CONFIGURACIÓN SEGURA: GOOGLE WORKSPACE

Esta obra está bajo una Licencia Creative Commons Atribución-CompartirIgual 4.0 Internacional.

Última actualización: Septiembre 2024

ÍNDICE

GOOGLE WORKSPACE

1. Consola de administrador
2. Configuraciones de usuarios
   a. Roles de administrador predefinidos
   b. Roles de administrador personalizados
   c. Asignar roles de administrador
   d. Asignar una cuenta de superadministrador adicional
   e. Cambiar o resetear contraseñas
   f. Configurar información de recuperación
   g. Crear un alias de correo
   h. Suspensión temporal de cuentas
   i. Buenas prácticas de seguridad para cuentas de administrador
3. Dispositivos: Habilitar actualizaciones automáticas

CONEXO

ÍNDICE

GOOGLE WORKSPACE

4. Configurar de seguridad:
    a. Requerimientos de contraseñas
    b. Forzar el uso de 2FA
    c. Habilitar la recuperación de contraseñas
    d. Generar códigos de seguridad de inicio de sesión con antelación
    e. Programa de protección avanzada
5. Grupos
    a. Beneficios
    b. Activar el uso de grupos
    c. Crear grupos
    d. Añadir miembros

CONEXO

ÍNDICE

GOOGLE WORKSPACE

6. Aplicaciones
   a. Gmail: activar el análisis mejorado
   b. Gmail: evitar el spam, spoofing y phishing con SPF, DKIM, DMARC
   c. Calendar: restringir acceso
   d. Drive: uso compartido con usuarios externos
   e. Drive: beneficios del uso de etiquetas
   f. Drive: crear etiquetas
   g. Drive: crear unidades compartidas (shared drives)
   h. Activar o desactivar servicios adicionales de Google
7. Recursos adicionales

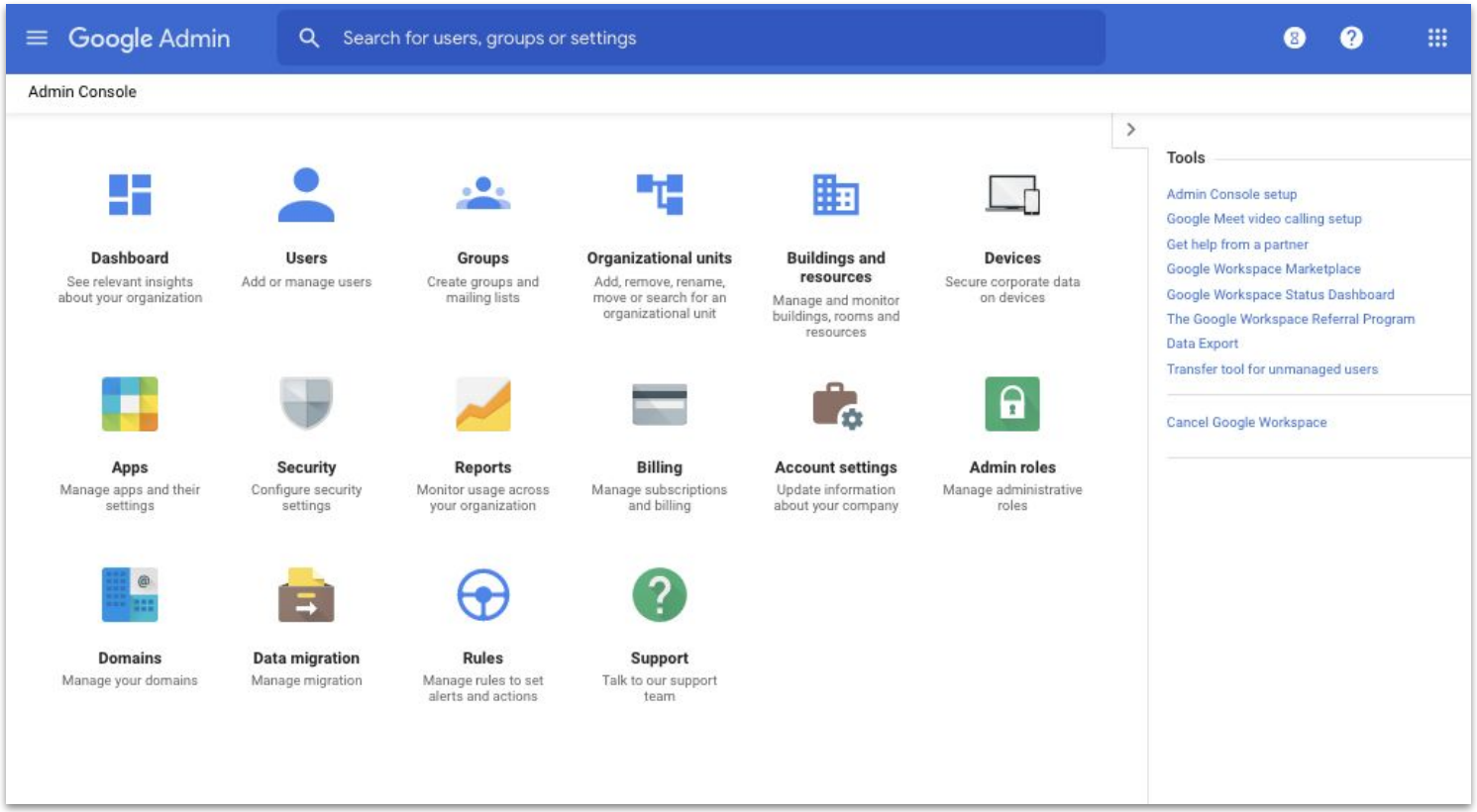
CONEXO

CONSOLA DE ADMINISTRADOR

Recuperado de:
https://support.google.com/a/answer/55955?hl=es&ref_topic=2413312

Accede a la consola de administrador

Como administrador, puedes utilizar la consola de administración de Google para gestionar todos tus servicios de Google Workspace, añadir o quitar usuarios, gestionar facturas y configurar dispositivos móviles, entre otras tareas. Puedes consultar la consola de administración en **admin.google.com. Mapa de la consola de administrador:**



CONSOLA DE ADMINISTRADOR

Recuperado de:
https://support.google.com/a/answer/55955?hl=es&ref_topic=2413312

Accede a la consola de administrador

	Usuarios: Añadir o quitar usuarios, asignarlos a unidades organizativas y darles funciones de administrador para que te ayuden a gestionar tus servicios de Google Workspace. Consulta el artículo Añadir nuevos usuarios o direcciones de correo.
	Facturación: Añadir métodos de pago, imprimir facturas, mejorar la edición de Google Workspace o cancelar la suscripción. Consulta el artículo Facturación y pagos.
	Novedades sobre productos: Leer las últimas entradas del Blog de novedades de Google Workspace.
	Alertas: Consultar las alertas más recientes en el Centro de alertas de la consola de administración.
	Gestión en la nube del navegador Chrome: Configura Gestión en la nube del navegador Chrome, registra navegadores, configura políticas del navegador y gestiona sus extensiones. Consulta el artículo Configurar la Gestión en la nube del navegador Chrome.
	Dispositivos: Gestionar los dispositivos móviles y los ordenadores de la cuenta de Google Workspace de tu organización. Consulta este artículo sobre cómo administrar dispositivos con la gestión de endpoints de Google.
	Seguridad: Gestionar la configuración de seguridad de Google Workspace: implementar obligatoriamente la verificación en dos pasos, o monitorizar y requerir contraseñas, entre otras opciones. Consulta el artículo Seguridad y protección de datos.



CONSOLA DE ADMINISTRADOR

Recuperado de:
https://support.google.com/a/answer/55955?hl=es&ref_topic=2413312

Accede a la consola de administrador

	Dominios: Verificar el dominio y añadir alias de dominio o más dominios, entre otras opciones. Consulta el artículo Añadir o cambiar dominios.
	Directory Sync: Sincroniza los datos de usuarios y de grupos de protocolo ligero de acceso a directorios con tu directorio de Google Cloud. Consulta el artículo Empezar a utilizar Directory Sync.
	Grupos: Crear grupos de empresa y listas de distribución para trabajar en equipo. Consulta el artículo Empezar a gestionar grupos de una organización
	Aplicaciones: Gestionar ajustes de aplicaciones y servicios de Google Workspace, como Gmail y Calendar.Consulta el artículo Configurar servicios para tu empresa.
	Migración de datos: Importar correos electrónicos, eventos de calendario y contactos mediante las diferentes herramientas de migración de Google. Consulta este artículo sobre el servicio de migración de datos.
	Configuración de la cuenta: Personalizar los detalles de la organización y establecer las preferencias de comunicación.
	Unidades organizativas: Configurar una estructura para asignar ajustes y aplicaciones a grupos o departamentos. Consulta el artículo Cómo funciona la estructura organizativa.



