu dominio. Comprueba quién quitó a un alumno de una clase, quién archivó una clase en una fecha determinada, etc.
- Con las plantillas personalizables del panel de control de Looker Studio, podrás entender mejor las tendencias generales y actuar en consecuencia más rápido.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Configurar la exportación a BigQuery y una plantilla de Looker Studio

Instrucciones: crear informes y paneles de uso

01 Configura y exporta un proyecto de BigQuery

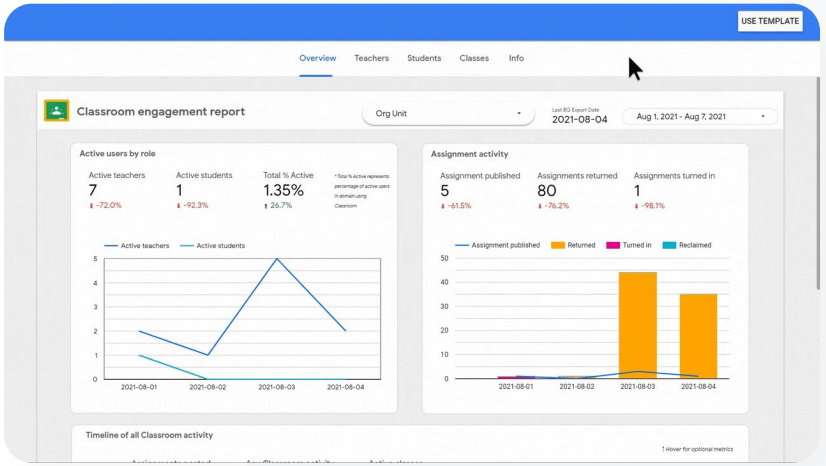
- Inicia sesión en console.cloud.google.com y haz clic en **Crear proyecto.**
- Inicia sesión en admin.google.com y haz clic en **Informes** > **BigQuery Export.**
- Haz clic en el **proyecto de BigQuery**, asigna un nombre al conjunto de datos y haz clic en **Guardar.**

02 Añade la exportación de BigQuery a Looker Studio

- Inicia sesión en Looker Studio y haz clic en **Crear** > **Fuente de datos.**
- Selecciona el conector de **BigQuery** > **Mis proyectos**, haz clic en el proyecto que has creado y, después, en **Actividad.**
- Marca la casilla situada debajo de **Tabla con particiones** y haz clic en **Conectar.**

03 Crea un panel de control de Looker Studio

- Abre la plantilla y selecciona **Usar plantilla.**
- En **Nueva fuente de datos**, selecciona la fuente de datos **actividad.**
- Haz clic en **Copiar informe.**



Documentación relacionada del Centro de Ayuda

- Configurar la exportación a BigQuery y una plantilla de Looker Studio

“Necesito hacer un seguimiento de las autorizaciones para excursiones que han enviado los padres a través de Gmail, Chat y Documentos.

¿Cómo puedo buscar estos archivos en todo el dominio?”

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

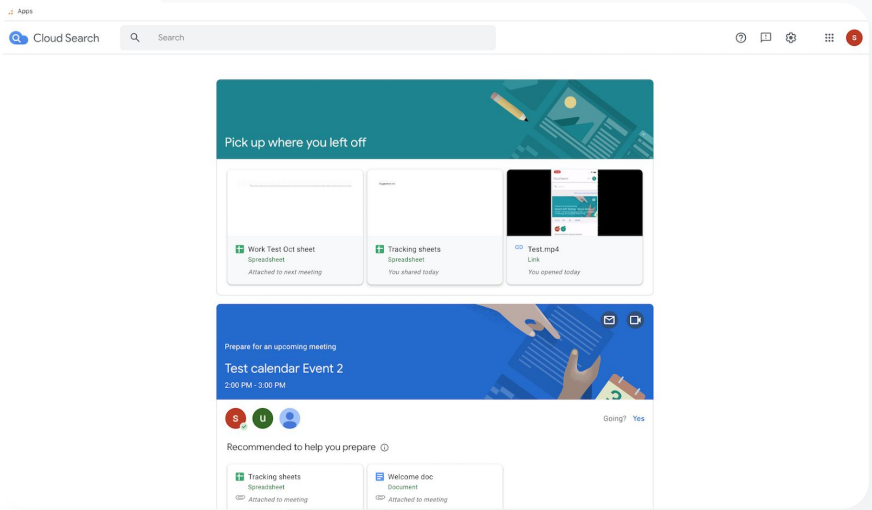
- Guía de Google Cloud Search
- Activar o desactivar Cloud Search en las cuentas de usuario

Buscar archivos de forma más sencilla

Con Google Cloud Search, el personal docente de tu institución puede buscar más rápido el contenido que necesite en Google Workspace y en aplicaciones de terceros.

- Busca la información que necesites desde cualquier lugar y con cualquier dispositivo, ya sea un portátil, un móvil o una tablet.
- Haz búsquedas en aplicaciones de Google Workspace como Drive, Contactos, Gmail y fuentes de datos de terceros.

Instrucciones: buscar archivos de forma más sencilla



Activar Cloud Search en las cuentas de usuario

- Inicia sesión en tu **consola de administración** y ve a **Menú** > **Aplicaciones**> **Google**.
- Haz clic en **Estado del servicio.**
- Para activar o desactivar un servicio para todos los miembros de la organización, haz clic en **Activado para todos** o **Desactivado para todos**.
- Haz clic en **Guardar.**
- Para activar un servicio en determinadas cuentas de usuario de varias unidades organizativas o de una misma unidad, selecciona un **grupo de acceso**.
- Haz clic en **Guardar**.

Documentación relacionada del Centro de Ayuda

- Guía de Google Cloud Search
- Activar o desactivar Cloud Search en las cuentas de usuario

Quiero aplicar etiquetas de información sensible a ciertos archivos de mi institución para seguir los requisitos de cumplimiento, evitar el uso inadecuado y tener mejor organizados los archivos".

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Gestionar etiquetas de Drive

Organizar los documentos en tu dominio

Las etiquetas de Drive ayudan a los usuarios a buscar, organizar y aplicar políticas en su dominio. Los administradores pueden crear y gestionar las etiquetas de Drive para evitar el uso inadecuado de los archivos y asegurarse de que los datos de los alumnos cumplen los requisitos normativos.

- Las etiquetas son metadatos que se utilizan para organizar archivos educativos sensibles, como programas educativos personalizados para alumnos, materiales de formación en el ámbito militar o documentos de cumplimiento normativo.
- Solo los administradores pueden crear y publicar etiquetas, así como definir sus estructuras. Los usuarios de tu organización pueden asignar etiquetas a los archivos que editen, así como definir el valor de cada campo.
- Las etiquetas de Drive pueden ser útiles para la función automatizada Prevención de la pérdida de datos (DLP).

Instrucciones: organizar los documentos en tu dominio

Cómo funciona

Google Drive ofrece etiquetas estándar y etiquetas con distintivos (indicadores visuales) para organizar los archivos de tu dominio.

Cómo activar las etiquetas de Drive en tu institución

- Inicia sesión en tu **consola de administración.**
- Haz clic en **Menú** > **Aplicaciones** > **Google Workspace** > **Drive y Documentos.**
- Selecciona **Etiquetas.**
- **Activa** o **desactiva las etiquetas.**
- Haz clic en **Guardar.**

Documentación relacionada del Centro de Ayuda

- Gestionar etiquetas de Drive

“¿Cómo puedo automatizar la pertenencia a un grupo para que cada vez que un nuevo docente se incorpore a la institución, se le incluya en la lista de correo electrónico 'Docentes'?”

Rellenar automáticamente grupos de departamentos

Los grupos dinámicos permiten a los administradores actualizar la pertenencia a un grupo de cualquier usuario del centro con criterios personalizados.

- Crea grupos dinámicos para gestionar a los miembros automáticamente.
- Crea consultas de pertenencia para mantener actualizados los grupos.
- Usa los grupos dinámicos como:
  - Listas de distribución y correo
  - Grupos moderados y bandejas de entrada colaborativas
  - Grupos de seguridad

Instrucciones paso a paso

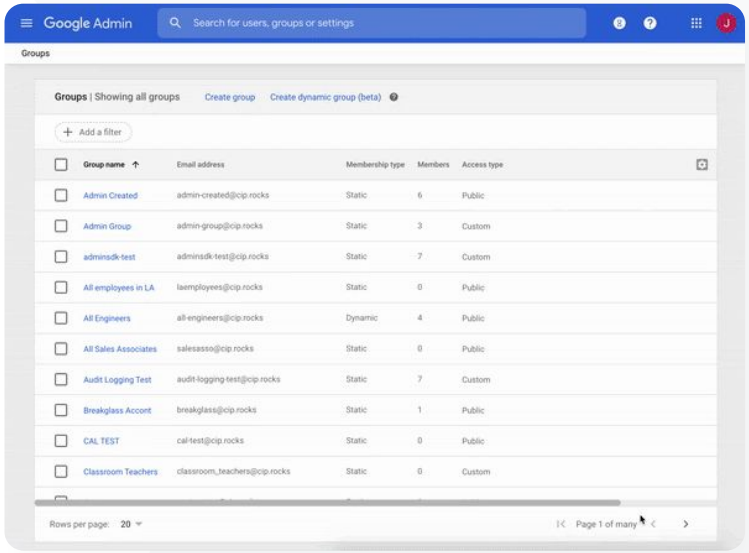
Documentación relacionada del Centro de Ayuda

- Gestionar miembros automáticamente con grupos dinámicos

Instrucciones: rellenar automáticamente los grupos

Crear grupos dinámicos

- Inicia sesión en tu **consola de administración** y ve a **Menú** > **Directorio** > **Grupos.**
- Haz clic en **Crear grupo dinámico.**
- Crea tu consulta de pertenencia al grupo según los siguientes elementos:
  - Lista de condiciones: criterios que se tendrán en cuenta para la pertenencia al grupo; por ejemplo, el departamento.
  - Campo Valor: el valor que quieras usar.
- Introduce la siguiente información:
  - Nombre: identifica al grupo en las listas y en los mensajes.
  - Descripción: indica el objetivo del grupo.
  - Correo electrónico del grupo: define la dirección de correo que se usará para el grupo.
- Haz clic en **Guardar.**
- Haz clic en **Hecho.**



Documentación relacionada del Centro de Ayuda

- Gestionar miembros automáticamente con grupos dinámicos

Algunos miembros del personal están compartiendo documentos por error con el resto de la organización, por lo que se ha puesto en peligro cierta información sensible. ¿Cómo puedo limitar sus permisos para compartir documentos con un grupo más reducido y pertinente?”

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Información sobre las audiencias objetivo
- Prácticas recomendadas para implementar audiencias objetivo
- Crear audiencias objetivo

Crear audiencias para el sistema interno de archivos compartidos

Los ajustes de Audiencia objetivo ayudan a mejorar la seguridad de los datos de tu organización al reducir la posibilidad de que se compartan por error archivos con usuarios indebidos.

- Asegúrate de que los archivos se comparten solo con las personas adecuadas, como un equipo o un departamento específicos.
- Las audiencias objetivo son grupos de personas que los administradores pueden recomendar a los usuarios para que compartan sus elementos con ellos.
- Los administradores pueden añadir audiencias objetivo a las opciones para compartir de los usuarios con el fin de animarles a compartir documentos con una audiencia más específica.
- Está disponible en Google Drive, Documentos de Google y Google Chat.

