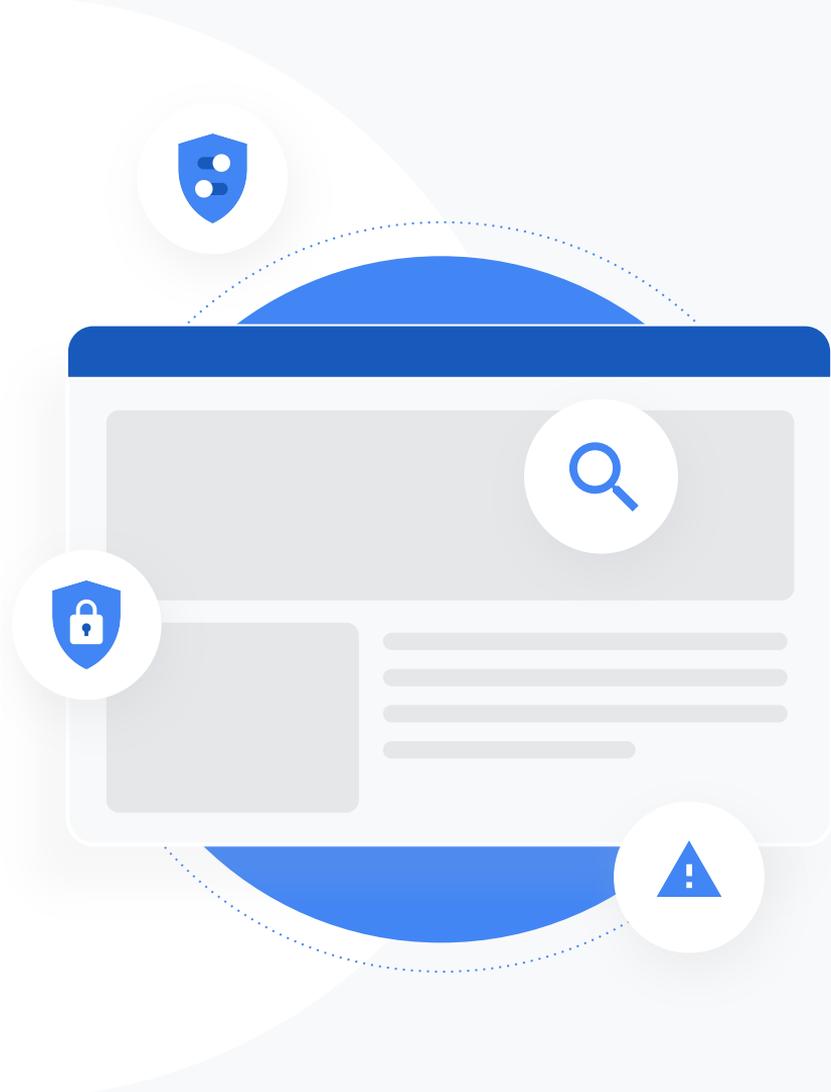


Google for Education

Más de 30 maneras de usar las ediciones de pago de Google Workspace for Education

goo.gle/use-edu-workspace



Cómo utilizar esta presentación

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

La presentación está organizada por funciones, seguidas de casos prácticos habituales e instrucciones sencillas sobre cómo usar cada una de ellas. Lee la presentación al completo para ver el amplio abanico de opciones que te ofrece Google Workspace for Education.

Ediciones de pago de Google Workspace for Education

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



Google Workspace for Education Standard

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



Teaching and Learning Upgrade

Las herramientas optimizadas para docentes ayudan a mejorar la comunicación y las experiencias en la clase, y sirven de guía para mantener la integridad académica.



Google Workspace for Education Plus

Una solución completa que incluye, entre otras ventajas, todas las funciones de Education Standard y Teaching and Learning Upgrade, es el entorno de aprendizaje más efectivo y unificado para tu comunidad educativa.

Índice



Herramientas de seguridad y analíticas

Herramientas incluidas en Education Standard y Education Plus

Herramienta de investigación

- Material inadecuado que se comparte
- Archivos compartidos accidentalmente
- Clasificación de correos
- Correos de suplantación de identidad (phishing) y software malicioso
- Poner freno a agentes perniciosos

Panel de seguridad

- Volumen de spam
- Compartir archivos externamente
- Aplicaciones de terceros
- Intentos de suplantación de identidad (phishing)

Estado de la seguridad

- Recomendaciones para áreas de riesgo
- Estar al día de las prácticas recomendadas
- Prácticas recomendadas de seguridad
- Aumentar la seguridad de centros escolares en expansión

Controles de administración avanzados

- Reglamentos sobre protección de datos
- Bases reguladoras de las becas
- Restricciones de aplicaciones
- Gestionar dispositivos móviles
- Migrar datos

Índice



Herramientas de enseñanza y aprendizaje

Herramientas incluidas en Teaching and Learning Upgrade y Education Plus

Informes de originalidad

- Detección de plagio
- Transforma la detección de plagio en una oportunidad de aprendizaje

Google Meet

- Videollamadas seguras
- Reforzar la seguridad de las videoconferencias
- Grabar clases
- Grabar reuniones de profesores
- Recuperar clases
- Emisiones en directo de reuniones
- Emisiones en directo de eventos escolares
- Hacer preguntas
- Recopilar comentarios
- Clases en grupos reducidos
- Registro de la asistencia



Herramientas de seguridad y analíticas

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



[Herramienta de investigación](#)



[Panel de seguridad](#)



[Página sobre el estado de la seguridad](#)



[Controles de administración avanzados](#)

Herramienta de investigación

¿Qué es?

Utiliza la herramienta de investigación para identificar y clasificar problemas de seguridad y privacidad en tu dominio, y para tomar medidas al respecto.

Casos prácticos

[Material inadecuado que se comparte](#)

 [Instrucciones paso a paso](#)

[Archivos compartidos accidentalmente](#)

 [Instrucciones paso a paso](#)

[Clasificación de correos](#)

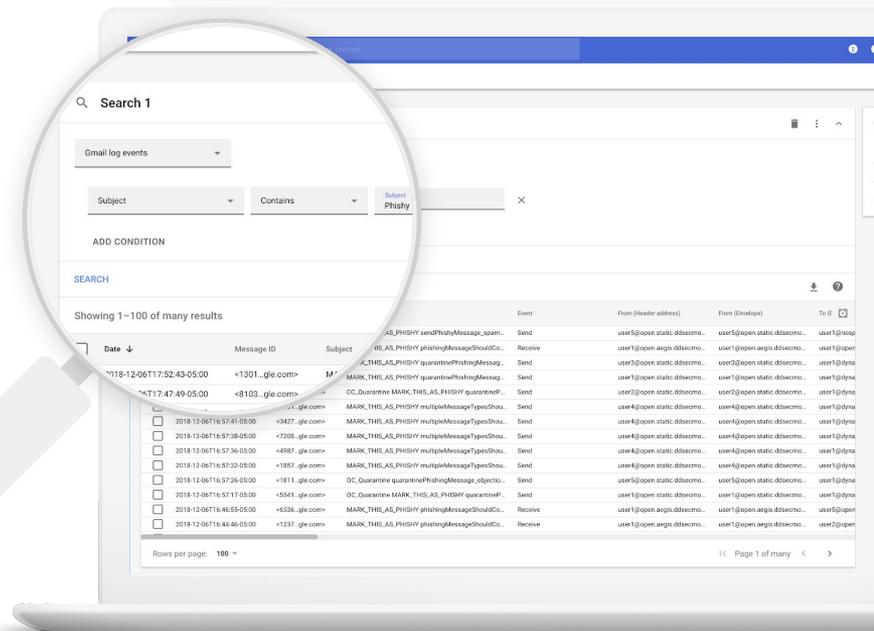
 [Instrucciones paso a paso](#)

[Correos de suplantación de identidad y software malicioso](#)

 [Instrucciones paso a paso](#)

[Poner freno a agentes perniciosos](#)

 [Instrucciones paso a paso](#)





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

[Instrucciones paso a paso](#)

Material inadecuado que se comparte

Los registros de Drive de la herramienta de investigación pueden servirte para encontrar, monitorizar, aislar o eliminar archivos no deseados en tu dominio. Al acceder a los [registros de Drive](#), puedes:

- ✓ Buscar documentos por nombre, actor y propietario, entre otros datos
- ✓ Tomar medidas cambiando los permisos del archivo o eliminándolo
- ✓ Consultar toda la información del registro relacionada con ese documento
 - Fecha de creación
 - A quién pertenece, quién lo ha visto y quién lo ha modificado
 - Fecha en la que se compartió

[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Condiciones de eventos de registro de Google Drive](#)

[Acciones con eventos de registro de Drive](#)

Archivos compartidos accidentalmente

Los registros de Drive de la herramienta de investigación pueden servirte para monitorizar y resolver los problemas relacionados con el sistema de archivos compartidos.

Al acceder a los [registros de Drive](#), puedes:

- ✓ Buscar documentos por nombre, actor y propietario, entre otros datos
- ✓ Consultar toda la información del registro relacionada con ese documento, como quién lo ha visto o cuándo se ha compartido
- ✓ Tomar medidas cambiando los permisos del archivo o inhabilitando las funciones de descarga, impresión y copia

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Condiciones de eventos de registro de Google Drive](#)

[Acciones con eventos de registro de Drive](#)



Se ha compartido accidentalmente un archivo con un grupo que NO debe tener acceso a él. Quiero que esos usuarios dejen de tener acceso".