CONSOLA DE ADMINISTRADOR

Recuperado de:
https://support.google.com/a/answer/55955?hl=es&ref_topic=2413312

Accede a la consola de administrador

	Informes: Consultar informes y registros de auditoría para detectar posibles riesgos de seguridad y analizar la actividad de los usuarios y los administradores Consulta el artículo Monitorizar el uso y la seguridad con informes.
	Edificios y recursos: Configurar Calendar para que los usuarios puedan reservar los recursos compartidos de tu empresa, como equipos o salas de conferencias. Consulta el artículo sobre cómo configurar edificios, características y recursos de Calendar.
	Reglas: Proteger los datos, los archivos y los dispositivos de tu organización. Consulta el artículo sobre cómo crear, editar y ver reglas de seguridad.
	Roles de administrador: Añadir a otros usuarios como administradores y seleccionar sus permisos. Consulta el artículo Información sobre los roles de administrador.
	Almacenamiento: Gestionar el almacenamiento de Google Workspace de tu organización. Consulta el artículo Revisar el uso del espacio de almacenamiento en toda tu organización.
	Asistencia: Recibir asistencia de Google por chat, teléfono o correo electrónico y buscar temas de ayuda concretos. Consulta el artículo Contactar con el equipo de Asistencia de Google Workspace.
	Panel de control: Consultar información, notificaciones y recomendaciones sobre tu organización. Consulta el artículo Descripción general de la gestión de Work Insights.



ROLES DE USUARIO

Recuperado de:
https://support.google.com/a/answer/2405986

Roles de administrador predefinidos

En Google Workspace se pueden asignar a los usuarios de tu organización algunos roles de administrador predefinidos que otorgan uno o varios privilegios que te permiten llevar una buena gestión de cuentas. **A continuación, se explican los diferentes roles:**



Superaministrador: Tiene acceso a todas las funciones de la consola de administración de Google y a la API Admin, por lo que puede gestionar todos los aspectos de la cuenta de tu organización



Administrador de grupos: Tiene control total sobre las tareas de los grupos de Google en la consola de administración, como crear nuevos grupos en la Consola de administración, entre otros



Administrador de usuarios: Puede realizar todas las acciones en los usuarios que no son administradores. Como crear y eliminar cuentas de usuario, Cambiar el nombre de los usuarios y las contraseñas, entre otros.



Administrador de Centro de ayuda: Puede cambiar las contraseñas de usuarios que no sean administradores, ver los perfiles de usuario y su estructura organizativa, entre otros.



Administrador de servicios: Puede gestionar algunos dispositivos y ajustes de servicios en la consola de administración, incluidos Google Calendar, Drive y Documentos.



USUARIOS

Recuperado de:
https://support.google.com/a/answer/2406043

Roles de administrador predefinidos



Administrador móvil: Puede gestionar dispositivos móviles y puntos finales con la gestión de puntos finales de Google. También concede acceso completo a los informes y a la configuración de Drive.



Administrador de Google Voice: Gestionar todos los ajustes y el aprovisionamiento de Google Voice. Añadir ubicaciones. Asignar números a usuarios. Transferir números. Cambiar direcciones de servicio.



Administrador de Directory Sync: Puede gestionar el proceso de sincronización mediante Directory Sync y Actualizar configuración de sincronización

Roles de administrador personalizados

Si ninguno de los roles predefinidos tienen todos la configuración de privilegios que necesitas, puedes crear hasta 750 roles personalizados para toda tu organización:

1. En la **consola de administrador.**, ve a Menú - Cuenta - Roles de administrador.
2. Haz clic en “Crear rol”, asigna un nombre o descripción y haz clic en “Continuar”.
3. En la lista “Nombre de privilegio”, marca las casillas de los privilegios que quieras que tengan los usuarios a los que asignes el rol ***(Más información sobre cada privilegio)***
4. Haz clic en “Continuar”.
5. Comprueba los privilegios y haz clic en “Crear rol”.



USUARIOS

Recuperado de:
https://support.google.com/a/answer/9807615#zippy=%2Casignar-roles-a-un-usuario

Asignar roles de administrador

Como super administrador, puedes asignar roles de administrador predefinidos o personalizados a los usuarios de la organización que te ayudarán con la gestión de las cuentas:

1. **Abre la consola de administrador.**
2. **Ve a Menú - Directorio - Usuarios.**
3. Localiza al usuario en la lista.
4. Haz clic en el nombre del usuario para abrir la página de su cuenta.
5. Desplázate hacia abajo y haz clic en “Roles y privilegios de administrador”.
6. Junto al rol predefinido o personalizado, haz clic en “Activar”
7. Haz clic en Guardar.





USUARIOS

Recuperado de:
https://support.google.com/a/answer/172176

Asignar una cuenta de superadministrador adicional

Es recomendable tener más de una cuenta de superadministrador, cada una de ellas gestionada por una persona diferente. De este modo, si se pierde una cuenta o se vulnera su seguridad, otro superadministrador puede hacer las tareas más importantes mientras se recupera la cuenta principal. A continuación, te indicamos cómo conceder a un usuario acceso completo a tu consola de administración:

Para hacer esta tarea, tienes que haber iniciado sesión como super administrador.

1. **Abre la consola de administrador.**
2. **Ve a Menú - Directorio - Usuarios.**
3. Localiza el usuario y haz clic para abrir la página de su cuenta.
4. Haz clic en “Privilegios y roles de administrador”.
5. Haz clic en el rol “Super administrador”.
6. Haz clic en el control deslizante para marcarla como “Asignada”
7. Haz clic en “Guardar”.



Notas:

- Pide al nuevo administrador que añada opciones de recuperación a su cuenta. Normalmente, el usuario se convierte en administrador en unos minutos. Sin embargo, esto puede tardar hasta 24 horas.
- Cuando un usuario con privilegios de superadministrador inicie sesión en su cuenta de Google, accede a la página de inicio de la consola de administración, que incluye todos los controles para administrar las cuentas de usuario y los servicios de tu organización.

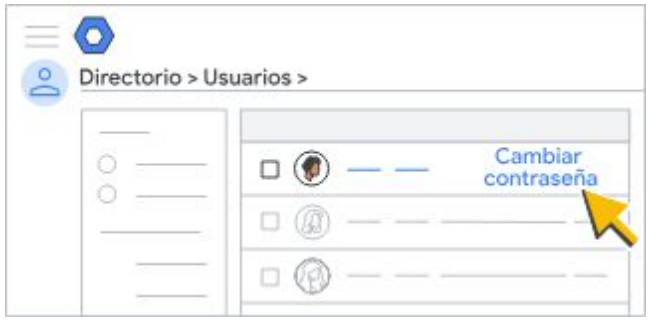


USUARIOS

Recuperado de:
https://support.google.com/a/answer/33319?sjid=6964848442061824748-NA#zippy=%2Ccambiar-la-contrase%C3%B1a-de-un-usuario

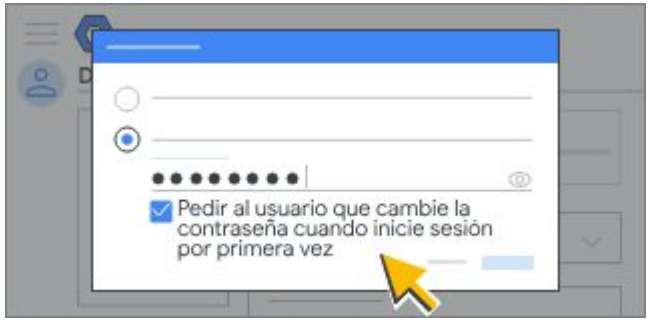
Cambiar o resetear la contraseña de tus usuarios

Para hacerlo, debes haber iniciado sesión con una cuenta de administrador que disponga de privilegios para cambiar contraseñas.



1. **Abre la consola de administrador.**
2. **Ve a Menú - Directorio - Usuarios**
3. Localiza el usuario
4. Coloca el cursor sobre el usuario y haz clic en “Cambiar contraseña”
5. Haz clic en “Crear contraseña” para escribir una contraseña provisional
6. Habilita la opción “Solicitar un cambio de contraseña la próxima vez que se inicie sesión.”
7. Haz clic en “Cambiar”
8. Haz clic en “Enviar contraseña por correo electrónico”
9. Se enviará automáticamente al usuario un enlace para cambiar la contraseña.
10. Borra los cookies de inicio de sesión haciendo clic en el nombre del usuario para abrir la página de su cuenta
11. Haz clic en Seguridad - Cookies de inicio de sesión - Restablecer.





Nota: Después de restablecer una contraseña y las cookies de inicio de sesión, se cierran todas las sesiones activas del usuario. Para volver a abrir sus aplicaciones, el usuario debe volver a iniciar sesión



USUARIOS

Recuperado de:
https://support.google.com/a/answer/3033063?sjid=4893983134334839434-NC

Configurar información de recuperación para usuarios



Como administrador puedes añadir un correo de recuperación para los usuarios de tu organización. Este correo permitirá a los usuarios recuperar el acceso a sus cuentas si no pueden iniciar sesión a través de la recepción de código de inicio de sesión. Es recomendable que utilices un dirección de correo electrónico de recuperación distinta a las del Google Workspace. No es recomendable utilizar números de teléfonos para la recuperación de cuentas.