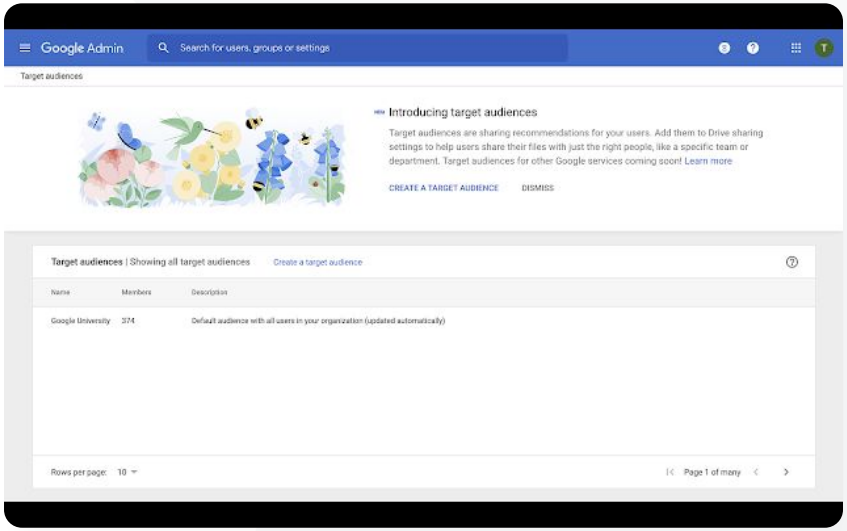
Instrucciones: crear audiencias para el sistema interno de archivos compartidos

Cómo funciona

Una vez que hayas creado una audiencia objetivo, puedes añadirle miembros y asignarla a Google Drive, de manera que aparezca en las opciones para compartir de los usuarios de ese servicio. Por ejemplo, puedes permitir que un miembro del personal vea una audiencia objetivo que sea “Todo el personal” al compartir los archivos de Drive.

Cómo activar las etiquetas de Drive en tu institución

- Inicia sesión en tu **consola de administración** y ve a **Menú** > **Directorio** > **Audiencias objetivo**.
- Haz clic en **Crear audiencia objetivo**.
- En **Nombre**, da nombre a la audiencia objetivo.
- Selecciona **Añadir miembros** e incluye los que quieras.
- Haz clic en **Hecho**.



Documentación relacionada del Centro de Ayuda

- Información sobre las audiencias objetivo
- Prácticas recomendadas para implementar audiencias objetivo
- Crear audiencias objetivo

“¿Cómo puedo evitar que mis alumnos de secundaria compartan documentos con los de primaria?”

Restringir el sistema de archivos compartidos

Para proteger la privacidad de los datos institucionales, las reglas de confianza de Drive permiten a los administradores definir reglas que controlan quién puede acceder a los archivos de Google Drive. Se pueden aplicar políticas a determinados usuarios, grupos, unidades organizativas y dominios.

- Protege la información sensible y cumple las normativas y los estándares del sector.
- Restringe la capacidad para compartir dentro y fuera del dominio. Los administradores pueden crear una regla de confianza para permitir que los alumnos compartan los archivos de Drive únicamente con otros miembros de la organización.
- Una vez que se habilitan las reglas de confianza, sustituyen a las opciones para compartir de los controles de administrador de Google Drive.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Crear y gestionar reglas de confianza para controlar el uso compartido en Drive

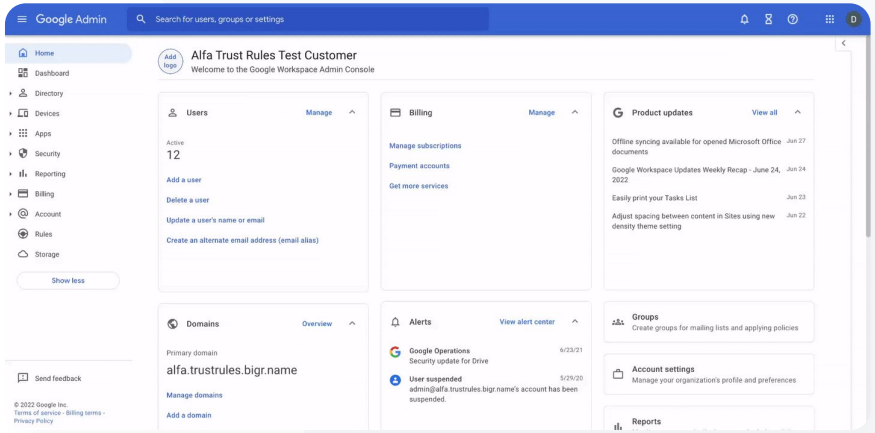
Instrucciones: restringir el sistema de archivos compartidos

Activar reglas de confianza de Drive

- Inicia sesión en tu **consola de administración** y ve a **Menú** > **Reglas**.
- En la tarjeta **Colaborar de forma segura**, situada en la parte superior de la página, haz clic en **Activar reglas de confianza**.
- La lista Tareas se abre automáticamente y muestra el progreso de la activación de las reglas de confianza.

Los administradores pueden crear y eliminar reglas de confianza, ver y editar sus detalles, así como consultar sus eventos de registro.

Para consultar las instrucciones paso a paso sobre la gestión de las reglas de confianza, visita el Centro de Ayuda para administradores.



Documentación relacionada del Centro de Ayuda

- Crear y gestionar reglas de confianza para controlar el uso compartido en Drive

Quiero limitar el acceso a aplicaciones específicas cuando los usuarios estén en nuestra red”.

Restricciones de las aplicaciones de Google Workspace

Con el **acceso contextual** puedes crear políticas de control de acceso detalladas para aplicaciones de **Google Workspace y SAML (lenguaje de marcado para confirmaciones de seguridad) de terceros** a partir de atributos, como la identidad del usuario, la ubicación, el estado de seguridad del dispositivo y la dirección IP. Incluso puedes restringir el acceso a aplicaciones que están fuera de la red.

- Puedes aplicar políticas de acceso contextual a los servicios principales de Google Workspace for Education.
- Por ejemplo, puedes restringir el acceso a las aplicaciones de Workspace desde dispositivos de la institución o el acceso a Drive solo si el dispositivo de almacenamiento del usuario está cifrado.

Instrucciones paso a paso

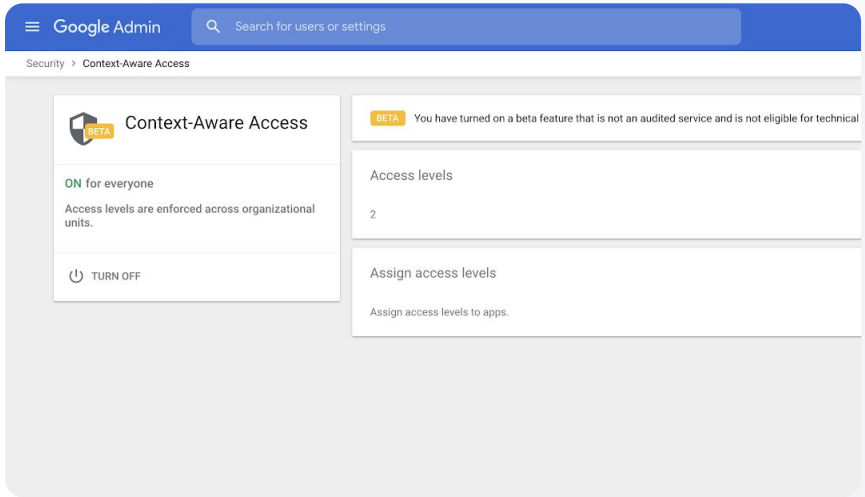
Documentación relacionada del Centro de Ayuda

- Introducción al acceso contextual
- Asignar niveles de acceso contextual a las aplicaciones

Instrucciones: restringir el uso de las aplicaciones de Google Workspace

Cómo usar el acceso contextual

- Inicia sesión en tu **consola de administración**.
- Selecciona **Seguridad** > **Acceso contextual** > **Asignar**.
- Selecciona **Asignar niveles de acceso** para ver tu lista de aplicaciones.
- Selecciona una **unidad organizativa o un grupo de configuración** para ordenar la lista.
- Selecciona **Asignar** junto a la aplicación que quieras configurar.
- Selecciona uno o varios niveles de acceso.
- Crea varios niveles si quieres que los usuarios cumplan más de una condición.
- Haz clic en **Guardar**.



Documentación relacionada del Centro de Ayuda

- Introducción al acceso contextual
- Asignar niveles de acceso contextual a las aplicaciones

Gestionar el almacenamiento en tu dominio

Quiero implementar un nuevo plan de gestión del almacenamiento en mi dominio”.

Las instituciones con Google Workspace for Education tienen un espacio almacenamiento compartido inicial de 100 TB. Este espacio permite almacenar más de 100 millones de documentos, 8 millones de presentaciones o 400.000 horas de vídeo. **Gestiona el almacenamiento compartido en Drive** para asegurarte de que tu institución lo aprovecha de forma eficaz.

Usa herramientas, informes y registros del administrador para:

- Saber cuánto almacenamiento estás usando.
- Definir límites de almacenamiento.
- Identificar cuentas que ocupan un espacio de almacenamiento desproporcionado.

Tanto Teaching and Learning Upgrade como Education Plus ofrecen más capacidad de almacenamiento, además del espacio que se proporciona inicialmente.

- Añade 100 GB al espacio de almacenamiento compartido por licencia con Teaching and Learning Upgrade.
- Añade 20 GB al espacio de almacenamiento compartido por licencia con Education Plus.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Guía de almacenamiento para administradores
- Información sobre la disponibilidad y el uso del espacio de almacenamiento
- Liberar o añadir más almacenamiento
- Definir límites de almacenamiento

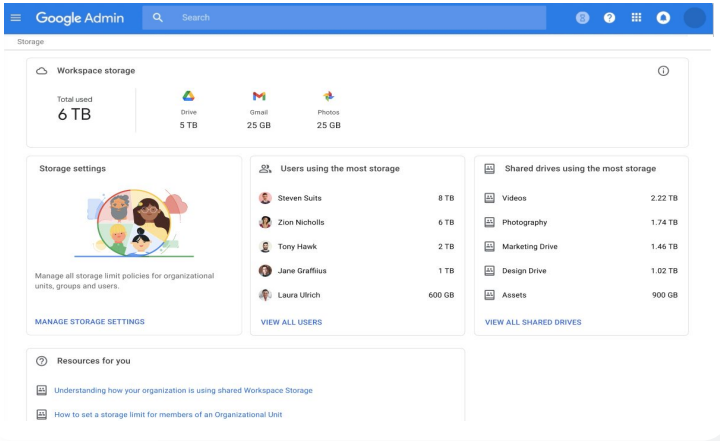
Instrucciones: gestionar el almacenamiento en tu dominio

Identificar el uso de almacenamiento por usuario

- Inicia sesión en tu **consola de administración** y ve a **Menú** > **Almacenamiento**.
- Consulta el uso de almacenamiento por organización y usuario.

Definir límites de almacenamiento

- En la **consola de administración**, ve a **Menú** > **Almacenamiento**.
- En **Ajustes de almacenamiento**, haz clic en **Gestionar**.
- Haz clic en **Límite de almacenamiento por usuario** y selecciona la entidad a la que quieres aplicar el límite:
  - Unidad organizativa: haz clic en la **unidad organizativa**.
  - Grupo: haz clic en **Grupos** y, después, en el **campo de búsqueda**. Indica el **nombre del grupo** y haz clic en el **grupo**.
- Selecciona **Activado** y **define la cantidad de almacenamiento**.
- Haz clic en **Guardar**.



Documentación relacionada del Centro de Ayuda

- Guía de almacenamiento para administradores
- Información sobre la disponibilidad y el uso del espacio de almacenamiento
- Liberar o añadir más almacenamiento
- Definir límites de almacenamiento

> Los datos de los alumnos, el profesorado y el personal del centro deben permanecer dentro de la Unión Europea debido a la legislación vigente".

Reglamentos en materia de datos

Como administrador, puedes decidir almacenar los datos en una ubicación geográfica concreta (Estados Unidos o Europa/Reino Unido) mediante una **política de la región de datos**.

- Los usuarios de Education Plus y Education Standard pueden elegir una región de datos para determinados usuarios o distintas regiones de datos para ciertos departamentos, y consultar el progreso de la transferencia entre regiones de datos.
- Coloca a usuarios en una unidad organizativa (para aplicar el ajuste por departamento) o en un grupo de configuración (para aplicárselo a usuarios concretos, ya sean del mismo departamento o de departamentos distintos).
- A los usuarios que no tienen una licencia de Education Standard o Education Plus no se les aplican las políticas de la región de datos.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Elegir la ubicación geográfica de los datos

“Las investigaciones del profesorado deben permanecer en Estados Unidos de acuerdo con las bases reguladoras de las becas”.