[Instrucciones paso a paso](#)

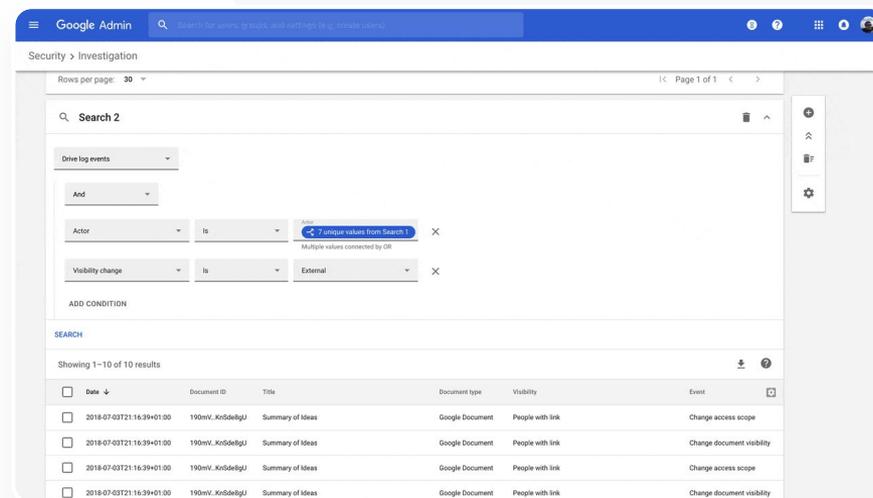
Instrucciones: eventos de registro de Drive

Cómo investigar

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

Cómo tomar medidas

- Selecciona todos los archivos que correspondan en los resultados de búsqueda
- Haz clic en Acciones > Auditar permisos de archivos para que se abra la página Permisos
- Haz clic en Personas para ver quién tiene acceso
- Haz clic en Enlaces para ver o modificar la configuración de uso compartido mediante enlace de los archivos seleccionados
- Haz clic en Cambios pendientes para revisar los cambios antes de guardarlos



<input type="checkbox"/>	Date	Document ID	Title	Document type	Visibility	Event
<input type="checkbox"/>	2018-07-03T21:16:39+01:00	190nv_Krd5delGJ	Summary of Ideas	Google Document	People with link	Change access scope
<input type="checkbox"/>	2018-07-03T21:16:39+01:00	190nv_Krd5delGJ	Summary of Ideas	Google Document	People with link	Change document visibility
<input type="checkbox"/>	2018-07-03T21:16:39+01:00	190nv_Krd5delGJ	Summary of Ideas	Google Document	People with link	Change access scope
<input type="checkbox"/>	2018-07-03T21:16:39+01:00	190nv_Krd5delGJ	Summary of Ideas	Google Document	People with link	Change document visibility

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Condiciones de eventos de registro de Google Drive](#)

[Acciones con eventos de registro de Drive](#)

“

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

[Instrucciones paso a paso](#)

Clasificación de correos

Los registros de Gmail de la herramienta de investigación pueden ayudarte a identificar y tomar medidas con respecto a los correos peligrosos o abusivos dentro de tu dominio.

Al acceder a los registros de Gmail, puedes:

- ✓ Buscar correos por asunto, ID de mensaje, archivo adjunto y remitente, entre otros datos.
- ✓ Ver los detalles del mensaje, como el autor, el destinatario y las veces que se ha abierto y reenviado.
- ✓ Tomar medidas en función de los resultados de búsqueda. Puedes hacer lo siguiente con los mensajes de Gmail: eliminarlos, restaurarlos, marcarlos como spam o suplantación de identidad (phishing), enviarlos a la bandeja de entrada o ponerlos en cuarentena.

[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Condiciones de los registros de Gmail y de los mensajes de Gmail](#)

[Acciones con mensajes de Gmail y eventos de registro de Gmail](#)

[Pasos para poder ver el contenido de un correo](#)



Correos de suplantación de identidad (phishing) y software malicioso

La herramienta de investigación, y los registros de Gmail en particular, pueden ayudarte a identificar y aislar los correos maliciosos que reciban los usuarios de tu dominio.

Al acceder a los registros de Gmail, puedes:



Buscar mensajes de correo por contenido concreto, incluidos los archivos adjuntos



Ver los mensajes y la conversación para determinar si son maliciosos



Ver información sobre correos concretos, como sus destinatarios o las veces que se han abierto



Tomar medidas; por ejemplo, marcar los mensajes como spam o como suplantación de identidad (phishing), enviarlos a una bandeja de entrada concreta, ponerlos en cuarentena o eliminarlos



[Documentación del Centro de Ayuda sobre este asunto](#)

[Condiciones de los registros de Gmail y de los mensajes de Gmail](#)

[Acciones con mensajes de Gmail y eventos de registro de Gmail](#)

[Pasos para poder ver el contenido de un correo](#)



Se ha enviado un correo de suplantación de identidad o software malicioso a los usuarios. Queremos saber si han hecho clic en el enlace del correo o si han descargado el archivo adjunto, ya que esto podría poner en peligro la seguridad de los usuarios o de nuestro dominio".

[Instrucciones paso a paso](#)

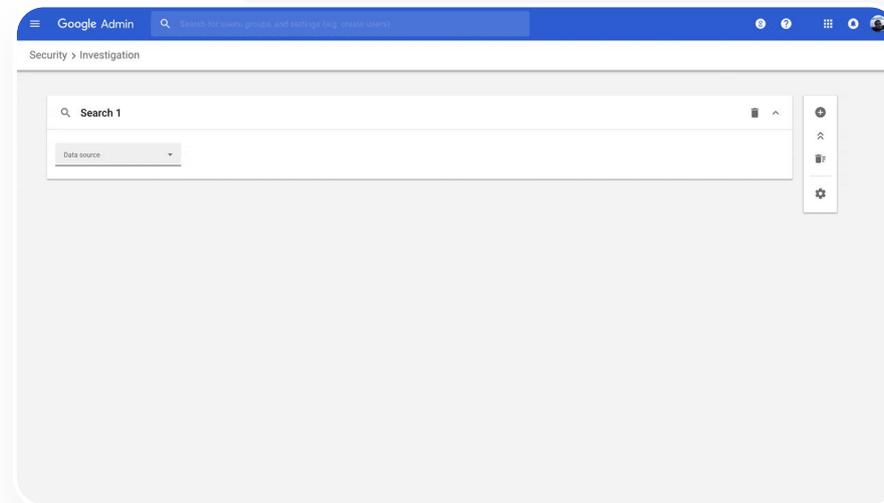
Instrucciones: registros de Gmail

Cómo investigar

- Inicia sesión en la consola de administración
- Haz clic en Seguridad > Herramienta de investigación
- Elige Eventos de registro de Gmail o bien Mensajes de Gmail
- Haz clic en Añadir condición > Buscar

Cómo tomar medidas

- Selecciona los mensajes pertinentes en los resultados de búsqueda
- Haz clic en Acciones
- Selecciona Eliminar mensaje de la bandeja de entrada
- Haz clic en Eliminar de la bandeja de entrada
- Para confirmar la acción, haz clic en Ver en la parte inferior de la página
- En la columna Resultado, puedes ver el estado de la acción



[🔗 Documentación del Centro de Ayuda sobre este asunto](#)
[Condiciones de los registros de Gmail y de los mensajes de Gmail](#)
[Acciones con mensajes de Gmail y eventos de registro de Gmail](#)
[Pasos para poder ver el contenido de un correo](#)

“

Un agente pernicioso se dedica a atacar constantemente a usuarios destacados de mi dominio mientras yo trato inútilmente de detenerlo. ¿Cómo puedo acabar con esta situación?"

[Instrucciones paso a paso](#)

Poner freno a agentes perniciosos

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

- ✓ Identificar e investigar los intentos de acceder sin autorización a cuentas de usuario de tu organización
- ✓ Supervisar los métodos de verificación en dos pasos que utilizan los usuarios de tu organización
- ✓ Obtener más información sobre los intentos fallidos de inicio de sesión de los usuarios de tu organización
- ✓ [Crear reglas de actividad con la herramienta de investigación](#); bloquear automáticamente los mensajes y otras actividades maliciosas de personas concretas
- ✓ Proteger a usuarios destacados con el [Programa de Protección Avanzada](#)
- ✓ Restaurar o suspender usuarios

[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Buscar e investigar eventos de registro de usuarios](#)

[Crear reglas de actividad con la herramienta de investigación](#)

Instrucciones: eventos de registro de usuarios

Cómo investigar

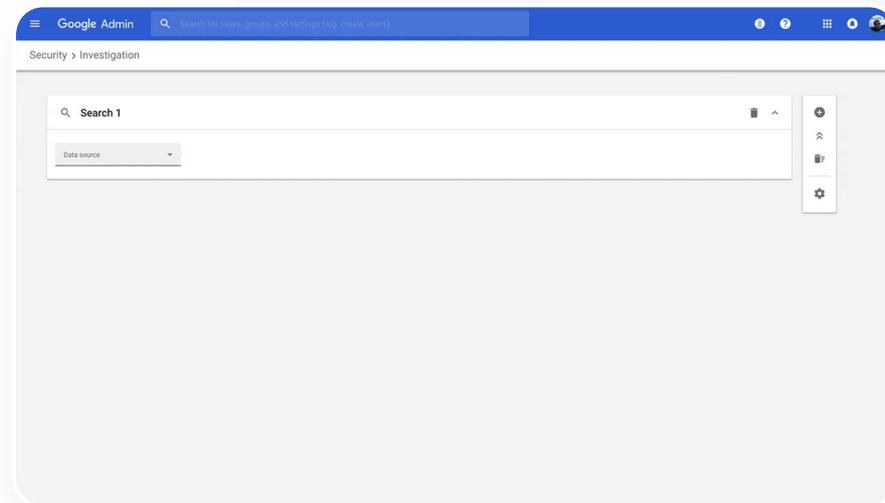
- Inicia sesión en la consola de administración
- Haz clic en Seguridad > Herramienta de investigación
- Selecciona Eventos de registro de usuarios
- Haz clic en Añadir condición > Buscar

Cómo restaurar o suspender usuarios

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

Cómo ver los detalles de un usuario concreto

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



[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Buscar e investigar eventos de registro de usuarios](#)

🔒 Panel de seguridad

¿Qué es?

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

Casos prácticos

[Volumen de spam](#)

🔗 [Instrucciones paso a paso](#)

[Compartir archivos externamente](#)

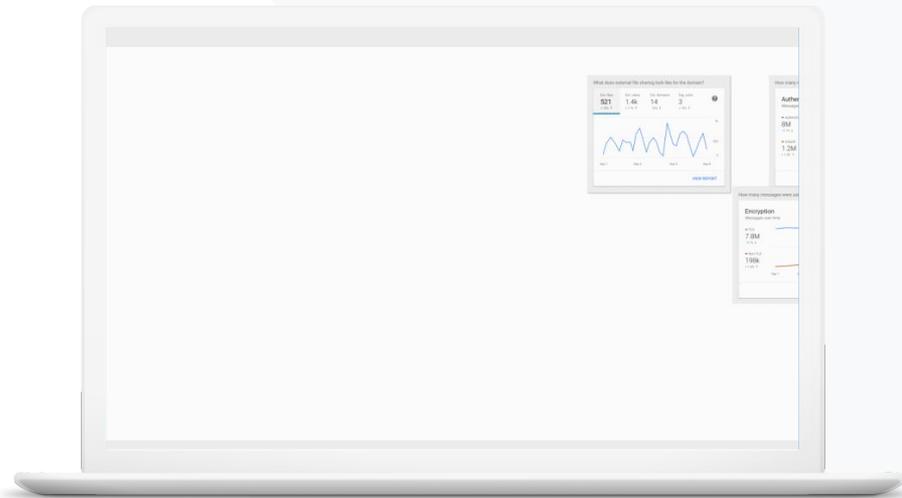
🔗 [Instrucciones paso a paso](#)

[Aplicaciones de terceros](#)

🔗 [Instrucciones paso a paso](#)

[Intentos de suplantación de identidad \(phishing\)](#)

🔗 [Instrucciones paso a paso](#)





