Google for Education

Descubre más de 40 formas de usar las ediciones pagadas de Google Workspace for Education

goo.gle/use-edu-workspace

Cómo usar esta presentación

Esta presentación incluye una selección de los casos de uso más populares de las **ediciones pagadas de Google Workspace for Education**. Estas herramientas permiten aumentar **la seguridad de los datos, la eficiencia de los profesores, la participación de los alumnos, la colaboración en toda la institución educativa** y mucho más.

La presentación está organizada por **función**; se incluyen **casos de uso comunes** y, además, **instructivos** para usar cada función. Revisa la presentación completa y descubre todo lo que puedes hacer con las ediciones pagadas de Google Workspace for Education.

Ediciones pagadas de Google Workspace for Education

Obtén más opciones, control y flexibilidad para satisfacer las necesidades de tu organización con estas tres ediciones pagadas de Google Workspace for Education.

Google Workspace for Education Plus

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

Education Plus proporciona a los alumnos, profesores, líderes del sector de la educación y administradores de TI una solución **integral** de tecnología educativa con herramientas fáciles de usar **que brindan seguridad y estadísticas avanzadas, y enseñanza y aprendizaje enriquecidos**.

Google Workspace for Education Standard

Herramientas avanzadas de seguridad y estadísticas que ayudan a reducir los riesgos y mitigar las amenazas con visibilidad aumentada y control en todo el entorno de aprendizaje.

Teaching and Learning Upgrade

Herramientas mejoradas de enseñanza y aprendizaje que generan un impacto en la educación, ayudan a personalizar más la recepción de conocimiento, impulsan la eficiencia en el aula y posibilitan la formación integral desde cualquier lugar.

Índice

Funciones avanzadas de seguridad y estadísticas

Panel de seguridad

- Volumen de spam
- Uso compartido externo de archivos
- Aplicaciones de terceros
- Intento de suplantación de identidad (phishing)

Página del estado de seguridad

- Prácticas recomendadas de seguridad
- Recomendaciones para áreas de riesgo

Herramienta de investigación

- Material inadecuado que se comparte
- Archivos que se comparten por accidente
- Correos electrónicos de suplantación de identidad (phishing) y software malicioso
- Frena a los actores malicios
- Estadísticas de seguridad más detalladas
- Evita las reuniones no supervisadas

Controles y administración del dominio

- Análisis de virus en archivos adjuntos de Gmail
- Crea informes y paneles de uso
- Encuentra archivos con mayor facilidad
- Documentos internos organizados
- Propaga automáticamente grupos de departamentos
- Crea públicos para el uso compartido interno de archivos
- Restringe el uso de archivos compartidos
- Restricciones de la app de Workspace
- Administración del almacenamiento
- Reglamentaciones de datos
- Reglamentaciones relacionadas con los permisos
- Administra dispositivos de extremo
- Administra dispositivos con Windows
- Parámetros de configuración personalizados para dispositivos con Windows
- Automatiza las actualizaciones de dispositivos con Windows
- Aprovecha la encriptación del cliente

Índice

Mejora las funciones de enseñanza y aprendizaje

Google Classroom

- Administra el acceso a los complementos de Classroom
- Integra contenido atractivo en Classroom
- Crea clases a gran escala

Informes de originalidad

- Detecta casos de plagio con los informes de originalidad
- Verifica la originalidad según los trabajos previos de los alumnos
- Convierte la detección de plagio en una oportunidad de aprendizaje

Documentos, Hojas de cálculo y Presentaciones

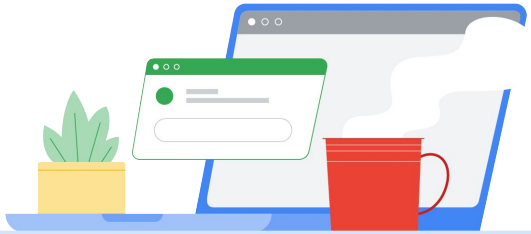
- Aprueba documentos internos

Google Meet

- Graba reuniones
- Haz referencia al contenido de las clases
- Derriba las barreras lingüísticas
- Transmite en vivo asambleas y eventos institucionales
- Haz preguntas
- Recopila comentarios
- Grupos pequeños de alumnos
- Seguimiento de la asistencia

Funciones avanzadas de seguridad y estadísticas

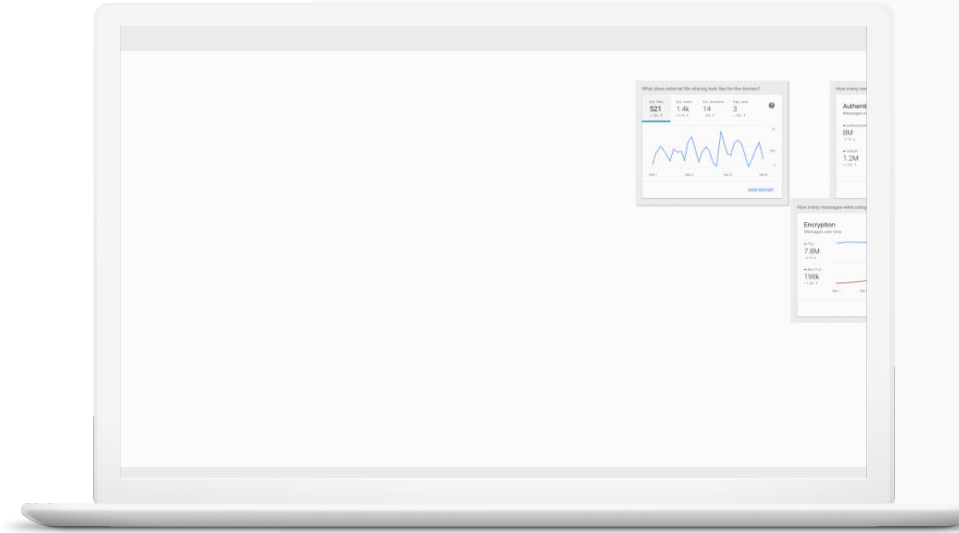
Obtén más control en todo tu dominio con herramientas de seguridad proactivas que te ayudan a protegerte de las amenazas, analizar incidentes de seguridad y proteger los datos de los alumnos y el cuerpo docente.



Panel de seguridad

¿De qué se trata?

Usa el panel de seguridad para ver una descripción general de varios informes de seguridad. De forma predeterminada, cada panel de informe de seguridad muestra datos de los últimos siete días. Puedes personalizar el panel para visualizar datos de hoy, ayer, esta semana, la semana anterior, este mes, el mes anterior o por días (hasta 180 días).



Casos de uso

Volumen de spam	Instructivo paso a paso
Uso compartido externo de archivos	Instructivo paso a paso
Aplicaciones de terceros	Instructivo paso a paso
Intento de suplantación de identidad (phishing)	Instructivo paso a paso

“Quiero tener la capacidad de controlar la cantidad excesiva de correos electrónicos innecesarios y, al mismo tiempo, reducir las amenazas para la escuela”.

Volumen de spam

El **panel de seguridad** proporciona una representación visual de las actividades en el entorno de Google Workspace for Education, incluidas las siguientes:

- Spam
- Suplantación de identidad (phishing)
- Software malicioso
- Archivos adjuntos sospechosos
- Y mucho más

Instructivo paso a paso

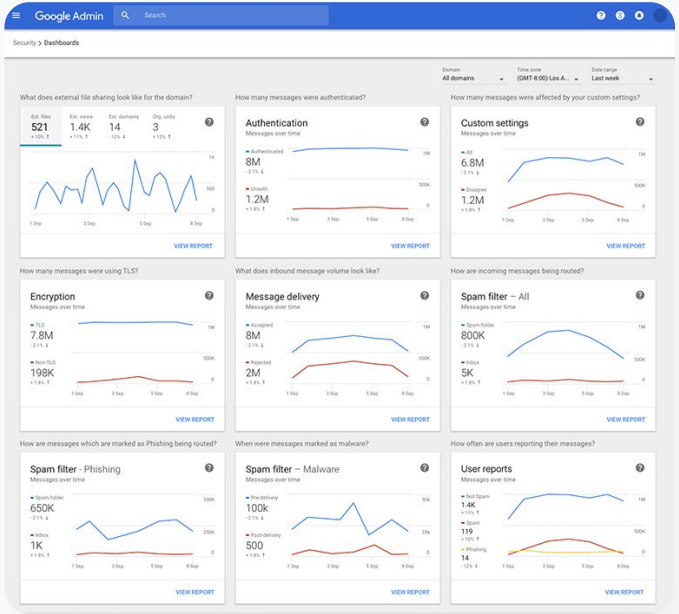
Documentación relevante del Centro de ayuda

- Acerca del panel de seguridad

Instructivo: Descripción general del panel

Cómo visualizar el panel de seguridad

- Accede a la **Consola del administrador.**
- Haz clic en **Seguridad** (Security) > **Panel** (Dashboard).
- Desde el panel de seguridad, puedes explorar detalles de los datos, exportarlos a Hojas de cálculo o a una herramienta de terceros, o iniciar una investigación en la herramienta de investigación.



Documentación relevante del Centro de ayuda

- Acerca del panel de seguridad

Quiero ver la actividad de uso compartido externo de archivos para prevenir que se compartan datos sensibles con terceros".

Uso compartido externo de archivos

Consulta el **informe "Visibilidad de archivos"** en el **panel de seguridad** para ver las métricas de uso compartido externo de archivos del dominio, que incluye la siguiente información:

- Cantidad de eventos de archivos compartidos a usuarios fuera del dominio por un período específico
- Cantidad de vistas de un archivo externo recibido durante un período especificado

Instructivo paso a paso

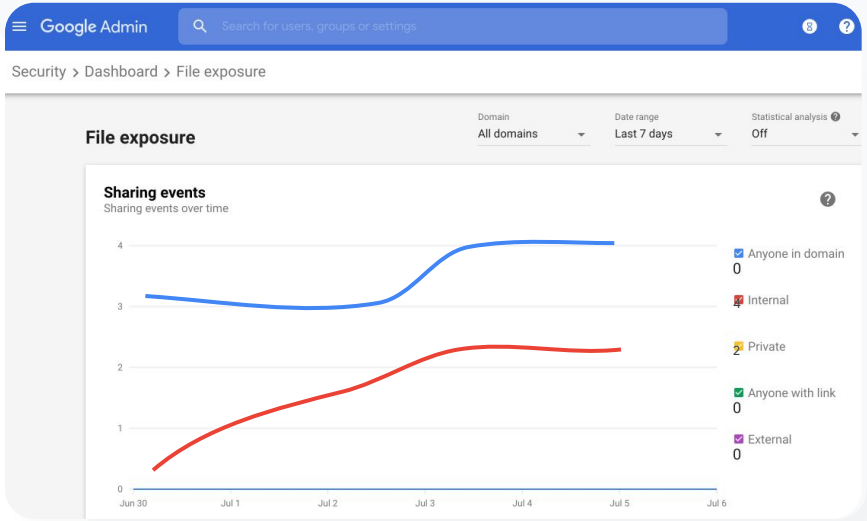
Documentación relevante del Centro de ayuda

- Comienza a usar la página Estado de seguridad

Instructivo: Uso compartido externo de archivos

Cómo consultar el informe “Visibilidad de archivos”

- Accede a la **Consola del administrador.**
- Haz clic en **Seguridad** (Security) > **Panel** (Dashboard).
- En el panel con el título, “**¿Cuál es el estado del uso compartido externo de archivos del dominio?**”, haz clic en **Ver informe** en la esquina inferior derecha.



Documentación relevante del Centro de ayuda

- Acerca del panel de seguridad
- Informe “Visibilidad de archivos”

Aplicaciones de terceros

Quiero ver las aplicaciones de terceros que tienen acceso a los datos del dominio”.

Consulta el **informe Actividad de permisos de OAuth** del **panel de seguridad** para supervisar las aplicaciones de terceros que están conectadas al dominio y verificar a qué datos pueden acceder.

- OAuth otorga permiso a servicios de terceros para que accedan a la información de la cuenta del usuario sin exponer su contraseña. Se recomienda limitar el acceso de apps de terceros.
- Usa el panel Actividad de permisos de OAuth para supervisar las actividades relacionadas por app, permiso o usuario, y para actualizar el otorgamiento de permisos.

Instructivo paso a paso

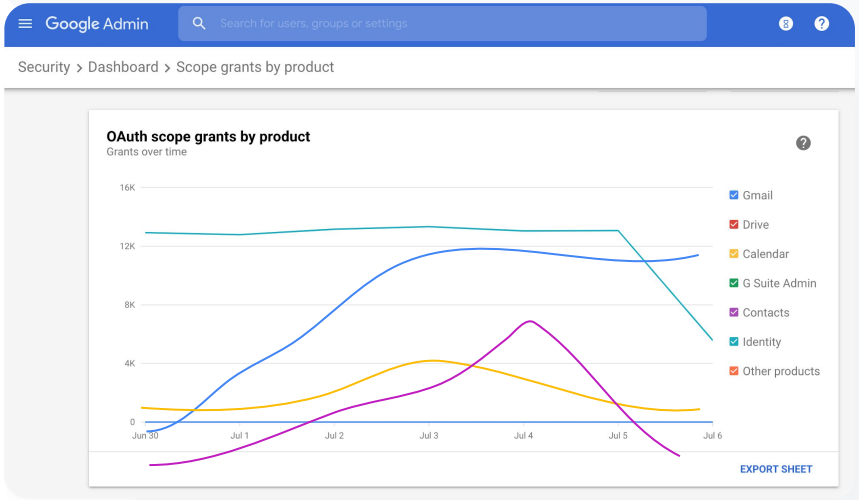
Documentación relevante del Centro de ayuda

- Informe Actividad de permisos de OAuth

Instructivo: Aplicaciones de terceros

Cómo visualizar el informe Actividad de permisos de OAuth

- Accede a la **Consola del administrador.**
- Haz clic en **Seguridad** (Security) > **Panel** (Dashboard).
- En la parte inferior, haz clic en **Ver informe**.
- Puedes ver la actividad de permiso de OAuth por producto (app), permiso o usuario.
- Para filtrar la información, haz clic en la **app**, el **permiso** o el **usuario** que quieras consultar.
- Para generar un informe en hoja de cálculo, haz clic en **Exportar hoja** (Export sheet).



Documentación relevante del Centro de ayuda

- Informe Actividad de permisos de OAuth

Los usuarios denunciaron un intento de suplantación de identidad (phishing). Quiero tener la capacidad de hacer un seguimiento del momento en que llegó el correo electrónico de suplantación de identidad, qué contenía exactamente y a qué riesgos estuvieron expuestos los usuarios que lo recibieron".

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- ¿Cómo marcan los usuarios sus correos electrónicos?
- Denuncias de usuarios

Intento de suplantación de identidad (phishing)

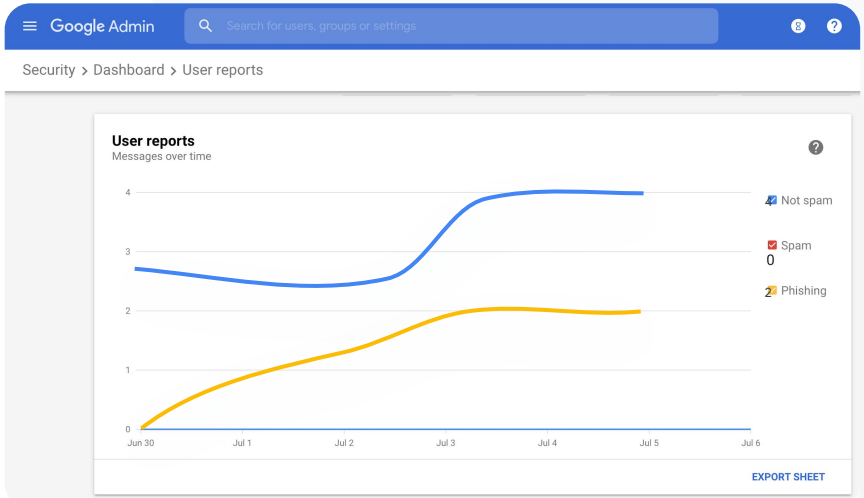
La sección **Denuncias de usuarios** del **panel de seguridad** te permite ver los mensajes que se marcaron como suplantación de identidad (phishing) o spam durante un período específico. Podrás ver información sobre los correos electrónicos marcados como suplantación de identidad, como los destinatarios y las veces que se abrieron.

- En Denuncias de usuarios, podrás ver cómo los usuarios marcan sus mensajes, ya sea como spam, no es spam o suplantación de identidad, durante un período específico.
- Puedes personalizar el gráfico para obtener detalles sobre ciertos tipos de mensajes únicamente (por ejemplo, si el mensaje se envió de forma interna o externa, por período, etcétera).

Instructivo: Intento de suplantación de identidad (phishing)

Cómo visualizar el panel Informes de los usuarios

- Accede a la **Consola del administrador.**
- Haz clic en **Seguridad** (Security) > **Panel** (Dashboard).
- En la esquina inferior derecha del **panel Denuncias de usuarios**, haz clic en **Ver informe**.



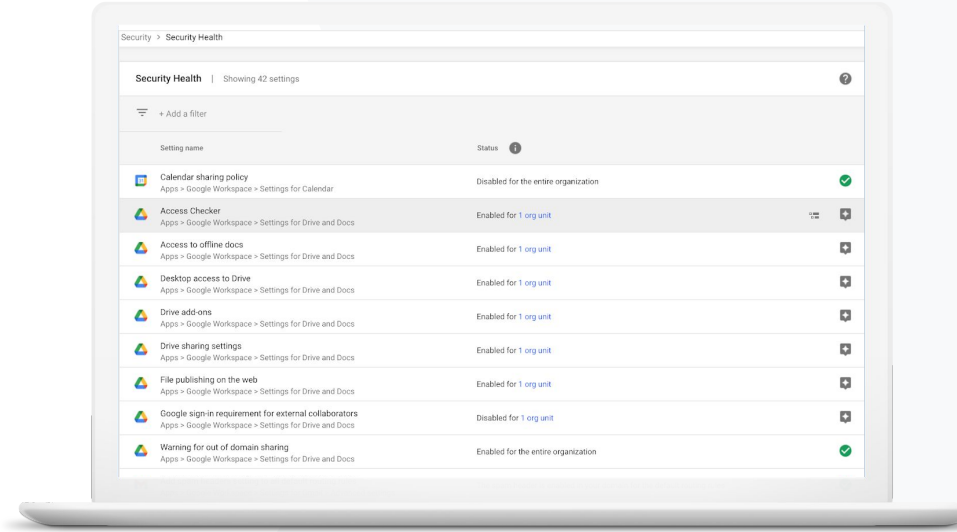
Documentación relevante del Centro de ayuda

- Acerca del panel de seguridad
- Informe “Visibilidad de archivos”

Estado de seguridad

¿De qué se trata?