Bases reguladoras de las becas

Como administrador, puedes elegir la ubicación geográfica donde se van a almacenar las investigaciones de los profesores (Estados Unidos o Europa) mediante una **política de la región de datos**.

- Las políticas de la región de datos cubren los datos primarios en reposo (incluidas las copias de seguridad) de la mayoría de los servicios principales de Google Workspace for Education.
- Valora las repercusiones antes de definir una política de la región de datos, ya que si los datos de los usuarios se almacenan fuera de su región, podrían experimentar una mayor latencia en ciertos casos.

Instrucciones paso a paso

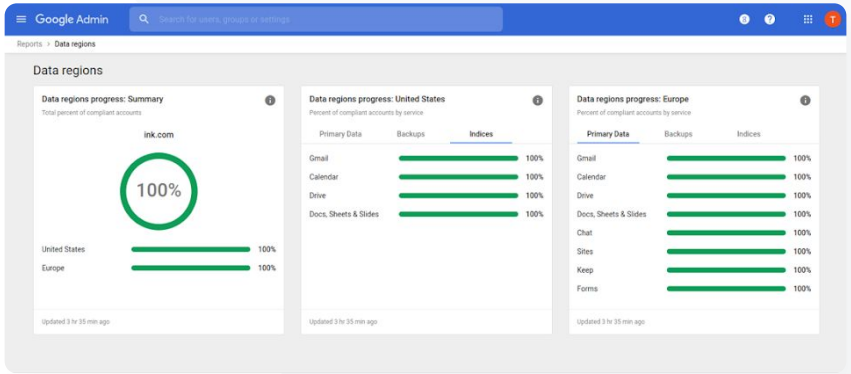
Documentación relacionada del Centro de Ayuda

- Elegir la ubicación geográfica de los datos

Instrucciones: reglamentos en materia de datos

Cómo definir regiones de datos

- Inicia sesión en tu **consola de administración**.
  - Nota: Tienes que haber iniciado sesión como superadministrador
- Haz clic en **Perfil de empresa** > **Mostrar más** > **Regiones de datos**.
- Selecciona **la unidad organizativa o el grupo de configuración** que quieras limitar a una región, o bien selecciona toda la columna para incluir todas las unidades y grupos.
- Selecciona tu región: **Sin preferencia, Estados Unidos o Europa**.
- Haz clic en **Guardar**.



Documentación relacionada del Centro de Ayuda

- Elegir la ubicación geográfica de los datos

“Necesito poder gestionar y aplicar políticas a todos los tipos de dispositivos (iOS, Windows 10, etc.) de mi distrito escolar, no solo a los Chromebooks, sobre todo si la seguridad de uno de ellos está en riesgo”.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Gestionar dispositivos con la gestión de endpoints de Google
- Configurar la gestión avanzada de dispositivos móviles

Gestionar dispositivos endpoint

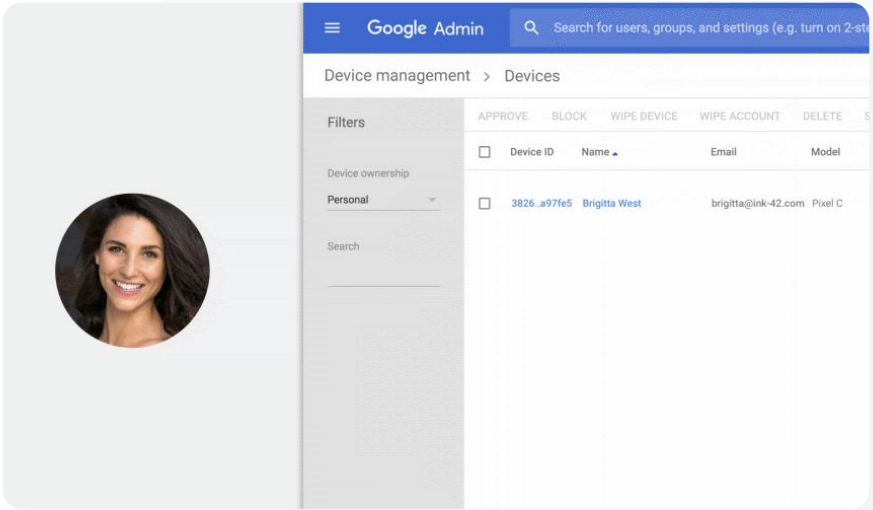
Gestión empresarial de endpoints puede darte un mayor control sobre los datos de tu organización en este tipo de dispositivos. Puedes restringir funciones de los dispositivos móviles, requerir el cifrado de dispositivos, gestionar aplicaciones en dispositivos Android, iPhones y iPads, e incluso borrar datos de dispositivos.

- Puedes aprobar, bloquear, desbloquear y eliminar dispositivos desde la consola de administración.
- Si alguien pierde su dispositivo o deja de formar parte del centro educativo, puedes borrar su cuenta de usuario, su perfil e incluso todos los datos del dispositivo gestionado (que se seguirían pudiendo consultar en un ordenador o en un navegador web).

Instrucciones: gestionar dispositivos endpoint

Instrucciones sobre la gestión avanzada de dispositivos móviles

- Inicia sesión en tu **consola de administración**.
- Ve a **Consola de administración** > **Dispositivos**.
- En la parte izquierda, haz clic en **Configuración** > **Configuración universal**.
- Haz clic en **General** > **Gestión de dispositivos móviles**.
- Si quieres aplicar la configuración a todos los usuarios, deja seleccionada la unidad organizativa superior. Si no es el caso, selecciona una unidad organizativa secundaria.
- Selecciona **Avanzado**.
- Haz clic en **Guardar**.



Documentación relacionada del Centro de Ayuda

- Gestionar dispositivos con la gestión de endpoints de Google
- Configurar la gestión avanzada de dispositivos móviles

Gestión de dispositivos Microsoft Windows

Algunos de mis docentes usan dispositivos con Windows 10. ¿Cómo puedo gestionar todos los dispositivos de mi institución desde el mismo lugar?”

Gestiona y protege los dispositivos con Windows 10 de tu institución a través de la consola de administración. Para ello, sigue el mismo procedimiento que con los dispositivos Android, iOS, Chrome y Jamboard.

- Habilita el inicio de sesión único para que los usuarios puedan acceder de forma más sencilla a Google Workspace desde sus dispositivos con Windows 10.
- Gestiona los dispositivos que se utilizan para acceder a Google Workspace desde la consola de administración para garantizar que estén actualizados y protegidos, y que cumplan los estándares pertinentes.
- Borra los datos de dispositivos, implementa actualizaciones de configuración, etc., en dispositivos con Windows 10 desde la nube.

Instrucciones paso a paso

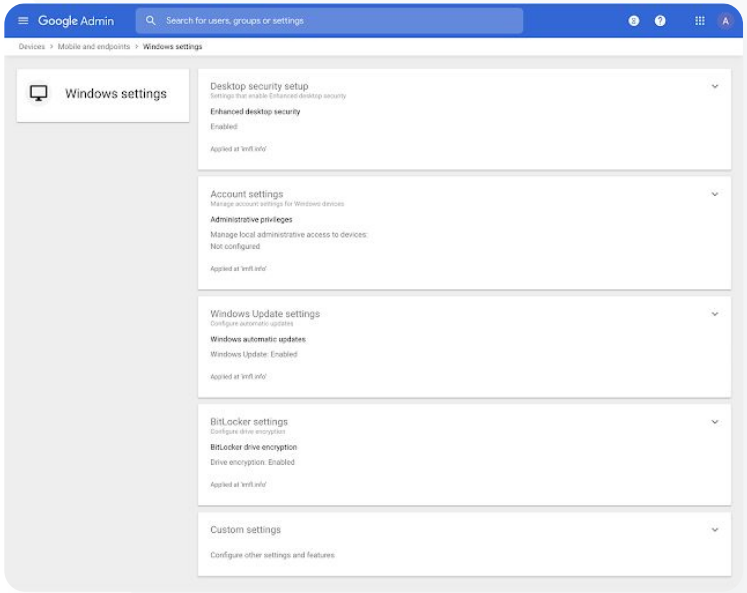
Documentación relacionada del Centro de Ayuda

- Habilitar el servicio de gestión de dispositivos Windows
- Registrar un dispositivo en el servicio de gestión de dispositivos Windows

Instrucciones: gestión de dispositivos Microsoft Windows

Habilitar el servicio de gestión de dispositivos Windows

- En la **consola de administración**, ve a **Menú** > **Dispositivos** > **Móviles y endpoints** > **Configuración** > **Configuración de Windows**.
- Selecciona **Configuración de la gestión de Windows**.
- Si quieres aplicar la configuración a todos los usuarios, deja seleccionada la unidad organizativa superior.
- Junto a **Gestión de dispositivos Windows**, selecciona **Habilitada**.
- Haz clic en **Guardar**.



Documentación relacionada del Centro de Ayuda

- Habilitar el servicio de gestión de dispositivos Windows
- Registrar un dispositivo en el servicio de gestión de dispositivos Windows

“¿Cómo puedo configurar los perfiles de Wi-Fi en mis dispositivos con Windows 10?”

Configuración personalizada para dispositivos con Windows 10

Con la gestión de dispositivos Windows de Google, los administradores pueden añadir ajustes personalizados a los dispositivos de su flota.

- Controla los ajustes personalizados de los dispositivos desde la consola de administración.
- Aplica ajustes en los siguientes ámbitos:
  - Gestión de dispositivos
  - Seguridad
  - Hardware y red
  - Software
  - Privacidad

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

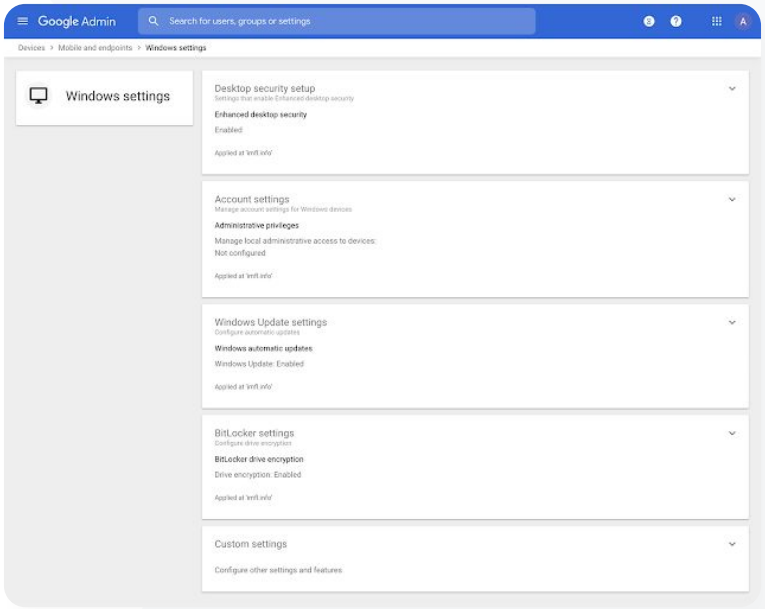
- Ajustes personalizados habituales
- Añadir ajustes personalizados

Instrucciones: configuración personalizada para dispositivos con Windows 10

Añadir ajustes personalizados

- En la **consola de administración**, ve a **Menú** > **Dispositivos** > **Móviles y endpoints** > **Configuración** > **Configuración de Windows**.
- Selecciona **Configuración personalizada**.
- Haz clic en **Añadir un ajuste personalizado** y completa los campos requeridos.
- Haz clic en **Siguiente**.
- Elige la **unidad organizativa** a la que quieres aplicar la configuración.
- Haz clic en **Aplicar**.

Ten en cuenta que Google no proporciona asistencia técnica ni se responsabiliza de la configuración ni los productos de terceros.



Documentación relacionada del Centro de Ayuda

- Ajustes personalizados habituales
- Añadir ajustes personalizados

Quiero asegurarme de que los dispositivos con Windows 10 de mi flota reciban las últimas actualizaciones”.

Automatización de actualizaciones en dispositivos con Windows 10

Especifica cuándo y cómo quieres que tus dispositivos con Windows 10 reciban actualizaciones de seguridad y otras descargas importantes a través de los servicios de actualización automática de Windows.