1. **Abre la consola de administrador.**
2. **Ve a Menú - Directorio - Usuarios**
3. Selecciona el Usuario - Seguridad - Información de recuperación
4. Introduce sólo un email de recuperación (deja el campo de número de teléfono vacío)
5. Haz clic en Guardar" para aplicar los cambios







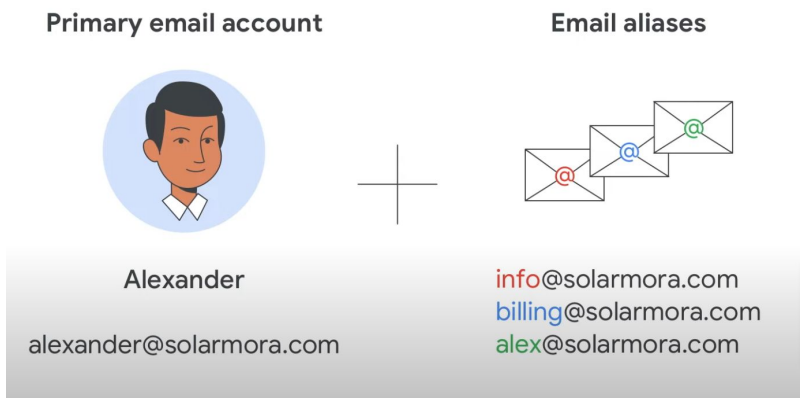
USUARIOS

Recuperado de:
https://support.google.com/a/answer/33327?hl=es&sjid=5011594127201206885-NA

Crear un alias de correo electrónico

Como administrador de Google Workspace, puedes crear una dirección de correo electrónico alternativa para que un usuario pueda enviar y recibir mensajes con otra dirección. Puedes añadir hasta **30 alias** de correo por usuario sin coste adicional. Para leer los mensajes enviados al alias de correo electrónico, los usuarios deben iniciar sesión en su cuenta principal de Google Workspace.

1. En la **consola de administrador**, ve a **Menú - Directorio - Usuarios.**
2. Para abrir la página de configuración del usuario, haz clic en su nombre.
3. En la parte izquierda, debajo del nombre del usuario, haz clic en “Añadir correos alternativos”.
4. Haz clic en “Dirección de correo electrónico alternativa” y escribe el nombre del alias (la parte de la dirección que aparece antes de la arroba [@]).
5. (Opcional) Si es necesario, selecciona un dominio secundario
6. (Opcional) Si quieres añadir más alias de correo, repite los pasos 5 y 6.
7. Haz clic en “Guardar”.





USUARIOS

Recuperado de:
https://support.google.com/a/answer/33312?hl=es&sjid=5011594127201206885-NA

https://support.google.com/a/answer/2789146?hl=es&sjid=5011594127201206885-NA

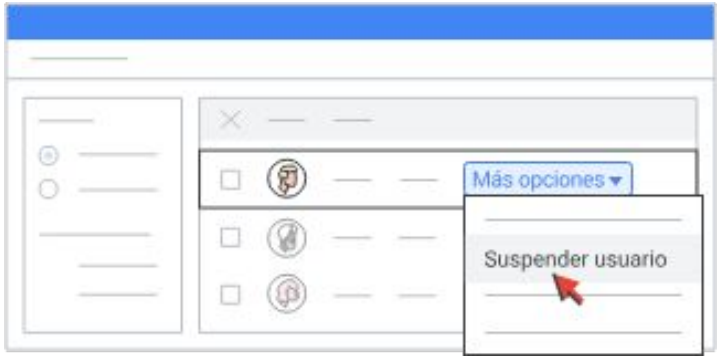
Suspensión temporal de cuentas

Como administrador, puedes suspender la cuenta de un usuario para bloquear temporalmente su acceso a los servicios de Google de tu organización. Al suspender una cuenta: El correo electrónico, los documentos, los calendarios y otros datos no se eliminan. Los colaboradores podrán seguir accediendo a los documentos compartidos. Se bloquearán las nuevas invitaciones del calendario y del correo electrónico.

Nota: puedes restaurar una cuenta de usuario cuando quieras.

Para suspender temporalmente usuarios:

1. **Abre la consola de administrador.**
2. **Ve a Menú - Directorio - Usuarios**
3. Selecciona el Usuario - Más opciones - Suspender usuario
4. Haz clic en “Suspender” para aplicar los cambios



Para Reactivar usuarios suspendidos:

1. **Abre la consola de administrador.**
2. **Ve a Menú - Directorio - Usuarios**
3. Haz clic en el nombre del usuario para abrir la página de su cuenta
4. En la parte superior derecha, haz clic en “Reactivar”.
5. Haz clic otra vez en “Reactivar” para confirmar la operación.
   Al cabo de 15 minutos se habilitará la cuenta de Gmail del usuario, que ya podrá iniciar sesión y acceder a su correo electrónico.



USUARIOS

Recuperado de:
https://support.google.com/a/answer/9011373

Buenas prácticas de seguridad para proteger cuentas de administrador

Proteger las cuentas de administrador

- ✓ Aplicar la verificación en dos pasos obligatoria a las cuentas de administrador
- ✓ Aplicar la verificación en dos pasos mediante llaves de seguridad
- ✓ No compartir cuentas de administrador entre usuarios
- ✓ Protección contra ataques dirigidos: registra las cuentas de administrador, super administrador y otras cuentas sensibles en el Programa de Protección Avanzada

Gestionar las cuentas de superadministrador

- ✓ Tener al menos dos cuentas de superadministrador en tu organización
- ✓ No utilizar cuentas de superadministrador para llevar a cabo actividades diarias. Asigna una cuenta adicional al miembro de la organización que será super administrador para sus actividades habituales. Los usuarios solo deben iniciar sesión en su cuenta de superadministrador para llevar a cabo tareas de super administrador, y es recomendable que cierren sesión en sus cuentas cuando no las estén utilizando.
- ✓ Asegurarse de recibir anuncios de administración importantes: Si no sueles iniciar sesión con tu cuenta de super administrador, es posible que te pierdas importantes avisos de servicio obligatorios de Google. Configura una cuenta para el reenvío de estas notificaciones. Reenviar notificaciones sobre la facturación y la cuenta
- ✓ Cerrar sesión siempre en las cuentas de superadministrador: recomendamos que los superadministradores inicien sesión cuando deban hacer tareas concretas y cierren sesión una vez que hayan terminado.



USUARIOS

Recuperado de:
https://support.google.com/a/answer/9011373

Buenas prácticas de seguridad para proteger cuentas de administrador

Supervisar la actividad de las cuentas de administrador

- ✓ Configurar alertas de actividad sospechosa de administradores por correo electrónico: Puedes controlar los posibles riesgos de seguridad configurando alertas para recibir notificaciones vía correo electrónico cuando se produzcan: intentos de inicio de sesión sospechosos, se vulneren dispositivos móviles u otro administrador haga cambios en la configuración. Alertas por correo enviadas a los administradores y reglas definidas por el sistema
- ✓ Revisar el registro de auditoría de la consola de administración: Consulta el registro de auditoría de la consola de administración para ver el historial de todas las tareas que se han hecho, qué administrador las llevó a cabo, cuándo lo hizo y desde qué dirección IP se conectó. Registro de auditoría de la consola de administración

Prepararse para recuperar cuentas de administrador

- ✓ Añadir opciones de recuperación a las cuentas de administrador
- ✓ Tener a mano la información necesaria para recuperar contraseñas, normarmalmente, Google solicita la siguiente información sobre la cuenta de la organización: Fecha en que se creó la cuenta, Dirección de correo electrónico alternativa que se asoció a la cuenta originalmente, Número de pedido de Google asociado a la cuenta (si procede), Número de cuentas de usuario creadas, Dirección de facturación vinculada a la cuenta, Tipo de tarjeta de crédito utilizada y sus últimos cuatro dígitos, Verificación de la propiedad de DNS del dominio.
- ✓ Registrar una llave de seguridad de repuesto: es recomendable que los administradores registren varias llaves de seguridad en su cuenta de administrador y las guarden en un lugar seguro.



DISPOSITIVOS

Recuperado de:
https://support.google.com/chrome/a/answer/9049675

Habilitar actualizaciones automáticas de aplicaciones y navegadores

Esta configuración está dirigida a administradores que gestionan el navegador Chrome o dispositivos Chrome OS de la organización. Como administrador puedes asegurarte que tus usuarios tengan habilitadas las actualizaciones automáticas:

1. **En la consola de administrador, ve a Menú - Dispositivos - Chrome - Configuración - Configuración de dispositivos.**
2. Selecciona la organización a la que aplicarás la configuración
3. Ve a “Configuración de actualización de dispositivos”.
4. Haz clic en “Configuración de actualizaciones automáticas”.
5. Selecciona “Permitir actualizaciones”.
6. Haz clic en Guardar.
7. Ve a “Actualizaciones de Chrome”.
8. Haz clic en Notificaciones de reinicio.
9. Selecciona “Forzar el reinicio después de un periodo”: a los usuarios se les mostrará un mensaje periódico en el que se les avisa de que deberán reiniciar el navegador
10. Define el periodo, entre 1 y 168 horas, durante el que se enviarán las notificaciones
11. Haz clic en Guardar.



SEGURIDAD: CONTRASEÑAS

Recuperado de:
https://support.google.com/a/answer/139399?hl=es&sjid=7634443477225182O5-NA

Configurar requerimientos de contraseñas

Como administrador, puedes obligar que los usuarios de tu organización cumplan con ciertos requerimientos en la configuración de las contraseñas que utilizan para la cuentas de Google. Posteriormente, puedes monitorear la fortaleza de las contraseñas utilizadas por los integrantes del Google Workspace. Puedes explicar la importancia de configurar contraseñas fuertes. Comparte estos tips de contraseñas.