Volumen de spam

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

- ✓ Spam
- ✓ Archivos adjuntos sospechosos
- ✓ Suplantación de identidad (phishing)
- ✓ Otros elementos
- ✓ Software malicioso

[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Acerca del panel de seguridad](#)



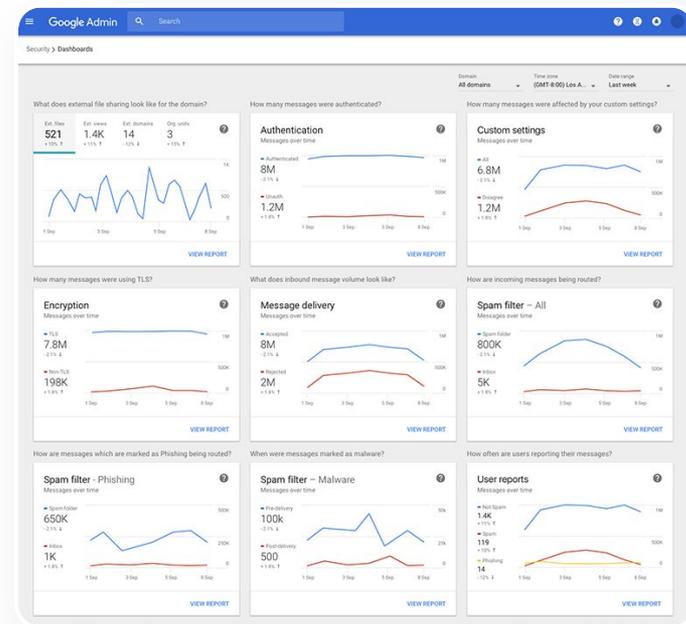
Quiero controlar el volumen excesivo de correos innecesarios y reducir las amenazas de seguridad en mi centro educativo”.

[Instrucciones paso a paso](#)

Instrucciones: información general sobre el panel de control

Cómo ver el panel de control

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



[Documentación del Centro de Ayuda sobre este asunto](#)
[Acercas del panel de seguridad](#)



Compartir archivos externamente

Con el informe "Visibilidad de archivos" del panel de seguridad, podrás consultar métricas del sistema de archivos compartidos externamente en tu dominio, como las siguientes:

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

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Introducción a la página sobre el estado de la seguridad](#)



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

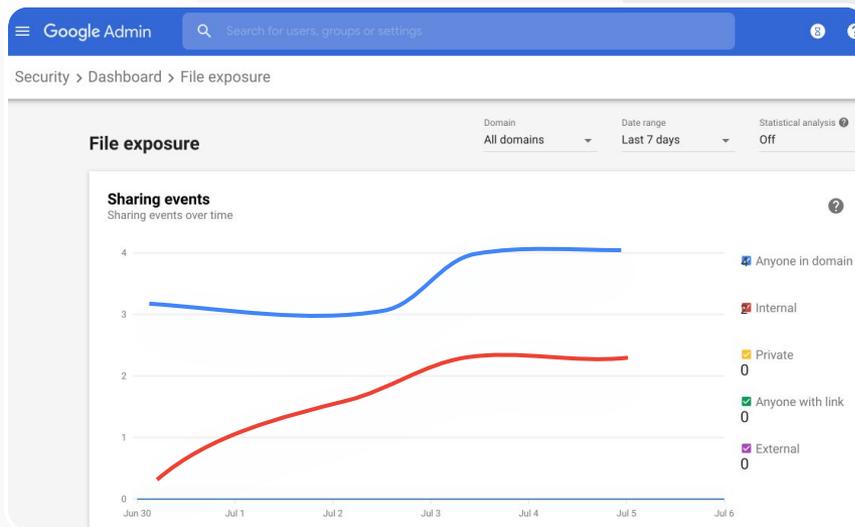
[Instrucciones paso a paso](#)



Instrucciones: informe "Visibilidad de archivos"

Cómo consultar el informe

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



[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Acerca del panel de seguridad](#)
[Informe "Visibilidad de archivos"](#)



Aplicaciones de terceros

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

- ✓ OAuth permite que servicios de terceros accedan a la información de la cuenta de un usuario sin exponer su contraseña. Puedes limitar qué aplicaciones de terceros tienen acceso.
- ✓ En el panel de actividad de Autenticación OAuth, puedes monitorizar la actividad de autenticación por aplicación, permiso y usuario. También te permite actualizar los permisos de autenticación.

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Informe "Actividad de autenticación OAuth"](#)



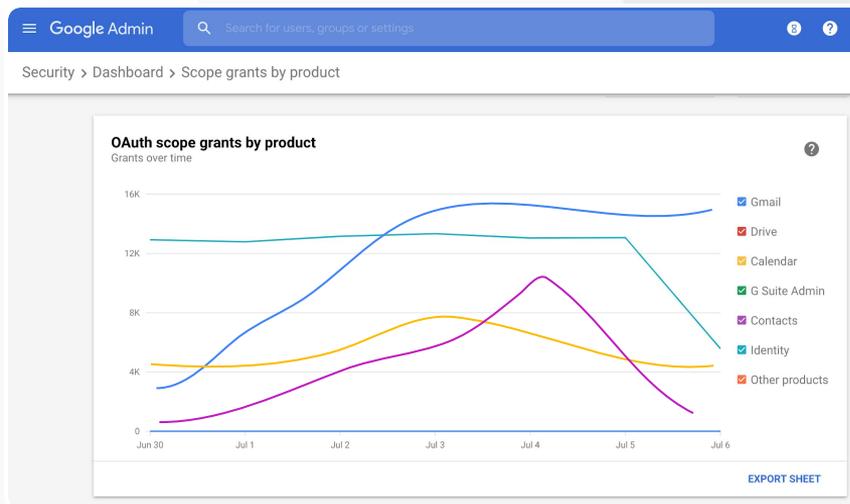
Quiero ver qué aplicaciones de terceros tienen acceso a los datos de mi dominio".

[Instrucciones paso a paso](#)

Instrucciones: informe "Actividad de autenticación OAuth"

Cómo consultar el informe

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



[Documentación del Centro de Ayuda sobre este asunto](#)
[Informe "Actividad de autenticación OAuth"](#)



“

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

[Instrucciones paso a paso](#)

Intentos de suplantación de identidad (phishing)

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

- ✓ En el informe "Clasificaciones de los usuarios", puedes consultar cuántos mensajes han marcado tus usuarios como spam, no spam o suplantación de identidad durante un periodo determinado
- ✓ Puedes personalizar el gráfico para que solo se muestren detalles de determinados tipos de mensajes; por ejemplo, mensajes que se han enviado interna o externamente, en un periodo concreto, etc.



[Documentación del Centro de Ayuda sobre este asunto](#)

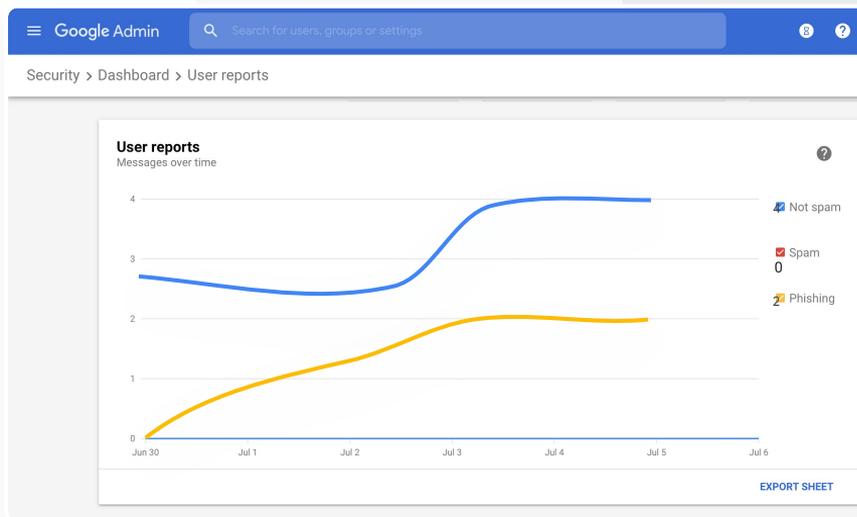
[Cómo marcan los usuarios sus correos electrónicos](#)

[Clasificaciones de los usuarios](#)

Instrucciones: panel Clasificaciones de los usuarios

Cómo consultar el informe

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



[Documentación del Centro de Ayuda sobre este asunto](#)

[Acerca del panel de seguridad informe "Visibilidad de archivos"](#)

Estado de la seguridad

¿Qué es?

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

Casos prácticos

[Recomendaciones para áreas de riesgo](#)



[Instrucciones paso a paso](#)

[Estar al día de las prácticas recomendadas](#)



[Instrucciones paso a paso](#)

[Prácticas recomendadas de seguridad](#)

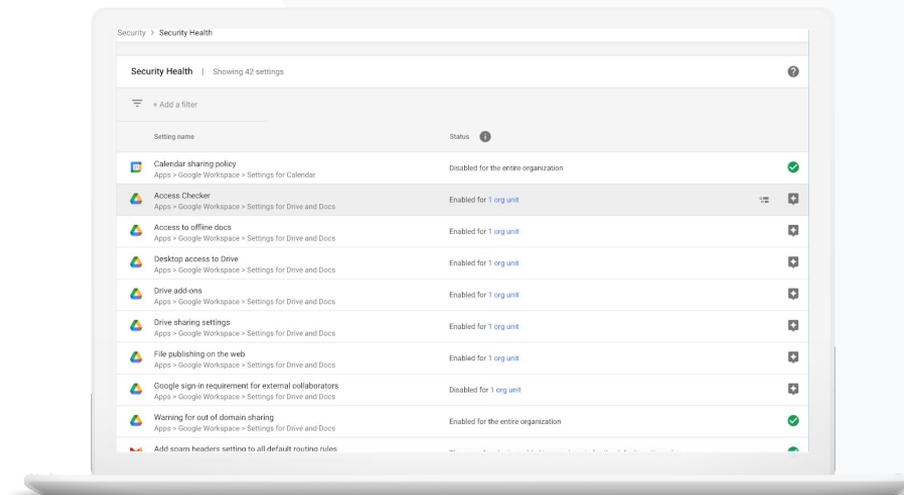


[Instrucciones paso a paso](#)

[Aumentar la seguridad de centros escolares en expansión](#)



[Instrucciones paso a paso](#)





Recomendaciones para áreas de riesgo

La página Estado de la seguridad te permite consultar tu configuración de seguridad y los cambios recomendados. En esta página, puedes hacer lo siguiente:

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

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Introducción a la página sobre el estado de la seguridad](#)



Quiero consultar una vista general resumida de la configuración de seguridad de mi dominio y recibir recomendaciones útiles para proteger áreas de posible riesgo".