- Configura notificaciones para descargar actualizaciones del panel de control de Windows Update, define un intervalo de horas en el que no se puedan programar reinicios de actualizaciones, etc.
- Aplica ajustes a toda la institución o a unidades organizativas concretas.
- Los cambios pueden tardar hasta 24 horas en surtir efecto, pero no es lo habitual.

Instrucciones paso a paso

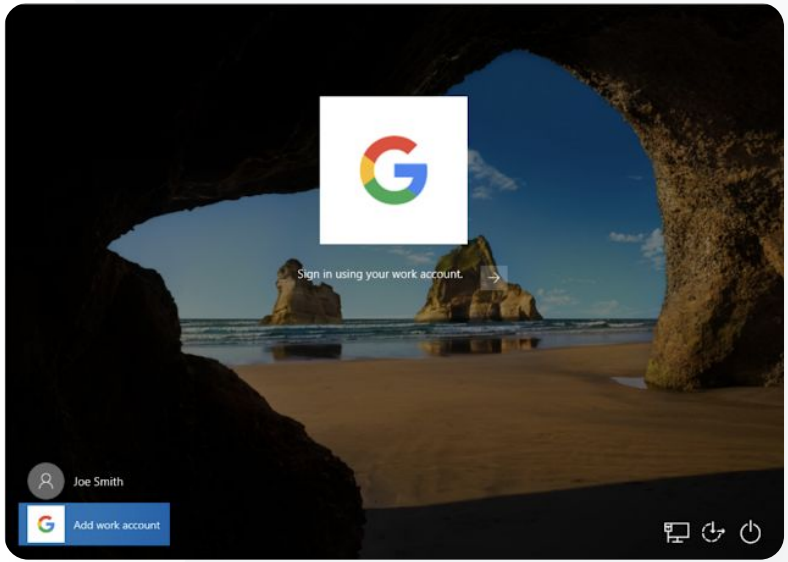
Documentación relacionada del Centro de Ayuda

- Gestionar actualizaciones automáticas

Instrucciones: automatización de actualizaciones en dispositivos con Windows 10

Configurar actualizaciones

- En la **consola de administración**, ve a **Menú** > **Dispositivos** > **Móviles y endpoints** > **Configuración** > **Configuración de Windows**.
- Selecciona **Configuración de Windows Update** > **Habilitada**.
- Junto a **Gestión de dispositivos Windows**, selecciona **Habilitada**.
- Configura las opciones que aparecen a continuación, entre otras:
  - Aceptar actualizaciones de aplicaciones de Microsoft
  - Comportamiento de actualizaciones automáticas
  - Automatizar frecuencia de actualización
- Haz clic en **Guardar**.



Documentación relacionada del Centro de Ayuda

- Gestionar actualizaciones automáticas

“Sé que Google tiene los estándares más altos en cuanto al cifrado de datos, pero me gustaría controlar las claves de cifrado de la propiedad intelectual de nuestra universidad y de las investigaciones subvencionadas por becas”.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Acerca del cifrado del lado del cliente

Uso del cifrado del lado del cliente

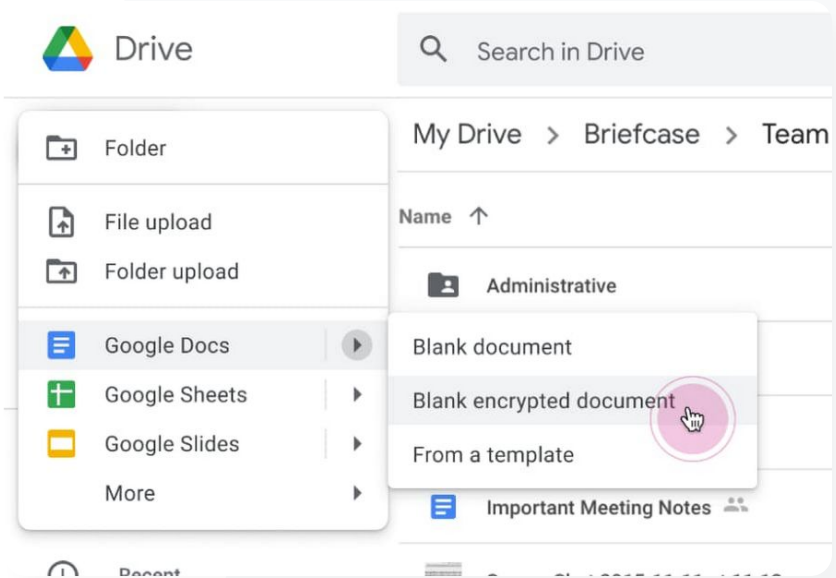
Google Workspace ya utiliza los últimos estándares criptográficos para cifrar todos los datos, tanto en reposo como en tránsito, en sus instalaciones. Gracias al **cifrado del lado del cliente**, los administradores tienen el control directo de las claves de cifrado y del proveedor de identidades que se usa para acceder a las claves.

- Utiliza tus propias claves de cifrado para cifrar datos sensibles, como la propiedad intelectual de tu institución.
- El cifrado de contenido se gestiona en tu navegador antes de que se transmita cualquier dato o se guarde en el sistema de almacenamiento basado en la nube de Google.
- Elige qué usuarios pueden crear contenido cifrado del lado del cliente y compartirlo o enviarlo de forma interna o externa.

Instrucciones: uso del cifrado del lado del cliente

Configurar el cifrado del lado del cliente (CLC)

- Configura el servicio de claves de cifrado.
  - Protege tus datos mediante sistemas de gestión de claves y capacidades de control creando un servicio de claves.
- Conecta Google Workspace a tu servicio de claves externo.
  - Añade y gestiona servicios de claves de cifrado del lado del cliente incluyendo la URL del servicio de claves en la consola de administración.
- Asigna tu servicio de claves a unidades organizativas o grupos.
  - Asigna un servicio de claves como el predeterminado para toda la institución.
- Conecta Google Workspace a tu proveedor de identidades.
  - Conéctate a tu proveedor de identidades (IdP) para que el cifrado del lado del cliente verifique la identidad de los usuarios antes de que puedan cifrar el contenido o acceder a contenido cifrado.
- Habilita el CLC para que lo utilicen los usuarios.
  - Activa el cifrado del lado del cliente para que las unidades organizativas o los grupos con usuarios que lo necesiten puedan crear contenido cifrado del lado del cliente.

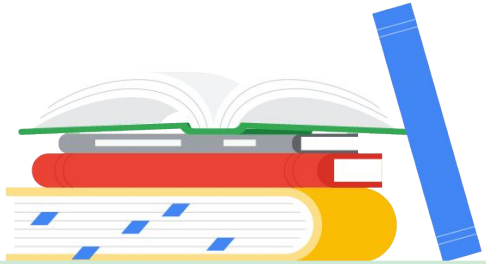


Documentación relacionada del Centro de Ayuda

- Acerca del cifrado del lado del cliente

Funciones de enseñanza y aprendizaje

Dota de más recursos a los docentes de tu entorno de aprendizaje digital proporcionándoles experiencias de clase enriquecidas, herramientas para fomentar la integridad académica y funciones avanzadas de comunicación por vídeo.

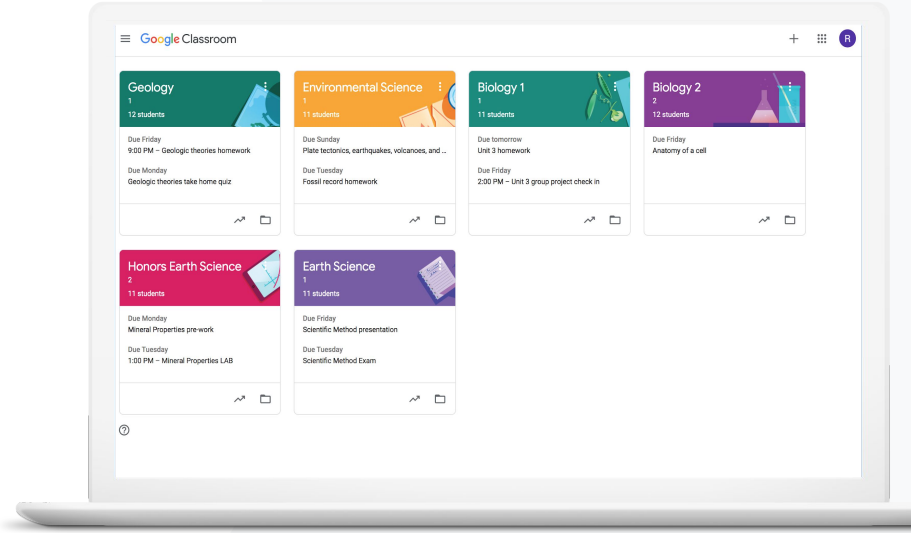


- Google Classroom
- Informes de originalidad
- Documentos, Hojas de cálculo y Presentaciones
- Google Meet

Google Classroom

¿Qué es?

Google Classroom es tu plataforma central de enseñanza y aprendizaje. Las funciones de pago de Classroom permiten agrupar las herramientas de clase en un único lugar. Los docentes pueden acceder a sus herramientas favoritas directamente en Classroom y mantener las listas de clase sincronizadas con los sistemas externos.



Casos prácticos

Gestión del acceso a los complementos de Classroom	Instrucciones paso a paso
Incluir contenido interesante en Classroom	Instrucciones paso a paso
Crear clases a gran escala	Instrucciones paso a paso

“Ojalá hubiera una forma de dar acceso con inicio de sesión único a las herramientas de tecnología educativa favoritas de mis docentes”.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Gestionar aplicaciones de Google Workspace Marketplace
- Utilizar complementos de Classroom
- Gestionar qué aplicaciones de Marketplace se añaden a la lista de permitidas
- Distribuir aplicaciones de Marketplace con los usuarios
- Complementos de Classroom [guía de introducción para administradores]

Gestión del acceso a los complementos de Classroom

Determina a qué aplicaciones de educación de terceros tiene acceso tu institución mediante una **lista de dominios permitidos**. Permite a los docentes instalar complementos de forma sencilla e inclúyelos en las tareas de los alumnos con solo unos clics.

- Crea una lista de permitidos en tu dominio para indicar qué aplicaciones de educación de terceros de Google Workspace Marketplace pueden instalarse.
- Promueve el aprendizaje con aplicaciones educativas complementarias. Los docentes pueden asignar, corregir y calificar tareas directamente en Google Classroom.
- Adobe Creative Cloud Express, BookWidgets, CK-12, Formative, Genially, Google Arts & Culture, IXL, Kahoot!, Nearpod, Newsela, Pear Deck, SAFARI Montage, Sora, Wordwall y muchos más están disponibles en Google Workspace Marketplace.

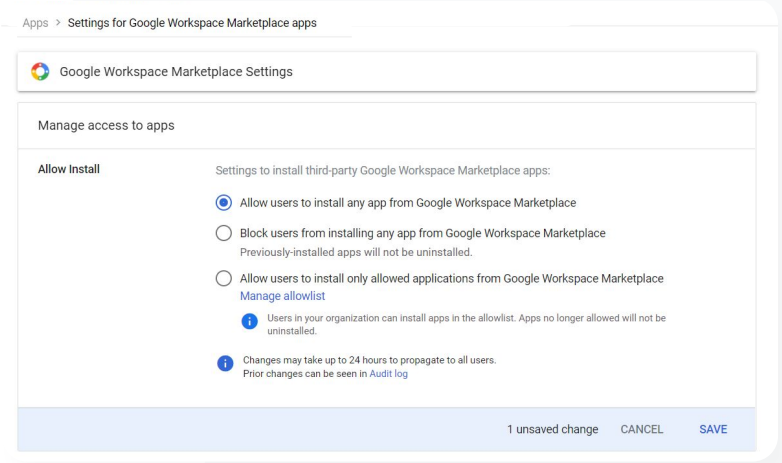
Instrucciones: gestión del acceso a los complementos de Classroom

Gestionar el acceso a complementos con una lista de dominios permitidos

- En la consola de administración, selecciona **Menú** > **Aplicaciones de Google Workspace Marketplace** > **Lista de aplicaciones**.
- Selecciona **Permitir aplicación**.
- Escribe o busca el nombre del complemento que quieras añadir.
- Haz clic en **Seleccionar** y asegúrate de que la opción **Permitir que los usuarios instalen esta aplicación** está seleccionada.
- Haz clic en **Continuar** y, después, en **Finalizar**.