1. **Abre la consola de administrador.**
2. **Ve a Menú - Seguridad - Autenticación - Gestión de Contraseñas**
3. En el Menú lateral izquierdo, selecciona la organización en donde aplicarás la configuración
4. En la sección de “Fortaleza de contraseña” habilita la opción “Obligar contraseña fuerte”
5. En la sección de “Longitud” introduce la cantidad mínima de caracteres que deben tener las contraseñas. Es recomendable que la contraseña tenga como mínimo 20 caracteres.
6. Opcionalmente, puede forzar que todos los usuarios realicen un cambio de contraseña que cumpla con los requerimientos configurados. Habilita la opción “Forzar Uso de contraseña en el próximo inicio de sesión”
7. Deshabilita la opción “Permitir la reutilización de contraseñas”
8. En la sección de “Expiración” selecciona el tiempo que expiración que tendrán las contraseñas
9. Haz clic en “Guardar” para aplicar los cambios
10. Adicional en la sección: Consola admin - Menú - Reportes - Reporte de usuarios - Cuentas, puedes constantemente monitorear la fortaleza y longitud de las contraseñas utilizada por tus usuarios.



SEGURIDAD: AUTENTICACIÓN 2FA

Recuperado de:
https://support.google.com/a/answer/9176657?hl=es&ref_topic=2759193&sjid=4893983134334839434-NC



Forzar el uso de 2FA en usuarios del Google Workspace

Debes iniciar como super administrador para esta configuración:

1. **Abre la consola de administrador.**
2. **Ve a Menú - Seguridad - Autenticación - 2FA**
3. Selecciona “Permitir que usuarios activen el 2FA”
4. Habilita la opción de “Forzar el uso de 2FA”.
5. Periodo para la activación del 2FA en nuevos usuarios: selecciona entre 1 día a 6 meses el tiempo en que los usuarios tendrán para habilitar el 2FA. Recomendamos períodos de tiempo pequeños para que el 2FA esté implementado en toda las organización
6. Habilita la opción “Permitir a usuarios seleccionar dispositivos de confianza” para evitar el uso de 2FA en estos dispositivos.
7. Para los métodos de 2FA selecciona la opción “Cualquiera menos la recepción de códigos vía SMS o llamadas”. Para mayor seguridad, opcionalmente puedes configurar la opción “Solo Llaves de seguridad”, de esta manera los usuarios de la organización sólo tendrán la opción de configurar una llave de seguridad como 2FA.

   Nota: en caso de activar esta segunda opción, si algún usuario pierde su llave, como administrador puedes generar códigos de seguridad de respaldo para cada usuario y así recuperar el acceso a su cuenta. Como administrador, serás el único que puede proveer estos códigos de respaldo para iniciar sesión.
8. Haz clic en Guardar” para aplicar los cambios



SEGURIDAD: RECUPERACIÓN

Recuperado de:
https://support.google.com/a/answer/33382#contact

Habilitar la recuperación de contraseña para usuarios

Como super administrador, puedes habilitar que los usuarios de tu organización reseteen la contraseña de sus cuentas, a través de las siguientes opciones:

Opción 1: Permitir que los propios usuarios cambien su contraseña activando la opción "Habilitar la recuperación de la contraseña de usuarios no administradores" en la consola de administrador:

1. **Abre la consola de administrador.**
2. **Ve a Menú - Seguridad - Autenticación - Recuperación de la cuenta**
3. Selecciona la organización en donde aplicarás la configuración
4. Haz clic en "Recuperación de cuentas de usuario"
5. Habilita la opción de "Permitir que los usuarios y administradores sin permisos de super administrador recuperen sus cuentas.
6. Haz clic en Guardar" para aplicar los cambios

Notas:

- Los usuarios de tu organización necesitan configurar la información de recuperación en donde puedan recibir las instrucciones para recuperar la contraseña.
- Como super administrador, para configurar la información de recuperación de los usuarios en la consola de administración, consulta la sección Configurar opciones de recuperación para usuarios de esta guía.
- Los usuarios que no hayan añadido información de recuperación deben ponerse en contacto con un administrador para recuperar el acceso a su cuenta.



SEGURIDAD: RECUPERACIÓN

Recuperado de:
https://support.google.com/a/answer/33382#contact

Habilitar la recuperación de contraseña para usuarios

Como super administrador, puedes habilitar que los usuarios de tu organización reseteen la contraseña de sus cuentas, a través de las siguientes opciones:

Opción 2: Pedir a los usuarios que se pongan en contacto con un administrador:

Cuando algún usuario de tu organización olvide su contraseña, y en la página de inicio de sesión hagan clic en **"¿Has olvidado tu contraseña?"**, recibirán un mensaje que les indicará que se pongan en contacto con su administrador.

Como super administrador, si un usuario olvida la contraseña de su cuenta de Google Workspace, o si crees que se ha vulnerado la seguridad de sus cuenta, puedes **"Cambiar o resetear la contraseña de un usuario"** desde la consola de administrador. Puedes consultar cómo hacerlo en la siguiente lámina de esta guía:







SEGURIDAD: RECUPERACIÓN

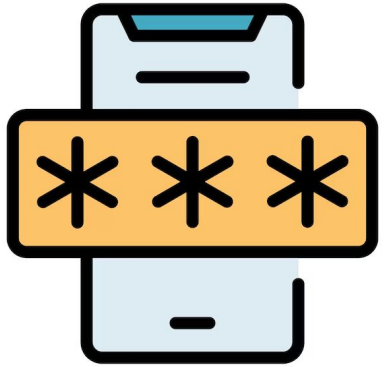
Recuperado de:
https://support.google.com/accounts/answer/11875 38?hl=es&sjid=18026003788840100187-NA

Generar códigos de seguridad de inicio de sesión con antelación

Si un usuario o un administrador pierde acceso al método 2FA configurado, no podrá iniciar sesión en su cuenta. En estos casos, los usuarios afectados pueden utilizar un código de seguridad. Estos códigos deben generarse e imprimirse con antelación y guardarse en un lugar seguro (como tu administrador de contraseña). Para guardar tus códigos de verificación alternativos haz lo siguiente:



1. **Ve a tu cuenta de Google**
2. **En la parte izquierda, haz clic en Seguridad.**
3. En "Cómo inicias sesión en Google", haz clic en “Verificación en dos pasos”. Es posible que tengas que iniciar sesión.
4. En "Códigos de verificación alternativos", haz clic en “Continuar”.
5. Haz clic en “Obtener códigos de verificación alternativos”.
6. O, si previamente lo tenías activos y perdiste el listado de código, haz clic en “Actualizar”.
7. Selecciona el listado de códigos y cópialos
8. Pegalos en una nota segura de tu administrador de contraseñas.
9. Imprimir tus códigos de verificación alternativos: haz clic en Imprimir .



Nota: Si pierdes los códigos, te quedas sin ellos o crees que te han robado los códigos de verificación alternativos, puedes crear otro conjunto de códigos. Cuando creas un nuevo conjunto de códigos, el anterior se desactiva automáticamente.



SEGURIDAD: PROTECCIÓN AVANZADA

Recuperado de:
https://support.google.com/a/answer/9378686?hl=es&sjid=4893983134334839434-NC&visit_id=638625317675772785-2648183412&ref_topic=9376233&rd=1

Programa de Protección Avanzada

La **Protección Avanzada** te ayuda a proteger a los usuarios con alto perfil de riesgo que pueden estar expuestos a recibir amenazas como ataques de phishing. Estos usuarios pueden pertenecer a Google Workspace (superadministradores o administradores), Campañas políticas, Grupos de activistas, Periodistas o Líderes empresariales.

El **Programa de Protección Avanzada** se ha diseñado para proteger las cuentas de Google frente a ataques intencionados online. Está disponible tanto para cuentas de Google de particulares como de empresas. Este programa incluye un conjunto de políticas de alta seguridad seleccionadas que se aplican a las cuentas registradas

La **Protección Avanzada** te permite aplicar todas estas protecciones a la vez y anular ajustes similares que hayas configurado manualmente. Estas políticas incluyen:

- Autenticación segura con llaves de seguridad
- Uso de códigos de seguridad con llaves de seguridad (según sea necesario)
- Restricciones sobre el acceso de terceros a los datos de la cuenta
- Análisis exhaustivos de Gmail
- Protecciones de Navegación Segura de Google en Chrome, cuando los usuarios inician sesión en Chrome con la misma identidad que la del Programa de Protección Avanzada
- Recuperación de la cuenta por medio del administrador



SEGURIDAD: PROTECCIÓN AVANZADA

Recuperado de:
https://support.google.com/a/answer/9378768?hl=es&ref_topic=9376233#zippy=%2Cpermite-que-los-usuarios-se-registren-en-el-programa%2Cavisa-a-los-usuarios-para-que-se-registren

Habilitar el registro de usuarios en el Programa de Protección Avanzada

1. Identifica a los usuarios que son vulnerables a los ataques para registrarlos
2. Compra llaves de seguridad para los usuario que participaran en el programa
3. Decide qué aplicaciones de terceros son de confianza para la Protección Avanzada
    - En la **consola de administrador**, ve a **Menú - Seguridad - Control de acceso y de datos - Controles de APIs - Gestionar acceso de apps de terceros.**
4. Configura el acceso al nivel organizativo superior con la verificación en dos pasos
5. Habilita el registro de usuarios
    - En la **consola de administrador**, ve a **Menú - Seguridad - Autenticación - Programa de Protección Avanzada.**
    - Selecciona la unidad organizativa que contiene a los usuarios cuyo registro necesitas habilitar.
    - Habilitar el registro de usuarios es el ajuste predeterminado; márcalo si no está seleccionado.
    - Especifica el tipo de código de seguridad que pueden generar los usuarios. Elige “No permitir que los usuarios generen códigos de seguridad” los usuarios no pueden generar códigos de seguridad. Es la opción que ofrece la máxima protección. Elige esta opción si todos los usuarios utilizan Google Chrome y tienen aplicaciones modernas.
6. Notifica a los usuarios en alto riesgo de que pueden registrarse en el Programa de Protección Avanzada