La página Estado de seguridad proporciona una descripción general completa de la postura que tiene tu entorno de Google Workspace con respecto a la seguridad y te permite comparar tu configuración con las recomendaciones de Google para proteger tu organización de forma proactiva.



Casos de uso

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

Necesito orientación sobre las prácticas recomendadas o las recomendaciones para configurar las políticas de seguridad".

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Comienza a usar la página Estado de seguridad

Prácticas recomendadas de seguridad

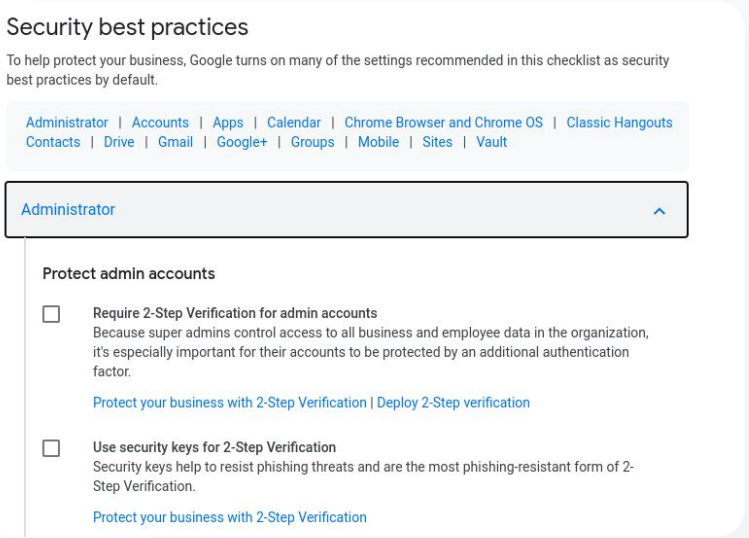
Abre la página Estado de seguridad para ver las prácticas recomendadas sobre políticas de seguridad mediante lo siguiente:

- Recomendaciones para posibles áreas de riesgo en el dominio
- Recomendaciones sobre los parámetros de configuración óptimos para aumentar la eficacia de la seguridad
- Vínculos directos a los parámetros de configuración
- Información adicional y artículos de asistencia

Instructivo: Lista de tareas de las prácticas recomendadas sobre seguridad

Para ayudarte a proteger tu organización, Google habilita de forma predeterminada muchos de los parámetros de configuración recomendados en la lista de tareas como prácticas recomendadas de seguridad. Te recomendamos revisar con más detalle las prácticas destacadas a continuación.

- **Administrador (Administrator):** Protege las cuentas de administrador.
- **Cuentas (Accounts):** Ayuda a prevenir y corregir problemas de cuentas hackeadas.
- **Apps:** Revisa el acceso de terceros a los servicios principales.
- **Calendario (Calendar):** Limita el uso compartido de calendarios de forma externa.
- **Drive:** Limita el uso compartido y las actividades de colaboración fuera del dominio.
- **Gmail:** Configura la autenticación y la infraestructura.
- **Vault:** Controla, audita y protege las cuentas de Vault.



Documentación relevante del Centro de ayuda

- Supervisa el estado de la configuración de seguridad

Quiero ver un resumen de la configuración de seguridad de mi dominio, con recomendaciones de medidas para abordar las posibles áreas de riesgo”.

Recomendaciones para áreas de riesgo

En la página **Estado de seguridad**, se analiza tu configuración de seguridad y se destacan los cambios recomendados. Podrás hacer lo siguiente:

- Identificar las posibles áreas de riesgo en tu dominio con rapidez
- Obtener recomendaciones sobre los parámetros de configuración óptimos para aumentar la eficacia de la seguridad
- Leer información adicional y artículos de asistencia sobre las recomendaciones

Instructivo paso a paso

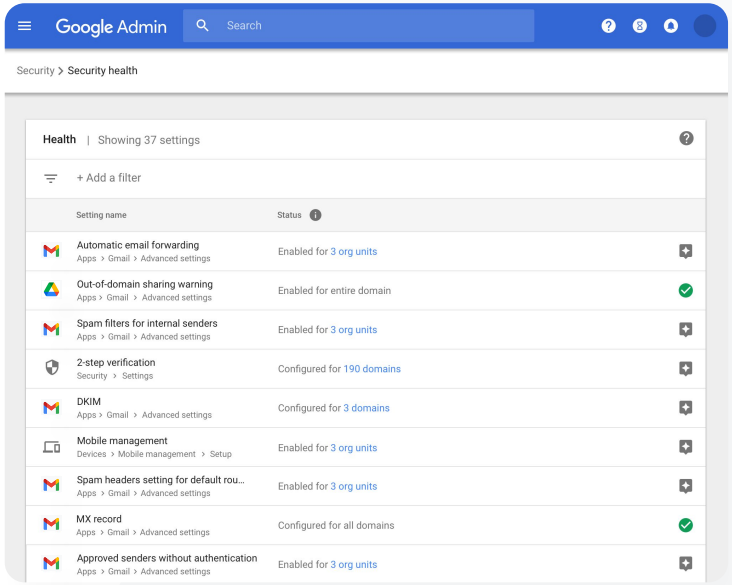
Documentación relevante del Centro de ayuda

- Comienza a usar la página Estado de seguridad

Instructivo: Recomendaciones de seguridad

Cómo ver las recomendaciones

- Accede a la **Consola del administrador.**
- Haz clic en **Seguridad** (Security) > **Estado de seguridad** (Security health).
- Verifica los parámetros de configuración del estado en la columna derecha:
  - Una marca de verificación verde indica un parámetro de configuración seguro.
  - Un ícono gris indica que se recomienda explorar ese parámetro de configuración. Haz clic en el ícono para ver los detalles y las instrucciones.



Documentación relevante del Centro de ayuda

- Comienza a usar la página Estado de seguridad

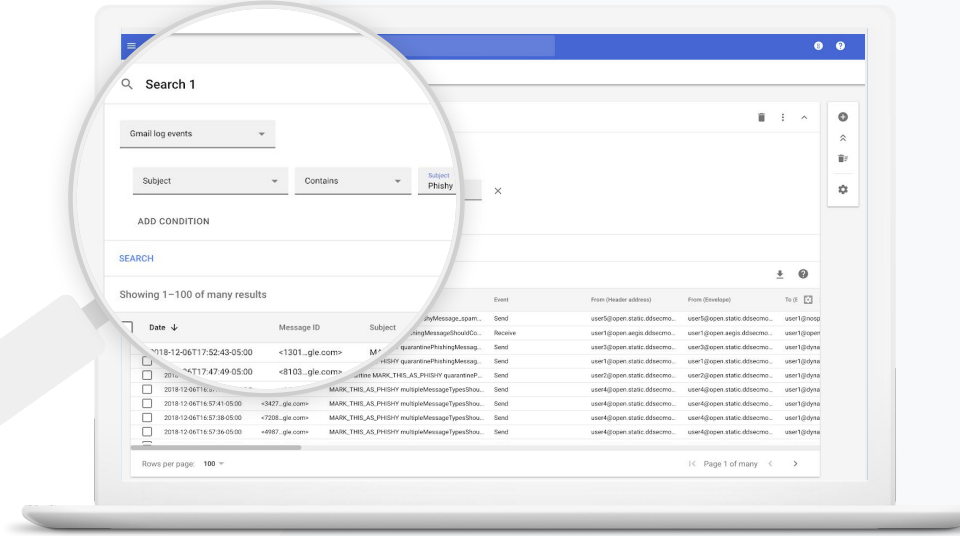
Herramienta de investigación

¿De qué se trata?

Usa la herramienta de investigación para identificar y clasificar problemas de seguridad y privacidad en tu dominio y tomar medidas para resolverlos.

Casos de uso

Material inadecuado que se comparte	Instructivo paso a paso
Archivos que se comparten por accidente	Instructivo paso a paso
Clasificación de correos electrónicos	Instructivo paso a paso
Correos electrónicos de suplantación de identidad y software malicioso	Instructivo paso a paso
Frena a los actores maliciosos	Instructivo paso a paso
Estadísticas de seguridad más detalladas	Instructivo paso a paso
Evita las reuniones no supervisadas	Instructivo paso a paso



“Sé que hay un archivo que contiene material inadecuado y que se está compartiendo. Quiero saber quién lo creó y cuándo, quién lo compartió y con quién, quién realizó modificaciones y, además, quiero borrarlo”.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Condiciones para eventos de registro de Drive
- Acciones para eventos de registro de Drive

Material inadecuado que se comparte

Los **eventos de registros de Drive**, que se encuentran en la **herramienta de investigación**, permiten encontrar, aislar o borrar archivos no deseados en el dominio y, además, hacer un seguimiento de ellos. Cuando accedas a los datos de eventos de registros de Drive, podrás hacer lo siguiente:

- Buscar documentos según el nombre, el actor, el propietario y otras opciones
- Tomar medidas como cambiar los permisos o borrar el archivo
- Buscar el contenido que los usuarios crean en Google Workspace y el que suben a Drive
- Visualizar toda la información de registro relacionada con ese documento
  - Fecha de creación
  - Quién es el propietario, quiénes lo vieron y quiénes lo editaron
  - Cuándo se compartió

Se compartió un archivo por accidente con un grupo que NO debería tener acceso a él.

Quiero quitarle el acceso al archivo”.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Ejecuta una búsqueda en la herramienta de investigación
- Toma medidas en función de los resultados de la búsqueda

Archivos compartidos por accidente

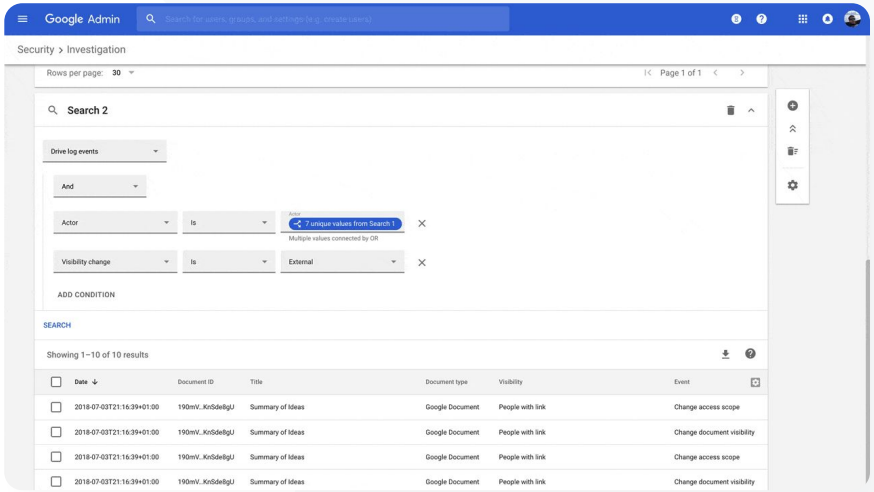
Los **eventos de registros de Drive**, que se encuentran en la **herramienta de investigación**, pueden ayudarte a hacer un seguimiento de los problemas relacionados con los archivos compartidos y a solucionarlos. Cuando accedas a los datos de eventos de registros de Drive, podrás hacer lo siguiente:

- Buscar documentos según el nombre, el actor, el propietario y otros criterios
- Visualizar toda la información de registro relacionada con el documento, incluida la información sobre quién lo vio y cuándo se compartió
- Tomar medidas como inhabilitar la descarga, la impresión y la copia, y cambiar los permisos

Instructivo: Eventos de registro de Drive

Cómo investigar los eventos de registro de Drive

- Accede a la **Consola del administrador.**
- Haz clic en **Seguridad** (Security) > **Herramienta de investigación** (Investigation tool).
- Selecciona **Eventos de registro de Drive** (Drive log events).
- Haz clic en **Agregar condición** (Add condition) > **Buscar** (Search).



Cómo tomar medidas

- Selecciona el archivo relevante en los resultados de la búsqueda.
- Haz clic en **Acciones** > **Auditar los permisos del archivo** para abrir la página Permisos.
- Haz clic en **Personas** para ver quiénes tienen acceso.
- Haz clic en **Vínculos** para ver o modificar la configuración de uso compartido de los archivos seleccionados.
- Haz clic en **Cambios pendientes** para revisar tus cambios antes de guardarlos.

Documentación relevante del Centro de ayuda

- Ejecuta una búsqueda en la herramienta de investigación
- Toma medidas en función de los resultados de la búsqueda

“Alguien envió un correo electrónico que NO debería haberse enviado. Queremos saber a quién se lo enviaron, si lo abrieron, si respondieron y, además, queremos borrarlo. También quiero conocer el contenido del correo electrónico”.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Condiciones para los registros y los mensajes de Gmail
- Acciones para los mensajes y los eventos de registro de Gmail
- Pasos para visualizar el contenido de un correo electrónico

Clasificación de correos electrónicos

Los **registros de Gmail**, que se encuentran en la **herramienta de investigación**, permiten identificar correos electrónicos peligrosos o infractores en tu dominio y tomar medidas con respecto a ellos. Al acceder a los registros de Gmail, puedes hacer lo siguiente:

- Buscar correos electrónicos específicos según el asunto, el ID del mensaje, el archivo adjunto, el remitente y otros criterios similares
- Ver los detalles del correo electrónico, como el autor, los destinatarios y cuántas veces lo abrieron y lo reenviaron
- Tomar medidas en función de los resultados de la búsqueda. Las acciones en los mensajes de Gmail incluyen borrar, restablecer, marcar como spam o suplantación de identidad (phishing), y enviar los mensajes a Recibidos y a cuarentena

Se recibió un correo electrónico de suplantación de identidad (phishing) o de software malicioso. Queremos ver si los usuarios hicieron clic en el vínculo en el correo electrónico o si descargaron el archivo adjunto, ya que, si lo hicieron, los usuarios y el dominio podrían encontrarse expuestos a daños".

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Condiciones para los registros y los mensajes de Gmail
- Acciones para los mensajes y los eventos de registro de Gmail
- Pasos para visualizar el contenido de un correo electrónico
- Consulta los informes de VirusTotal

Correos electrónicos de suplantación de identidad (phishing) y software malicioso

Acceder a la **herramienta de investigación**, específicamente a los **registros de Gmail**, te permite encontrar y aislar los correos electrónicos maliciosos en tu dominio. Cuando accedas a los registros de Gmail, podrás hacer lo siguiente:

- Buscar contenido específico, incluidos archivos adjuntos, en los correos electrónicos
- Ver información sobre correos electrónicos específicos, incluidos los destinatarios y cuantas veces se abrieron
- Ver los mensajes y las conversaciones para determinar si son maliciosos
- Analizar archivos adjuntos del correo electrónico para obtener datos detallados sobre el contexto de las amenazas y la reputación con los informes de VirusTotal
- Tomar medidas marcando los mensajes como spam o suplantación de identidad, enviarlos a una bandeja de Recibidos específica o a cuarentena, o borrarlos

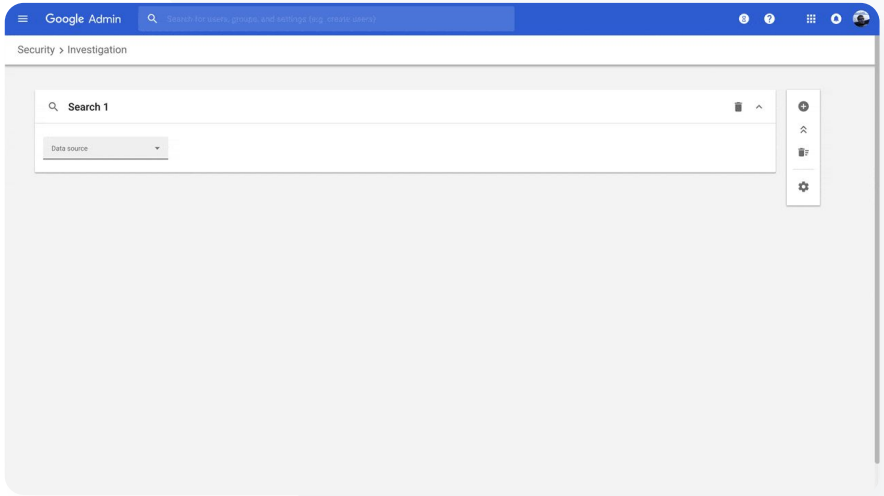
Instructivo: Registros de Gmail

Cómo investigar registros de Gmail

- Accede a la **Consola del administrador.**
- Haz clic en **Seguridad** (Security) > **Herramienta de investigación** (Investigation tool).
- Selecciona **Eventos de registro de Gmail** O **Mensajes de Gmail.**
- Haz clic en **Agregar condición** > **Buscar**.

Cómo tomar medidas

- Selecciona el archivo relevante en los resultados de la búsqueda.
- Haz clic en **Acciones**.
- Selecciona **Borrar mensaje (De la bandeja de Recibidos del propietario)**.
- Para confirmar la acción, haz clic en Ver en la parte inferior de la página.
- En la columna **Resultado**, podrás ver el estado de la acción.



Documentación relevante del Centro de ayuda

- Condiciones para los registros y los mensajes de Gmail
- Acciones para los mensajes y los eventos de registro de Gmail
- Pasos para visualizar el contenido de un correo electrónico

Una persona que actúa de mala fe ataca constantemente a usuarios de alto perfil en mi dominio, mientras mis esfuerzos por detenerla son inútiles.