Permitir el acceso a complementos a las listas de permitidos que quieras

- En la consola de administración, selecciona **Menú** > **Aplicaciones de Google Workspace Marketplace** > **Lista de aplicaciones**.
- Selecciona el complemento que quieras distribuir.
- En **Acceso de usuario**, haz clic en **Ver grupos y unidades organizativas**.
- Decide si quieres que esté **disponible para todo el mundo** o si prefieres acotar el acceso a **determinados grupos** o **unidades organizativas**.
- Haz clic en **Guardar**.



Documentación relacionada del Centro de Ayuda

- Gestionar aplicaciones de Google Workspace Marketplace
- Utilizar complementos de Classroom
- Gestionar qué aplicaciones de Marketplace se añaden a la lista de permitidas
- Distribuir aplicaciones de Marketplace con los usuarios
- Complementos de Classroom [guía de introducción para administradores]

“Me gustaría asignar una sesión del juego educativo Kahoot! a mis alumnos y calificar los resultados sin salir de Google Classroom”.

Incluir contenido interesante en Classroom

Con los **complementos de Classroom**, los docentes pueden compartir contenido y actividades interesantes con su clase adjuntando complementos a tareas, preguntas, materiales o anuncios desde Classroom.

- Permite a los docentes y alumnos usar sus herramientas favoritas, como Kahoot!, Nearpod y Pear Deck, sin salir de Classroom.
- Gracias a los complementos, los alumnos no tendrán que gestionar varias contraseñas ni ir a sitios web externos.
- Califica y revisa el trabajo de los alumnos desde los complementos, directamente en Classroom.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Utilizar complementos de Classroom
- Complementos de Classroom [guía de introducción para docentes]

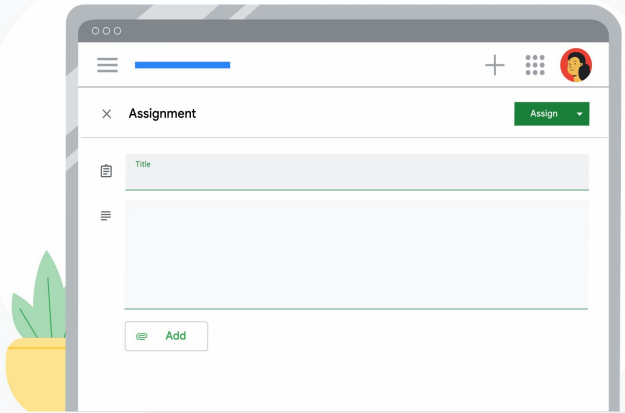
Instrucciones: incluir contenido interesante en Classroom

Cómo adjuntar complementos a una tarea, a un cuestionario o a una pregunta

- Inicia sesión en tu cuenta de Classroom (**classroom.google.com**).
- En la lista, selecciona la clase que corresponda y elige **Trabajo de clase**.
- Selecciona **Crear** y escoge lo que quieras crear.
- Escribe el título y las instrucciones.
- En **Complementos**, elige el complemento que quieras usar.
- Selecciona **Asignar**.

Cómo adjuntar complementos a un anuncio

- Desde la página **Tablón** de tu clase, selecciona **Anuncia algo a tu clase**.
- Escribe el anuncio.
- En **Complementos**, elige el complemento que quieras usar.
- Selecciona **Publicar**.



Documentación relacionada del Centro de Ayuda

- Utilizar complementos de Classroom
- Complementos de Classroom [guía de introducción para docentes]

Necesito una forma de automatizar la configuración de las clases y gestionar las listas de alumnos en Google Classroom".

Crear clases a gran escala

La función para importar listas de alumnos desde un SIA permite crear automáticamente clases y sincronizar listas de alumnos con el sistema de información sobre alumnos (SIA) de tu institución mediante Clever.

- Está disponible en distritos de enseñanza primaria y secundaria de EE. UU. y Canadá que usen Education Plus.
- Los administradores pueden importar listas de clases de tu SIA a Google Classroom para configurar las clases de forma automática.
- Permite automatizar y gestionar listas de clases en Google Classroom sin contratiempos.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Empezar a usar la función de importación de listas de SIAs
- Configurar la importación de listas del SIA a través de Clever

Instrucciones: crear clases a gran escala

Cómo configurar la importación de listas de SIAs

- Configura la sincronización de listas de Google Classroom desde Clever.
- El administrador del distrito de Clever y el superadministrador de Google Workspace pueden seguir las instrucciones paso a paso de Clever.

Si tu distrito no tiene una cuenta de Clever:

- Crea una cuenta de Clever.

Si tu distrito tiene una cuenta de Clever:

- Solicita la importación de la lista desde el panel de control de Clever.

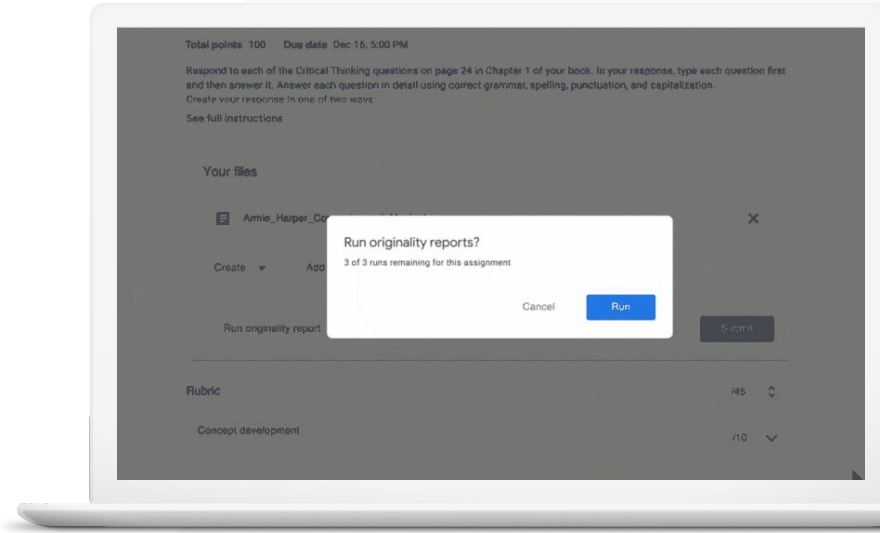
Documentación relacionada del Centro de Ayuda

- Configurar la importación de listas del SIA a través de Clever

Informes de originalidad

¿Qué son?

Los informes de originalidad permiten a los docentes y a los alumnos comprobar la autenticidad de su trabajo usando la Búsqueda de Google para cotejar los trabajos de los alumnos con el contenido de miles de millones de páginas web y más de 40 millones de libros. Las funciones de pago de los informes de originalidad proporcionan acceso ilimitado, de manera que los docentes pueden comparar las entregas de los alumnos con un repositorio propio de trabajos de alumnos anteriores.



Casos prácticos

Detectar plagios	Instrucciones paso a paso
Comprobar la originalidad con ayuda de los trabajos de antiguos alumnos	Instrucciones paso a paso
Transformar la detección de plagio en oportunidades de aprendizaje	Instrucciones paso a paso

“Quiero detectar el plagio y las citas incorrectas en los trabajos de mis alumnos”.

Detectar plagios

Los docentes pueden comprobar la autenticidad de los trabajos de sus alumnos usando los **informes de originalidad**. En el informe se incluyen enlaces a las fuentes detectadas y se marca el texto que no se ha citado.

- Genera informes de originalidad en archivos de Microsoft Word, Presentaciones y Documentos.

- Los docentes que utilizan Teaching and Learning Upgrade o Education Plus tienen además:
  - Acceso ilimitado a los informes de originalidad.
  - La posibilidad de cotejar las coincidencias entre alumnos con un repositorio de trabajos entregados en años anteriores, propiedad de la institución.

Los datos serán siempre de tu propiedad; nuestra responsabilidad es mantener su privacidad y seguridad.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Activar los informes de originalidad
- Informes de originalidad y privacidad

Instrucciones: detectar plagios

Activar los informes de originalidad en tareas desde Classroom

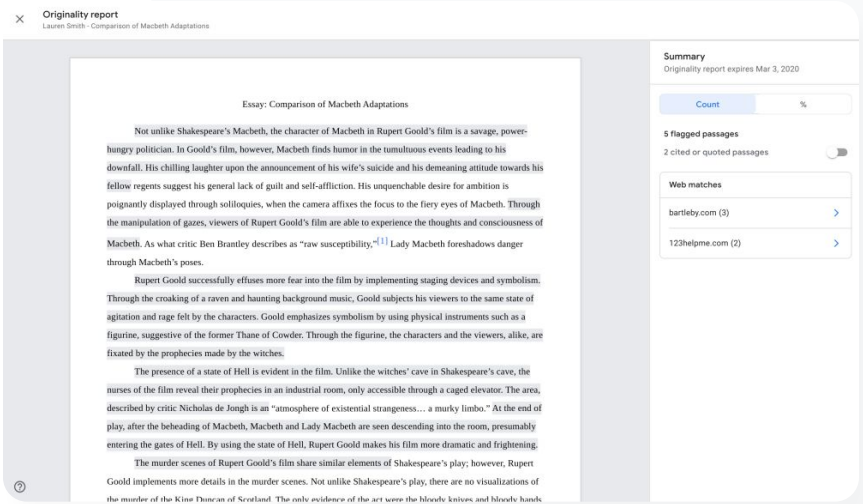
- Inicia sesión en tu cuenta de Classroom (**classroom.google.com**).
- En la lista, selecciona la clase que corresponda y elige **Trabajo de clase**.
- Selecciona **Crear** > **Tarea**.
- Marca la casilla junto a **Informes de originalidad** para activar esta función.

Generar un informe de originalidad sobre trabajos de alumnos

- Selecciona el archivo del alumno en la lista y haz clic para abrirlo en la herramienta de calificación.
- En la tarea del alumno, haz clic en **Comprobar originalidad**.

Activar los informes de originalidad en tareas desde la LMS

- Inicia sesión en tu **plataforma de aprendizaje online (LMS)**.
- Selecciona el **curso pertinente**.
- Crea una tarea y selecciona **Tareas de Google**.
- Marca la casilla **Habilitar informes de originalidad**.



Documentación relacionada del Centro de Ayuda

- Classroom: Activar los informes de originalidad
- Tareas de Google: Activar los informes de originalidad

“

¿Cómo puedo permitir que los docentes comparen el trabajo de un alumno con los trabajos de alumnos de años anteriores para buscar posibles casos de plagio?”

Comprobar la originalidad con ayuda de los trabajos de antiguos alumnos

Las coincidencias dentro del centro en los informes de originalidad permiten a los docentes comparar trabajos de los alumnos con los trabajos de antiguos alumnos entregados en años anteriores. Para ello, se cotejan con el contenido de un repositorio privado de trabajos de alumnos, propiedad de la institución.

- Compara las coincidencias entre alumnos que haya entre los trabajos actuales y los entregados en años anteriores para detectar casos de plagio con Teaching and Learning Upgrade o Education Plus.
- Los trabajos de los alumnos pueden almacenarse y archivarse de forma segura en el repositorio privado de todo el dominio, propiedad de la institución.