GRUPOS

Recuperado de:
https://support.google.com/a/answer/9400082?hl=es&sjid=5011594127201206885-NA

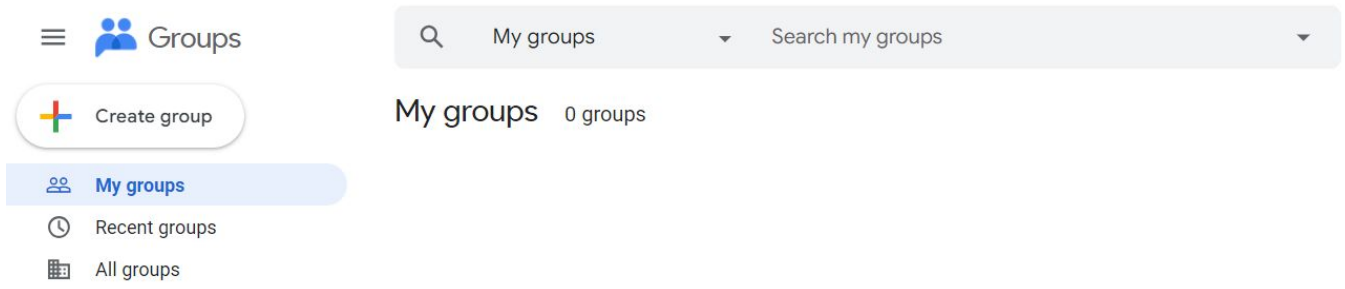
Beneficios de Grupos para organizaciones

Como administrador de Grupos, puedes crear grupos para departamentos, equipos u otros conjuntos de usuarios de tu organización. Puedes utilizar grupos para colaborar o para configurar funciones o servicios. La mejor manera de crear un grupo es usando la consola de administración, donde te resultará más fácil encontrar miembros del grupo o añadir muchos miembros a la vez. **Beneficios de crear y utilizar grupos:**

Comunicación o colaboración (incluidas listas de correo electrónico): Crea un grupo en la consola de administración o con Grupos de Google para que tus usuarios puedan hacer lo siguiente:

- Enviar correos a todos los miembros del grupo con una única dirección
- Invitar a miembros del grupo a una reunión
- Compartir contenido con los miembros del grupo, ya sean documentos, sitios web, vídeos o calendarios
- Participar en debates o en una Bandeja de entrada colaborativa de Grupos de Google

Configuración de funciones o servicios: *El grupo debe crearse en la consola de administración, no en Grupos de Google.* Se puede utilizar para Activar un servicio en un grupo o Configurar los ajustes de un servicio en un grupo





GRUPOS

Recuperado de:
https://support.google.com/a/answer/167096

https://support.google.com/a/answer/9400082?hl=es&sjid=5011594127201206885-NA#zippy=%2Cpaso-crea-un-grupo

Activar el uso de Grupos para organizaciones

Como administrador de grupos, puedes controlar si los usuarios pueden acceder a los grupos internos de tu organización desde la aplicación de Grupos de Google, que tienen disponible en el Menú de aplicaciones y en groups.google.com. Para ello, activa el servicio Grupos para empresas en sus cuentas desde la consola de administración.

1. En la **consola de administrador**, ve a **Menú - Aplicaciones - Google Workspace - Grupos para empresas.**
2. Haz clic en “Estado del servicio”.
3. Haz clic en “Activado” para todos

Crear Grupos para organizaciones

1. En la **consola de administrador**, ve a **Menú - Directorio - Grupos**
2. Haz clic en “Crear grupo”.
3. Introduce los siguientes datos: Nombre del grupo, crea un dirección de correo para el grupo, descripción, y propietarios del grupo
4. Para añadir la etiqueta de seguridad al grupo, marca la casilla Seguridad.
5. Elige el tipo de acceso del grupo: Público, Equipo, Solo anuncio o Restringido.
6. Para restringir quién puede ser miembro de este grupo, selecciona Restringir pertenencia y añade las condiciones de la consulta.
7. Haz clic en Crear grupo.



GRUPOS

Recuperado de:
https://support.google.com/a/answer/9400082?hl=es&sjid=5011594127201206885-NA#zippy=%2Cpaso-crea-un-grupo

Añadir miembros de la organización al Grupo

1. Haz clic en Añadir miembros.
2. Para buscar usuarios o grupos, introduce los primeros caracteres de su dirección de correo
3. Para buscar cuentas de servicio, introduce la dirección de correo electrónico completa.
4. Repite los pasos anteriores según sea necesario.
5. Haz clic en “Añadir al grupo”.

Nota: A todos los nuevos miembros se les asigna el rol "Miembro" y la suscripción "Todo el correo electrónico".



Después de crear un grupo

- Un grupo recién creado puede tardar hasta 24 horas en aparecer en el directorio de grupos
- Antes de enviar un mensaje al grupo nuevo, espera unos minutos hasta que se active. Si no esperas, es posible que se te notifique que el mensaje no se ha podido entregar.



APLICACIONES: GMAIL

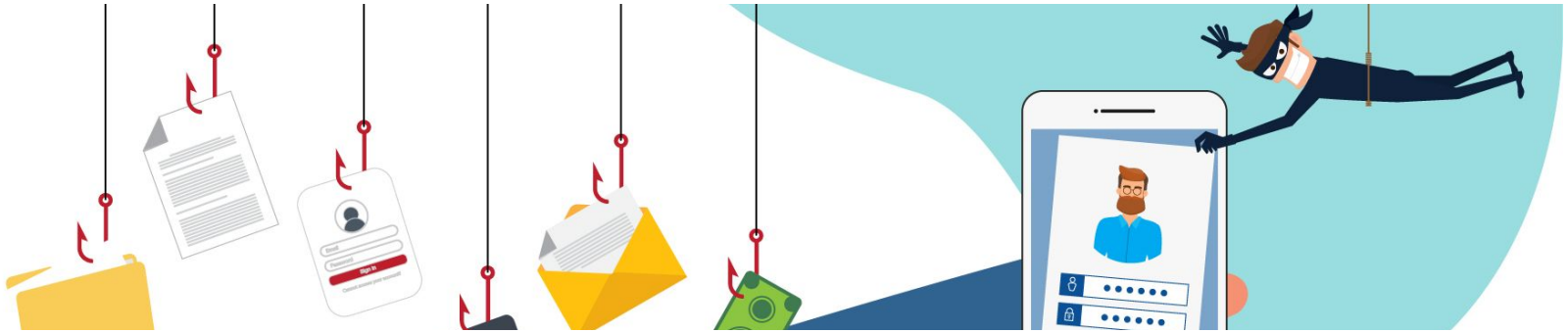
Recuperado de:
https://support.google.com/a/answer/33382#contact

Activar el análisis mejorado antes de la entrega de correos

La suplantación de identidad (phishing) es una práctica maliciosa que consiste en enviar correos electrónicos con el objetivo de engañar a los usuarios para extraer información sensible. Como administrador, puedes aumentar la capacidad de Gmail para identificar contenido sospechoso y así proteger las cuentas contra ataques de suplantación de identidad.

Con esta opción, cuando Gmail detecta contenido sospechoso, el envío se retrasa un poco para que Gmail pueda hacer comprobaciones de seguridad adicionales en el mensaje. Para activarla sigue estos pasos:

1. **En la consola de administrador, ve a Menú - Aplicaciones - Google Workspace - Gmail - Spam, phishing y software malicioso.**
2. Selecciona la organización a la que aplicarás la configuración
3. Desplázate hasta el ajuste “Análisis mejorado de mensajes antes de la entrega”.
4. Marca la casilla para aplicarlo a tu dominio.



APLICACIONES: GMAIL

Recuperado de:
https://support.google.com/a/answer/10583557?hl=es&ref_topic=9061731&sjid=15868097732270403277-NA

Evitar el spam, el spoofing y el phishing con la autenticación de Gmail

Configurar SPF, DKIM y DMARC para la organización: Es recomendable que los administradores de Gmail configuren la autenticación de correo para proteger los mensajes de su organización y evitar que se marquen como spam. Esto también ayuda a evitar que los spammers suplanten la identidad del dominio o la organización con técnicas de spoofing o phishing.

	**En primer lugar, asegura la entrega de correo y evita el spoofing con SPF:** SPF te permite especificar qué servidores y dominios pueden enviar correo de tu organización. Cuando los servidores de correo reciben un mensaje que procede de tu organización, comparan el servidor que lo envía con la lista de servidores permitidos. Así confirman que el mensaje procede realmente de quien debe. Más información: Asegurar la entrega de correo y evitar el spoofing (SPF)
	**A continuación, utiliza DKIM para aumentar la seguridad del correo que envías:** DKIM añade una firma digital cifrada a cada mensaje que se envía desde tu organización. Los servidores de correo que reciben el mensaje utilizan una clave pública para descifrar la firma y verificar que el mensaje procede realmente de quien debe. DKIM también impide que el contenido del mensaje cambie mientras se envía entre servidores. Más información: Configurar DKIM para prevenir el spoofing de correo electrónico
	**Por último, gestiona los correos sospechosos con DMARC:** DMARC indica a los servidores qué deben hacer con los mensajes que les llegan sin haber superado el paso por SPF o DKIM. Además, DMARC envía informes en los que señala qué mensajes han superado o no han superado este paso por SPF y DKIM. Estos informes ayudan a identificar posibles ataques al correo y otras vulnerabilidades. Consulta cómo configurar DMARC para evitar el spoofing y la suplantación de identidad (phishing).