¿Cómo evito que esto suceda?”

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Busca e investiga eventos de registro de usuarios
- Crea reglas de actividad con la herramienta de investigación

Frena a los actores maliciosos

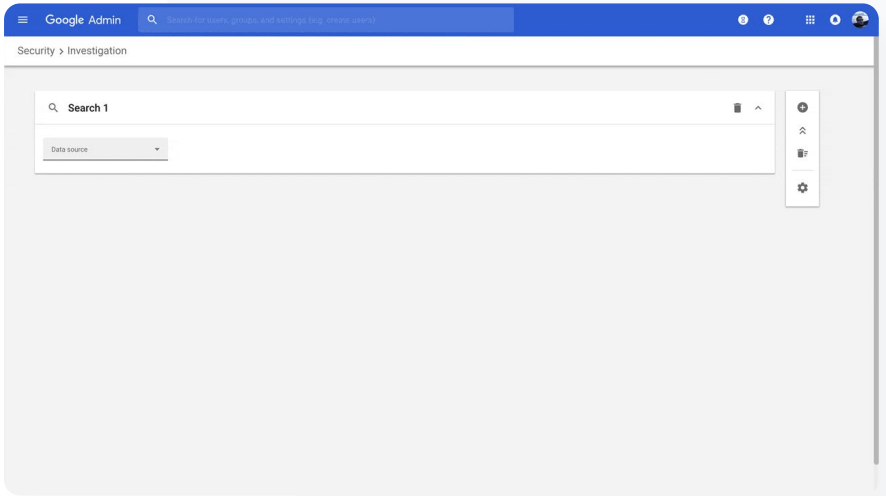
El **registro de usuarios** de la **herramienta de investigación** permite hacer lo siguiente:

- Identificar e investigar intentos de usurpación de las cuentas de los usuarios de la organización
- Supervisar qué métodos de verificación en 2 pasos usan los usuarios de la organización
- Obtener más información sobre los intentos de acceso de los usuarios de la organización
- Crear reglas de actividad con la herramienta de investigación: Bloquea mensajes y otras actividades maliciosas de actores específicos de forma automática
- Ofrecer mayor protección a los usuarios de alto perfil con el Programa de Protección Avanzada
- Restablecer o suspender usuarios

Instructivo: Frena a los actores maliciosos

Cómo investigar un evento de registro del usuario

- Accede a la **Consola del administrador.**
- Haz clic en **Seguridad** (Security) > **Herramienta de investigación** (Investigation tool).
- Selecciona **Eventos de registro del usuario.**
- Haz clic en **Agregar condición** > **Buscar**.



Cómo restablecer o suspender usuarios

- En los resultados de la búsqueda, selecciona uno o varios usuarios.
- Haz clic en el menú desplegable **Acciones**.
- Haz clic en **Restablecer usuario** o **Suspender usuario**.

Cómo ver detalles de un usuario específico

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

Documentación relevante del Centro de ayuda

- Busca e investiga eventos de registro de usuarios

Uno de nuestros profesores indicó que recibió un archivo sospechoso en Gmail.

¿Existe alguna forma para que el departamento de TI determine si el archivo es una amenaza de seguridad?”

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Ejecuta una búsqueda en la herramienta de investigación
- Consulta informes de VirusTotal en la herramienta de investigación

Obtén estadísticas de seguridad más detalladas

Los informes de VirusTotal amplían los resultados de las investigaciones de seguridad mediante una descripción exhaustiva para que los administradores comprueben la seguridad de un dominio, un archivo adjunto, una dirección IP o una URL en función de estadísticas recopiladas de forma colectiva. Podrás hacer lo siguiente:

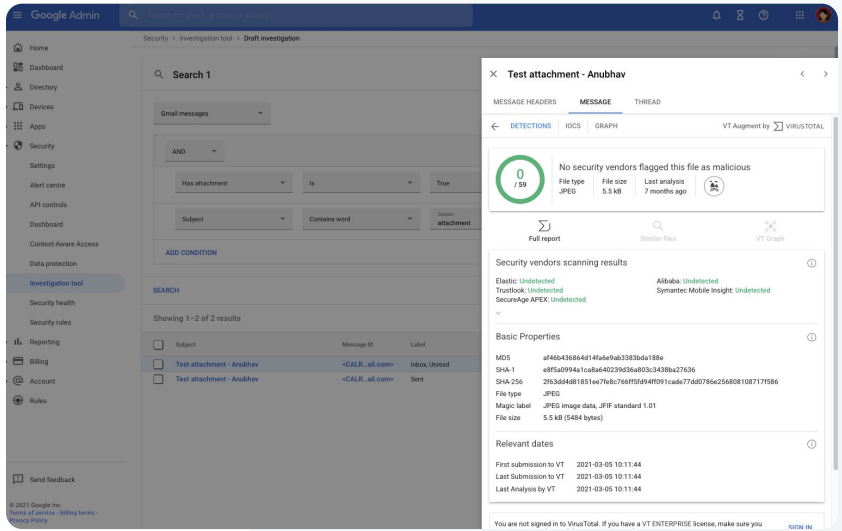
- Obtener estadísticas adicionales de seguridad sobre los eventos de registro de Gmail y Chrome
- Analizar archivos, URLs, dominios y direcciones IP sospechosas
- Acceder a detalles recopilados de forma colectiva sobre el motivo por el que se consideraría riesgoso un archivo adjunto o un sitio web
- Obtener asistencia sobre la toma de decisiones y abordar inquietudes relacionadas con la seguridad

Instructivo: Obtén estadísticas de seguridad más detalladas

Cómo ver informes de VirusTotal relacionados con Gmail

- Accede a la **Consola del administrador**.
- Haz clic en **Seguridad** (Security) > **Centro de seguridad** > **Herramienta de investigación** (Investigation tool).
- Elige **Mensajes de Gmail** (Gmail messages).
- Haz clic en **Agregar condición** (Add condition) > **Contiene un archivo adjunto** (Has attachment).
- En el resultado de la búsqueda, haz clic en **ID del mensaje** o en el vínculo **Asunto** (Subject).
- En el panel lateral, haz clic en las pestañas **Mensaje** (Message) o **Conversación** (Thread).
- Selecciona **Ver el informe de VirusTotal**.

Los administradores también pueden ver los informes de VirusTotal relacionados con Chrome. Solo debes seguir las instrucciones anteriores y seleccionar **Eventos de registro de Chrome** en la herramienta de investigación.



Documentación relevante del Centro de ayuda

- Consulta informes de VirusTotal en la herramienta de investigación

“Los alumnos se quedan en las llamadas de Google Meet después de que termina la clase. Me gustaría tener la capacidad de finalizar una Llamada de Meet para todos con el fin de evitar interrupciones en el aprendizaje”.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Usa la herramienta de investigación para finalizar las reuniones

Evita las reuniones virtuales no supervisadas

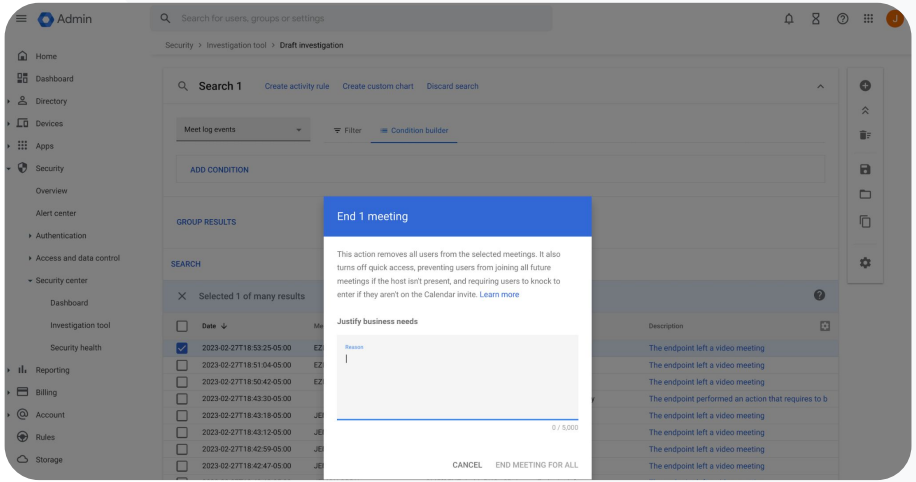
Los administradores de Google Workspace pueden usar la acción **Finalizar reunión para todos los participantes** en la herramienta de investigación para quitar a todos los usuarios de una reunión de la organización. Los organizadores de reuniones también pueden usarla para sus Llamadas de Google Meet individuales.

- La reunión finalizará para todos los usuarios que se encuentren actualmente en ella, incluidos los que están en sesiones separadas.
- Los usuarios no podrán asistir a instancias futuras de esa reunión si el organizador no está presente.

Instructivo: Evita las reuniones virtuales no supervisadas

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

- Accede a la **Consola del administrador.**
- Haz clic en **Seguridad** (Security) > **Centro de seguridad** > **Herramienta de investigación** (Investigation tool).
- Elige **Eventos de registro de Meet** (Meet log events).
- Haz clic en **Buscar** (Search). En los resultados de la búsqueda, verás una lista de los eventos de registro de Meet.
- Marca las casillas de las reuniones que quieras finalizar para todos los usuarios.
- Selecciona **Acciones**.
- Haz clic en **Finalizar reunión para todos los participantes** (End meeting for all).



Documentación relevante del Centro de ayuda

- Usa la herramienta de investigación para finalizar las reuniones

Controles y administración del dominio

Los administradores tienen acceso a las herramientas avanzadas de Google Workspace para administrar los datos de la organización, establecer controles, supervisar el uso y ayudar a cumplir los estándares educativos.

Casos de uso

Crea informes y paneles de uso	Instructivo paso a paso
Encuentra archivos con mayor facilidad	Instructivo paso a paso
Organiza documentos internos	Instructivo paso a paso
Propaga automáticamente grupos de departamentos	Instructivo paso a paso
Crea públicos para el uso compartido interno de archivos	Instructivo paso a paso
Restringe el uso de archivos compartidos	Instructivo paso a paso
Restricciones de la app de Workspace	Instructivo paso a paso
Administración del almacenamiento	Instructivo paso a paso
Reglamentaciones de datos	Instructivo paso a paso
Reglamentaciones relacionadas con los permisos	Instructivo paso a paso
Administra dispositivos de extremo	Instructivo paso a paso
Administra dispositivos con Windows	Instructivo paso a paso
Parámetros de configuración personalizados para dispositivos con Windows	Instructivo paso a paso
Automatiza las actualizaciones de dispositivos con Windows	Instructivo paso a paso
Aprovecha la encriptación del cliente	Instructivo paso a paso

“¿Cómo puedo proteger mejor mi dominio contra el software malicioso de día cero y las amenazas de ransomware?”

Análisis de virus en archivos adjuntos de Gmail

Los archivos adjuntos a los correos electrónicos pueden contener software malicioso. A fin de identificar estas amenazas, Gmail analiza o ejecuta esos archivos adjuntos en la Zona de pruebas de seguridad y los archivos adjuntos identificados como amenazas se envían a la carpeta de Spam.

- Detecta el software malicioso “ejecutándolo” de manera virtual en un entorno privado y seguro, y analiza los efectos secundarios para determinar el comportamiento malicioso
- Analiza archivos de Microsoft Word, PowerPoint, PDF, comprimidos (ZIP), etc.
- Activa el análisis para todo el dominio o crea reglas de análisis según condiciones específicas como remitente, dominio, etc.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Configurar reglas para detectar archivos adjuntos dañinos

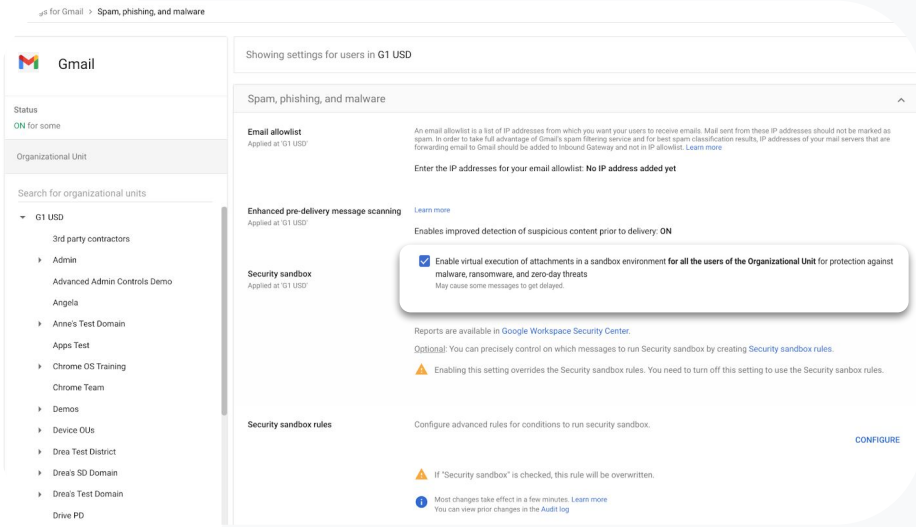
Instructivo: Analiza archivos adjuntos de Gmail en busca de virus

Cómo funciona

Los archivos adjuntos del correo electrónico se desactivan dentro de una zona de pruebas de seguridad unos minutos antes de la entrega del correo electrónico, lo cual proporciona una capa adicional de seguridad.

Cómo analizar los archivos adjuntos en la Zona de pruebas de seguridad

- Accede a la **Consola del administrador.**
- Haz clic en **Menú** > **Apps** > **Google Workspace** > **Gmail** > **Spam, phishing y software malicioso.**
- Selecciona una unidad organizativa o aplica la configuración a todo tu dominio.
- Desplázate hasta **Zona de pruebas de seguridad** dentro de **Spam, phishing y software malicioso.**
- Marca la casilla **Habilitar ejecución virtual de archivos adjuntos en zona de pruebas de seguridad.**
- Haz clic en **Guardar.**



Documentación relevante del Centro de ayuda

- Configurar reglas para detectar archivos adjuntos dañinos

“¿Cómo puedo comprender el uso de Classroom en todo mi dominio?”

Crea informes y paneles de uso

Con la **plantilla de Looker Studio y BigQuery Export**, los administradores pueden usar los registros de actividad de Classroom para crear paneles personalizados y realizar informes con herramientas de estadísticas, como Looker Studio y socios de visualización externos integrados en BigQuery.

- Exporta datos de registro de Classroom de la Consola del administrador a BigQuery y Looker Studio.
- Consulta rápidamente los informes sobre el uso y la adopción en todo tu dominio. Identifica quién quitó a un alumno de una clase, quién archivó una clase en una fecha concreta y mucho más.
- Con las plantillas de paneles de Looker Studio, comprende las tendencias dominantes y toma medidas más rápido.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Configura BigQuery Export y la plantilla de Data Studio

Instructivo: Crea informes y paneles de uso

01 Configura y exporta un proyecto de BigQuery

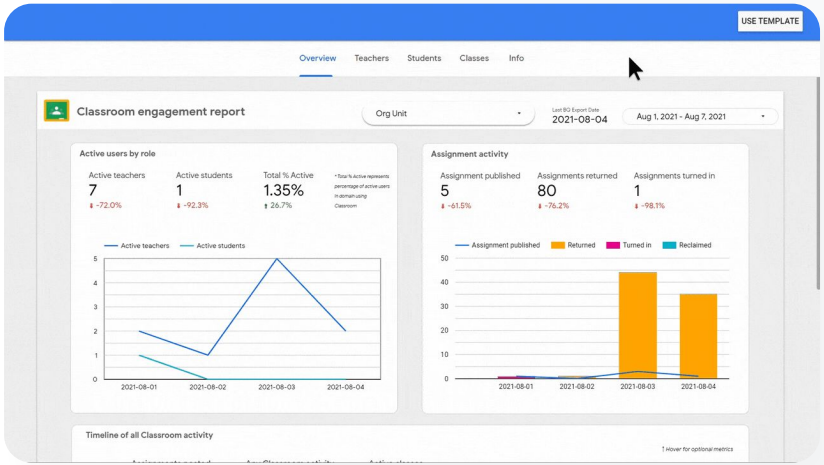
- Accede a console.cloud.google.com > **Crear un nuevo proyecto.**
- Accede a admin.google.com > **Informes** > **BigQuery Export.**
- Haz clic en el **proyecto de Cloud BigQuery.** Asígnale un nombre al conjunto de datos y elige **Guardar.**

02 Agrega el archivo de BigQuery Export en Looker Studio

- Accede a Looker Studio > **Crear** > **Fuente de datos.**
- Selecciona **BigQuery** > **Mis proyectos.** Haz clic en el proyecto que creaste y elige **Actividad.**
- Marca la casilla en **Tabla particionada** y haz clic en **Conectar.**

03 Crea un panel de Looker Studio

- Abre la plantilla y selecciona **Utilizar plantilla.**
- En **Nueva fuente de datos**, elige la fuente de datos **Actividad.**
- Haz clic en **Copiar informe.**



Documentación relevante del Centro de ayuda

- Configura BigQuery Export y la plantilla de Data Studio

Necesito hacer un seguimiento de los permisos de excursión que enviaron los padres a través de Gmail, Chat y Documentos.

¿Cómo puedo encontrar estos archivos en mi dominio?”