Instrucciones paso a paso

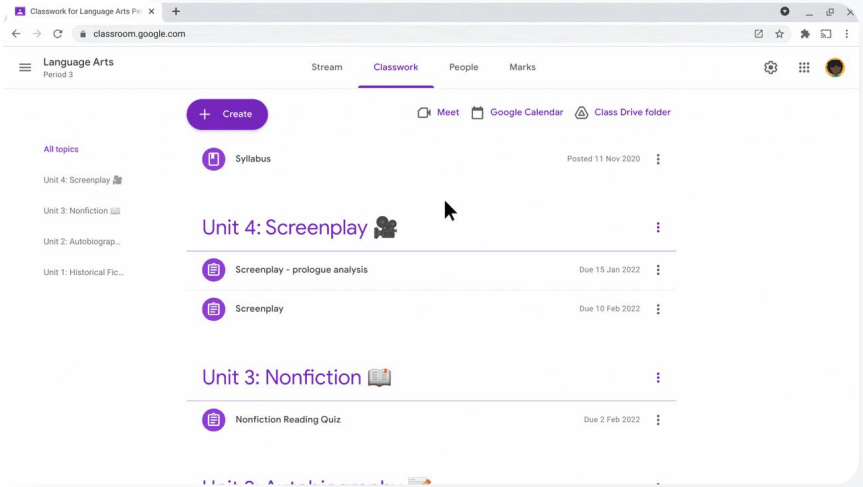
Documentación relacionada del Centro de Ayuda

- Activar los informes de originalidad
- Activar las coincidencias dentro del centro en los informes de originalidad de Classroom

Instrucciones: comprobar la originalidad con ayuda de los trabajos de antiguos alumnos

Cómo activar las coincidencias dentro del centro en los informes de originalidad

- En la consola de administración, selecciona **Menú** > **Aplicaciones** > **Servicios adicionales de Google** > **Classroom**.
- Selecciona la **unidad organizativa del docente**.
- Haz clic en **Informes de originalidad** y marca la casilla **Habilitar coincidencias dentro del centro en informes de originalidad**.
- Haz clic en **Guardar**.



Documentación relacionada del Centro de Ayuda

- Activar las coincidencias dentro del centro en los informes de originalidad de Classroom

“Quiero ofrecer a mis alumnos una oportunidad de aprendizaje sobre cómo citar correctamente sus fuentes”.

Transformar la detección de plagio en oportunidades de aprendizaje

Los alumnos pueden identificar el contenido sin citar y el plagio involuntario antes de entregar su trabajo generando un **informe de originalidad** hasta tres veces por cada tarea. Los informes de originalidad cotejan los trabajos de los alumnos con diversas fuentes y marcan el texto sin citar. De este modo, los alumnos pueden aprender, corregir errores y entregar sus tareas de clase con total confianza.

- Los docentes que usan Teaching and Learning Upgrade o Education Plus pueden generar todos los informes de originalidad que quieran, mientras que los que tienen Education Fundamentals solo pueden activar esta función cinco veces por clase.
- Después de entregar un trabajo, Classroom genera automáticamente un informe que solo el profesor puede ver y, si un alumno anula la entrega de una tarea y la vuelve a enviar, Classroom generará otro informe de originalidad.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

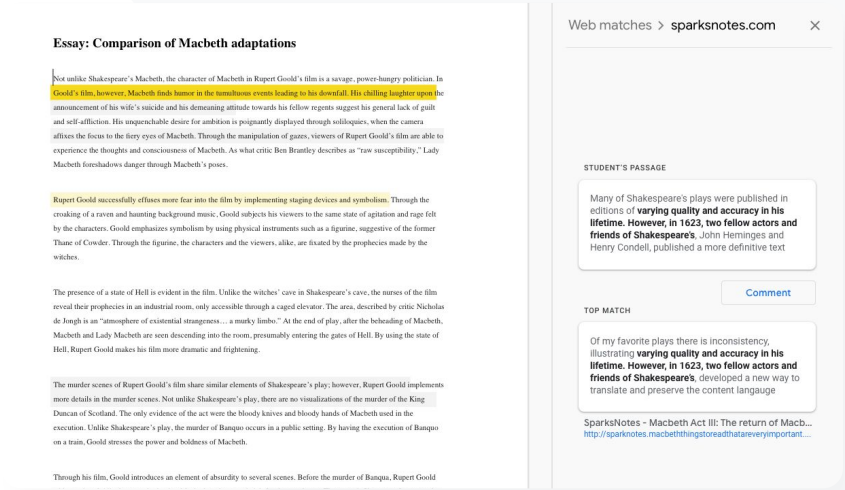
- Generar un informe de originalidad sobre un trabajo

Instrucciones: transformar la detección de plagio en oportunidades de aprendizaje

Cómo pueden los alumnos generar informes de originalidad en Classroom

- Inicia sesión en tu cuenta de Classroom (classroom.google.com).
- En la lista, selecciona la clase que corresponda y elige **Trabajo de clase**.
- Selecciona la tarea que quieras en la lista y haz clic en **Ver tarea**.
- En **Tu trabajo**, selecciona la opción para **subir** o **crear tu archivo**.
- Junto a **Informes de originalidad**, haz clic en **Ejecutar**.
- Para abrir el informe, debajo del nombre del archivo de la tarea, haz clic en **Ver informe de originalidad**.
- Para revisar la tarea o reescribir o citar correctamente fragmentos marcados, en la parte inferior, haz clic en **Editar**.

Los alumnos pueden generar informes de originalidad desde su LMS con Tareas de Google.



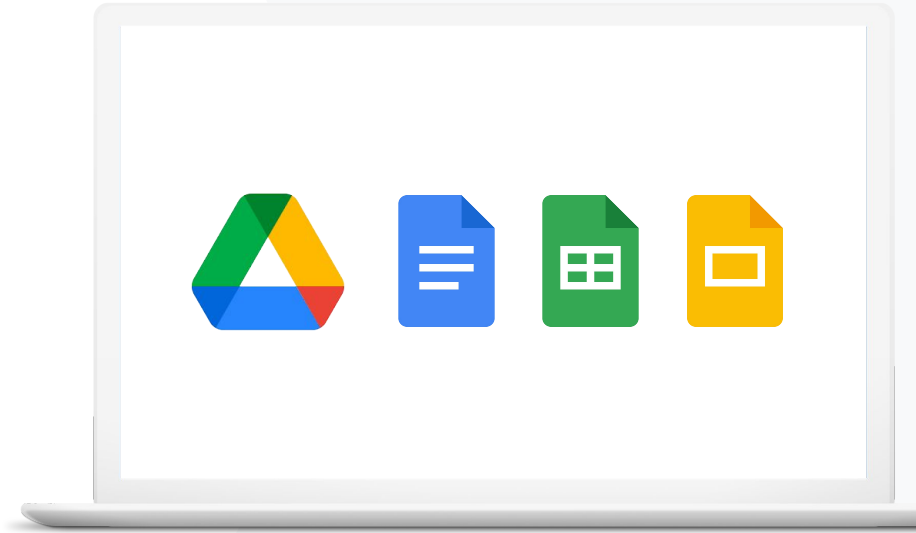
Documentación relacionada del Centro de Ayuda

- Generar un informe de originalidad en Classroom
- Generar un informe de originalidad en la LMS

Documentos, Hojas de cálculo y Presentaciones

¿Qué son?

Estas herramientas permiten a las comunidades educativas colaborar, cocrear, revisar y editar documentos simultáneamente. Las funciones de pago de Education Plus permiten a los docentes y administradores establecer un proceso de aprobación para la documentación interna de tu institución.



Casos prácticos

Aprobar documentos internos — Instrucciones paso a paso

Aprobar documentos internos

Con la función **Aprobaciones**, la comunidad de tu centro educativo puede enviar documentos a Google Drive para someterlos a un proceso de aprobación formal.

- Los revisores pueden aprobar los documentos, rechazarlos o hacer comentarios sobre ellos directamente desde Drive, Documentos y otras aplicaciones de Google Workspace.
- Los responsables de aprobación hacen clic en un enlace que los lleva al documento, donde pueden revisarlo, dejar comentarios y rechazar o aprobar el archivo.
- Gestiona aprobaciones sobre contratos o nuevas contrataciones, aprueba cambios en un documento antes de su publicación, etc.

“El departamento de Ciencias está desarrollando un nuevo plan de estudios.

¿Cómo pueden asegurarse de que todos los jefes de los distintos departamentos aprueben la propuesta del plan de estudios?”

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Gestionar aprobaciones

Documentos, Hojas de cálculo y Presentaciones

Herramientas de enseñanza y aprendizaje

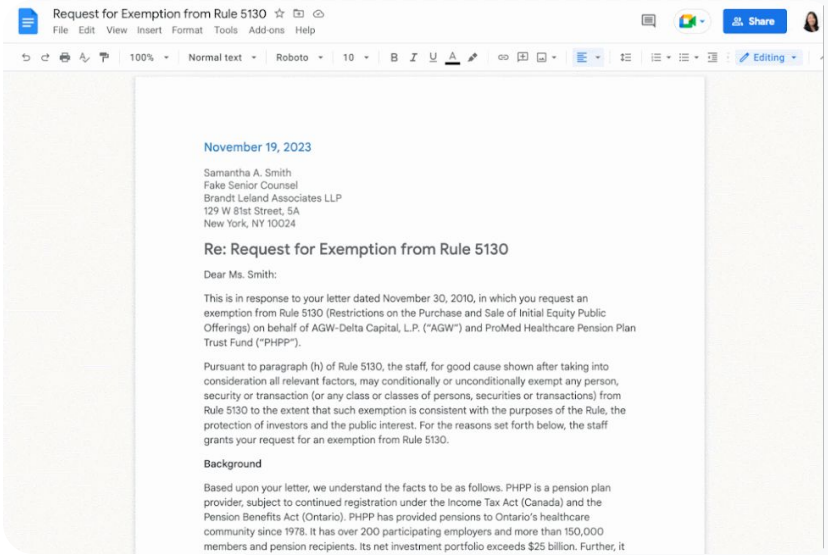
Instrucciones: aprobar documentos internos

Cómo funciona

Los administradores pueden controlar en qué grado participan en el proceso de aprobación los usuarios y los archivos.

Cómo gestionar las aprobaciones

- Inicia sesión en tu **consola de administración** y ve a **Menú** > **Aplicaciones** > **Google Workspace** > **Drive y Documentos**.
- Haz clic en **Aprobaciones**.
- Si quieres aplicar la configuración a todos los usuarios, selecciona una **unidad organizativa** secundaria o un **grupo de configuración**.
- Haz clic en **Guardar**.



Documentación relacionada del Centro de Ayuda

- Gestionar aprobaciones

Google Meet

¿Qué es?

Entre las funciones avanzadas de Google Meet se incluyen emisiones en directo, grupos de trabajo, reuniones con un número de asistentes mayor, grabaciones de reuniones, subtítulos con traducción instantánea y muchas más.

Casos prácticos

Grabar reuniones — Instrucciones paso a paso	Hacer preguntas — Instrucciones paso a paso
Transcribir lo que se ha tratado en clase — Instrucciones paso a paso	Recopilar comentarios — Instrucciones paso a paso
Eliminar la barrera del idioma — Instrucciones paso a paso	Grupos pequeños de alumnos — Instrucciones paso a paso
Emitir asambleas y eventos escolares — Instrucciones paso a paso	Registrar asistencias — Instrucciones paso a paso

“Nuestra institución ofrece clases online de desarrollo profesional con muchos asistentes y necesitamos grabarlas para los docentes que no pueden asistir”.

Grabar reuniones

Con Teaching and Learning Upgrade y Education Plus, los docentes pueden grabar clases, reuniones del profesorado, formaciones de desarrollo profesional, etc. Las reuniones se guardan automáticamente en Drive.

- Las grabaciones se guardan en la cuenta de Drive del organizador de la reunión. Antes de grabar, asegúrate de que haya suficiente espacio en Drive.
- Se recomienda que los administradores de TI solo permitan grabar reuniones a los profesores y al personal del centro.

Instrucciones paso a paso

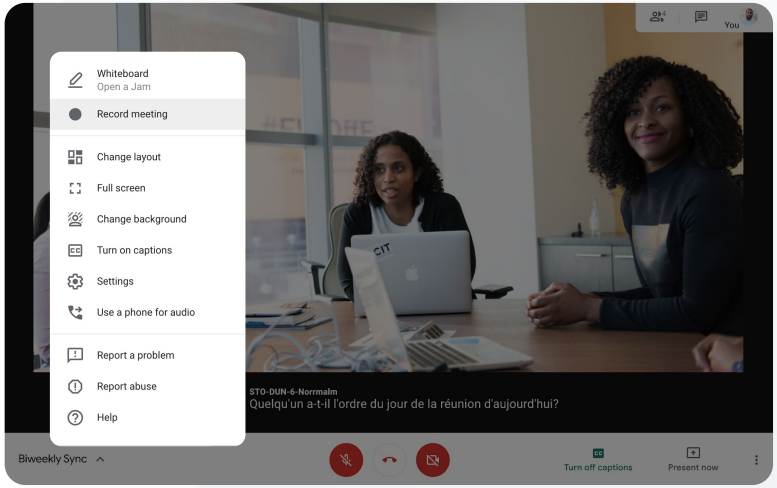
Documentación relacionada del Centro de Ayuda

- Grabar videollamadas

Instrucciones: grabar reuniones

Cómo iniciar una grabación

- Inicia sesión en **Google Meet o únete a una reunión.**
- Haz clic en **Actividades** > **Grabación.**
- Selecciona **Iniciar grabación.**
- En la ventana que se abre, haz clic en **Iniciar.**
- Aparecerá un círculo rojo en la parte inferior derecha de la pantalla para indicar que la reunión se está grabando.
- Se guardará automáticamente un archivo de vídeo de la reunión en tu unidad de Drive.