APLICACIONES: GOOGLE CALENDAR

Recuperado de:
https://support.google.com/a/answer/60765?hl=es#zippy=%2Cpermitir-o-restringir-que-se-comparta-informaci%C3%B3n-con-personas-externas

Restringir acceso al calendario de la organización

Como administrador, puedes controlar cuánta información de los calendarios pueden compartir las personas de tu organización con usuarios externos. Una vez que limites la información que se puede compartir con personas ajenas a tu organización, tus usuarios no podrán superar ese límite cuando compartan eventos

1. **En la consola de administrador, ve a Menú - Aplicaciones - Google Workspace - Calendar.**
2. Haz clic en “Opciones para compartir”.
3. Selecciona la organización a la que aplicarás la configuración
4. En la sección “Opciones para compartir de forma externa”, selecciona qué nivel de información sobre sus calendarios pueden compartir tus usuarios con personas ajenas a la organización:
    - **Compartir solo información de libre/ocupado (ocultar detalles del evento):** los usuarios externos pueden ver si una persona está ocupada o no, pero no pueden ver el nombre ni los detalles de los eventos.
    - **Compartir toda la información, pero no permitir que los usuarios externos modifiquen los calendarios:** los usuarios externos pueden ver los detalles de todos los eventos, salvo los que están marcados como privados.
5. Haz clic en “Guardar”



APLICACIONES: GOOGLE DRIVE

Recuperado de:
https://support.google.com/a/answer/60781?hl=es&ref_topic=6097537&sjid=5011594127201206885-NA

Activar o desactivar el uso compartido en Drive con usuarios externos

Como administrador, puedes controlar si los usuarios pueden compartir archivos y carpetas de Google Drive con usuarios que no pertenezcan a la organización. Esto se aplica a Documentos, Hojas de cálculo, Presentaciones de Google, Carpetas y cualquier otro elemento que se almacene en Drive. Si activas la opción para compartir contenido de forma externa, tendrás opciones para limitar las opciones para compartir contenido, como advertir a los usuarios antes de que compartan contenido o impedir que se comparta mediante enlace.

1. **En la consola de administrador, ve a Menú - Aplicaciones - Google Workspace - Drive y documentos**
2. Haz clic en “Opciones para compartir” - “Opciones para compartir”.
3. Selecciona la organización a la que aplicarás la configuración
4. Para **activar** el uso compartido con usuarios externos, haz clic en “Activado” y elige las opciones para compartir.
5. Para **desactivar** el uso compartido con usuarios externos, haz clic en “Desactivado”. También puedes bloquear contenido externo para que no se comparta con tus usuarios, incluido el contenido de sistemas de almacenamiento de terceros.
6. Opcionalmente, también puedes controlar que se comparta información con dominios de confianza. Haz clic en “**Lista de dominios permitidos**” y elige las opciones para compartir.
7. Haz clic en “Guardar”

Google Drive



APLICACIONES: GOOGLE DRIVE

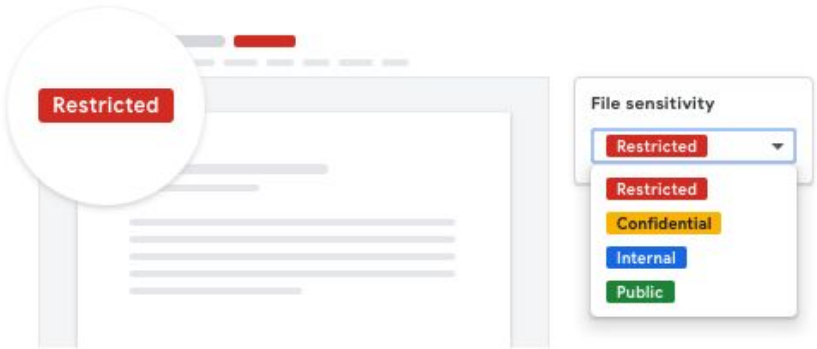
Recuperado de:
https://support.google.com/a/answer/9292382?hl=es&sjid=16346929581010696302-NA

Beneficios: uso de etiquetas en Google Drive

Como administrador, puedes crear etiquetas para aplicarlas a los archivos almacenados en Drive. Las etiquetas de Drive son metadatos que pueden ayudar a tu organización a organizar, encontrar y aplicar políticas a los archivos de Drive. Las etiquetas de tu organización se pueden aplicar a cualquier archivo de Drive de tu organización.

Ejemplos de casos prácticos en los que se pueden usar etiquetas de Drive

- **Clasificación de contenido** para seguir una estrategia de gobernanza de la información: Usa una etiqueta para identificar contenido sensible o que deba tratarse de un modo especial.
- **Aplicar política a elementos:** Utiliza una etiqueta como condición o acción en Reglas de Prevención de la pérdida de datos (DLP) o Reglas de conservación de Vault para satisfacer los requisitos de cumplimiento.
- **Encuentra archivos más rápido:** Los miembros de tu organización pueden encontrar contenido por etiquetas y campos. Por ejemplo, con los campos de etiqueta "Estado de contrato" y "Fecha de vencimiento" puedes buscar en Drive todos los contratos que aún no se han firmado y que vencen el viernes.





APLICACIONES: GOOGLE DRIVE

Recuperado de:
https://support.google.com/a/answer/60781?hl=es&ref_topic=6097537&sjid=5011594127201206885-NA

Uso de etiquetas en Google Drive

Tipos de etiquetas de Drive y dónde se muestran

- **Etiquetas con insignia** se utilizan para los documentos más importantes de la organización y se destacan visualmente en los archivos a los que se aplican. La etiqueta con insignia aparece junto al nombre del archivo cuando los usuarios abren un archivo en Documentos, Hojas de cálculo o Presentaciones de Google en la Web. **Solo puedes crear una** etiqueta con insignia para tu organización. Por ejemplo, la etiqueta con insignia debe tener al menos un campo de selección. **La etiqueta "Archivo sensible" contiene las opciones "Alto secreto", "Interno", "Público" y "Privado", cada una de un color diferente.**

- **Etiquetas estándar** se usan con otros metadatos. Puedes crear 150 etiquetas estándar (o 149 si creas una etiqueta con insignia). Con las etiquetas estándar, puedes configurarlas como una etiqueta sencilla sin la intervención del usuario, o bien añadir campos estructurados para que los usuarios proporcionen más información.



1 **Etiquetas con insignia**

2 **Etiqueta estándar**

APLICACIONES: GOOGLE DRIVE

Recuperado de:
https://support.google.com/a/answer/13127870

Crear etiquetas para usar en Google Drive

1. **En la consola de administrador, ve a Menú - Seguridad - Control de acceso y de datos - Clasificación de datos - Gestor de etiquetas.**
2. Haz clic en “Nueva etiqueta”.
3. Asigna un nombre a la etiqueta.
4. Añada una descripción a la etiqueta. Los usuarios verán la descripción de la etiqueta cuando abran el panel Etiquetas de un archivo.
5. En el caso de las etiquetas que tengan un campo con insignia, añade un enlace a la documentación sobre la etiqueta. Los usuarios ven este enlace "Más información" cuando apuntan a la etiqueta con insignia o abren el panel Etiquetas de un archivo.
6. Haz clic en Publicar.
7. Confirma que quieres publicar la etiqueta haciendo clic en Publicar.
8. Aplicar etiquetas a archivos en Google Drive



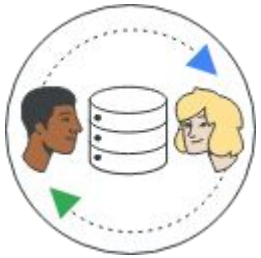


APLICACIONES: GOOGLE DRIVE

Recuperado de:
https://support.google.com/a/answer/7337469?hl=es&sjid=5011594127201206885-NA

https://support.google.com/a/users/answer/9310249?hl=es&ref_topic=9298590&sjid=15868097732270403277-NA

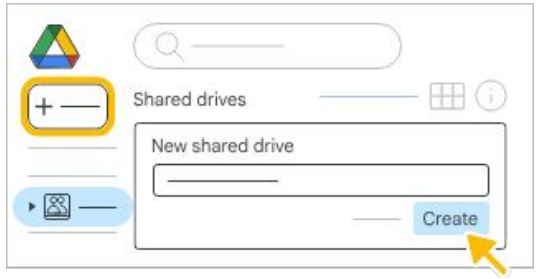
Crear Unidades compartidas “Shared Drives”

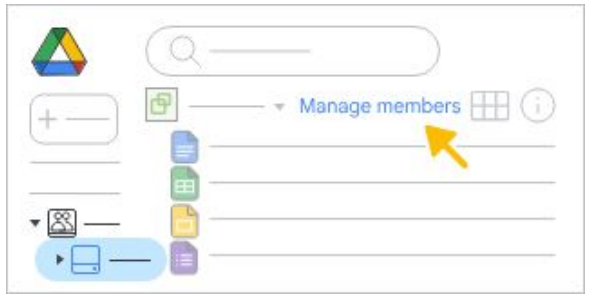


Como administrador, puedes gestionar cómo pueden los usuarios de tu organización crear y utilizar unidades compartidas para colaborar en Google Drive. Los archivos de las unidades compartidas pertenecen a tu organización y no a un usuario concreto.