Instructivo paso a paso

Documentación relevante del Centro de ayuda

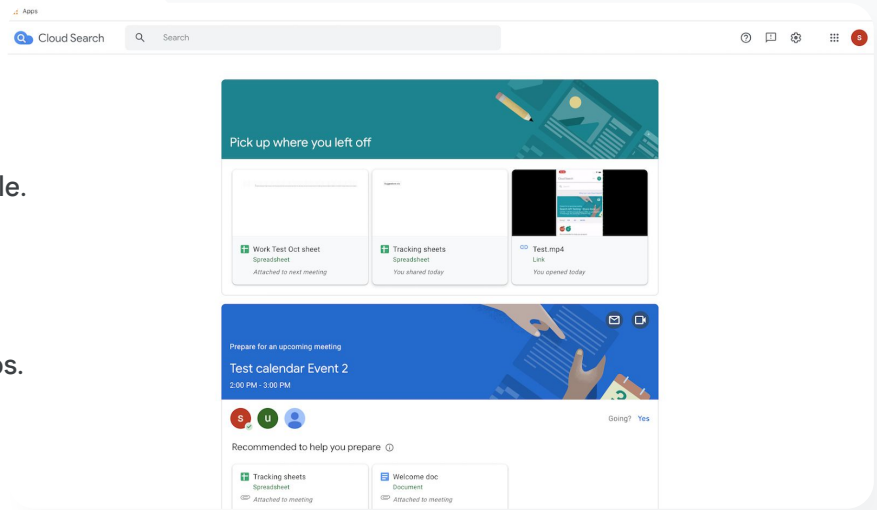
- Guía de Google Cloud Search
- Activa o desactiva Cloud Search para los usuarios

Encuentra archivos con mayor facilidad

Con Google Cloud Search, los educadores de tu institución pueden encontrar rápidamente contenido en todas las herramientas de Google Workspace y apps de terceros.

- Encuentra la información que necesitas desde cualquier lugar con tu laptop, teléfono celular o tablet.
- Realiza búsquedas en todas las apps de Google Workspace, como Drive, Contactos, Gmail y fuentes de datos de terceros.

Instructivo: Encuentra archivos con mayor facilidad



Activa Cloud Search para los usuarios

- Accede a la **Consola del administrador**. Ve a **Menú** > **Apps** > **Google**.
- Haz clic en **Estado del servicio**.
- Activa o desactiva un servicio para todos en tu organización. Para hacerlo, haz clic en **Activado para todos** o **Desactivado para todos**.
- Haz clic en **Guardar**.
- Si quieres activar un servicio para un conjunto de usuarios de una misma unidad organizativa o de varias, selecciona un **grupo de acceso**.
- Haz clic en **Guardar**.

Documentación relevante del Centro de ayuda

- Guía de Google Cloud Search
- Activa o desactiva Cloud Search para los usuarios

Quiero aplicar etiquetas de sensibilidad para que los archivos de mi institución se alineen con los requisitos de cumplimiento, evitar el uso inadecuado y mejorar la organización de los archivos".

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Administra etiquetas de Drive

Organiza los documentos de todo tu dominio

Las **etiquetas de Drive** ayudan a los usuarios a encontrar, organizar y aplicar políticas en todos sus dominios. Los administradores pueden crear y administrar las etiquetas de Drive para evitar el uso inadecuado de los archivos y garantizar que los datos de los alumnos cumplan con los requisitos de cumplimiento.

- Las etiquetas son metadatos que ayudan a organizar los archivos educativos sensibles, como los documentos relacionados con el cumplimiento, los planes de estudio individuales y el departamento de Defensa.
- Solo los administradores pueden crear, definir estructuras y publicar etiquetas. Los usuarios de tu organización pueden aplicar etiquetas a los archivos que editan y establecer los valores de campo.
- Las etiquetas de Drive se pueden usar para respaldar la Prevención de pérdida de datos automatizada.

Instructivo: Organiza los documentos de todo tu dominio

Cómo funciona

Google Drive ofrece etiquetas estándar y con insignias (un indicador visual) para ayudar a organizar los archivos en tu dominio.

Cómo activar las etiquetas de Drive para tu institución

- Accede a la **Consola del administrador**.
- Haz clic en **Menú** > **Apps** > **Google Workspace** > **Drive y Documentos**.
- Selecciona **Etiquetas**.
- **Activa** o **desactiva** las etiquetas.
- Haz clic en **Guardar**.

Documentación relevante del Centro de ayuda

- Administra etiquetas de Drive

“¿Cómo puedo automatizar la pertenencia a un grupo para que, cada vez que un nuevo educador se vincule a la institución, se incluya en la lista de correo electrónico correspondiente?”

Propaga automáticamente grupos de departamentos

Los **grupos dinámicos** permiten que los administradores actualicen la pertenencia a un grupo para todo el centro educativo con criterios personalizados.

- Crea grupos dinámicos que administran las membresías automáticamente.
- Mantén los grupos actualizados según la búsqueda de membresías que creaste.
- Puedes usar los grupos dinámicos para lo siguiente:
  - Listas de correo electrónico y distribución
  - Grupos moderados y bandejas de entrada colaborativas
  - Grupos de seguridad

Instructivo paso a paso

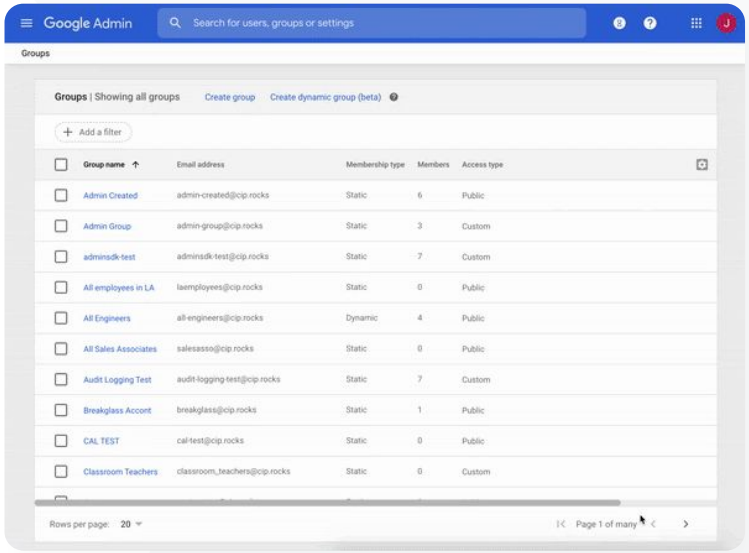
Documentación relevante del Centro de ayuda

- Administra la membresía automáticamente con grupos dinámicos

Instructivo: Propaga grupos automáticamente

Crea un grupo dinámico

- Accede a la **Consola del administrador**. Ve a **Menú** > **Directorio** > **Grupos**.
- Haz clic en **Crear un grupo dinámico** (Create dynamic group).
- Crea tu búsqueda de membresías con los siguientes elementos:
  - Lista de condiciones: Criterios para determinar la membresía (p. ej., el departamento)
  - Campo de valor: El valor que quieres usar
- Ingresa la siguiente información:
  - Nombre: Identifica el grupo en listas y mensajes
  - Descripción: Propósito del grupo
  - Correo electrónico del grupo: Dirección de correo electrónico que se usa para el grupo
- Haz clic en **Guardar**.
- Haz clic en **Listo**.



Documentación relevante del Centro de ayuda

- Administra la membresía automáticamente con grupos dinámicos

Mi personal comparte sin querer documentos con toda la organización, lo que pone en peligro los datos sensibles. ¿Cómo puedo ayudar a limitar las opciones para compartir a un grupo más pequeño y relevante?”

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Acerca de los usuarios objetivo
- Prácticas recomendadas para implementar usuarios objetivo
- Crea un público objetivo

Crea públicos para el uso compartido interno de archivos

La configuración de **usuarios objetivo** ayuda a mejorar la seguridad de los datos de tu organización reduciendo la posibilidad de que los usuarios compartan archivos en exceso accidentalmente.

- Asegúrate de que los archivos se compartan con las personas correctas, por ejemplo, un equipo o un departamento específico.
- Los usuarios objetivo son grupos de personas que los administradores pueden recomendar a los usuarios para que compartan sus elementos con ellos.
- Los administradores pueden agregar usuarios objetivo a la configuración de uso compartido para incentivar el intercambio de contenido con un público más específico.
- Esta opción está disponible en Google Drive, Documentos y Chat.

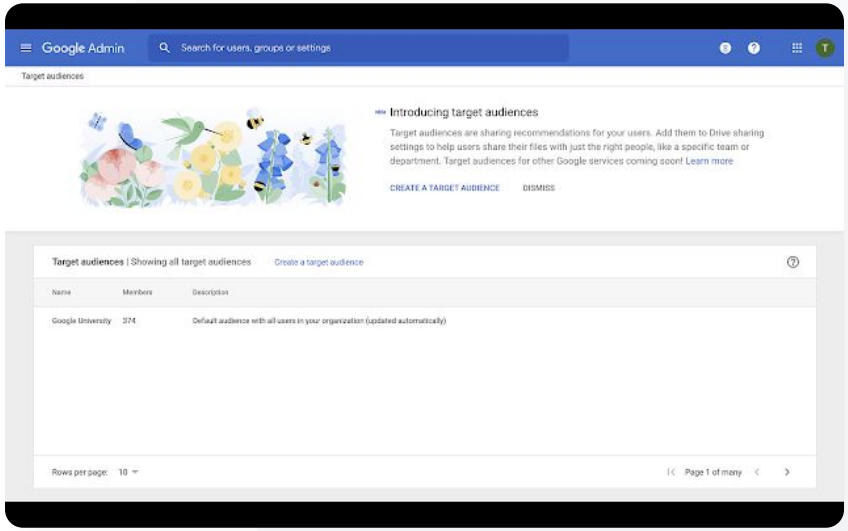
Instructivo: Crea públicos para el uso compartido interno de archivos

Cómo funciona

Luego de crear un grupo de usuarios objetivo, puedes agregarle miembros y aplicarlo a Google Drive para que esté disponible en la configuración de uso compartido de los usuarios. Por ejemplo, puedes permitir que un miembro del personal vea un usuario objetivo llamado “Todo el personal” cuando comparta archivos de Drive.

Cómo activar las etiquetas de Drive para tu institución

- Accede a la **Consola del administrador**. Ve a **Menú** > **Directorio** > **Públicos objetivo** (Target audiences).
- Haz clic en **Crea un público objetivo** (Create target audience).
- En **Nombre** (Name), ingresa el nombre de los usuarios objetivo.
- Selecciona **Agregar miembros** e incluye a los miembros que quieras.
- Haz clic en **Listo**.



Documentación relevante del Centro de ayuda

- Acerca de los usuarios objetivo
- Prácticas recomendadas para implementar usuarios objetivo
- Crea un público objetivo

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

Restringe el uso de archivos compartidos

Con las **reglas de confianza de Drive**, los administradores definen reglas para controlar quién tiene acceso a los archivos de Google Drive, lo que ayuda a garantizar la privacidad de los datos institucionales. Las políticas pueden aplicarse a usuarios individuales, grupos, unidades organizativas y dominios.

- Protege la información sensible y cumple con las reglamentaciones y los estándares de la industria.
- Restringe el uso compartido externo o interno al dominio. Los administradores pueden crear una regla de confianza para permitir que los alumnos compartan archivos de Drive únicamente en tu organización.
- Una vez que se habilitan las “reglas de confianza”, se reemplazan las “Opciones para compartir” en los controles del administrador de Google Drive.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Crea y administra reglas de confianza para controlar el uso compartido en Drive

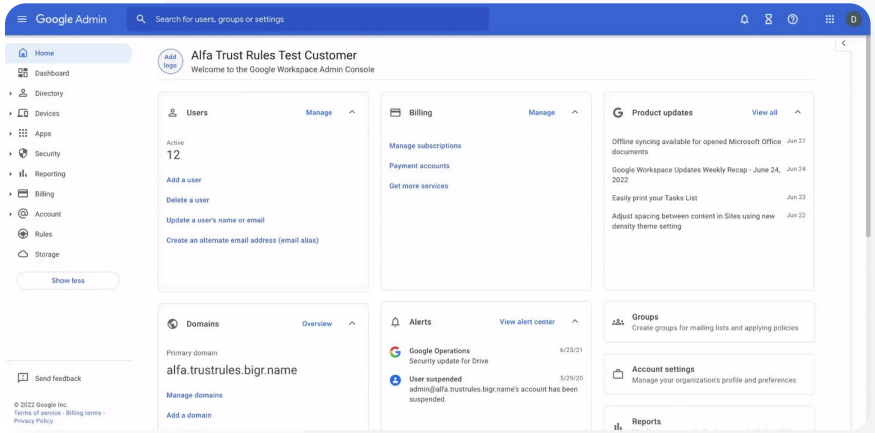
Instructivo: Restringe el uso de archivos compartidos

Activa las reglas de confianza de Drive

- Accede a la **Consola del administrador**.
  Ve a **Menú** > **Reglas** (Rules).
- En la tarjeta **Colabora de forma segura** que está en la parte superior de la página, haz clic en **Activar reglas de confianza**.
- Tus listas de tareas se abren automáticamente. Verás el progreso de las activación de las reglas de confianza.

Los administradores pueden crear una regla de confianza, ver y editar sus detalles, borrarla y consultar sus eventos de registro.

Visita el Centro de ayuda para administradores si necesitas instrucciones paso a paso sobre la administración de las reglas de confianza.



Documentación relevante del Centro de ayuda

- Crea y administra reglas de confianza para controlar el uso compartido en Drive

Restricciones de apps de Google Workspace

Quiero limitar el acceso a determinadas apps cuando los usuarios se conectan a nuestra red".

Con el **Acceso adaptado al contexto**, puedes crear políticas de control de acceso detalladas para las apps de **Google Workspace y de SAML de terceros** (lenguaje de marcado para confirmaciones de seguridad) basadas en atributos como la identidad, la ubicación, el estado de seguridad del dispositivo y la dirección IP del usuario. Incluso puedes restringir el acceso a las apps que están fuera de la red.

- Puedes aplicar políticas de Acceso adaptado al contexto a los servicios principales de Google Workspace for Education.
- Por ejemplo, restringe el acceso a las apps de Workspace de los dispositivos proporcionados por la institución educativa o el acceso a Drive solo si el dispositivo de almacenamiento de un usuario está encriptado.

Instructivo paso a paso

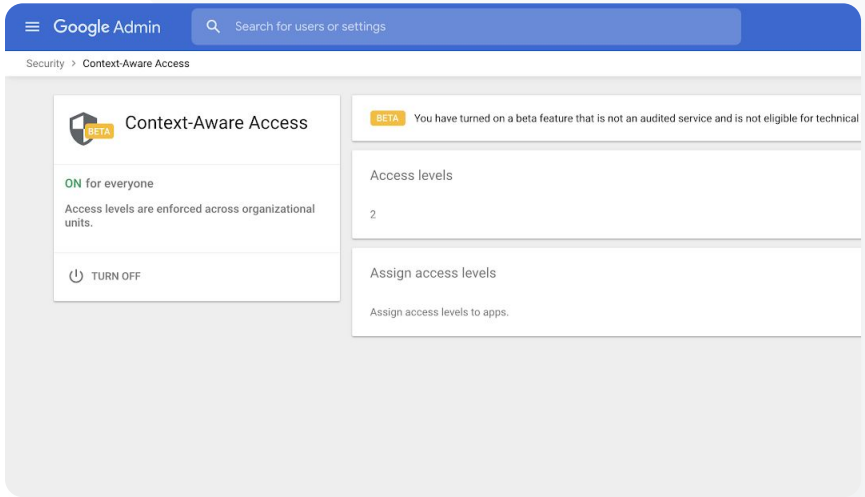
Documentación relevante del Centro de ayuda

- Descripción general del Acceso adaptado al contexto
- Asigna niveles de Acceso adaptado al contexto a las apps

Instructivo: Restringe el uso de la app de Google Workspace

Cómo usar el Acceso adaptado al contexto

- Accede a la **Consola del administrador**.
- Selecciona **Seguridad** (Security) > **Acceso adaptado al contexto** (Context-Aware Access) > **Asignar**.
- Selecciona **Asignar niveles de acceso** (Assign access levels) para ver la lista de apps.
- Selecciona **una unidad organizativa o un grupo de configuración** para ordenar la lista.
- Selecciona **Asignar** junto a la app que quieras ajustar.
- Selecciona uno o más niveles de acceso.
- Crea varios niveles si quieres que los usuarios cumplan con más de una condición.
- Haz clic en **Guardar**.



Documentación relevante del Centro de ayuda

- Descripción general del Acceso adaptado al contexto
- Asigna niveles de Acceso adaptado al contexto a las apps

“Quiero implementar un plan de administración de almacenamiento nuevo en mi dominio”.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Guía de almacenamiento por administradores
- Comprende la disponibilidad y el uso del almacenamiento
- Libera almacenamiento o adquiere más
- Define límites de almacenamiento

Administra el almacenamiento en todo tu dominio

Las instituciones que trabajan con Google Workspace for Education tienen una base de 100 TB de almacenamiento conjunto, que es suficiente almacenamiento para aproximadamente 100 millones de documentos, 8 millones de presentaciones y 400,000 horas de video. **Administra el almacenamiento conjunto en Drive** para garantizar que tu institución lo utilice de forma eficaz.

Usa las herramientas, los informes y los registros del administrador para hacer lo siguiente:

- Comprender la cantidad de almacenamiento que utilizas
- Definir límites de almacenamiento
- Identificar las cuentas que usan una cantidad excesiva de almacenamiento

Los planes Teaching and Learning Upgrade y Education Plus ofrecen una capacidad de almacenamiento adicional además del básico proporcionado.

- Agrega 100 GB al conjunto compartido por licencia con Teaching and Learning Upgrade.
- Agrega 20 GB al conjunto compartido por licencia con Education Plus.

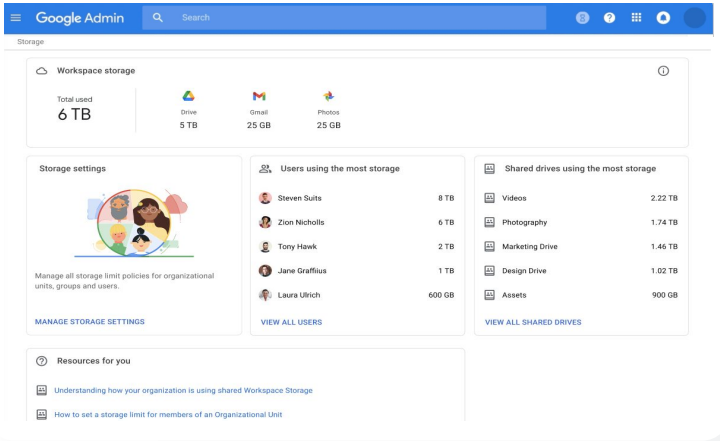
Instructivo: Administra el almacenamiento en todo tu dominio

Identifica el uso del almacenamiento por usuario

- Accede a la **Consola del administrador**. Ve a **Menú** > **Almacenamiento** (Storage).
- Consulta el uso del almacenamiento por organización y usuario.