Documentación relacionada del Centro de Ayuda

- Grabar videollamadas

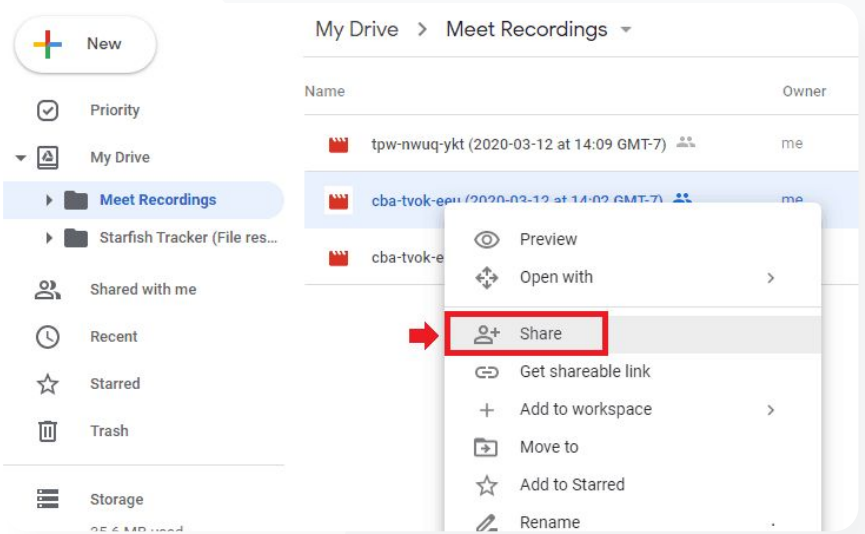
Instrucciones: ver y compartir grabaciones

Cómo iniciar una grabación

- Selecciona el archivo.
- Haz clic en el icono para **compartir**.
- **Añade a los** usuarios autorizados a verla.

O

- Selecciona el icono del **enlace**.
- **Pega** el enlace en un correo o en un mensaje de Chat.



Cómo descargar una grabación

- Selecciona el archivo.
- Haz clic en el icono **Más** y, después, en Descargar.
- **Haz doble clic** en el archivo descargado para reproducirlo.

Cómo reproducir una grabación en Drive

- En Drive, haz doble clic en el archivo de una grabación para reproducirlo. Se mostrará el mensaje "Aún se está procesando" hasta que el archivo se pueda ver online.
- Para añadir una grabación a tu unidad de Drive, selecciona el archivo y haz clic en **Añadir a Mi unidad.**

Documentación relacionada del Centro de Ayuda

- Grabar videollamadas

“¿Cómo puedo transcribir una clase virtual para que los alumnos repasen los conceptos más adelante?”

Transcribir lo que se ha tratado en clase

Gracias a las transcripciones de reuniones, los docentes pueden grabar automáticamente las clases y los temas tratados, lo que permite que los alumnos repasen los conceptos. Las transcripciones hacen un seguimiento de la asistencia a la reunión y muestran qué comentarios hizo cada usuario.

- Esta función está disponible en inglés para los usuarios de Google Meet que usen un ordenador de sobremesa o un portátil.
- Los administradores pueden habilitar la función de transcripción para su comunidad escolar.
- Las transcripciones se guardan automáticamente en la cuenta de Drive del anfitrión de la reunión.
- Cuando se activa la función de transcripciones de reuniones, se muestra en la parte superior izquierda de la pantalla de la reunión de todos los usuarios el icono correspondiente.
- Las transcripciones registran todo lo que se ha hablado en una reunión. Para obtener una transcripción de los mensajes de chat, deberás grabar la reunión.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Utilizar la función de transcripciones con Google Meet
- Activar o desactivar la transcripción

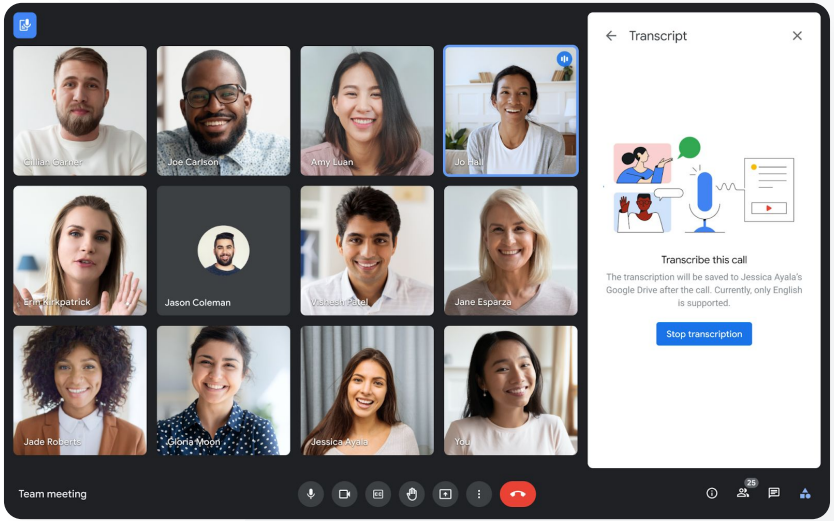
Instrucciones: transcribir lo que se ha tratado en clase

Cómo activar las transcripciones en Google Meet

- En una reunión, selecciona el icono **Actividades**, situado en la esquina inferior derecha.
- Haz clic en **Transcripciones** > **Iniciar transcripción** > **Iniciar**.

Cómo detener las transcripciones en Google Meet

- Selecciona el icono **Actividades** > **Transcripciones** > **Detener transcripción** > **Detener**.



Documentación relacionada del Centro de Ayuda

- Utilizar la función de transcripciones con Google Meet
- Activar o desactivar la transcripción

Organizamos encuentros digitales entre padres y profesores, pero hay ocasiones en las que no todos los asistentes hablan el mismo idioma.

¿Cómo puedo conseguir que estas reuniones sean inclusivas y superar la barrera del idioma?"

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Usar subtítulos traducidos en Google Meet

Eliminar la barrera del idioma

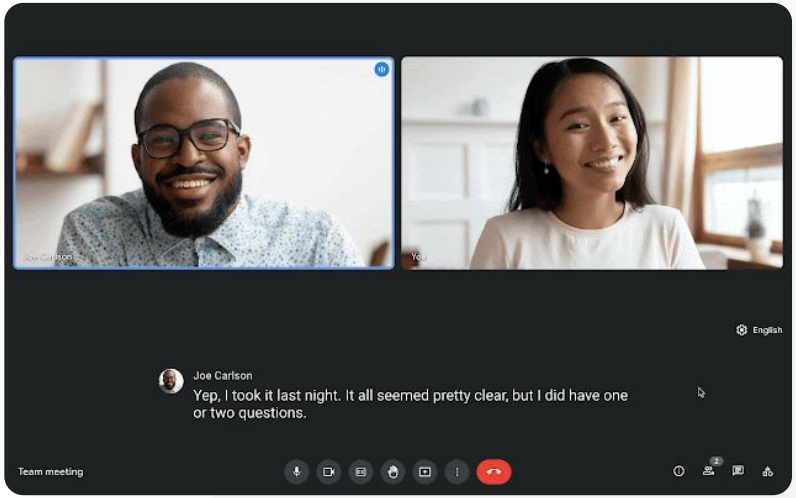
La función de traducción de subtítulos permite que las reuniones sean más inclusivas al eliminar la barrera del idioma. Cuando los participantes de una reunión reciben el contenido en su idioma de preferencia, esto proporciona un equilibrio en la colaboración, el aprendizaje y el uso compartido de la información.

- Los docentes pueden interactuar con los alumnos, los padres y los miembros de la comunidad que hablen un idioma distinto.
- La función de traducción de subtítulos se puede utilizar para traducir del inglés al alemán, español, francés, portugués y viceversa.
- También puedes traducir del inglés al japonés, mandarín o sueco.

Instrucciones: eliminar la barrera del idioma

Cómo activar la traducción de subtítulos

- En una reunión, en la parte inferior de la pantalla, haz clic en **Más opciones** > **Ajustes** > **Subtítulos**.
- Activa la opción **Subtítulos**.
- Selecciona el **idioma de la reunión**.
- Activa la opción **Subtítulos traducidos**.
- Selecciona el **idioma al que los quieras traducir**.



Documentación relacionada del Centro de Ayuda

- Usar subtítulos traducidos en Google Meet

“Necesitamos emitir en directo las reuniones del profesorado y el personal del centro para que un amplio grupo de colaboradores y padres puedan verlas”.

Emitir asambleas, eventos escolares y reuniones

Emite en directo para hasta 10.000 usuarios con Teaching and Learning Upgrade o hasta 100.000 con Education Plus. Los participantes pueden unirse a las emisiones en directo seleccionando el enlace que el organizador incluya en un correo o en una invitación de Calendar.

- Determina el alcance que tendrá la emisión en directo. Escoge entre las siguientes opciones:
  - Solo será visible para los usuarios de tu organización (dominio).
  - Podrá compartirse con otros dominios de Google Workspace de confianza.
  - Podrá verse en YouTube.
- Lo recomendable es que los administradores de TI habiliten las emisiones en directo exclusivamente para el profesorado y el personal del centro.
- Si un usuario se pierde la emisión en directo de una reunión, podrá verla cuando esta termine.
- Añade subtítulos, encuestas y preguntas a las emisiones en directo para aumentar la inclusividad y la participación.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Activar o desactivar la función de emisión en directo de Meet
- Emitir videollamadas en directo

Instrucciones: emitir asambleas, eventos escolares y reuniones

Cómo crear un evento de emisión en directo

- Abre **Google Calendar**.
- Selecciona **+ Crear** > **Más opciones**.
- Añade los detalles del evento, como la fecha, la hora y una descripción.
- Añade a los usuarios que puedan participar plenamente en la videollamada (es decir, aquellos que estén dispuestos a activar la cámara, a que se les escuche y a presentar).
- Haz clic en **Añadir videollamada de Google Meet** > **Meet**.
- Junto a la opción Unirme con Google Meet, selecciona la **flecha hacia abajo** y, a continuación, **Añadir emisión en directo**.
- Para invitar a tantos usuarios como permita la edición pagada, haz clic en **Copiar** y comparte la URL de la emisión en directo.
- Selecciona **Guardar**.
- La emisión no se inicia automáticamente. Durante la reunión, deberás seleccionar **Más** > **Iniciar emisión**.

Documentación relacionada del Centro de Ayuda

- Activar o desactivar la función de emisión en directo de Meet
- Emitir videollamadas en directo

“Necesito un método rápido para plantear preguntas, evaluar los conocimientos de los alumnos e interactuar con ellos para que participen”.

Hacer preguntas

Usa la sección **Preguntas** de Google Meet para que los alumnos participen y hacer que la clase sea más interactiva. Los docentes obtendrán un informe detallado de todas las preguntas y respuestas al final de la clase virtual.

- Los moderadores pueden hacer todas las preguntas que quieran, así como filtrar u ordenar preguntas, marcarlas como respondidas e, incluso, ocultarlas o priorizarlas.
- Una vez finalizadas las reuniones que tengan activada la función Preguntas, se enviará por correo un informe con las preguntas al moderador.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Hacer preguntas a los participantes en Google Meet

Instrucciones: hacer preguntas

Hacer una pregunta

- En la esquina superior derecha de una reunión, selecciona el **icono Actividades** > **Preguntas** (para activar las preguntas, selecciona **Activar Preguntas**).
- Para plantear una pregunta, en la esquina inferior derecha, haz clic en **Haz una pregunta**.
- **Escribe tu pregunta** y selecciona **Publicar**.