Nota: Solo puedes crear unidades compartidas si tu edición las admite y tu administrador te permite crearlas. ***Requiere acceso de administrador***

1. En un ordenador, ve a drive.google.com.
2. Haz clic en “Unidades compartidas”.
3. Haz clic en “Nuevo”.
4. Asigna un nombre a la unidad compartida.
5. Haz clic en “Crear”.
6. Haz clic en “Gestionar miembros”.
7. Añade direcciones de correo electrónico o un grupo de Google
8. Selecciona el rol que quieres asignar en el Menú desplegable.
9. Haz clic en “Notificar a los usuarios”.
10. Haz clic en “Enviar”.







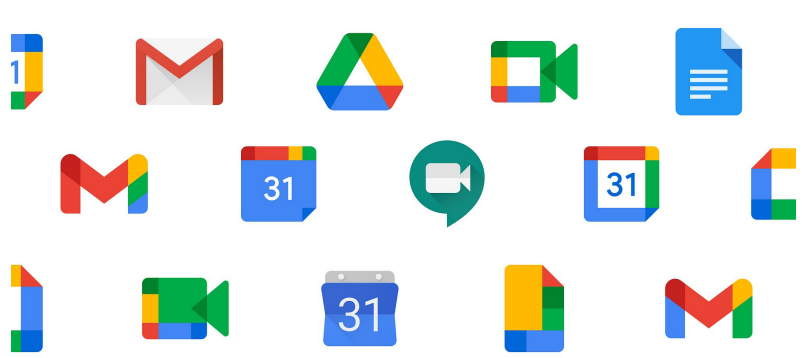
APLICACIONES

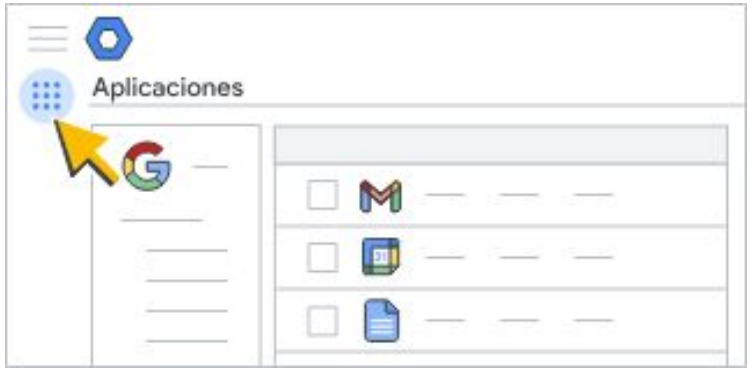
Recuperado de:
https://support.google.com/a/answer/181865?hl=es&sjid=18026003788840100187-NA#zippy=%2Cturn-services-on-or-off-for-users%2Cactivar-o-desactivar-servicios-en-cuentas-de-usuario

Activar o desactivar servicios adicionales de Google

Como administrador, puedes controlar el acceso a estos servicios adicionales. Algunos servicios tienen un control de activación o desactivación propio en la consola de administración, mientras que otros no. Los servicios que no tienen este control se pueden activar y desactivar todos a la vez.

1. **En la consola de administrador, ve a Menú - Aplicaciones - Servicios adicionales**
2. Haz clic en el nombre del servicio que quieres activar o desactivar para abrir su página de configuración.
3. Haz clic en “Estado del servicio”.
4. Para activar o desactivar un servicio en toda tu organización, haz clic en “Activado” para todos o en “Desactivado” para todos
5. Haz clic en “Guardar”.



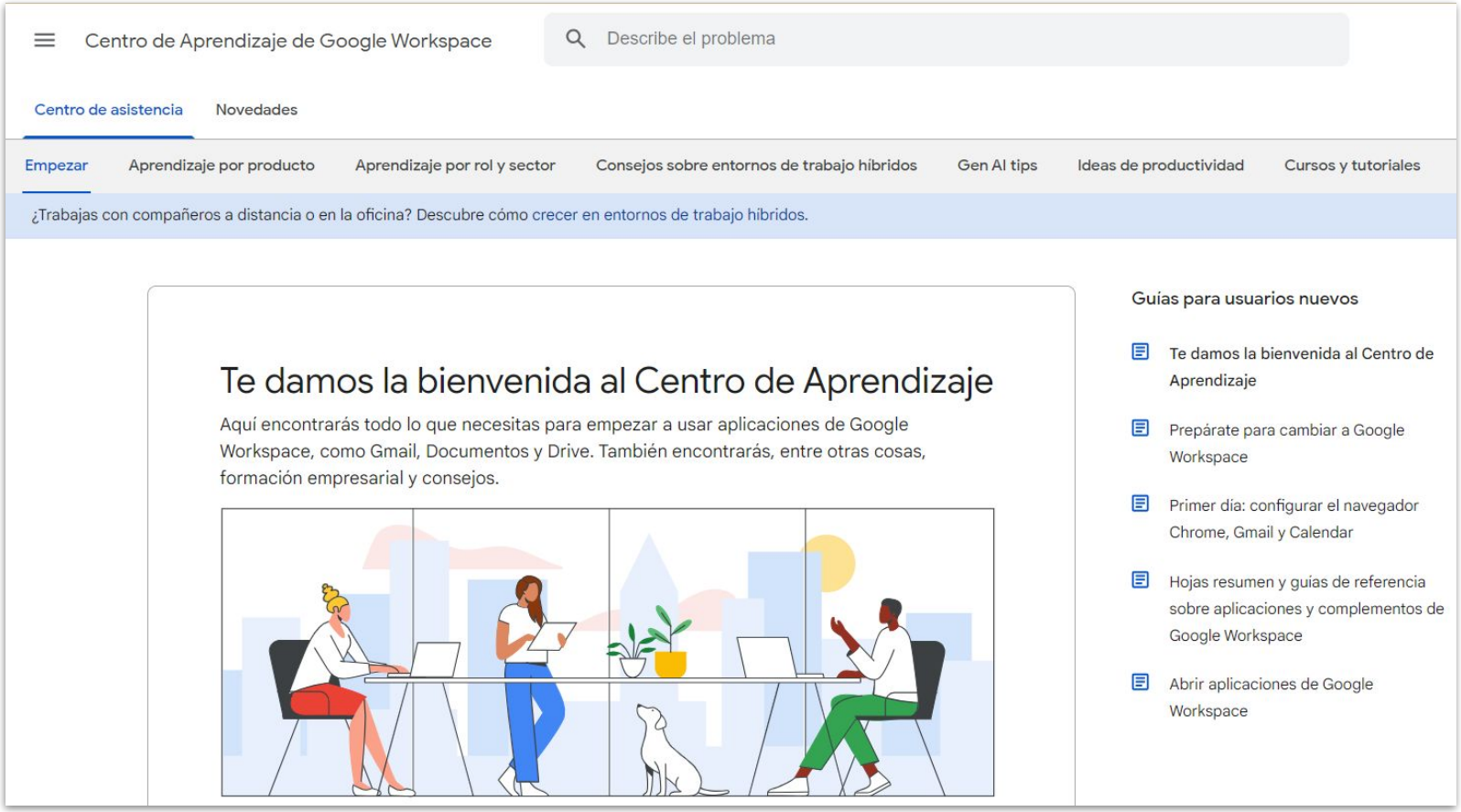




RECURSOS ADICIONALES

Nota: para obtener más información específica para cada área de Google Workspace puedes acceder a los siguientes recursos:

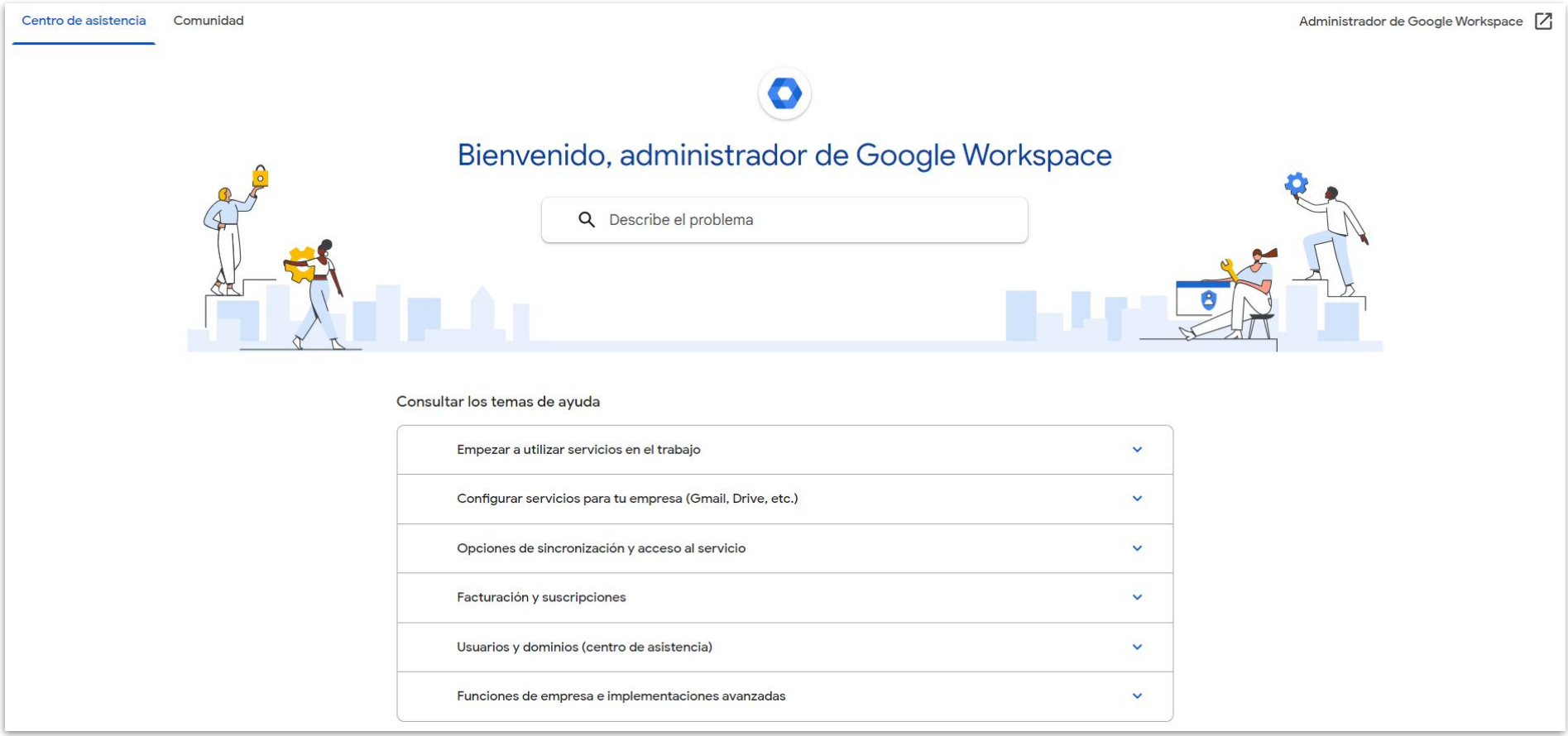
Accede al Centro de aprendizaje de Google Workspace