[Instrucciones paso a paso](#)



Estar al día de las prácticas recomendadas

La página Estado de la seguridad te permite consultar tu configuración de seguridad y los cambios recomendados. En esta página, puedes obtener lo siguiente:

- ✓ Recomendaciones para áreas de posible riesgo de tu dominio
- ✓ Recomendaciones sobre la configuración óptima para aumentar la eficacia de las medidas de seguridad
- ✓ Información adicional y artículos de ayuda

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Introducción a la página sobre el estado de la seguridad](#)



Yo me encargo de gestionar nuestro dominio, pero hay cosas que se me escapan. Necesito que me ayudéis a mantenerlo todo protegido con la configuración adecuada".

[Instrucciones paso a paso](#)



Prácticas recomendadas de seguridad

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

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

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Introducción a la página sobre el estado de la seguridad](#)



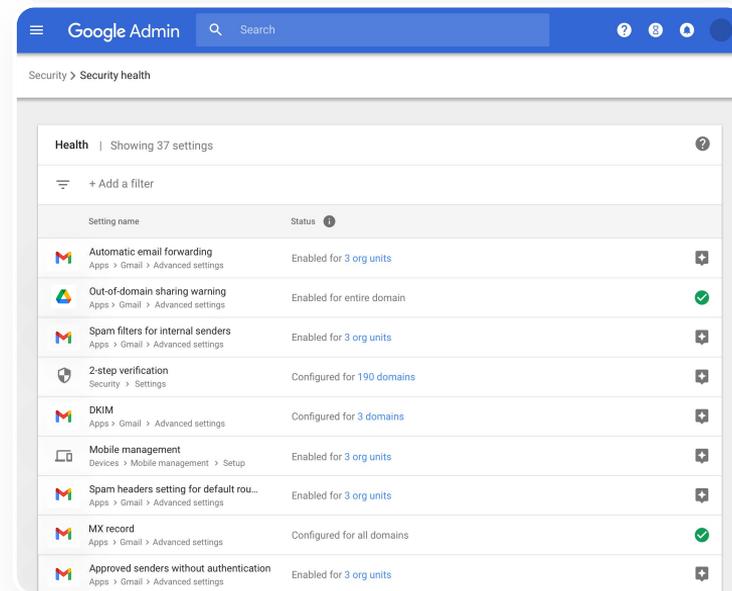
Decidme dónde puedo encontrar prácticas recomendadas o sugerencias sobre cómo configurar políticas de seguridad".

[Instrucciones paso a paso](#)

Instrucciones: recomendaciones de seguridad

Cómo ver las recomendaciones

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



 [Documentación del Centro de Ayuda sobre este asunto](#)
[Introducción a la página sobre el estado de la seguridad](#)



“

Quiero que mi centro educativo esté lo más seguro posible a medida que aumenta el número de profesores y alumnos”.

[Instrucciones paso a paso](#)

Aumentar la seguridad de centros escolares en expansión

Los administradores de TI deben seguir estas [prácticas recomendadas en materia de seguridad](#) para mejorar la seguridad y la privacidad de los datos de su empresa. Para implementar cada una de estas prácticas recomendadas, puedes configurar al menos un ajuste de la consola de administración de Google.

- ✓ Recomendaciones para prevenir y solucionar problemas de vulneración de cuentas
- ✓ Pasos para limitar el uso compartido y la colaboración con usuarios que no pertenezcan a tu dominio
- ✓ Funciones para revisar el acceso de terceros a los servicios principales

[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Lista de comprobación de seguridad para organizaciones medianas y grandes](#)



Instrucciones: lista de comprobación de seguridad

Para proteger a tu organización, Google habilita de manera predeterminada muchos de los ajustes recomendados incluidos en esta lista de comprobación como prácticas recomendadas en materia de seguridad. Te recomendamos que prestes especial atención a los que aparecen destacados abajo.

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

Security best practices

To help protect your business, Google turns on many of the settings recommended in this checklist as security best practices by default.

[Administrator](#) | [Accounts](#) | [Apps](#) | [Calendar](#) | [Chrome Browser and Chrome OS](#) | [Classic Hangouts](#)
[Contacts](#) | [Drive](#) | [Gmail](#) | [Google+](#) | [Groups](#) | [Mobile](#) | [Sites](#) | [Vault](#)

Administrator 

Protect admin accounts

- Require 2-Step Verification for admin accounts**
Because super admins control access to all business and employee data in the organization, it's especially important for their accounts to be protected by an additional authentication factor.
[Protect your business with 2-Step Verification](#) | [Deploy 2-Step verification](#)
- Use security keys for 2-Step Verification**
Security keys help to resist phishing threats and are the most phishing-resistant form of 2-Step Verification.
[Protect your business with 2-Step Verification](#)

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Supervisar el estado de la configuración de seguridad](#)

Controles de administración avanzados

¿Qué es?

Monitorizan y controlan qué usuarios y dispositivos tienen acceso a tu dominio y a tus datos.

Casos prácticos

[Reglamentos sobre protección de datos](#)



[Instrucciones paso a paso](#)

[Bases reguladoras de las becas](#)



[Instrucciones paso a paso](#)

[Restricciones de aplicaciones](#)



[Instrucciones paso a paso](#)

[Gestionar dispositivos móviles](#)

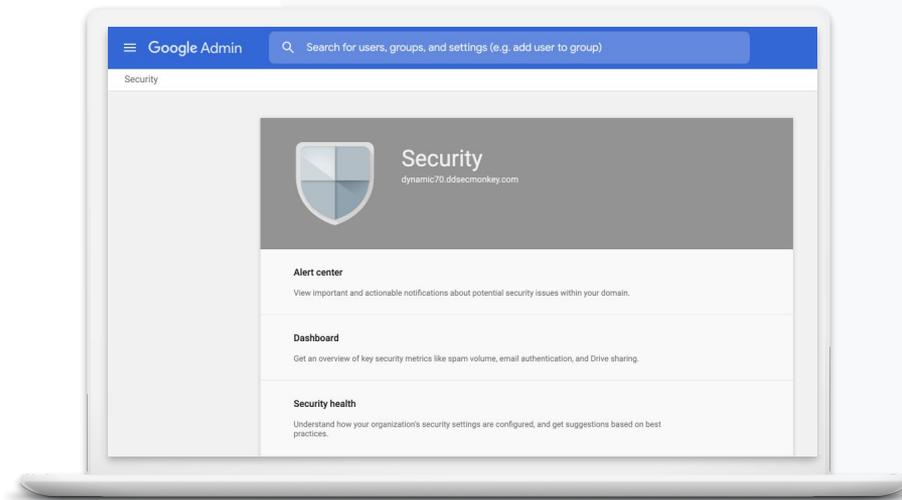


[Instrucciones paso a paso](#)

[Migrar datos](#)



[Instrucciones paso a paso](#)





Reglamentos sobre protección de datos

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

- ✓ Puedes elegir una región de datos para algunos de tus usuarios, o regiones de datos diferentes para departamentos o equipos específicos
- ✓ Coloca a usuarios en una unidad organizativa para aplicar el ajuste por departamento o en un grupo de configuración para aplicárselo a usuarios concretos, ya sean del mismo departamento o de otros distintos
- ✓ A los usuarios que no disponen de una licencia Education Standard o Education Plus no se les aplican políticas de la región de datos

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Elegir la ubicación geográfica de los datos](#)



Los datos de alumnos, profesores y demás personal deben permanecer en Estados Unidos de acuerdo con la legislación vigente."

[Instrucciones paso a paso](#)



Bases reguladoras de las becas

Como administrador, puedes definir una política de la región de datos para decidir la ubicación geográfica donde se van a almacenar las investigaciones de los profesores: Estados Unidos o Europa.



Las políticas de la región de datos cubren los datos primarios en reposo (incluidas las copias de seguridad) de la mayoría de los servicios principales de Google Workspace for Education. Consulta la [lista de servicios](#)



Valora las repercusiones antes de definir una política de la región de datos, ya que si los datos de los usuarios se almacenan fuera de su región, podrían experimentar una mayor latencia en ciertos casos



Documentación del Centro de Ayuda sobre este asunto

[Elegir la ubicación geográfica de los datos](#)



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

[Instrucciones paso a paso](#)



Instrucciones: regiones de datos*

Cómo definir regiones de datos

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

* Solo las instituciones que tengan las licencias Education Standard o Education Plus pueden optar a almacenar sus datos en regiones concretas con la función de regiones de datos.

[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Elegir la ubicación geográfica de los datos](#)



Restricciones de aplicaciones

Con el **acceso contextual***, puedes controlar el acceso a aplicaciones mediante políticas detalladas que se basen en determinados atributos, como la identidad de los usuarios, su ubicación, la seguridad de los dispositivos y la dirección IP. Incluso puedes restringir el acceso a aplicaciones que están fuera de la red.

- ✓ Puedes aplicar políticas de acceso contextual a los servicios principales de Google Workspace for Education
- ✓ Por ejemplo, si un usuario inicia sesión en un servicio principal de Google Workspace en un centro educativo y luego se va a una cafetería, se vuelve a comprobar la política de acceso contextual de ese servicio cuando el usuario cambia de ubicación

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Introducción al acceso contextual](#)

[Asignar niveles de acceso contextual a las aplicaciones](#)



Quiero limitar el acceso a aplicaciones específicas cuando los usuarios estén usando la red".

[Instrucciones paso a paso](#)

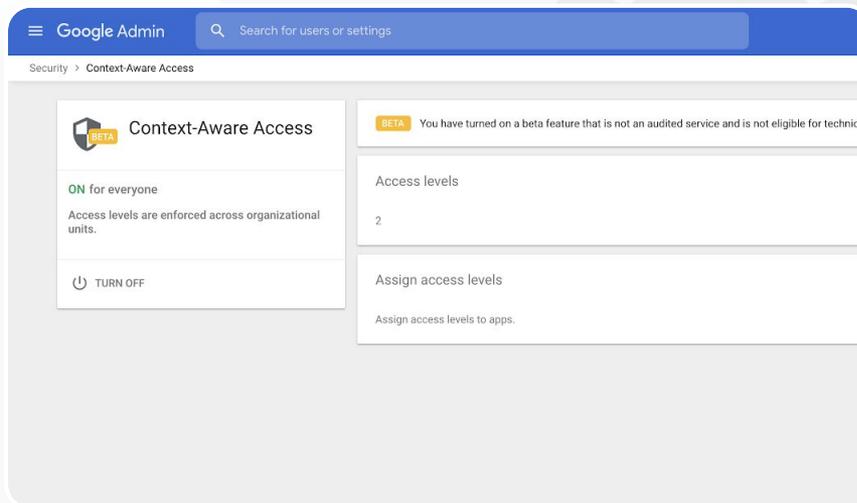
* Solo las instituciones que tengan las licencias Education Standard o Education Plus pueden optar a usar políticas de acceso contextual.