Define límites de almacenamiento

- En la **Consola del administrador**, ve a **Menú** > **Almacenamiento** (Storage).
- En **Configuración de almacenamiento**, haz clic en **Administrar**.
- Haz clic en **Límite de almacenamiento del usuario** y selecciona la entidad a la que se le aplicará el límite:
  - Unidad organizativa: Haz clic en la **unidad organizativa**.
  - Grupo: Haz clic en **Grupos**. En el **campo de búsqueda**, ingresa el **nombre del grupo** y haz clic en el **grupo**.
- Selecciona **Activar** y **define la cantidad de almacenamiento**.
- Haz clic en **Guardar**.



Documentación relevante del Centro de ayuda

- Guía de almacenamiento por administradores
- Comprende la disponibilidad y el uso del almacenamiento
- Libera almacenamiento o adquiere más
- Define límites de almacenamiento

“De conformidad con ciertas leyes normativas, los datos de los alumnos, el cuerpo docente y el personal deben permanecer en la UE”.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Elige una ubicación geográfica para los datos

Reglamentaciones de datos

Los administradores pueden almacenar los datos en una ubicación geográfica específica, ya sea en Estados Unidos o el Reino Unido y Europa, estableciendo una **política de la región de datos**.

- Los usuarios de Education Plus y Education Standard pueden elegir una región de datos para algunos de sus usuarios o diferentes regiones para departamentos específicos, así como consultar el progreso de una transferencia entre regiones de datos.
- Coloca a los usuarios en una unidad organizativa por departamento o asígnalos a un grupo de configuración si quieres ajustar esta opción para los usuarios de todos los departamentos o solo de algunos.
- Las políticas de las regiones de datos no se aplican a los usuarios que no tienen asignada una licencia de Education Standard o Education Plus.

“De conformidad con las reglamentaciones sobre los permisos, los datos de investigación del cuerpo docente deben permanecer en Estados Unidos”.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Elige una ubicación geográfica para los datos

Reglamentaciones relacionadas con los permisos

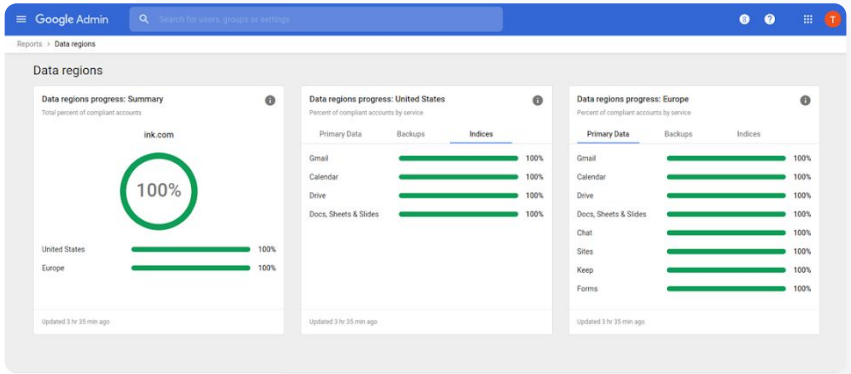
Los administradores pueden almacenar la investigación del cuerpo docente en una ubicación geográfica específica (Estados Unidos o Europa) estableciendo una **política de la región de datos**.

- Las políticas de las regiones de datos se aplican a los datos en reposo principales (incluidas las copias de seguridad) para la mayoría de los servicios principales de Google Workspace for Education que se indican aquí.
- Considera las desventajas antes de configurar una política de la región de datos; por ejemplo, los usuarios fuera de la región en la que están ubicados los datos podrían experimentar mayor latencia en algunos casos.

Instructivo: Reglamentaciones de datos

Cómo definir regiones de datos

- Accede a la **Consola del administrador**.
  - Nota: Debes acceder como administrador avanzado.
- Haz clic en **Perfil de la empresa** > **Ver más** > **Regiones de datos**.
- Selecciona **la unidad organizativa o el grupo de configuración** que quieres limitar a una región, o selecciona toda la columna para incluir todas las unidades y grupos.
- Selecciona una región; por ejemplo, **Sin preferencias, Estados Unidos o Europa**.
- Haz clic en **Guardar**.



Documentación relevante del Centro de ayuda

- Elige una ubicación geográfica para los datos

Administra dispositivos de extremo

Con la **Administración empresarial de extremos**, puedes obtener mayor control sobre los datos de la organización mediante dispositivos móviles. Restringe funciones, exige la encriptación y administra apps en dispositivos Android, o iPhones y iPads, incluida la capacidad de limpiar los datos de un dispositivo.

- Puedes aprobar, bloquear, desbloquear o borrar dispositivos desde la Consola del administrador.
- Si un usuario pierde su dispositivo o abandona la institución, puedes limpiar la cuenta del usuario, su perfil o, incluso, todos los datos del dispositivo específico del módulo administrado. Estos datos aún estarían disponibles en una computadora o un navegador web.

> “Necesito tener la capacidad de administrar y enviar políticas a todo tipo de dispositivos (iOS, Windows 10, etc.) de todo mi distrito, no solo a Chromebooks, sobre todo si alguno está comprometido”.

Instructivo paso a paso

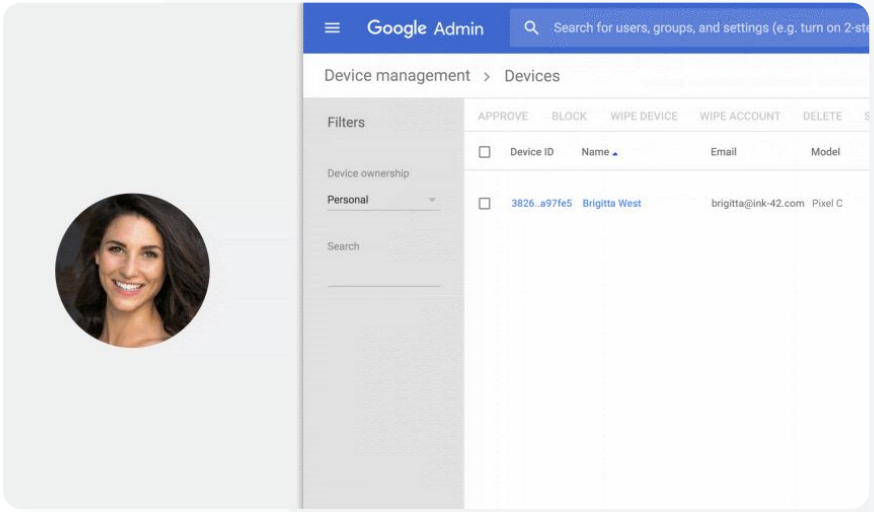
Documentación relevante del Centro de ayuda

- Gestiona dispositivos con la Administración de extremos de Google
- Configura la Administración avanzada de dispositivos móviles

Instructivo: Administra dispositivos de extremo

Cómo usar la Administración avanzada de dispositivos móviles

- Accede a la **Consola del administrador**.
- En la **Consola del administrador**, ve a **Dispositivos**.
- A la izquierda, haz clic en **Configuración** > **Configuración universal**.
- Haz clic en **General** > **Administración de dispositivos móviles**.
- Para aplicar esta configuración a todos, deja seleccionada la unidad organizativa superior. De lo contrario, selecciona una unidad organizativa secundaria.
- Selecciona **Avanzada**.
- Haz clic en **Guardar**.



Documentación relevante del Centro de ayuda

- Gestiona dispositivos con la Administración de extremos de Google
- Configura la Administración avanzada de dispositivos móviles

Algunos de mis educadores usan dispositivos con Windows 10. ¿Cómo puedo administrar todos los dispositivos de mi institución en el mismo lugar?”

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Habilita la administración de dispositivos con Windows
- Inscribe un dispositivo en la administración de dispositivos con Windows

Administra los dispositivos con Microsoft Windows

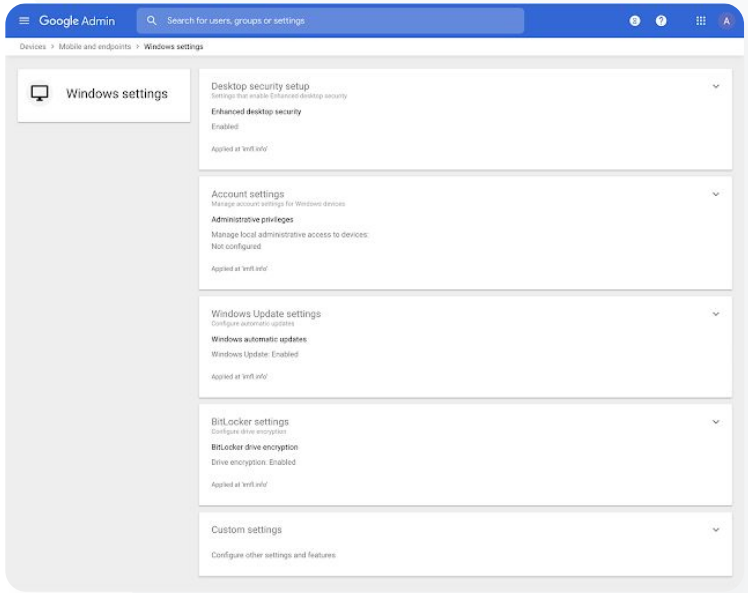
Administra y protege los dispositivos con Windows 10 de tu institución mediante la Consola del administrador, tal como lo haces con dispositivos Android, iOS, Chrome y Jamboard.

- Habilita el inicio de sesión único para que los usuarios accedan de manera más sencilla a Google Workspace en sus dispositivos con Windows 10.
- Asegúrate de que los dispositivos que se utilizan para acceder a Google Workspace estén actualizados, protegidos y que cumplan con los estándares de cumplimiento, gestionándolos en la Consola del administrador.
- Envía actualizaciones de configuración de los dispositivos, límpialos y realiza más acciones en los dispositivos con Windows 10 desde la nube.

Instructivo: Administra los dispositivos con Microsoft Windows

Habilita la administración de dispositivos con Windows

- En la **Consola del administrador**, ve a **Menú** > **Dispositivos** (Devices) > **Dispositivos móviles y extremos** (Mobile and endpoints) > **Configuración** > **Configuración de Windows** (Windows settings).
- Selecciona **Configuración de la administración de Windows**.
- Para aplicar el parámetro de configuración a todos, deja seleccionada la unidad organizativa superior.
- Junto a **Administración de dispositivos de Windows**, selecciona **Habilitado**.
- Haz clic en **Guardar**.



Documentación relevante del Centro de ayuda

- Habilita la administración de dispositivos con Windows
- Inscribe un dispositivo en la administración de dispositivos con Windows

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

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Parámetros de configuración personalizados comunes
- Agrega parámetros de configuración personalizados

Parámetros de configuración personalizados para dispositivos con Windows 10

Con la administración de dispositivos con Windows de Google, los administradores pueden agregar parámetros de configuración personalizados a los dispositivos de su flota.

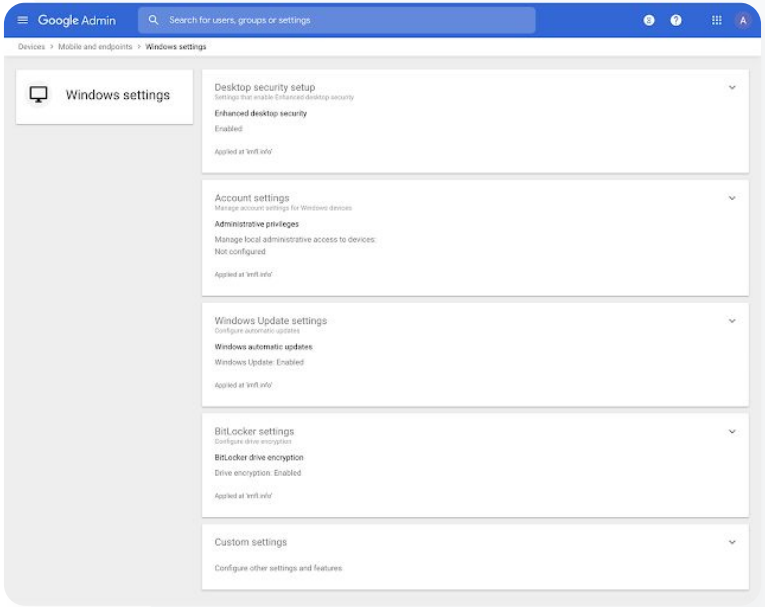
- Controla los parámetros de configuración personalizados de los dispositivos de la Consola del administrador.
- Aplica los parámetros de configuración en las siguientes opciones:
  - Administración de dispositivos
  - Seguridad
  - Hardware y red
  - Software
  - Privacidad

Instructivo: Parámetros de configuración personalizados para dispositivos con Windows 10

Agrega un nuevo parámetro de configuración personalizado

- En la **Consola del administrador**, ve a **Menú** > **Dispositivos** (Devices) > **Dispositivos móviles y extremos** (Mobile and endpoints) > **Configuración** > **Configuración de Windows** (Windows settings).
- Selecciona **Configuración personalizada** (Custom settings).
- Haz clic en **Agregar un parámetro de configuración personalizado** y completa los campos solicitados.
- Haz clic en **Siguiente**.
- Elige la **unidad organizativa** en la que quieres aplicar el parámetro de configuración.
- Haz clic en **Aplicar**.

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



Documentación relevante del Centro de ayuda

- Parámetros de configuración personalizados comunes
- Agrega parámetros de configuración personalizados

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

Automatiza las actualizaciones de los dispositivos con Windows 10

Especifica cuándo y cómo los dispositivos con Windows 10 de tu institución reciben actualizaciones de seguridad y otras descargas importantes mediante el servicio de actualización automático de Windows.

- Configura las notificaciones para descargar actualizaciones del panel de control de Windows Update, define un horario en el que no se programen reinicios y mucho más.
- Aplica parámetros de configuración en toda la institución o en unidades organizativas específicas.
- Los cambios pueden tardar hasta 24 horas en aplicarse, aunque suelen ocurrir antes.

Instructivo paso a paso

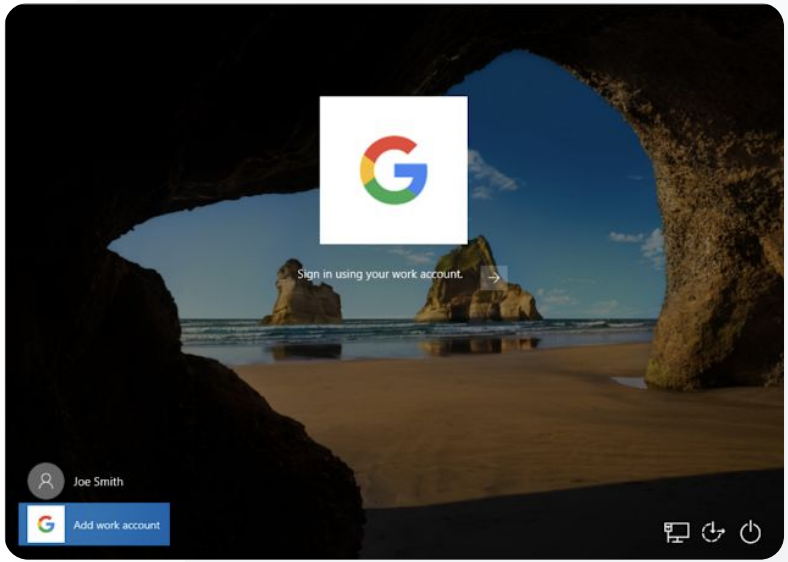
Documentación relevante del Centro de ayuda

- Administra las actualizaciones automáticas

Instructivo: Automatiza las actualizaciones de los dispositivos con Windows 10

Configura las actualizaciones

- En la **Consola del administrador**, ve a **Menú** > **Dispositivos** (Devices) > **Dispositivos móviles y extremos** (Mobile and endpoints) > **Configuración** > **Configuración de Windows** (Windows settings).
- Selecciona **Configuración de Windows Update** > **Habilitado**.
- Junto a **Administración de dispositivos de Windows**, selecciona **Habilitado**.
- Configura las siguientes opciones, entre otras:
  - Aceptar las actualizaciones de aplicaciones de Microsoft
  - Comportamiento de las actualizaciones automáticas
  - Frecuencia de las actualizaciones automáticas
- Haz clic en **Guardar**.



Documentación relevante del Centro de ayuda

- Administra las actualizaciones automáticas

Sé que Google tiene los estándares más altos en relación con la encriptación de datos, pero quiero controlar las claves de encriptación de la propiedad intelectual y la investigación financiada de nuestra universidad".

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Acerca de la encriptación del cliente

Aprovecha la encriptación del cliente

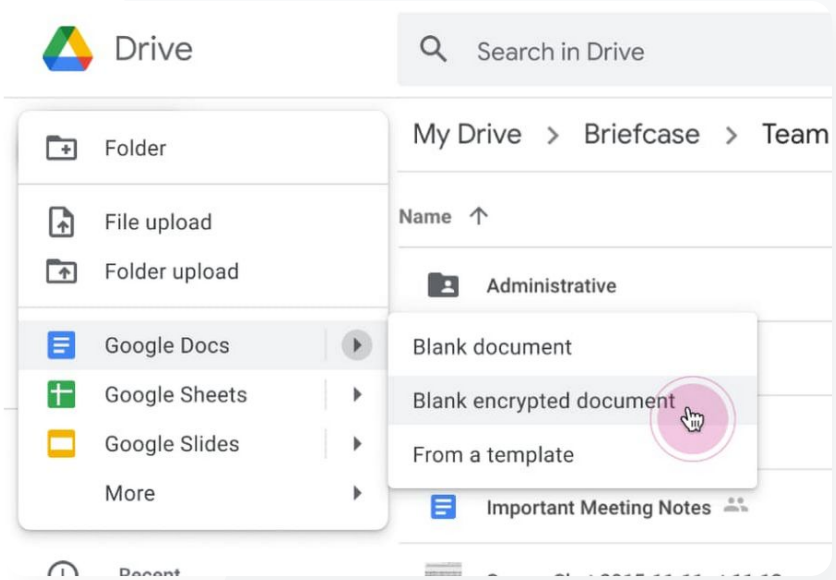
Google Workspace ya adopta las normas criptográficas más recientes para encriptar todos los datos en reposo y en tránsito entre sus instalaciones. Con la **encriptación del cliente**, los administradores tienen el control directo de las claves de encriptación y el proveedor de identidad que se usa para acceder a esas claves.