RECURSOS ADICIONALES

Nota: para obtener más información específica para cada área de Google Workspace puedes acceder a los siguientes recursos:

Accede al Centro de asistencia de administrador de Google Workspace



RECURSOS ADICIONALES

Nota: para obtener más información específica para cada área de Google Workspace puedes acceder a los siguientes recursos:

Configuraciones de aplicaciones de Google Workspace

Gmail

Ayuda para Google Workspace **administradores**
Configura tu correo electrónico de empresa y activa las funciones de Gmail para tus usuarios de Google Workspace.

También disponible: Seguridad avanzada de Gmail

- Activar Gmail con Google Workspace (@tu-empresa)
- Gestionar los registros MX (Mail Exchange)
- Añadir o eliminar una dirección de correo electrónico alternativa (alias de correo electrónico)
- Cambiar la dirección de correo electrónico de un usuario
- Personalizar funciones de Gmail en cuentas de usuario
- Evitar el spoofing, el phishing y el spam
- Cómo utilizar clientes IMAP o POP
- Comparar las funciones de Gmail de las distintas ediciones de Google Workspace
- Límites y políticas de Gmail



RECURSOS ADICIONALES

Nota: para obtener más información específica para cada área de Google Workspace puedes acceder a los siguientes recursos:

Configuraciones de aplicaciones de Google Workspace

Calendar

Gestionar Calendar en un equipo de Google Workspace

Con Google Calendar, tu equipo y tú podéis programar eventos y recursos, participar en reuniones, compartir calendarios de grupo y realizar muchas más tareas fácilmente.

- Gestionar Calendar para tus usuarios
- Configurar las opciones de uso compartido de Calendar
- Controlar las conferencias de eventos de Calendar (para administradores)
- Configurar reuniones
- Crear y compartir calendarios de grupo
- Permitir complementos en Calendar
- Activar o desactivar Calendar en las cuentas de usuario
- Activar o desactivar el lugar de trabajo en cuentas de usuario
- Invitar a los usuarios a indicar su lugar de trabajo
- Definir si se muestra el estado en Calendar de los usuarios
- Activar o desactivar Estadísticas de tiempo para los usuarios
- Cancelar o transferir eventos de calendario antes de eliminar un usuario



RECURSOS ADICIONALES

Nota: para obtener más información específica para cada área de Google Workspace puedes acceder a los siguientes recursos:

Configuraciones de aplicaciones de Google Workspace

Drive

Gestiona Drive en tu empresa o centro educativo.

Con Google Drive, tú y tu organización podréis crear copias de seguridad de t odos los documentos y compartirlos fácilmente desde cualquier lugar y con cualquier dispositivo, ya sea un portátil, un teléfono móvil o un tablet.

- Primeros pasos: guía de configuración de Drive para administradores
- Gestionar el uso compartido de archivos
- Restaurar y transferir archivos de los usuarios
- Gestionar unidades compartidas
- Implementar Drive para ordenadores
- Límites de almacenamiento y subida para Google Workspace
- Preguntas frecuentes de administradores sobre Drive
- Solucionar problemas de Drive
- Gestionar Drive en organizaciones de gran tamaño



RECURSOS ADICIONALES

Nota: para obtener más información específica para cada área de Google Workspace puedes acceder a los siguientes recursos:

Configuraciones de aplicaciones de Google Workspace

Meet

Gestiona Google Meet de cara a tu equipo de Google Workspace.
Con Google Meet, puedes realizar llamadas y reuniones tanto dentro como fuera de tu organización. Los usuarios pueden organizar reuniones y llamadas desde un ordenador, un teléfono móvil o un sistema de videoconferencias popular.

- Set up Meet for your organization
- Usar Meet en los centros educativos
- Prácticas recomendadas sobre reuniones híbridas de Google Meet para administradores
- Activar las funciones de Meet para los usuarios
- Track Meet usage
- Utilizar Meet con sistemas de videoconferencia de terceros
- Utilizar Meet con hardware de vídeo
- Comparar las funciones de Meet de las distintas ediciones de Google Workspace
- Implementar Meet en organizaciones grandes
- Organiza emisiones en directo de gran envergadura con menos ancho de banda con eCDN
- Solucionar problemas de Meet y supervisar su uso



RECURSOS ADICIONALES

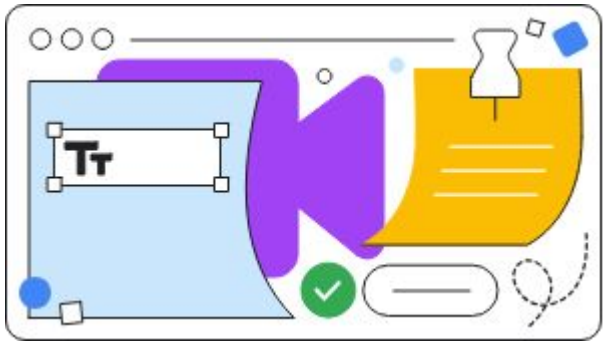
Nota: para obtener más información específica para cada área de Google Workspace puedes acceder a los siguientes recursos:

Configuraciones de aplicaciones de Google Workspace

Documentos, Hojas de cálculo, Presentaciones, Sites, Formularios, Keep y Vids

Gestiona estas aplicaciones de edición de Google Workspace para tu equipo:

Documentos: procesamiento de texto
Hojas de cálculo: hojas de cálculo
Presentaciones: presentaciones
Sites: sitios web
Formularios: encuestas y cuestionarios
Keep: notas
Vids: vídeos



- Gestionar Documentos y otras aplicaciones de edición en tu organización
- Gestionar las opciones para compartir de Documentos y otros editores
- Configurar el acceso sin conexión a Documentos, Hojas de cálculo y Presentaciones
- Permitir que los usuarios vean la actividad de los archivos (Panel de actividad)
- Gestionar plantillas de Presentaciones, Formularios y Sites
- Usar aplicaciones del editor para empresas
- Configuración avanzada

RECURSOS ADICIONALES

Nota: para obtener más información específica para cada área de Google Workspace puedes acceder a los siguientes recursos:

Configuraciones de aplicaciones de Google Workspace

Grupos



Con Google Workspace, tu organización puede utilizar grupos como listas de correo electrónico, Bandejas de entrada colaborativas, debates moderados y mucho más. Los administradores también pueden usar grupos para activar o desactivar ajustes de la consola de administración en equipos o departamentos concretos.

- Empezar a gestionar grupos de una organización
- Acerca de las interfaces y los servicios de Grupos
- Crear, actualizar o eliminar grupos
- Opciones para limitar la actividad de los grupos y el acceso a ellos
- Configurar y gestionar Grupos para empresas
- Gestionar información sobre grupos en la lista Grupos
- Información sobre las políticas y los límites de los grupos
- Novedades de Grupos de Google
- Preguntas frecuentes de los administradores de Grupos de Google
- Gestión avanzada de grupos



RECURSOS ADICIONALES

Nota: para obtener más información específica para cada área de Google Workspace puedes acceder a los siguientes recursos:

Configuraciones de aplicaciones de Google Workspace

Espacios de almacenamiento

- Revisar el uso del espacio de almacenamiento en toda tu organización
- Fijar límites de almacenamiento para los usuarios
- Definir límites de almacenamiento en unidades compartidas
- Liberar o añadir más almacenamiento en organizaciones
- Comprar más espacio de almacenamiento de Google Workspace para tu organización
- Límites de almacenamiento y subida para Google Workspace
- Prepárate para el almacenamiento compartido
- Preguntas frecuentes sobre el espacio de almacenamiento de Google Workspace para administradores
- Almacenamiento de Google Workspace for Education