Instrucciones: acceso contextual

Cómo utilizar el acceso contextual

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



 [Documentación del Centro de Ayuda sobre este asunto](#)

[Introducción al acceso contextual](#)

[Asignar niveles de acceso contextual a las aplicaciones](#)



“

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

[Instrucciones paso a paso](#)

Gestionar dispositivos móviles

La **gestión avanzada de dispositivos móviles** puede darte un mayor control sobre los datos de tu organización en dispositivos móviles. Puedes restringir funciones de los dispositivos móviles, requerir el cifrado de dispositivos, gestionar aplicaciones en dispositivos Android, iPhones e iPads, e incluso borrar datos de dispositivos.

- ✓ Puedes aprobar, bloquear, desbloquear y eliminar dispositivos desde la consola de administración.
- ✓ Si alguien pierde su dispositivo o deja el centro educativo, puedes borrar su cuenta de usuario, su perfil e incluso todos los datos asociados a su dispositivo gestionado. No obstante, se podrá seguir accediendo a los datos desde un ordenador o un navegador web.

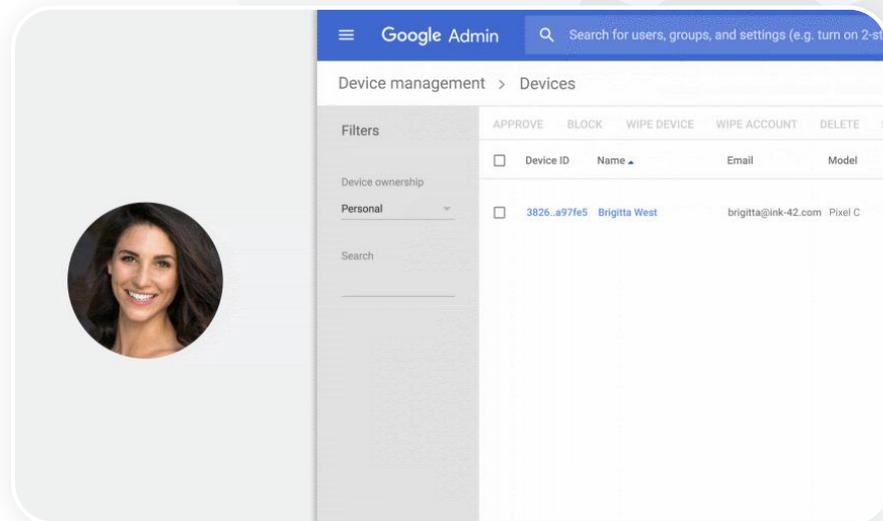
 [Documentación del Centro de Ayuda sobre este asunto](#)
[Configurar la gestión avanzada de dispositivos móviles](#)
[Aprobar, bloquear, desbloquear o eliminar un dispositivo](#)
[Borrar datos de un dispositivo](#)



Instrucciones: activar la gestión avanzada de dispositivos móviles

Cómo activarla

- Inicia sesión en la consola de administración.
- Ve a **Consola de administración > Dispositivos**.
- En la parte izquierda, haz clic en **Configuración > Configuración universal**.
- Haz clic en **General > Gestión de dispositivos móviles**.
- Si quieres aplicar el ajuste a todos los usuarios, deja seleccionada la unidad organizativa superior. De lo contrario, selecciona una unidad organizativa secundaria.
- Selecciona **Avanzado**.
- Haz clic en **Guardar**.



[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Configurar la gestión avanzada de dispositivos móviles](#)
[Aprobar, bloquear, desbloquear o eliminar un dispositivo](#)
[Borrar datos de un dispositivo](#)



Controles de administración avanzados



Herramientas de seguridad y analíticas

Migrar datos

Usa las guías de migración para migrar los datos de toda tu organización (como correos, calendarios, contactos, carpetas, archivos y permisos) a Google Workspace.

Datos de < 1000 usuarios

- ✓ Consulta la matriz de productos para hacerte una idea de qué solución se adapta mejor a las necesidades de tu centro.

[Más información](#)

Datos de más de 1000 usuarios

- ✓ Con Google Workspace Migrate podrás migrar un gran volumen de datos de forma eficaz.

[Más información](#)

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Migrar los datos de tu organización a Google Workspace](#)

[Matriz de productos de migración de Google Workspace](#)

[Información sobre Google Workspace Migrate](#)

[Instalar y configurar Google Workspace Migrate](#)



Hemos empezado a usar Google Workspace y necesitamos migrar todos nuestros datos a nuestro nuevo entorno de Google."

[Instrucciones paso a paso](#)



Instrucciones: Google Workspace Migrate

Antes de empezar

Regístrate en el programa [beta](#) y confirma que cumples los [requisitos del sistema](#).

Procedimiento

1. Configurar la consola de Google Cloud

[Habilitar APIs](#)

[Crear el ID de cliente web de OAuth](#)

[Crear una cuenta de servicio de Google Workspace](#)

2. Configurar la consola de administración

[Configurar roles de administrador](#)

[Autorizar tu ID de cliente](#)

3. Descargar e instalar

[Descargar los instaladores](#)

[Instalar las bases de datos](#)

[Instalar y configurar la plataforma](#)

[Instalar los servidores de nodo](#)

[\(Opcional\) Configurar el servidor de nodo para que use TLS](#)

4. Configurar el producto de migración

[Configurar la clave de encriptado](#)

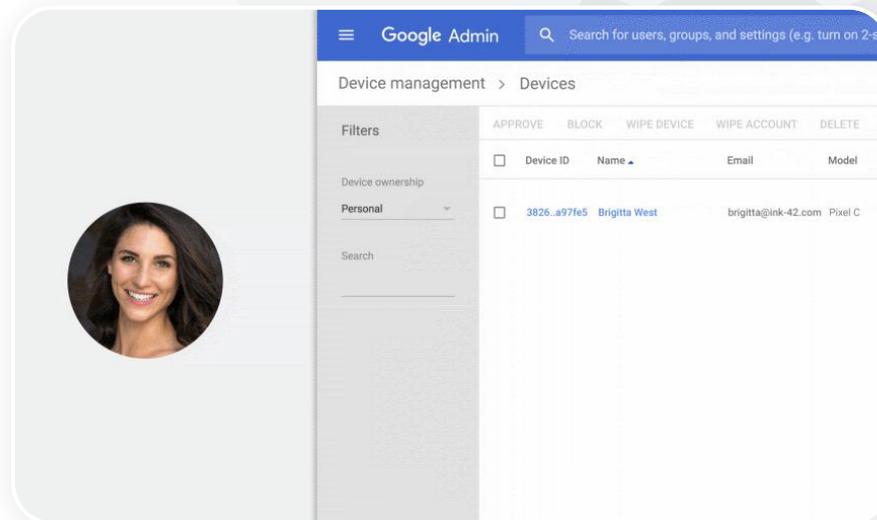
[Configurar ajustes de bases de datos](#)

[Configurar la dirección de retrollamada](#)

[Añadir los servidores de nodo](#)

[Crear un proyecto](#)

¿Necesitas ayuda? Ponte en contacto con un [Google Cloud Partner](#).



Documentación del Centro de Ayuda sobre este asunto

[Información sobre Google Workspace Migrate](#)

[Instalar y configurar Google Workspace Migrate](#)

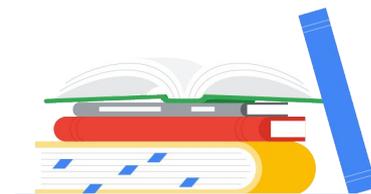
[Migrar los datos de tu organización a Google Workspace](#)

[Matriz de productos de migración de Google Workspace](#)



Herramientas de enseñanza y aprendizaje

Proporciona más herramientas y recursos a los docentes en tu entorno de aprendizaje digital a través de funciones avanzadas de comunicación mediante vídeo, experiencias de clase enriquecidas y herramientas para fomentar la integridad académica.



[Informes de originalidad](#)



[Google Meet](#)

Informes de originalidad

¿Qué es?

Tanto profesores como alumnos pueden comprobar si hay plagios en los trabajos. Esta herramienta utiliza la Búsqueda de Google para comparar el trabajo de un alumno con miles de millones de páginas web y millones de libros. Los informes de originalidad incluyen enlaces a las páginas web detectadas y marcan el texto que no se ha citado.

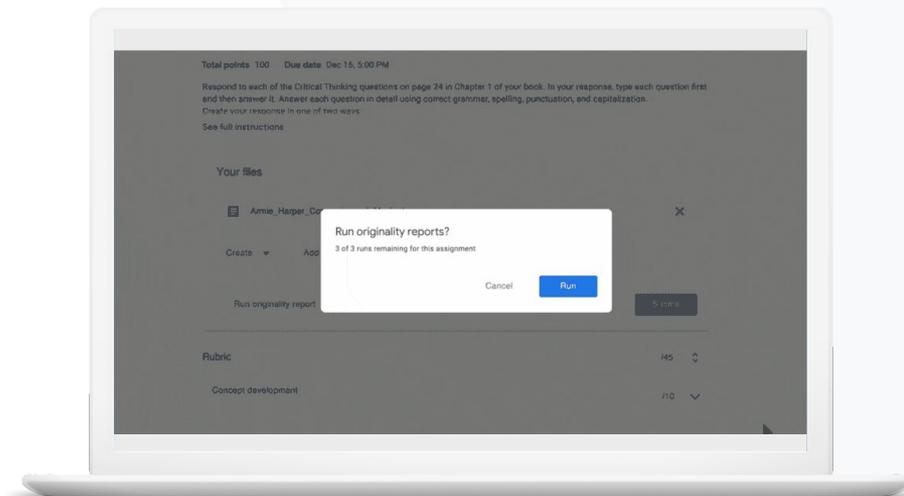
Casos prácticos

Detección de plagio

[🔗 Instrucciones paso a paso](#)

Transforma la detección de plagio en una oportunidad de aprendizaje

[🔗 Instrucciones paso a paso](#)





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

[Instrucciones paso a paso](#)

Detección de plagio

Los profesores pueden comprobar la autenticidad de los trabajos de sus alumnos mediante los **informes de originalidad**. Esta herramienta utiliza la Búsqueda de Google para comparar el trabajo de un alumno con miles de millones de páginas web y millones de libros originales.