- Usa tus propias claves para encriptar datos sensibles, como la propiedad intelectual de tu institución.
- Tu navegador controla la encriptación de contenido antes de que los datos se transmitan o almacenen en la nube de Google.
- Elige los usuarios que pueden crear contenido con encriptación del cliente y compártelo de forma interna o externa.

Instructivo: Aprovecha la encriptación del cliente

Configura la encriptación del cliente (CSE)

- Configura tu servicio de claves de encriptación.
  - Protege tus datos con las funciones de administración y control de claves mediante la creación de tu propio servicio de claves.
- Conecta Google Workspace a tu servicio de claves externo.
  - Agrega y administra servicios de claves para la encriptación del cliente incluyendo la URL del servicio de claves en la Consola del administrador.
- Asigna tu servicio de claves a unidades organizativas o grupos.
  - Asigna un servicio de claves como la opción predeterminada para toda tu institución.
- Conecta Google Workspace a tu IdP.
  - Conecta tu proveedor de identidad (IdP) a la encriptación del cliente para verificar la identidad de los usuarios antes de permitirles encriptar contenido o acceder al contenido encriptado.
- Habilita la CSE para los usuarios.
  - Activa la encriptación del cliente para habilitar las unidades organizativas o grupos con los usuarios que necesitan crear contenido con encriptación del cliente.

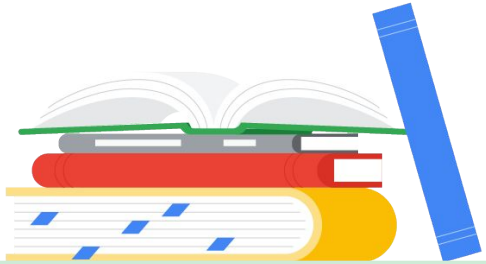


Documentación relevante del Centro de ayuda

- Acerca de la encriptación del cliente

Capacidades de enseñanza y aprendizaje

Equipa a los educadores con capacidades adicionales que puedan usar en el entorno de aprendizaje digital con experiencias de clase enriquecidas, herramientas para impulsar la integridad académica y una comunicación de video mejorada.

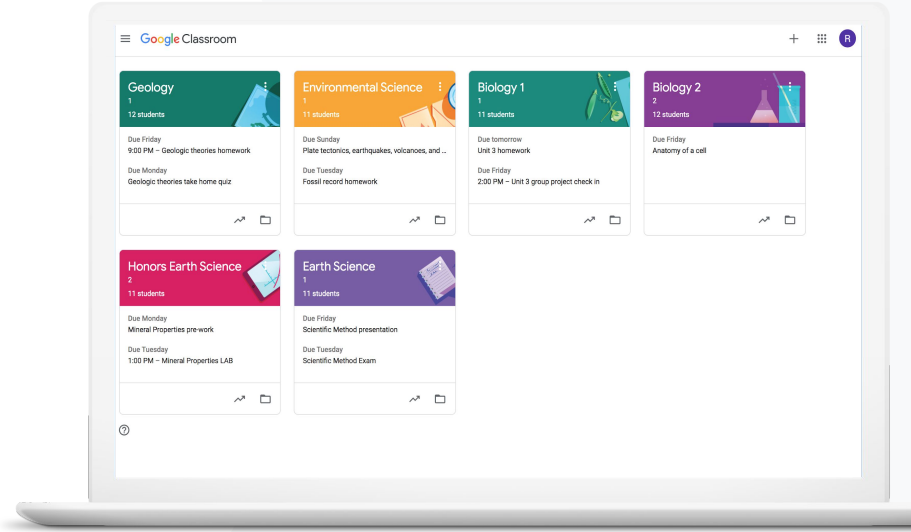


- Google Classroom
- Informes de originalidad
- Documentos, Hojas de cálculo y Presentaciones
- Google Meet

Google Classroom

¿De qué se trata?

Google Classroom es tu lugar central de enseñanza y aprendizaje. Sus funciones pagadas agrupan las herramientas de las clases en un solo lugar. Los educadores pueden acceder a sus herramientas favoritas directamente en Classroom y mantener las listas de las clases sincronizadas con los sistemas externos.



Casos de uso

Administra el acceso a los complementos de Classroom	Instructivo paso a paso
Integra contenido atractivo en Classroom	Instructivo paso a paso
Crea clases a gran escala	Instructivo paso a paso

“Me gustaría poder facilitarles a mis educadores un acceso de inicio de sesión único a sus herramientas de tecnología educativa favoritas”.

Administra el acceso a los complementos de Classroom

Determina a qué apps educativas de terceros puede acceder tu institución con una **lista de dominios permitidos**. Permite que los educadores instalen complementos fácilmente y los incluyan en las tareas de los alumnos con solo unos clics.

- Crea una lista de entidades permitidas en tu dominio para determinar qué apps de terceros pueden instalar los educadores desde Google Workspace Marketplace.
- Respalda los resultados de aprendizaje con apps educativas complementarias. Los educadores pueden asignar, revisar y calificar tareas desde Google Classroom.
- Google Workspace Marketplace incluye Adobe Creative Cloud Express, BookWidgets, CK-12, Formative, Genially, Google Arts & Culture, IXL, Kahoot!, Nearpod, Newsela, Pear Deck, SAFARI Montage, Sora y Wordwall, entre otras apps.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Administra las apps de Google Workspace Marketplace
- Usa complementos en Classroom
- Administra las apps de Marketplace en tu lista de entidades permitidas
- Distribuye una app de Marketplace a los usuarios
- Complementos de Classroom (guía de introducción para profesores)

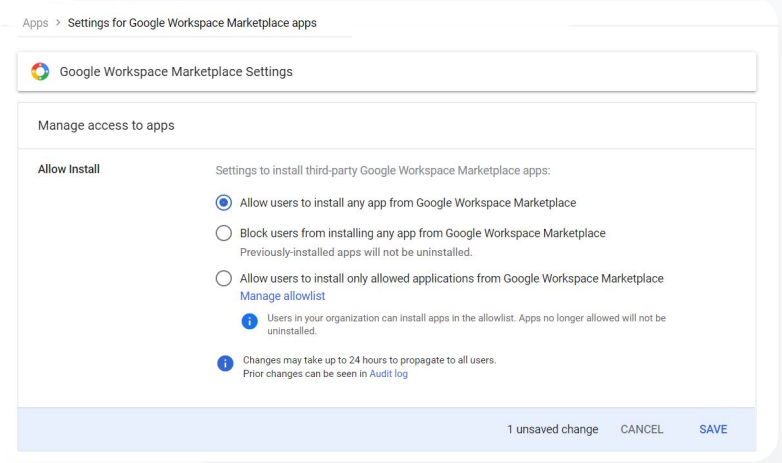
Instructivo: Administra el acceso a los complementos de Classroom

Administra el acceso a los complementos con una lista de dominios permitidos

- En la Consola del administrador, selecciona **Menú** > **Apps de Google Workspace Marketplace** (Google Workspace Marketplace apps) > **Lista de apps**.
- Selecciona **Incluir la app en la lista de entidades permitidas**.
- Ingresa el nombre del complemento que quieras o búscalo.
- Haz clic en **Seleccionar** y asegúrate de que esté seleccionada la opción **Permitir que los usuarios instalen esta app**.
- Haz clic en **Continuar** y **Terminar**.

Otorga a los complementos acceso a la lista de entidades permitidas que quieras

- En la Consola del administrador, selecciona **Menú** > **Apps de Google Workspace Marketplace** (Google Workspace Marketplace apps) > **Lista de apps**.
- Selecciona el complemento que quieras distribuir.
- En **Acceso de usuario**, haz clic en **Ver los grupos y las unidades organizativas**.
- Elige **Disponible para todos** o define mejor el acceso para **grupos** o **unidades organizativas** seleccionados.
- Haz clic en **Guardar**.



Documentación relevante del Centro de ayuda

- Administra las apps de Google Workspace Marketplace
- Usa complementos en Classroom
- Administra las apps de Marketplace en tu lista de entidades permitidas
- Distribuye una app de Marketplace a los usuarios
- Complementos de Classroom (guía de introducción para profesores)

“Quiero asignar y evaluar un juego de aprendizaje de Kahoot! a mis alumnos sin salir de Google Classroom”.

Integra contenido atractivo en Classroom

Con los **complementos de Classroom**, los educadores pueden compartir actividades y contenido atractivo con su clase agregando complementos a las tareas, las preguntas, los materiales o los anuncios sin salir de Classroom.

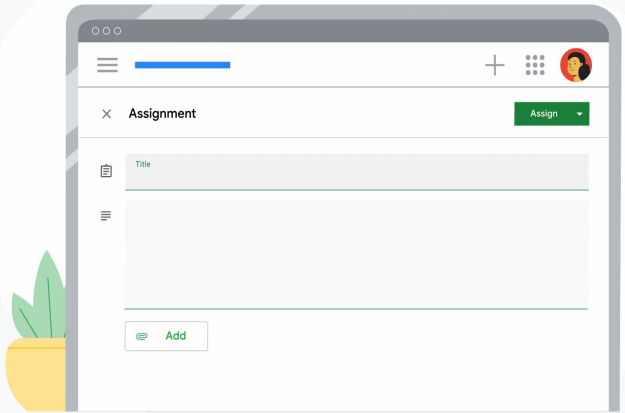
- Permite que los educadores y alumnos usen sus herramientas favoritas, como Kahoot!, Nearpod y Pear Deck sin tener que salir de Classroom.
- Con los complementos, los alumnos no tendrán que administrar múltiples contraseñas ni navegar a sitios web externos.
- Califica y revisa los trabajos de los alumnos con complementos directamente desde Classroom.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Usa complementos en Classroom
- Complementos de Classroom (guía de introducción para profesores)

Instructivo: Integra contenido atractivo en Classroom



Cómo adjuntar complementos a una tarea, un cuestionario una pregunta

- Accede a tu cuenta de Classroom en **classroom.google.com**.
- Selecciona la clase que deseas de la lista y elige **Trabajo en clase**.
- Selecciona **Crear** y elige lo que quieras crear.
- Ingresa el título y las instrucciones.
- En **Complementos**, elige el complemento que quieras usar.
- Selecciona **Asignar** (Assign).

Cómo adjuntar complementos a un anuncio

- En la página **Novedades**, selecciona **Anuncia algo a la clase**.
- Ingresa el anuncio.
- En **Complementos**, elige el complemento que quieras usar.
- Selecciona **Publicar**.

Documentación relevante del Centro de ayuda

- Usa complementos en Classroom
- Complementos de Classroom (guía de introducción para profesores)

“Necesito una forma para automatizar la configuración de clases y administrar listas de alumnos en Google Classroom”.

Crea clases a gran escala

La importación de listas del SIA te permite crear clases de forma automática y mantener sincronizadas las listas de la clase con el sistema de información de alumnos (SIA) de tu institución educativa con Clever.

- Esta función está disponible para los distritos de preescolar a bachillerato en EE.UU. y Canadá que tengan Education Plus.
- Los administradores pueden importar listas de clases de tu SIA en Google Classroom para configurar automáticamente las clases.
- Automatiza y administra a la perfección las listas de clases en Google Classroom.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Comienza a importar listas de SIA
- Configura la importación de listas del SIA con Clever

Instructivo: Crea clases a gran escala

Cómo configurar la importación de listas del SIA

- Configura la sincronización de listas de Google Classroom con Clever.
- El administrador de tu distrito en Clever y el administrador avanzado de Google Workspace pueden seguir las instrucciones paso a paso de Clever.

Sigue estos pasos si tu distrito no tiene una cuenta de Clever:

- Crea una cuenta de Clever.

Sigue estos pasos si tu distrito tiene una cuenta de Clever:

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

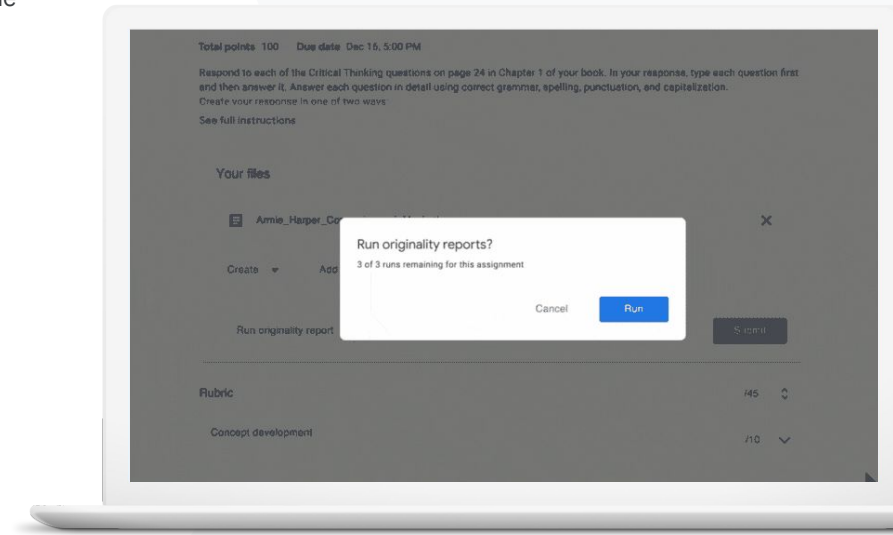
Documentación relevante del Centro de ayuda

- Configura la importación de listas del SIA con Clever

Informes de originalidad

¿De qué se trata?

Los informes de originalidad permiten que los educadores verifiquen la autenticidad de los trabajos mediante la Búsqueda de Google para comparar el trabajo de un alumno con miles de millones de páginas web y más de 40 millones de libros. Las funciones pagadas de los informes de originalidad proporcionan acceso ilimitado para que los educadores analicen las entregas de los alumnos con un repositorio de la institución educativa en el que se almacenan los trabajos anteriores de los alumnos.



Casos de uso

Análisis de plagio	Instructivo paso a paso
Verifica la originalidad según los trabajos previos de los alumnos	Instructivo paso a paso
Convierte la detección de plagio en una oportunidad de aprendizaje	Instructivo paso a paso

“Quiero verificar si hay plagio o citas incorrectas en el trabajo de mis alumnos”.

Análisis de plagio

Los profesores pueden verificar la autenticidad de los trabajos de sus alumnos con los **informes de originalidad**. En el informe se incluyen vínculos a las fuentes detectadas y se marca el texto sin citar.

- Ejecuta informes de originalidad con Documentos, Presentaciones y documentos de Microsoft Word.
- Los educadores que usan Teaching and Learning Upgrade o Education Plus obtienen los siguientes beneficios:
  - Acceso ilimitado a los informes de originalidad
  - Comparaciones de las coincidencias entre alumnos con un repositorio de trabajos entregados anteriormente

Los datos siempre son tuyos; la responsabilidad de mantener su seguridad y privacidad es nuestra.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

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

Instructivo: Análisis de plagio

Activa los informes de originalidad para una tarea en Classroom

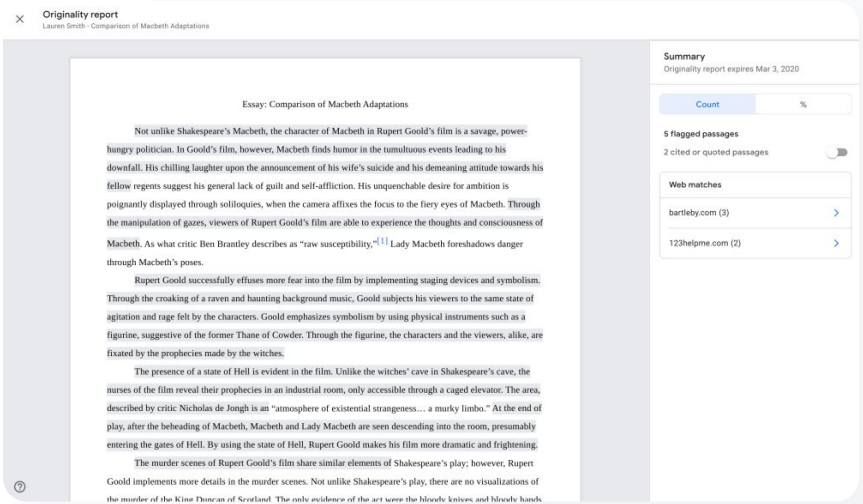
- Accede a tu cuenta de Classroom en **classroom.google.com**.
- Selecciona la clase relevante de la lista y elige **Trabajo en clase**.
- Selecciona **Crear** > **Tarea**.
- Marca la casilla junto a **Informes de originalidad** para activarlos.

Ejecuta un informe de originalidad en el trabajo de un alumno

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

Activa los informes de originalidad para una tarea en tu SGA

- Accede a tu **sistema de gestión de aprendizaje**.
- Selecciona el **curso** relevante.
- Crea una tarea y selecciona **Tareas de Google**.
- Marca la casilla **Habilitar informes de originalidad**.



Documentación relevante del Centro de ayuda

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

“¿Cómo puedo habilitar a los profesores para que analicen el trabajo de sus alumnos en busca de plagio comparándolo con trabajos de años anteriores?”