Consultar el informe de preguntas

- Después de una reunión, los moderadores **reciben un informe de preguntas por correo**.
- Abre el correo y haz clic en el **informe adjunto**.

Documentación relacionada del Centro de Ayuda

- Hacer preguntas a los participantes en Google Meet

“Necesito recopilar fácilmente comentarios de los alumnos y de otros profesores mientras doy una clase o dirijo una reunión del claustro”.

Recopilar comentarios

La persona que ha programado o iniciado una reunión virtual puede crear una **encuesta** para los participantes de la reunión. Esta función sirve para agrupar la información de todos los alumnos o participantes de una reunión de manera rápida e interactiva.

- Los moderadores pueden guardar las encuestas para publicarlas más tarde durante la reunión. Se guardan en la sección Encuestas de las reuniones virtuales.
- Tras la reunión, el informe con los resultados de la encuesta se envía automáticamente por correo al moderador.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Hacer encuestas en Google Meet

Instrucciones: recopilar comentarios

Crear encuestas

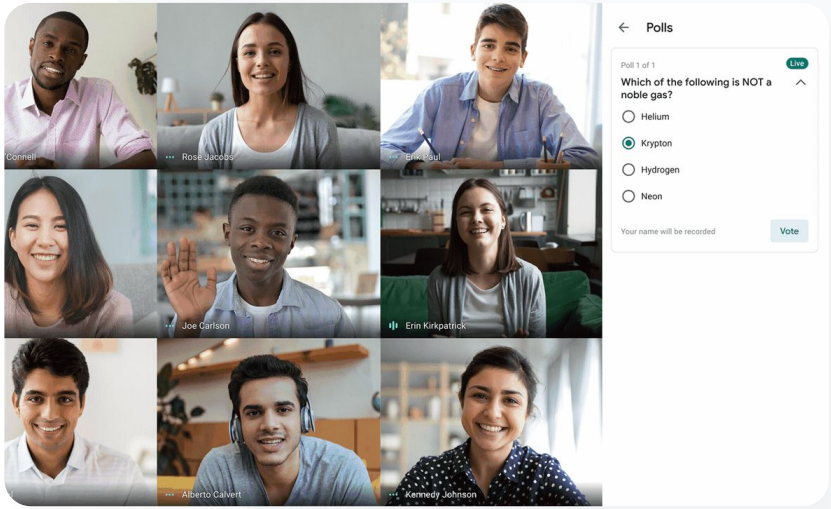
- En la esquina superior derecha de una reunión, selecciona el **icono Actividades** y, después, haz clic en **Encuesta.**
- Selecciona **Iniciar una encuesta.**
- Escribe una pregunta.
- Selecciona **Iniciar** o **Guardar.**

Moderar encuestas

- En la esquina superior derecha de una reunión, selecciona el **icono Actividades** > **Encuesta.**
- Para permitir que los participantes vean los resultados de la encuesta en tiempo real, junto a la opción **Mostrar los resultados a todo el mundo**, selecciona el **interruptor para activarla.**
- Para cerrar una encuesta y no permitir respuestas, haz clic en **Terminar la encuesta**
- Para eliminar una encuesta de forma permanente, selecciona el **icono Eliminar.**

Ver informes de encuestas

- Después de una reunión, los moderadores **reciben un informe por correo.**
- Abre el correo y selecciona el **informe adjunto.**



Documentación relacionada del Centro de Ayuda

- Hacer encuestas en Google Meet

“Algunos de nuestros alumnos reciben formación desde casa. Cuando hacemos trabajos en grupos reducidos, necesito tener una forma de crear grupos de trabajo de forma sencilla a partir de grupos predefinidos”.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Utilizar grupos de trabajo en Google Meet

Clases en grupos reducidos

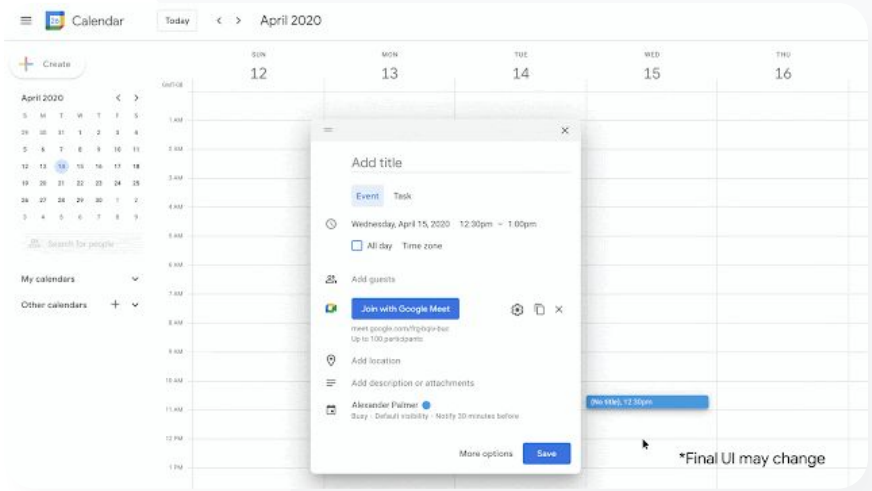
Los docentes pueden usar los grupos de trabajo para dividir a los alumnos en grupos reducidos durante las sesiones de formación virtuales, **híbridas o presenciales**. Solo los moderadores pueden iniciar grupos de trabajo, y únicamente durante una videollamada y desde un ordenador.

- Los grupos de trabajo pueden prepararse con antelación, al crear un evento o mientras tiene lugar la reunión.
- Se pueden crear hasta 100 grupos de trabajo por reunión virtual.
- Los profesores pueden pasar fácilmente de un grupo de trabajo a otro para ofrecer ayuda cuando la necesiten.
- Los administradores pueden asegurarse de que solo los profesores o el personal del centro puedan crear grupos de trabajo.

Instrucciones: crear grupos reducidos de alumnos

Crear grupos de trabajo antes de la reunión

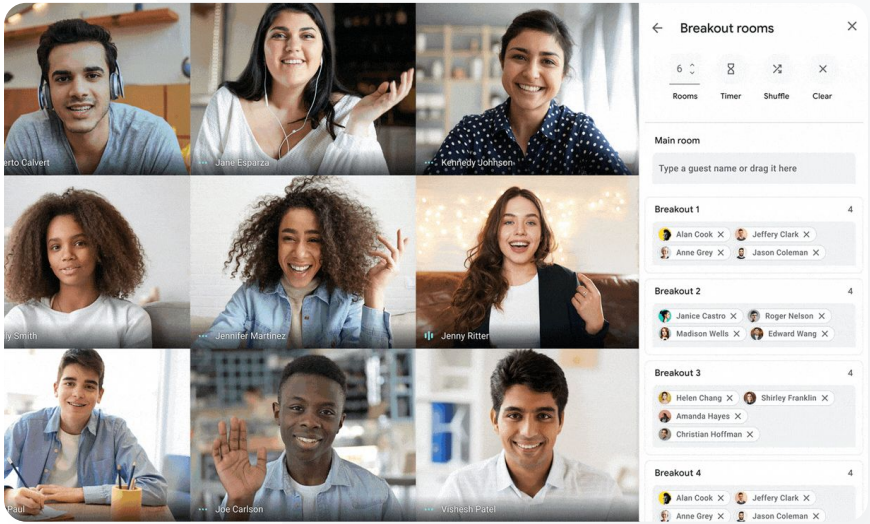
- Crea un evento de Google Calendar.
- Haz clic en **Añadir videollamada de Google Meet**.
- Añade a los participantes y selecciona **Cambiar configuración de conferencia**.
- Haz clic en **Grupos de trabajo.**
- Selecciona el número de grupos de trabajo y, después, elige entre una de las siguientes opciones:
  - Arrastra a los participantes a diferentes salas.
  - Escribe los nombres directamente en una sala.
  - Haz clic en **Distribuir aleatoriamente** para crear grupos de participantes mezclados al azar.
- Haz clic en **Guardar**.



Documentación relacionada del Centro de Ayuda

- Utilizar grupos de trabajo en Google Meet

Instrucciones: crear grupos reducidos de alumnos



Crear grupos de trabajo durante la reunión

- Inicia una videollamada.
- En la parte superior derecha, selecciona el **icono Actividades** > **Grupos de trabajo**.
- En el panel **Grupos de trabajo**, selecciona el número de grupos que necesites.
- A continuación, se divide a los alumnos en grupos. Los moderadores pueden cambiarlos manualmente de grupo si fuera necesario.
- En la parte inferior derecha, haz clic en **Abrir grupos**.

Responder preguntas en distintos grupos de trabajo

- Cuando algún participante pida ayuda, se mostrará una notificación en la parte inferior de la pantalla de los moderadores. Selecciona Unirme para acceder al grupo de trabajo de ese participante.

Documentación relacionada del Centro de Ayuda

- Utilizar grupos de trabajo en Google Meet

“Nos cuesta llevar un seguimiento de quiénes asisten a las clases online. Queremos una herramienta que nos permita registrar la asistencia a las clases fácilmente en todo el dominio”.

Registrar asistencias

Seguimiento de asistencia proporciona automáticamente un informe de asistencia de todas las reuniones que tengan cinco participantes o más. Los informes muestran quién se ha unido a la llamada e incluyen los correos de los participantes y durante cuánto tiempo han asistido a la clase virtual.

- Puedes registrar la asistencia durante los eventos emitidos en directo gracias a los informes de emisión en directo.
- Los moderadores pueden activar o desactivar los informes de Seguimiento de asistencia y de emisión en directo desde el evento de Calendar.

Instrucciones paso a paso

Documentación relacionada del Centro de Ayuda

- Registrar la asistencia en Google Meet

Instrucciones: registrar asistencias

Cómo registrar la asistencia desde una reunión

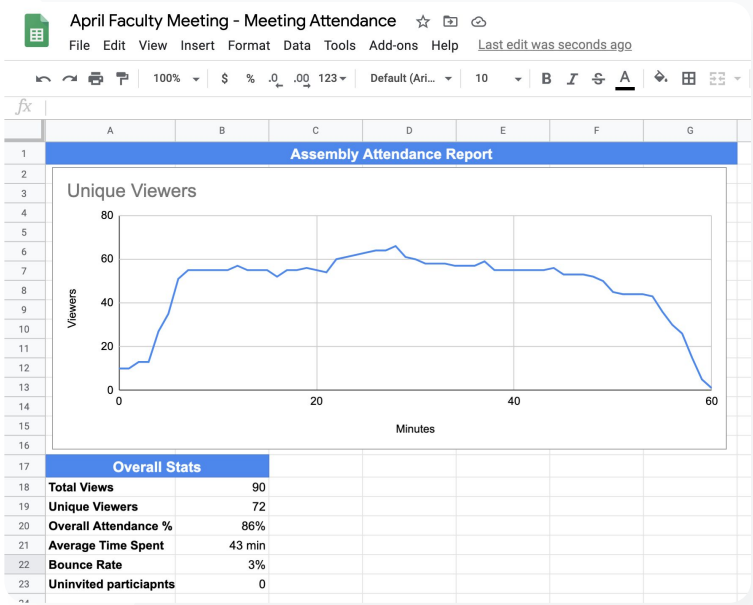
- Inicia una videollamada.
- En la parte inferior, selecciona el **icono del menú**.
- Selecciona el **icono de Ajustes** > **Controles del organizador**.
- Activa o desactiva **Seguimiento de asistencia**.

Cómo registrar la asistencia en Calendar

- **Habilita las conferencias de Google Meet** desde un evento de Calendar.
- En la parte derecha, selecciona el **icono de Configuración**.
- Marca la casilla junto a **Seguimiento de asistencia** y haz clic en **Guardar**.

Obtener el informe de asistencia

- Después de una reunión, los moderadores **reciben un informe por correo**.
- Abre el correo y selecciona el **informe adjunto**.



Documentación relacionada del Centro de Ayuda

- Registrar la asistencia en Google Meet

¡Gracias!