- ✓ Los docentes que usen Teaching and Learning Upgrade o Education Plus tienen acceso ilimitado a los informes de originalidad
- ✓ Por el momento, los informes de originalidad solo están disponibles con:
 - Cuentas de Google configuradas en inglés
 - Trabajos realizados en Documentos
 - Cuentas de Google for Education

[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Activar los informes de originalidad](#)



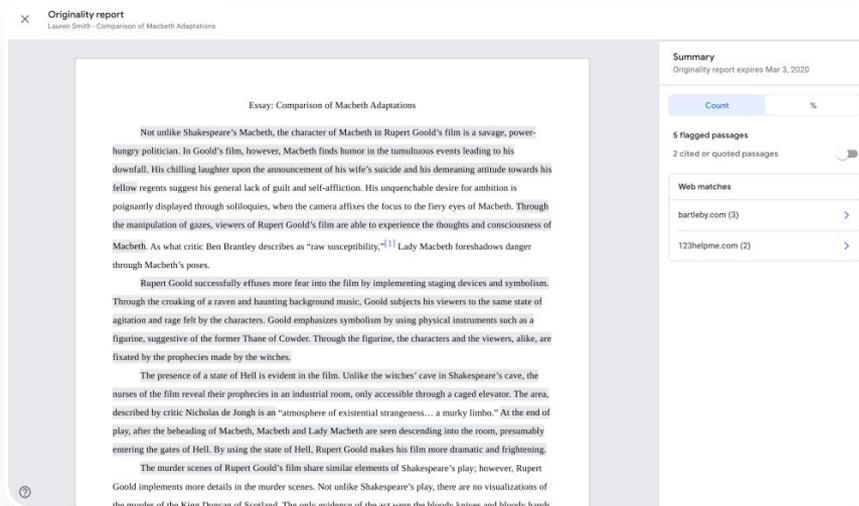
Instrucciones: comprobación del profesor tras la entrega

Cómo activar los informes de originalidad en una tarea

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

Cómo generar un informe de originalidad del trabajo de un alumno

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



Originality report
Lorah Smith - Comparison of Macbeth Adaptations

Essay: Comparison of Macbeth Adaptations

Not unlike Shakespeare's Macbeth, the character of Macbeth in Rupert Goold's film is a savage, power-hungry politician. In Goold's film, however, Macbeth finds humor in the tumultuous events leading to his downfall. His chilling laughter upon the announcement of his wife's suicide and his demeaning attitude towards his fellow regents suggest his general lack of guilt and self-affliction. His unquenchable desire for ambition is poignantly displayed through soliloquies, when the camera affixes the focus to the fiery eyes of Macbeth. Through the manipulation of gazes, viewers of Rupert Goold's film are able to experience the thoughts and consciousness of Macbeth. As what critic Ben Brantley describes as "raw susceptibility,"¹¹ Lady Macbeth foreshadows danger through Macbeth's poses.

Rupert Goold successfully effuses more fear into the film by implementing staging devices and symbolism. Through the croaking of a raven and haunting background music, Goold subjects his viewers to the same state of agitation and rage felt by the characters. Goold emphasizes symbolism by using physical instruments such as a figurine, suggestive of the former Thane of Cowder. Through the figurine, the characters and the viewers, alike, are fixated by the prophecies made by the witches.

The presence of a state of Hell is evident in the film. Unlike the witches' cave in Shakespeare's play, the nurses of the film reveal their prophecies in an industrial room, only accessible through a caged elevator. The area, described by critic Nicholas de Jongh is an "atmosphere of existential strangeness... a murky limbo." At the end of play, after the beheading of Macbeth, Macbeth and Lady Macbeth are seen descending into the room, presumably entering the gates of Hell. By using the state of Hell, Rupert Goold makes his film more dramatic and frightening.

The murder scenes of Rupert Goold's film share similar elements of Shakespeare's play; however, Rupert Goold implements more details in the murder scenes. Not unlike Shakespeare's play, there are no visualizations of the murder of the King Duncan in Scotland. The only evidence of the act were the bloody knives and bloody hands

Summary
Originality report expires Mar 3, 2020

Count %

5 flagged passages
2 cited or quoted passages

Web matches

bartleby.com (3)	>
123helpme.com (2)	>

[🔗 Documentación del Centro de Ayuda sobre este asunto](#)
[Activar los informes de originalidad](#)



Quiero que mis alumnos puedan comprobar si hay plagios en sus propios trabajos y que la detección de trampas se convierta en una oportunidad de aprendizaje".

[Instrucciones paso a paso](#)

Transforma la detección de plagio en una oportunidad de aprendizaje

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

- ✓ Tanto con Teaching and Learning Upgrade como con Education Plus, los docentes pueden generar todos los informes de originalidad que quieran. Con Education Fundamentals, solo se puede usar esta función cinco veces por clase.
- ✓ Después de entregar un trabajo, Classroom genera automáticamente un informe que solo el profesor puede ver. Si un alumno anula la entrega de una tarea y la vuelve a enviar, Classroom generará otro informe de originalidad.

[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Generar un informe de originalidad sobre un trabajo](#)

Instrucciones: comprobación del alumno antes de la entrega

Cómo pueden los alumnos generar informes de originalidad

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

Essay: Comparison of Macbeth adaptations

Not unlike Shakespeare's Macbeth, the character of Macbeth in Rupert Goold's film is a savage, power-hungry politician. In Goold's film, however, Macbeth first hovers in the limbo of a man torn between his ambition and his conscience. His chilling laughter upon announcement of his wife's suicide and his derisive attitude towards his fellow rebels suggest his general lack of guilt and self-affliction. His unrepentant desire for ambition is poignantly displayed through soliloquies, when the camera affixes the focus to the fiery eyes of Macbeth. Through the manipulation of gases, viewers of Rupert Goold's film are able to experience the thoughts and consciousness of Macbeth. As what critic Ben Brantley describes as "raw susceptibility," Lady Macbeth foreshadows danger through Macbeth's poses.

Rupert Goold successfully effuses more fear into the film by implementing staging devices and symbolism. Through the croaking of a raven and haunting background music, Goold subjects his viewers to the same state of agitation and rage felt by the characters. Goold emphasizes symbolism by using physical instruments such as a figurine, suggestive of the former Thane of Cowdrie. Through the figurine, the characters and the viewers, alike, are fixated by the prophecies made by the witches.

The presence of a state of Hell is evident in the film. Unlike the witches' cave in Shakespeare's play, the nurses of the film reveal their prophecies in an industrial room, only accessible through a caged elevator. The area, described by critic Nicholas de Jongh as an "atmosphere of existential strangeness... a murky limbo." At the end of play, after the beheading of Macbeth, Macbeth and Lady Macbeth are seen descending into the room, presumably entering the gates of Hell. By using the state of Hell, Rupert Goold makes his film more dramatic and frightening.

The murder scenes of Rupert Goold's film share similar elements of Shakespeare's play; however, Rupert Goold implements more details in the murder scenes. Not unlike Shakespeare's play, there are no visualizations of the murder of the King Duncan of Scotland. The only evidence of the act were the bloody knives and bloody hands of Macbeth used in the execution. Unlike Shakespeare's play, the murder of Banquo occurs in a public setting. By having the execution of Banquo on a train, Goold stresses the power and boldness of Macbeth.

Through his film, Goold introduces an element of absurdity to several scenes. Before the murder of Banquo, Rupert Goold

Web matches > sparksnotes.com ✕

STUDENT'S PASSAGE

Many of Shakespeare's plays were published in editions of **varying quality and accuracy in his lifetime. However, in 1623, two fellow actors and friends of Shakespeare's**, John Heminges and Henry Condell, published a more definitive text

[Comment](#)

TOP MATCH

Of my favorite plays there is inconsistency, illustrating **varying quality and accuracy in his lifetime. However, in 1623, two fellow actors and friends of Shakespeare's**, developed a new way to translate and preserve the content language

SparksNotes - Macbeth Act III: The Return of Macb...
<http://sparksnotes.macbethingstoreadthataveryimportant...>

[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Generar un informe de originalidad sobre un trabajo](#)

Google Meet

¿Qué es?

Entre las funciones avanzadas de Google Meet se incluyen las emisiones en directo, los grupos de trabajo, las grabaciones de reuniones guardadas en Drive, los informes de asistencia y las reuniones con hasta 250 participantes.

Casos prácticos

[Videollamadas seguras](#)  [Instrucciones paso a paso](#)

[Reforzar la seguridad de las videoconferencias](#)  [Instrucciones paso a paso](#)

[Grabar clases](#)  [Instrucciones paso a paso](#)

[Grabar reuniones de profesores](#)  [Instrucciones paso a paso](#)

[Recuperar clases](#)  [Instrucciones paso a paso](#)

[Emisiones en directo de reuniones](#)  [Instrucciones paso a paso](#)

[Emisión en directo de eventos escolares](#)  [Instrucciones paso a paso](#)

[Hacer preguntas](#)  [Instrucciones paso a paso](#)

[Recopilar comentarios](#)  [Instrucciones paso a paso](#)

[Grupos pequeños de alumnos](#)  [Instrucciones paso a paso](#)

[Registro de la asistencia](#)  [Instrucciones paso a paso](#)

Videollamadas seguras

Con Google Meet, los centros educativos pueden aprovechar la infraestructura segura, la protección integrada y la red global que utiliza Google para proteger la información y la privacidad de los usuarios. Google Meet cuenta con las siguientes medidas de seguridad:

- ✓ **Privacidad y cumplimiento:** se ajusta a estándares educativos estrictos en materia de seguridad para proteger mejor los datos de los alumnos y de los centros educativos
- ✓ **Cifrado:** se cifran todos los datos que comparten los clientes con Google
- ✓ **Medidas contra el uso inadecuado:** puedes proporcionar a los moderadores control de asistencia para asegurarte de que solo accedan los usuarios adecuados
- ✓ **Implementación, acceso y controles seguros:** se toman multitud de precauciones para que las reuniones sean privadas y seguras
- ✓ **Respuesta a incidentes:** esta medida forma parte del programa general de seguridad y privacidad de Google, y es clave para cumplir con las normativas globales sobre privacidad
- ✓ **Fiabilidad:** cuenta con una infraestructura multicapa nativa de la nube que está diseñada para ser escalable y que puede responder a los picos de uso
- ✓ **Control de asistencia:** incluye mejoras para gestionar solicitudes de asistencia por lotes y bloquearlas si se cumplen determinados criterios
- ✓ **Controles de bloqueo:** los moderadores pueden controlar quién puede chatear, presentar o hablar durante una reunión virtual

[Instrucciones paso a paso](#)



¿Qué nivel de seguridad ofrece Google Meet realmente?"



¿Qué puedo hacer para que las videoconferencias de mi centro educativo sean aún más seguras?"

[Instrucciones paso a paso](#)

Reforzar la seguridad de las videoconferencias

Tanto Teaching and Learning Upgrade como Education Plus incluyen otras medidas contra el uso inadecuado, como la aprobación obligatoria en el caso de los participantes externos, controles de moderación de reuniones mejorados y **reuniones con alias** para evitar que se reutilicen reuniones ya finalizadas. Una vez que el último participante abandone una reunión, ninguno podrá volver a unirse. Los alumnos solo podrán acceder de nuevo a una reunión con alias cuando un profesor la reinicie.