Instructivo paso a paso

Documentación relevante del Centro de ayuda

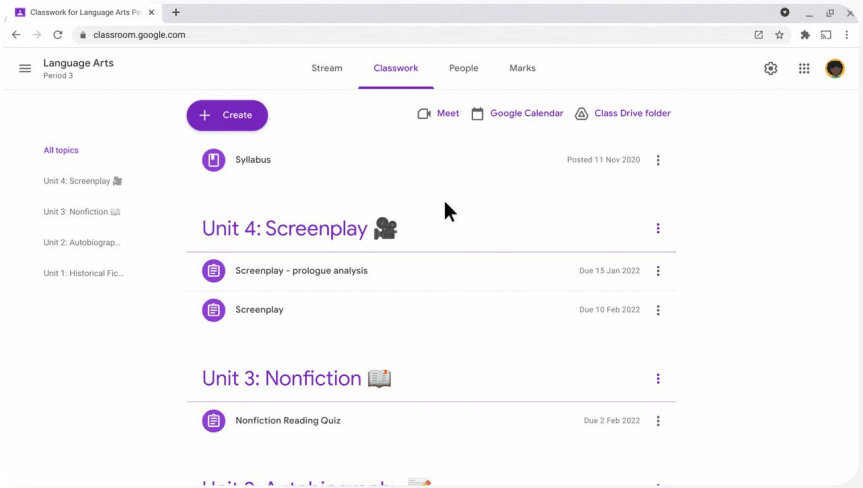
- Activa los informes de originalidad
- Activa las coincidencias en la institución educativa para los informes de originalidad en Classroom

Verifica la originalidad según los trabajos previos de los alumnos

Las **coincidencias en la institución educativa** de los informes de originalidad permiten que los educadores comparen el trabajo de sus alumnos con entregas pasadas mediante el análisis de las tareas con el repositorio privado con los trabajos estudiantiles de la institución educativa.

- Compara las coincidencias entre alumnos con los trabajos actuales y anteriores para detectar el plagio con los planes Teaching and Learning Upgrade o Education Plus.
- Puedes almacenar el trabajo de los alumnos de forma segura y reabastecer tu repositorio privado de todo el dominio propiedad de la institución educativa.

Instructivo: Verifica la originalidad según los trabajos previos de los alumnos



Cómo activar las coincidencias en la institución educativa para los informes de originalidad

- En la Consola del administrador, selecciona **Menú** > **Apps** > **Servicios adicionales de Google** > **Classroom**.
- Selecciona la **unidad organizativa del profesor**.
- Haz clic en **Informes de originalidad** y marca la casilla **Habilitar las coincidencias en la institución educativa de los informes de originalidad**.
- Haz clic en **Guardar**.

Documentación relevante del Centro de ayuda

- Activa las coincidencias en la institución educativa para los informes de originalidad en Classroom

“Quiero que mis alumnos aprendan a citar correctamente las fuentes que usan”.

Convierte la detección de plagio en oportunidad de aprendizaje

Los alumnos pueden verificar si hay contenido sin citas y plagio no intencional antes de entregar sus trabajos ejecutando un **informe de originalidad** hasta tres veces por tarea. Los informes de originalidad comparan los trabajos de los alumnos con varias fuentes y los alertan de textos sin citas, lo que les da la oportunidad de aprender, corregir errores y entregar sus trabajos con confianza.

- En Teaching and Learning Upgrade y Education Plus, los educadores pueden usar los informes de originalidad las veces que quieran, mientras que, en Education Fundamentals, pueden hacerlo solo cinco veces por clase.
- Después de la entrega del trabajo, Classroom ejecuta automáticamente un informe que solo el profesor puede ver. Si cancelas el envío de una tarea y la vuelves a enviar, Classroom ejecutará otro informe de originalidad para el profesor.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

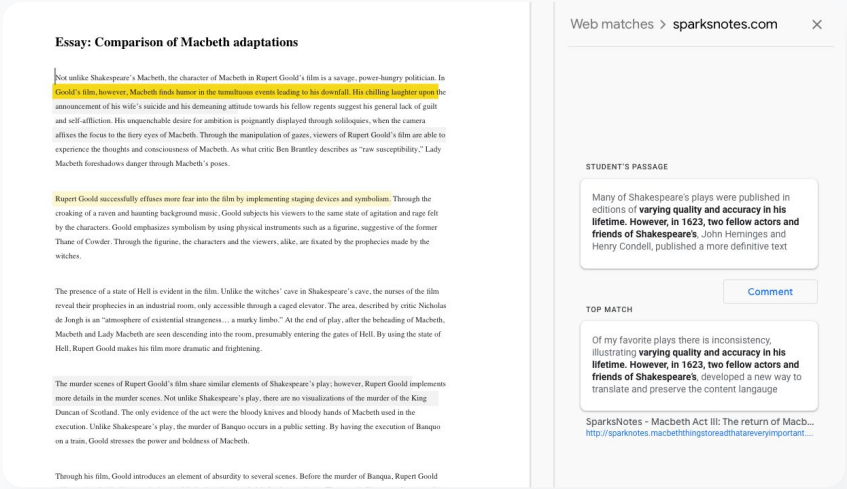
- Ejecuta un informe de originalidad en un trabajo

Instructivo: Convierte la protección contra el plagio en oportunidad de aprendizaje

Cómo pueden los alumnos ejecutar informes de originalidad en Classroom

- Accede a tu cuenta de Classroom en classroom.google.com.
- Selecciona la clase relevante de la lista y elige **Trabajo en clase**.
- Selecciona la tarea relevante de la lista y haz clic en **Ver tarea**.
- En **Tu trabajo**, selecciona **Subir** o **crea un archivo**.
- Junto a **Informes de originalidad**, haz clic en **Ejecutar**.
- Para abrir el informe, haz clic en **Ver informe de originalidad** debajo del nombre del archivo de la tarea.
- Si quieres revisar la tarea para reescribirla o incluir citas sobre los pasajes marcados, haz clic en **Editar** en la parte inferior.

Los alumnos pueden ejecutar informes de originalidad en el SGA mediante Tareas de Google.



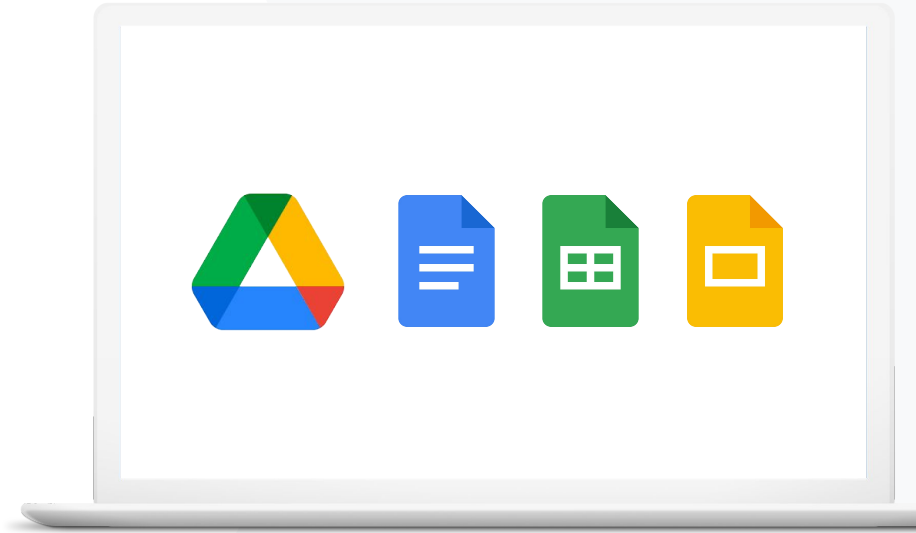
Documentación relevante del Centro de ayuda

- Ejecuta un informe de originalidad en Classroom
- Ejecuta un informe de originalidad en tu SGA

Documentos, Hojas de cálculo y Presentaciones

¿De qué se trata?

Documentos, Hojas de cálculo y Presentaciones permiten a las comunidades escolares colaborar, crear en conjunto, revisar y editar simultáneamente en tiempo real. Las funciones pagadas de Education Plus permiten que educadores y administradores establezcan un proceso de aprobación para la documentación interna en toda tu institución.



Casos de uso

Aprueba documentos internos — Instructivo paso a paso

“

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

¿Cómo puedo garantizar que todos los jefes de departamentos aprueben la propuesta?”

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Administra las aprobaciones

Aprueba documentos internos

Con las **aprobaciones**, tu comunidad educativa puede enviar documentos en Google Drive mediante un proceso formal de aprobación.

- Los revisores pueden aprobar el documento, rechazarlo o dejar comentarios en ellos directamente en Drive, Documentos y otras apps de Google Workspace.
- Los responsables de aprobación deberán seguir un vínculo al documento donde podrán revisarlo, dejar comentarios, rechazarlo o aprobarlo.
- Administra la aprobación de un contrato o un empleado nuevo, los cambios en un documento antes de su publicación y mucho más.

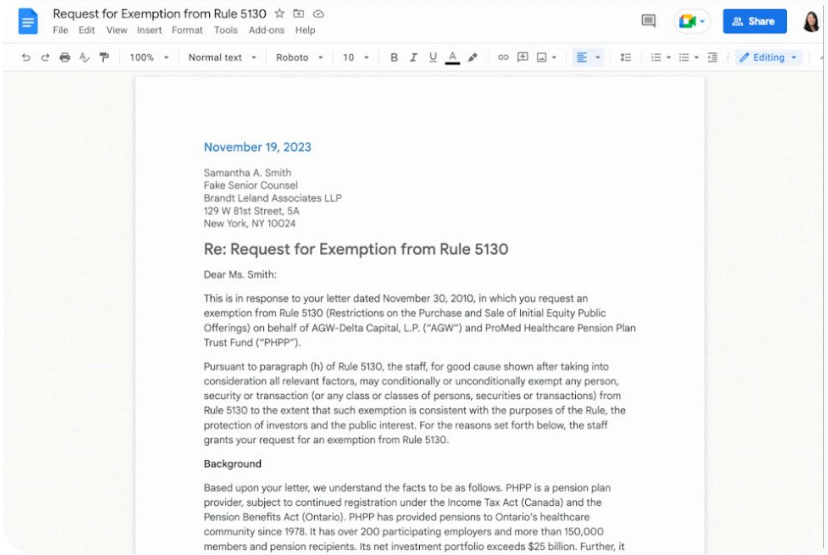
Instructivo: Aprueba documentos internos

Cómo funciona

Los administradores pueden controlar la participación de usuarios y archivos en el proceso de aprobación.

Cómo administrar aprobaciones

- Accede a la **Consola del administrador**, ve a **Menú** > **Apps** > **Google Workspace** > **Drive y Documentos**.
- Haz clic en **Aprobaciones**.
- Para aplicar el parámetro de configuración a todos, selecciona una **unidad organizativa** secundaria o un **grupo de configuración**.
- Haz clic en **Guardar**.



Documentación relevante del Centro de ayuda

- Administra las aprobaciones

Google Meet

¿De qué se trata?

Las funciones avanzadas de Google Meet incluyen transmisiones en vivo, sesiones separadas, reuniones más grandes, grabaciones de las reuniones, subtítulos traducidos instantáneamente y mucho más.

Casos de uso

Graba reuniones — Instructivo paso a paso	Haz preguntas — Instructivo paso a paso
Haz referencia al contenido de las clases — Instructivo paso a paso	Recopila información — Instructivo paso a paso
Derriba las barreras lingüísticas — Instructivo paso a paso	Grupos pequeños de alumnos — Instructivo paso a paso
Transmite en vivo asambleas y eventos institucionales — Instructivo paso a paso	Seguimiento de la asistencia — Instructivo paso a paso

“Nuestra institución ofrece cursos de desarrollo profesional en línea a gran escala que necesitamos grabar para los educadores que no pueden asistir”.

Graba reuniones

Con Teaching and Learning Upgrade y Education Plus, los educadores pueden grabar clases, reuniones de la facultad, capacitaciones para el desarrollo profesional y mucho más. Las reuniones se guardan automáticamente en Drive.

- Las grabaciones se guardan en la unidad de Drive del organizador de la reunión. Antes de grabar, asegúrate de tener suficiente espacio.
- Se recomienda que los administradores de TI habiliten la grabación solo para el cuerpo docente y el personal.

Instructivo paso a paso

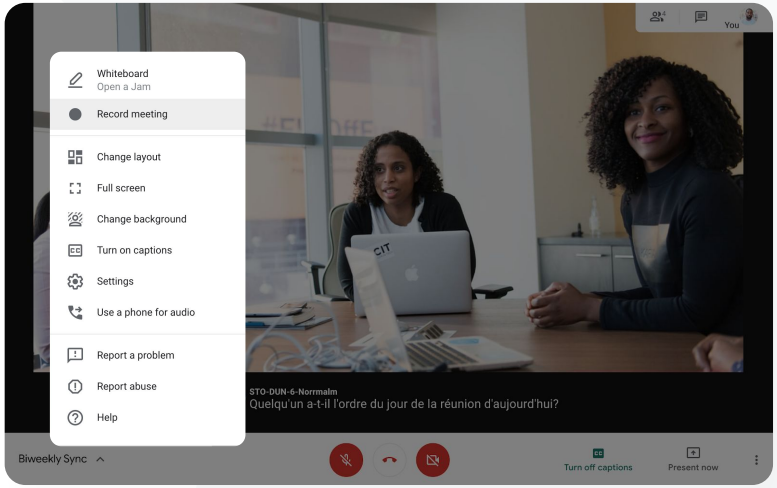
Documentación relevante del Centro de ayuda

- Graba una videoconferencia

Instructivo: Graba reuniones

Cómo comenzar una grabación

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



Documentación relevante del Centro de ayuda

- Graba una videoconferencia

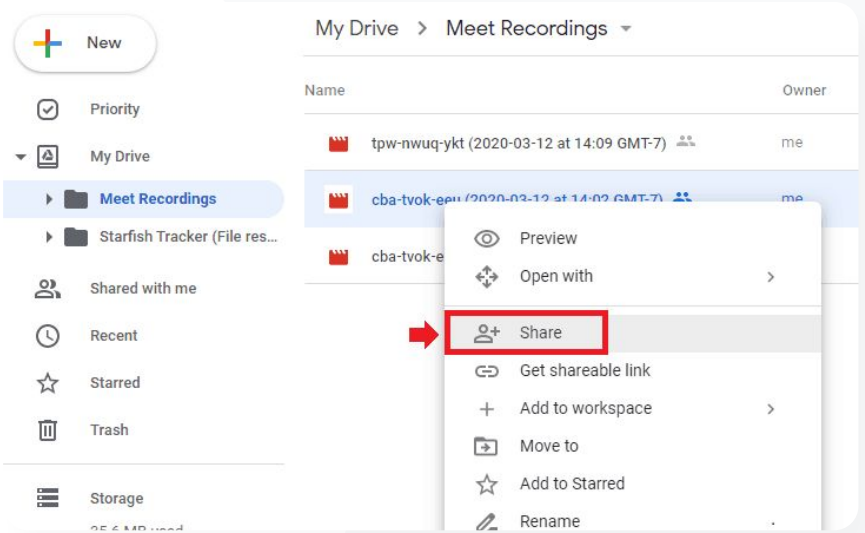
Instructivo: Ve y comparte grabaciones

Cómo comenzar una grabación

- Selecciona el archivo.
- Haz clic en el ícono **Compartir**.
- **Agrega** usuarios aprobados.

O

- Selecciona el ícono de **vínculo**.
- **Pega** el vínculo en un correo electrónico o mensaje de Chat.



Cómo descargar una grabación

- Selecciona el archivo.
- Haz clic en el ícono de **más** > Descargar.
- **Haz doble clic** en el archivo descargable para reproducir la grabación.

Cómo reproducir la grabación desde Drive

- En Drive, haz doble clic en el archivo de la grabación para reproducirla; el mensaje “Aún se está procesando” aparecerá hasta que el archivo esté listo para reproducirse en línea.
- Para agregar una grabación a tu unidad de Drive, selecciona el archivo y haz clic en **Agregar a Mi unidad**.

Documentación relevante del Centro de ayuda

- Graba una videoconferencia

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

Haz referencia al contenido de las clases

Con las transcripciones de las reuniones, los educadores pueden registrar automáticamente las sesiones y los debates de la clase, de modo que a los alumnos les resulte más fácil repasar los conceptos. Las transcripciones registran la asistencia a las reuniones y muestran las intervenciones de los asistentes.

- La función está disponible en inglés para los usuarios de Google Meet en una computadora o laptop.
- Los administradores pueden habilitar la transcripción para sus comunidades educativas.
- Las transcripciones se guardan automáticamente en la unidad de Drive del anfitrión de la reunión.
- Cuando se activan las transcripciones, aparece el ícono Transcripciones en la esquina superior izquierda para todos los participantes de la reunión.
- Las transcripciones contienen las palabras que se dijeron en una reunión. Para obtener una transcripción de los mensajes de chat, debes grabar la reunión.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Usa transcripciones con Google Meet
- Activa o desactiva las transcripciones

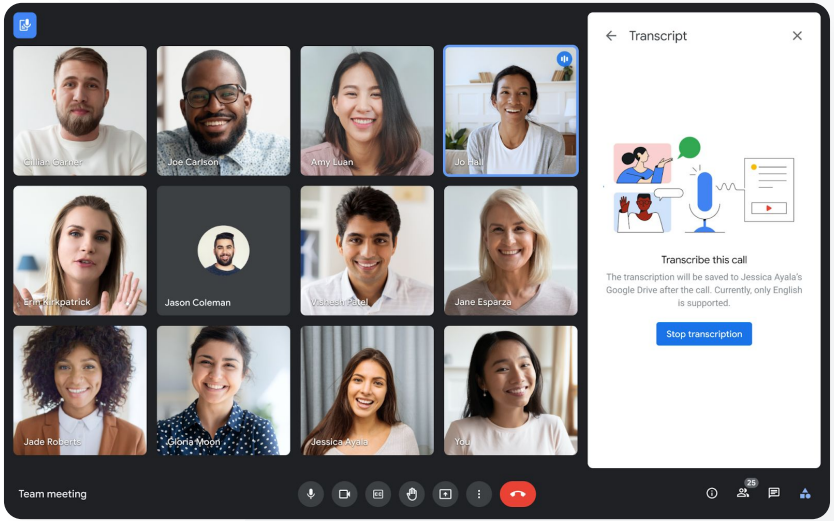
Instructivo: Haz referencia al contenido de las clases

Cómo activar las transcripciones en Google Meet

- Durante una reunión, selecciona el ícono **Actividades** que se encuentra en la esquina inferior derecha.
- Haz clic en **Transcripciones** > **Iniciar transcripción** > **Iniciar**.