- ✓ En las **reuniones con alias**, una vez que el último participante se marche, ninguno podrá volver a unirse y el código de reunión de 10 dígitos dejará de funcionar.
- ✓ Los alumnos no pueden volver a acceder a una reunión con alias hasta que un profesor la reinicia
- ✓ Los profesores pueden finalizar la reunión para todos los participantes; de ese modo, nadie podrá quedarse una vez que el profesor se marche

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Seguridad y privacidad en Google Meet para centros educativos](#)

[Iniciar una videollamada con Google Meet](#)

Instrucciones: reuniones con alias

Cómo crear una reunión con alias

- Utiliza un enlace corto, como [g.co/meet/\[ALIAS\]](https://g.co/meet/[ALIAS])
- Ve a meet.google.com o a la aplicación móvil Google Meet e introduce un alias de reunión en el campo **Iniciar o unirme a una reunión**

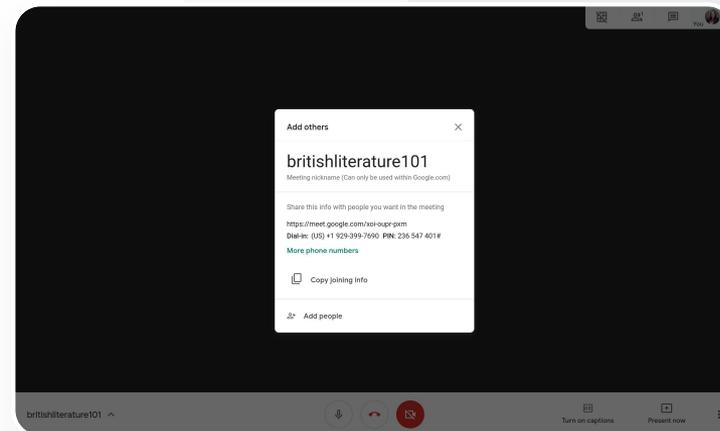
Cómo funciona

Cuando un profesor inicia una reunión con alias, se crea un código de reunión de 10 caracteres que se asocia temporalmente a ese alias.

Una vez que la última persona abandona la reunión o el profesor la finaliza, el código de reunión temporal caduca, así como la asociación entre el alias y el código de reunión.

Si a los alumnos no se les ha concedido permiso para crear reuniones, no podrán utilizar el alias ni el código de la reunión.

Los profesores pueden volver a utilizar el alias, lo que creará un nuevo código de reunión temporal. A partir de ese momento, los alumnos podrán volver a unirse mediante el alias.



[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Seguridad y privacidad en Google Meet para centros educativos](#)

[Iniciar una videollamada con Google Meet](#)



En nuestro campus se ofrecen clases online con muchos alumnos, y debemos grabarlas para aquellos que opten por la educación a distancia y para los que no puedan asistir."

[Instrucciones paso a paso](#)

Grabar clases

Con Teaching and Learning Upgrade y Education Plus, los usuarios pueden **grabar** sus reuniones y guardarlas automáticamente y de forma indefinida en Drive.

De esta forma, resulta fácil archivar y compartir clases, talleres y sesiones de trabajo.

- ✓ Si tus profesores utilizan Classroom, con la integración de Google Meet pueden crear un enlace único para cada clase, que se mostrará en las páginas Tablón y Trabajo de clase de Classroom
- ✓ Este enlace sirve como un espacio de reuniones específico para cada clase, que tanto profesores como alumnos pueden usar fácilmente
- ✓ Usa esta integración para grabar clases de forma óptima

[!\[\]\(5ed4e929f29e555498ea58f609acf062_img.jpg\) Documentación del Centro de Ayuda sobre este asunto](#)

[Configurar Google Meet para la educación a distancia](#)

Grabar reuniones de profesores

Con Teaching and Learning Upgrade y Education Plus, las grabaciones de las videollamadas se guardan automáticamente en Drive y permanecen ahí todo el tiempo que los usuarios las necesitan. De esa forma, resulta fácil archivar y compartir reuniones, cursos de desarrollo profesional y reuniones de la junta directiva.

- ✓ Se recomienda que el administrador de TI permita que solo puedan grabar reuniones los profesores y el personal del centro
- ✓ Puedes agrupar a los profesores y a los alumnos de tu centro en unidades organizativas separadas y, después, aplicar reglas de acceso distintas a cada una
- ✓ Si utilizas Classroom y tienes profesores verificados, puedes habilitar el acceso para tu grupo de profesores

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Configurar Google Meet para la educación a distancia](#)



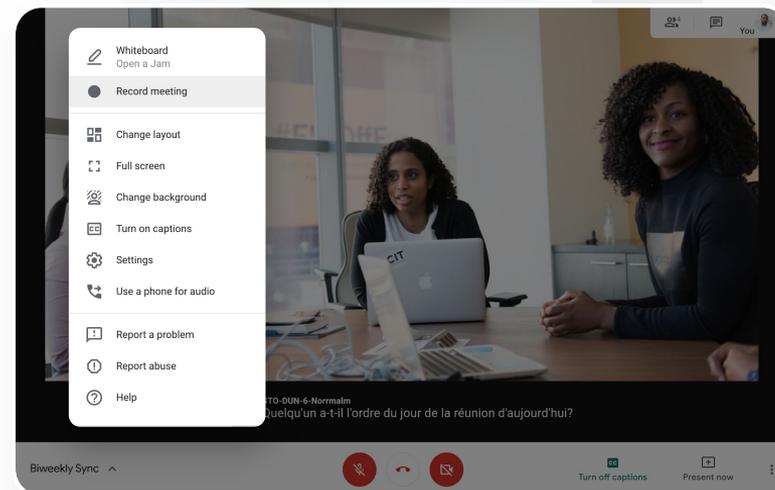
Solemos celebrar reuniones de personal online y tenemos que grabarlas todas. Además, nos gusta grabar los cursos de desarrollo profesional que impartimos y las reuniones de la junta directiva".

[Instrucciones paso a paso](#)

Instrucciones: grabar

Cómo grabar una reunión

- Abre la reunión desde Calendar y selecciona **Unirme con Google Meet**
- En la página de confirmación de la reunión, **abre el menú de opciones** seleccionando los tres puntos verticales que aparecen en la esquina inferior derecha
- Haz clic en **Grabar la reunión**. Al hacerlo, aparecerá un punto rojo en la esquina inferior derecha de la pantalla para indicar que la reunión se está grabando
- Se guardará automáticamente un archivo de vídeo de la reunión en tu Drive



[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Configurar Google Meet para la educación a distancia](#)

Recuperar clases

Todos los usuarios tienen acceso al almacenamiento de Drive del dominio del centro educativo. Las grabaciones de las videollamadas se guardan automáticamente en la cuenta de Drive del organizador de la reunión con Teaching and Learning Upgrade y Education Plus. Para ver la grabación de la reunión, pide al organizador el enlace de la grabación o accede a él desde el evento del calendario.

- ✓ Las grabaciones se guardan en la cuenta de Drive del organizador de la reunión
- ✓ A los participantes de la reunión que estén en la misma unidad organizativa que el organizador se les concederá acceso a la grabación automáticamente
- ✓ Si el organizador de la reunión cambia, el enlace de la grabación se envía a quien creó originalmente el evento

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Grabar videollamadas](#)



Quiero ver la grabación de una clase a la que no acudí”.

[Instrucciones paso a paso](#)

Instrucciones: ver y compartir reuniones

Cómo compartir una grabación

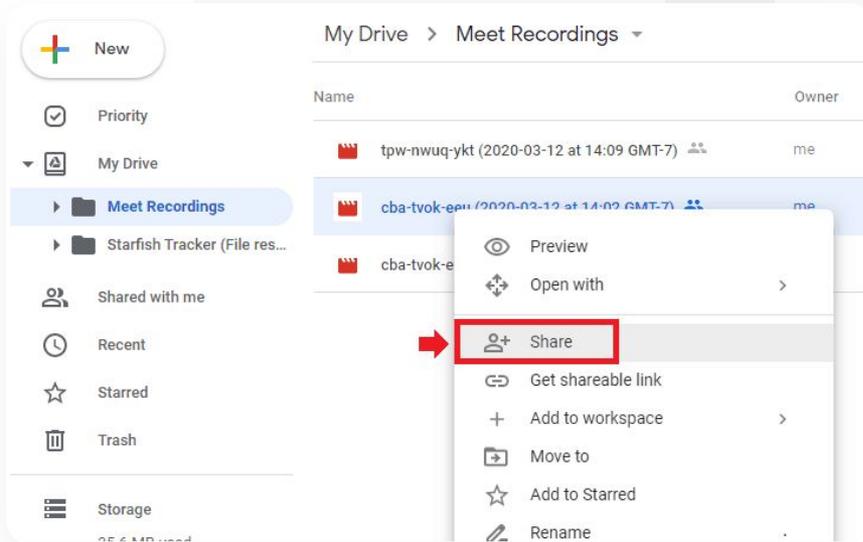
- Selecciona el archivo
 - Haz clic en el icono para **compartir**
 - Añade a los usuarios que pueden verla
 - Selecciona el icono del **enlace**
 - Pega el enlace en un correo o en un mensaje de Chat
- O bien**

Cómo descargar una grabación

- Selecciona el archivo
- Haz clic en el icono **Más > Descargar**
- Haz **doble clic** en el archivo descargado para reproducirlo

Cómo reproducir una grabación en Drive

- En Drive, haz **doble clic** en el archivo de una grabación para reproducirlo; aparecerá el mensaje "Aún se está procesando" hasta que esté listo para verlo online
- Para añadir una grabación a tu Drive, selecciona el archivo y haz clic en **Añadir a Mi unidad**



[Documentación del Centro de Ayuda](#)
sobre este asunto

[Grabar videollamadas](#)



Necesitamos poder emitir en directo las reuniones del profesorado y el personal del centro para que otros colaboradores y los padres puedan verlas".

[Instrucciones paso a paso](#)

Emisiones en directo de reuniones

Emite en directo para hasta 10.000 usuarios del dominio con Teaching and Learning Upgrade. Además, con Education Plus, tienes la posibilidad de emitir en directo para hasta 100.000 usuarios del dominio. Los participantes pueden unirse a las emisiones en directo seleccionando el enlace que comparta con ellos el organizador mediante un correo o una invitación de Calendar. Consulta a tu administrador de TI para asegurarte de que tienes los privilegios necesarios para emitir en directo.

- ✓ Se recomienda que el administrador de TI permita que solo puedan emitir en directo los profesores y el personal del centro
- ✓ En eventos multitudinarios, para que los usuarios disfruten de una mejor experiencia, utiliza una emisión en directo en lugar de organizar una videollamada interactiva a la que tengan que unirse
- ✓ Si un usuario se pierde la emisión en directo de una reunión, podrá verla una vez que termine

[!\[\]\(ea67c407d9a120459b7f2259b0d26990_img.jpg\) Documentación del Centro de Ayuda sobre este asunto](#)

[Configurar Google Meet para la educación a distancia](#)

Emisión en directo de eventos escolares

Emite en directo para la comunidad de tu centro educativo. Selecciona el enlace de la emisión en directo que te facilitará el organizador por correo o mediante el evento de Calendar. Consulta a tu administrador de TI para asegurarte de que tienes los privilegios necesarios para emitir en directo. De lo contrario, podrás [ver](#) la reunión una vez que termine.