Cómo detener las transcripciones en Google Meet

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



Documentación relevante del Centro de ayuda

- Usa transcripciones con Google Meet
- Activa o desactiva las transcripciones

Organizamos reuniones virtuales para padres y profesores, pero a veces no todos hablamos el mismo idioma.

¿Cómo puedo hacer que las reuniones sean inclusivas y superar las barreras lingüísticas?”

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Usa subtítulos traducidos en Google Meet

Derriba las barreras lingüísticas

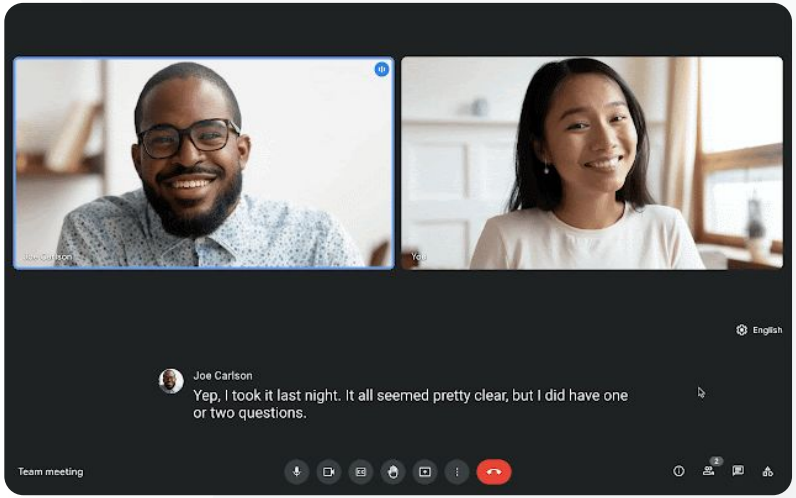
Los subtítulos traducidos hacen que las reuniones sean más inclusivas, ya que derriban las barreras lingüísticas. Cuando los participantes de una reunión usan contenido en su idioma de preferencia, facilitan el uso compartido de información, el aprendizaje y la colaboración.

- Los educadores pueden interactuar con alumnos, padres y partes interesadas de la comunidad que hablen otro idioma.
- Utiliza subtítulos para traducir del inglés al francés, alemán, portugués o español.
- También puedes traducir del inglés al japonés, mandarín o sueco.

Instructivo: Derriba las barreras lingüísticas

Cómo activar la traducción de subtítulos

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



Documentación relevante del Centro de ayuda

- Usa subtítulos traducidos en Google Meet

“Necesitamos hacer transmisiones en vivo de las reuniones con nuestro personal y cuerpo docente a un amplio grupo de partes interesadas, madres y padres”.

Transmite asambleas, eventos escolares y reuniones

Transmite en vivo a un máximo de 10,000 usuarios con Teaching and Learning Upgrade y a un máximo de 100,000 usuarios con Education Plus. Los participantes se pueden unir mediante el vínculo de la transmisión en vivo proporcionado por el organizador en un correo electrónico o una invitación de Calendario.

- Determina el alcance con el que se compartirá tu transmisión en vivo. Elige las condiciones de la transmisión:
  - Visible únicamente para los usuarios de tu organización (dentro del dominio)
  - Compartida con otros dominios de confianza de Google Workspace
  - Disponible para mirarla en YouTube
- Se recomienda que los administradores de TI habiliten la transmisión en vivo solo para el cuerpo docente y el personal.
- Si un usuario no pudo asistir a la transmisión en vivo, podrá acceder a la grabación después de que termine la reunión.
- Agrega subtítulos, encuestas y preguntas y respuestas a una transmisión en vivo para aumentar la inclusión y participación.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Activa o desactiva la transmisión en vivo en Meet
- Transmite en vivo una videoconferencia

Instructivo: Transmite asambleas, eventos escolares y reuniones

Cómo crear un evento de transmisión en vivo

- Abre el **Calendario de Google**.
- Selecciona **+ Crear** > **Evento** > **Más opciones**.
- Agrega los detalles del evento, como la fecha, la hora y la descripción.
- Agrega invitados que tendrán participación total en la videoconferencia (podrán presentar y los demás podrán verlos y escucharlos).
- Haz clic en **Agregar una videoconferencia de Google Meet**.
- Junto a Únete con Google Meet, selecciona la **flecha hacia abajo** y, luego, **Agregar transmisión en vivo**.
- Para invitar a la mayor cantidad de usuarios que te permita tu edición pagada, haz clic en **Copiar** y comparte la URL de la transmisión en vivo.
- Selecciona **Guardar**.
- La transmisión en vivo no se inicia automáticamente. Para iniciarla, selecciona **Más** > **Iniciar transmisión**.

Documentación relevante del Centro de ayuda

- Activa o desactiva la transmisión en vivo en Meet
- Transmite en vivo una videoconferencia

“Necesito contar con una forma rápida de hacer preguntas, medir el conocimiento de los alumnos y, además, interactuar con la clase para motivar la participación”.

Haz preguntas

Usa la función de **Preguntas y respuestas** de Google Meet para motivar la participación de los alumnos y hacer que las clases sean más interactivas. Los educadores incluso recibirán un informe detallado de todas las preguntas y respuestas al final de la clase virtual.

- Los moderadores pueden hacer todas las preguntas que sean necesarias. Pueden ordenar o filtrar las preguntas, marcarlas como respondidas y, además, ocultar o priorizar preguntas.
- Después de cada reunión que tenga las preguntas habilitadas, se enviará automáticamente por correo electrónico un informe de preguntas al moderador.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Haz preguntas a los participantes en Google Meet

Instructivo: Haz preguntas

Haz una pregunta

- Durante la reunión, selecciona el **ícono de actividades** > **Preguntas**, que se encuentra en la esquina superior derecha (para activar las Preguntas y respuestas, selecciona **Activar Preguntas y respuestas**).
- Para hacer una pregunta, haz clic en **Hacer una pregunta** en la esquina inferior derecha.
- **Escribe las preguntas** y haz clic en **Publicar.**

Visualiza el informe de preguntas

- Después de una reunión, el moderador recibirá un **informe por correo electrónico**.
- Abre el correo electrónico y haz clic en el **informe adjunto**.

Documentación relevante del Centro de ayuda

- Haz preguntas a los participantes en Google Meet

Necesito contar con una forma sencilla de recopilar información que me proporcionen los alumnos y otros educadores mientras dirijo una clase o una reunión de personal".

Recopila información

El usuario que programó o inició una reunión virtual puede crear una **encuesta** para los participantes. Esta función permite agregar información de todos los alumnos o participantes de una reunión de forma participativa y con rapidez.

- Los moderadores pueden guardar la encuesta y publicarla durante otra reunión futura. Se guardan en la sección Encuestas de una reunión virtual.
- Después de la reunión, un informe de los resultados de la encuesta se enviará por correo electrónico al moderador automáticamente.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Realiza encuestas en Google Meet

Instructivo: Recopila información

Crea una encuesta

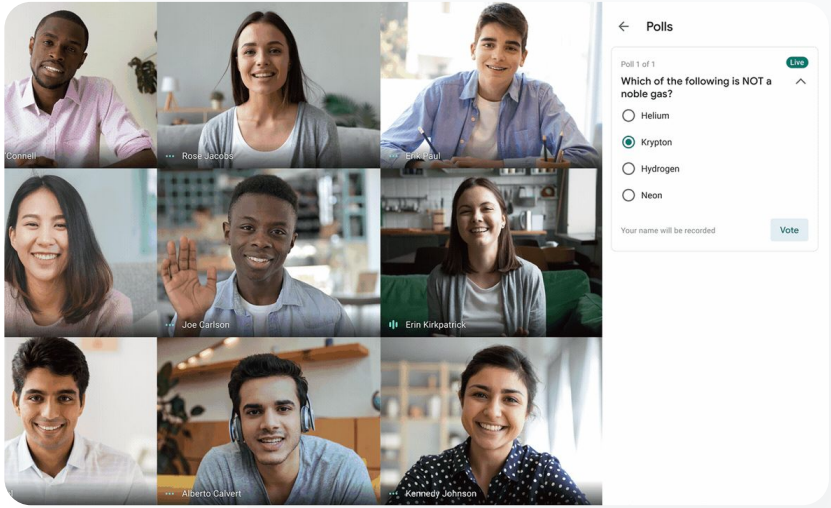
- En la esquina superior derecha de una reunión, selecciona el **ícono de actividades** > **Encuesta**.
- Haz clic en **Iniciar una encuesta**.
- Ingresa una pregunta.
- Haz clic en **Lanzar** o **Guardar**.

Modera una encuesta

- Durante una reunión, selecciona el **ícono de actividades** > **Encuesta**, que se encuentra en la esquina superior derecha.
- Para que los alumnos vean los resultados de la encuesta en tiempo real, junto a **Mostrar los resultados a todos**, **activa la opción con el botón**.
- Para cerrar una encuesta y ya no permitir que se envíen más respuestas, haz clic en **Finalizar encuesta**.
- Para borrar una encuesta de forma permanente, haz clic en el **ícono Borrar**.

Consulta el informe de una encuesta

- Después de una reunión, los moderadores recibirán un **informe por correo electrónico**.
- Abre el correo electrónico y selecciona el **archivo adjunto del informe**.



Documentación relevante del Centro de ayuda

- Realiza encuestas en Google Meet

“En ocasiones, tenemos alumnos que estudian desde sus casas. Necesitamos crear fácilmente salas de reuniones basadas en grupos predefinidos cuando trabajamos en grupos pequeños”.

Grupos pequeños de alumnos

Los educadores pueden usar las sesiones separadas para dividir a los alumnos en grupos más pequeños durante las clases virtuales, **híbridas o presenciales**. Los moderadores deben iniciar las sesiones separadas durante una videollamada en una computadora.

- Las sesiones separadas se pueden crear de antemano durante la preparación de un evento o durante una reunión en curso.
- Crea hasta 100 sesiones separadas por reunión virtual.
- El profesor puede cambiar con facilidad de una sesión separada a otra para ayudar a los grupos cuando sea necesario.
- Los administradores pueden asegurarse de que solo los miembros del cuerpo docente o el personal puedan crear sesiones separadas.

Instructivo paso a paso

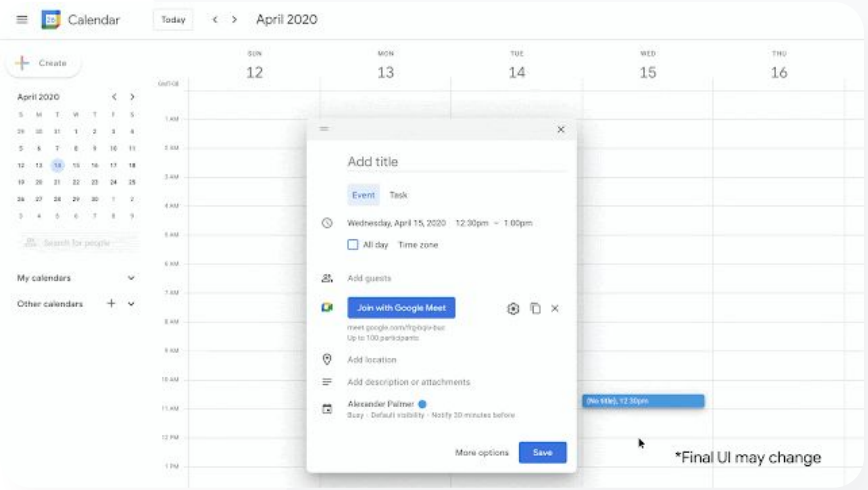
Documentación relevante del Centro de ayuda

- Usa sesiones separadas en Google Meet

Instructivo: Crea grupos pequeños de alumnos

Crea sesiones separadas antes de la reunión

- Crea un nuevo evento de Calendario de Google.
- Haz clic en **Agregar videoconferencia de Google Meet**.
- Agrega participantes y selecciona **Cambiar configuración de la reunión**.
- Haz clic en **Sesiones separadas**.
- Elige la cantidad de sesiones separadas y selecciona una de las siguientes opciones:
  - Arrastrar los participantes a diferentes sesiones separadas.
  - Ingresar los nombres directamente en una sesión separada.
  - Mezclar los grupos haciendo clic en **Aleatorio**.
- Haz clic en **Guardar**.



Documentación relevante del Centro de ayuda

- Usa sesiones separadas en Google Meet

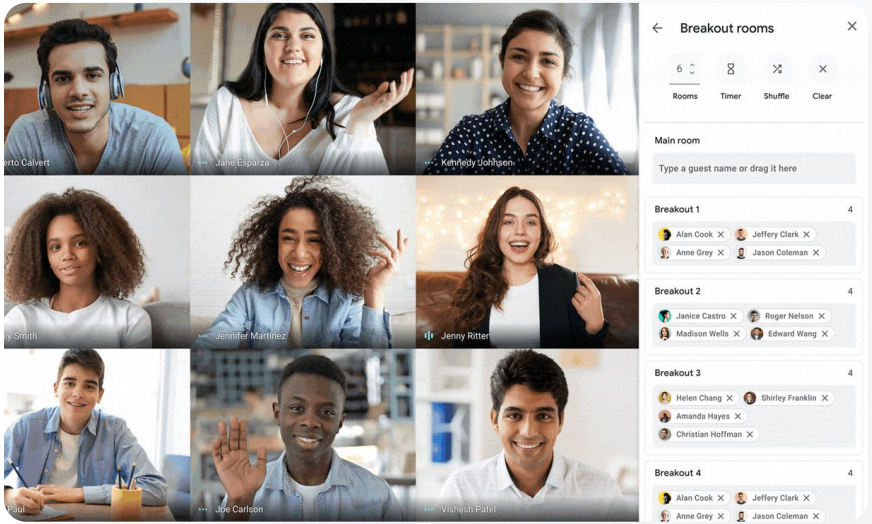
Instructivo: Crea grupos pequeños de alumnos

Crea sesiones separadas durante la reunión

- Inicia una videollamada
- En la parte superior derecha, selecciona el **ícono de actividades** > **Sesiones separadas**.
- En el panel de Sesiones separadas, **elige la cantidad de sesiones** que necesitas crear.
- Los alumnos se distribuirán en salas, pero los moderadores podrán mover a los alumnos de una sala a otra de forma manual si es necesario.
- En la parte inferior derecha, haz clic en **Abrir sesiones separadas**.

Responde preguntas en diferentes sesiones separadas

- Una notificación en la parte inferior de la pantalla del moderador se mostrará cuando los participantes estén pidiendo ayuda. Haz clic en Unirse para ingresar a la sesión separada del participante.



Documentación relevante del Centro de ayuda

- Usa sesiones separadas en Google Meet

“Tenemos dificultades para hacer un seguimiento de quiénes asisten a las clases en línea. Necesitamos contar con una forma sencilla de generar informes de asistencia a las clases en todo el dominio”.

Seguimiento de la asistencia

El **seguimiento de la asistencia** genera un informe de asistencia automático para cualquier reunión con cinco o más participantes. Los informes muestran quiénes se unieron a la llamada, los correos electrónicos de los participantes y cuánto tiempo estuvieron en la clase virtual.

- Puedes hacer un seguimiento de la asistencia durante los eventos de transmisión en vivo con los informes de las transmisiones en vivo.
- Los moderadores pueden activar o desactivar los informes de seguimiento de la asistencia y de las transmisiones en vivo desde una reunión o desde el evento de Calendario.

Instructivo paso a paso

Documentación relevante del Centro de ayuda

- Haz un seguimiento de la asistencia en Google Meet

Instructivo: Seguimiento de la asistencia

Cómo hacer un seguimiento de la asistencia a una reunión

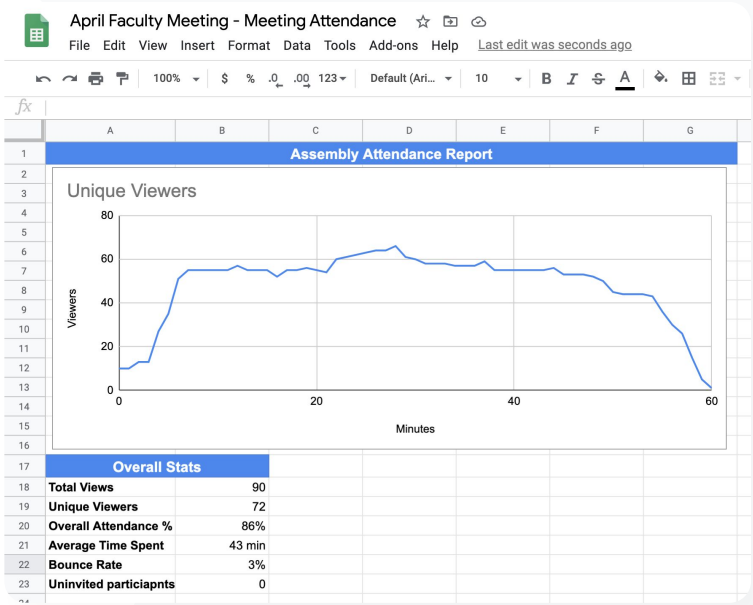
- Inicia una videollamada
- En la parte inferior, selecciona el **ícono de menú**.
- Selecciona el **ícono de configuración** > **Controles del organizador**.
- Activa o desactiva el **Seguimiento de la asistencia**.

Cómo hacer un seguimiento de la asistencia en Calendario

- **Habilita las conferencias de Google Meet** desde un evento de Calendario.
- A la derecha, selecciona el **ícono de configuración**.
- Selecciona la casilla junto a **Seguimiento de la asistencia** y haz clic en **Guardar**.

Obtén el informe de asistencia

- Después de una reunión, el moderador recibirá un **informe por correo electrónico**.
- Abre el correo electrónico y selecciona el **informe adjunto**.



Documentación relevante del Centro de ayuda

- Haz un seguimiento de la asistencia en Google Meet

Gracias