- ✓ Puedes usar la función de emisión en directo de Google Meet para conectar a toda tu comunidad emitiendo en directo ceremonias de graduación, eventos deportivos o reuniones de asociaciones de padres y profesores
- ✓ Emite en directo para hasta 10.000 usuarios del dominio con Teaching and Learning Upgrade, o para hasta 100.000 usuarios del dominio con Education Plus

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Configurar Google Meet para la educación a distancia](#)



Nos gusta emitir en directo eventos deportivos y otros acontecimientos importantes que celebramos, como graduaciones u obras de teatro, para quienes no puedan asistir en persona".

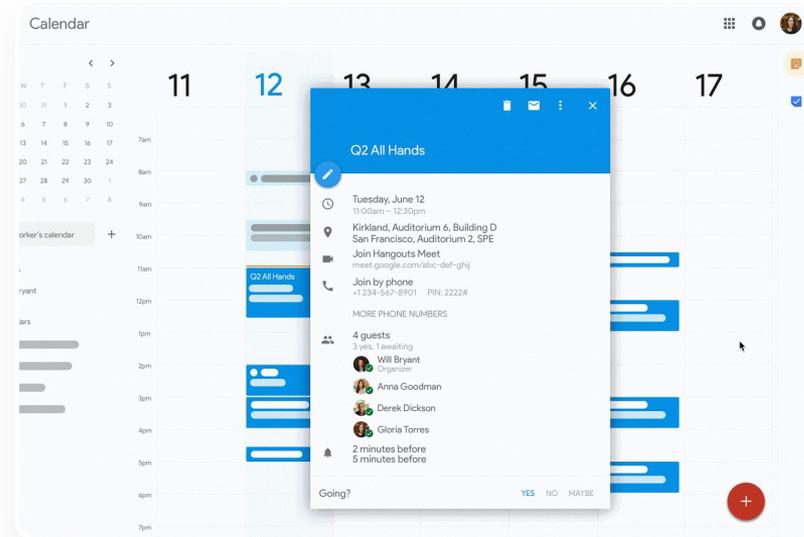
[Instrucciones paso a paso](#)

Instrucciones: emisión en directo

Cómo conceder permiso para una emisión en directo

- Abre Google Calendar
- Selecciona + Crear > más opciones
- Añade los detalles del evento, como la fecha, la hora y una descripción
- Añade hasta a 250 invitados que participarán plenamente en la videollamada, lo que significa que podrán presentar y que se les verá y oirá; también puedes añadir a personas de otras organizaciones
- Haz clic en **Añadir conferencia > Meet**
- Junto a la opción Unirme con Google Meet, selecciona la **flecha hacia abajo** y, a continuación, **Añadir emisión en directo**
- Para invitar a tantos usuarios del dominio como sea posible con tu edición de pago, copia la URL de la emisión en directo y compártela mediante un correo o un mensaje de Chat
- Selecciona **Guardar**
- La emisión no se inicia automáticamente; durante la reunión, selecciona **Más > Iniciar emisión**

Nota: Solo los invitados de tu organización podrán ver la emisión en directo



[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Configurar Google Meet para la educación a distancia](#)

Hacer preguntas

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

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

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Hacer preguntas a los participantes en Google Meet](#)



Necesito un método rápido para hacer preguntas, evaluar los conocimientos de los alumnos e interactuar con ellos para que participen".

[Instrucciones paso a paso](#)

Instrucciones: preguntas

Cómo hacer una pregunta:

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

Cómo ver el informe de preguntas:

- Después de una reunión, el moderador recibe un informe "Preguntas" por correo electrónico
- Abre el correo > haz clic en el archivo adjunto con el informe



[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Hacer preguntas a los participantes en Google Meet](#)

Recopilar comentarios

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

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

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Hacer encuestas en Google Meet](#)



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

[Instrucciones paso a paso](#)

Instrucciones: hacer encuestas

Cómo crear una encuesta:

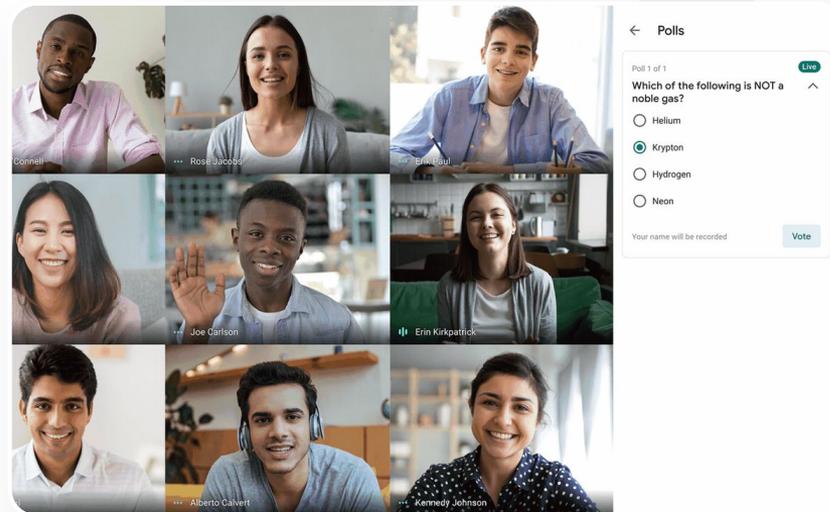
- En la esquina superior derecha de la reunión, selecciona el icono **Actividades > Encuesta**
- Selecciona **Iniciar una encuesta**
- Hacer preguntas
- Selecciona **Iniciar** o **Guardar**

Cómo moderar una encuesta:

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

Cómo ver el informe de una encuesta:

- Después de una reunión, el moderador recibe un informe por correo electrónico
- Abre el correo > selecciona el archivo adjunto con el informe



[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Hacer encuestas en Google Meet](#)

Grupos pequeños de alumnos

Los docentes pueden usar **grupos de trabajo** para dividir a los alumnos en grupos más pequeños durante las clases virtuales. Solo los moderadores pueden iniciar grupos de trabajo, y únicamente durante una videollamada y desde un ordenador. Actualmente, no es posible emitir en directo ni grabar los grupos de trabajo.

- ✓ Se pueden crear hasta 100 grupos de trabajo en una reunión virtual
- ✓ Los profesores pueden pasar fácilmente de un grupo de trabajo a otro para ofrecer ayuda cuando la necesiten
- ✓ Los administradores pueden garantizar que solo los profesores o el personal del centro puedan crear grupos de trabajo

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Utilizar grupos de trabajo en Google Meet](#)



Hemos optado por un modelo de enseñanza 100 % remoto y necesitamos poder imitar tareas de clase sencillas: dividir a los niños en grupos, escuchar qué tiene que decir cada uno, participar en sus conversaciones y volver a unir a los alumnos en un solo grupo de manera fluida".

[Instrucciones paso a paso](#)

Instrucciones: crear grupos de trabajo

Cómo crear grupos de trabajo

- Inicia una videollamada.
- En la parte superior derecha, selecciona el icono **Actividades > Grupos de trabajo**
- En el panel Grupos de trabajo selecciona el número que necesitas
- Luego se divide en varios grupos a los alumnos, pero los moderadores pueden moverlos manualmente de grupo si resulta necesario
- Abajo a la derecha, haz clic en **Abrir grupos**

Cómo responder a preguntas en distintos grupos de trabajo

- Aparecerá una notificación en la parte inferior de la pantalla del moderador cuando algún participante pida ayuda. Selecciona **Unirme** para acceder al grupo de trabajo de ese participante.



[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Utilizar grupos de trabajo en Google Meet](#)

Registro de la asistencia

El **registro de asistencia** facilita un informe de asistencia automáticamente en las clases que tengan cinco o más participantes. Los informes muestran quién se unió a la llamada e incluyen los correos de los participantes y el tiempo que han asistido a la clase virtual.

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

 [Documentación del Centro de Ayuda sobre este asunto](#)

[Registrar la asistencia en Google Meet](#)



Nos cuesta llevar un seguimiento de quiénes asisten a las clases online.

Queremos una herramienta que nos permita registrar fácilmente la asistencia a las clases en todo el dominio".

[Instrucciones paso a paso](#)

Instrucciones: informes de asistencia

Cómo activarlos en una reunión:

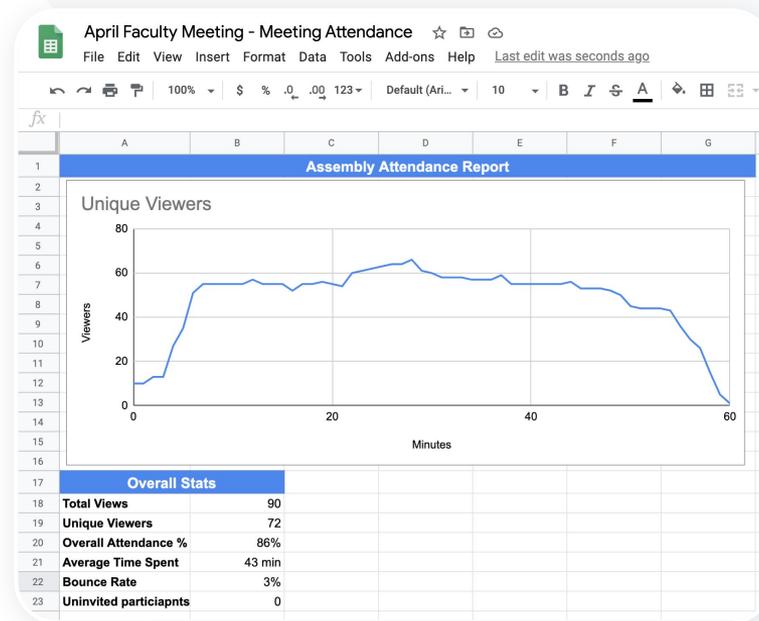
- Inicia una videollamada
- En la parte inferior, selecciona el icono del menú
- Selecciona el icono Configuración > Controles del anfitrión
- Activa o desactiva el registro de asistencia

Cómo activarlos en Calendar:

- Habilita las videoconferencias de Google Meet desde un evento de Calendar
- A la derecha, selecciona el icono Configuración
- Selecciona la casilla junto a Seguimiento de asistencia > haz clic en Guardar

Cómo generar el informe de asistencia:

- Después de una reunión, el moderador recibe un informe por correo electrónico
- Abre el correo > selecciona el archivo adjunto del informe



[🔗 Documentación del Centro de Ayuda sobre este asunto](#)

[Registrar la asistencia en Google Meet](#)

Gracias