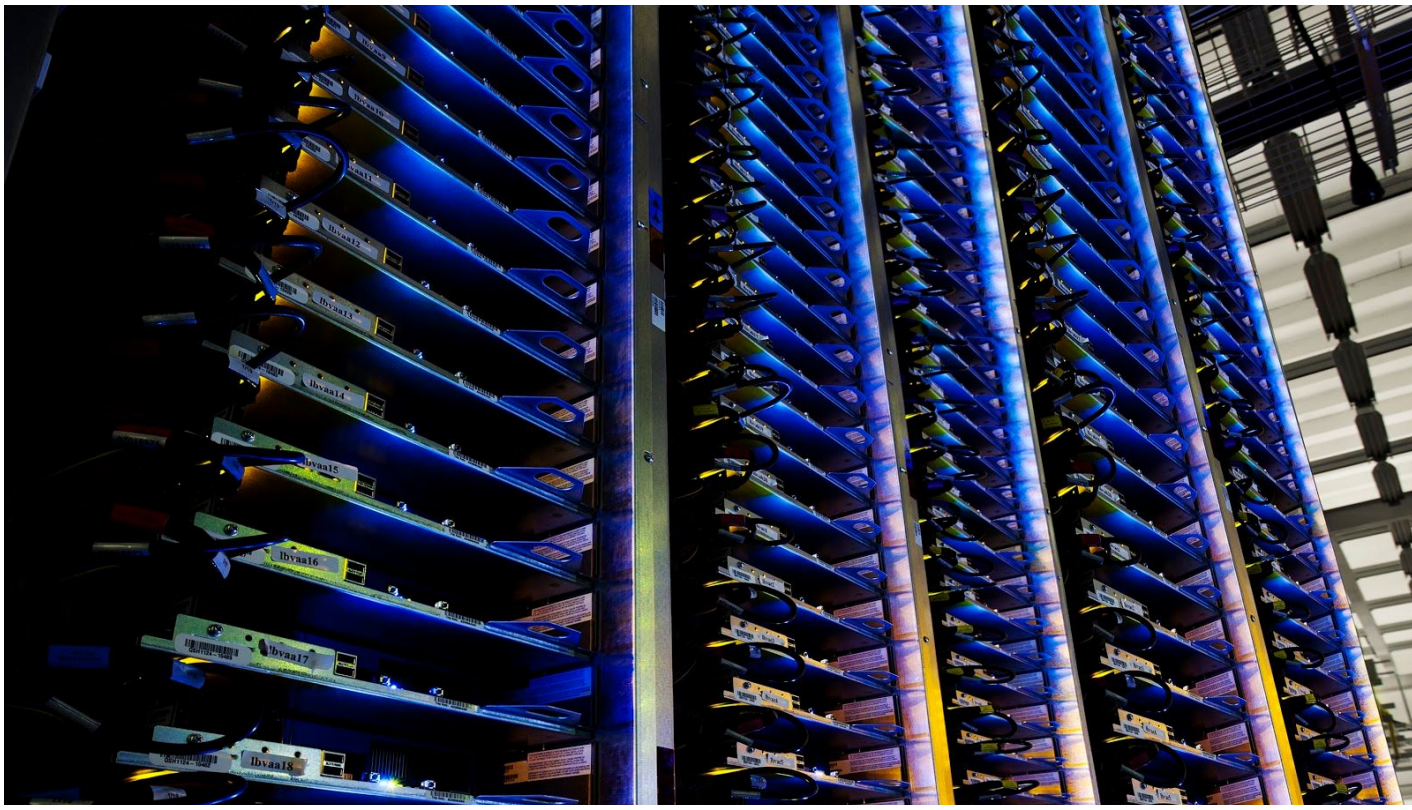
Informe de Google Cloud
Diciembre del 2020

Guía de implementación para cumplir con las obligaciones sobre protección de datos en Google Workspace



Google Cloud

Índice

Renuncia de responsabilidad

Esta guía está dirigida a los administradores de Google Workspace. En ella se explica cómo usar y personalizar los servicios y la configuración de Google Workspace para cumplir los requisitos sobre protección de datos. La información incluida en esta guía no constituye ningún asesoramiento de carácter jurídico, por lo que te recomendamos que recurras a una persona experta en cuestiones legales para que te oriente sobre los requisitos que se aplican específicamente a tu organización.

El contenido de esta guía es correcto a fecha de Diciembre del 2020 y representa la situación del momento en que se redactó. Es posible que los sistemas y las políticas de seguridad de Google cambien a medida que mejoramos la protección de nuestros clientes.

Tratamiento de los Datos Personales de los Clientes en nuestros servicios

Requisitos de protección de datos que debes cumplir

En Google tenemos el firme compromiso de ayudar a nuestros clientes a cumplir con sus obligaciones globales de protección de datos, incluidos los requisitos que establece el Reglamento General de Protección de Datos (RGPD). Para ello, ofrecemos productos y herramientas útiles, integramos potentes medidas de protección de la privacidad y la seguridad en nuestros servicios y contratos, y proporcionamos certificaciones e informes de auditoría.

Según refleja la Adenda sobre Tratamiento de Datos de Google Workspace, Google actúa como encargado del tratamiento de los Datos Personales de los Clientes que tu organización envía, almacena o recibe por medio de los servicios de Google Workspace, y trata estos datos en tu nombre y de acuerdo con tus instrucciones. Como cliente, eres responsable del tratamiento de esos Datos Personales de los Clientes[1], lo que significa que determinas su finalidad y los medios que se emplean en su tratamiento.

Te recomendamos que estudies tu Contrato de Google Workspace, la Adenda sobre Tratamiento de Datos de Google Workspace y los términos aplicables a cualquier otro servicio de Google que pongas a disposición de tus usuarios finales mientras estén conectados a las cuentas gestionadas de su organización (por ejemplo, los servicios adicionales que hayas activado en tu dominio).

Nuestros compromisos de privacidad

Consideramos que nuestra responsabilidad primordial cuando utilizas nuestras soluciones empresariales es proteger tu negocio. Por eso, Google asume estos compromisos de privacidad de Google Cloud con las empresas en todos los productos de Google Workspace. Estos compromisos se apoyan en el sólido compromiso contractual que adquirimos contigo.

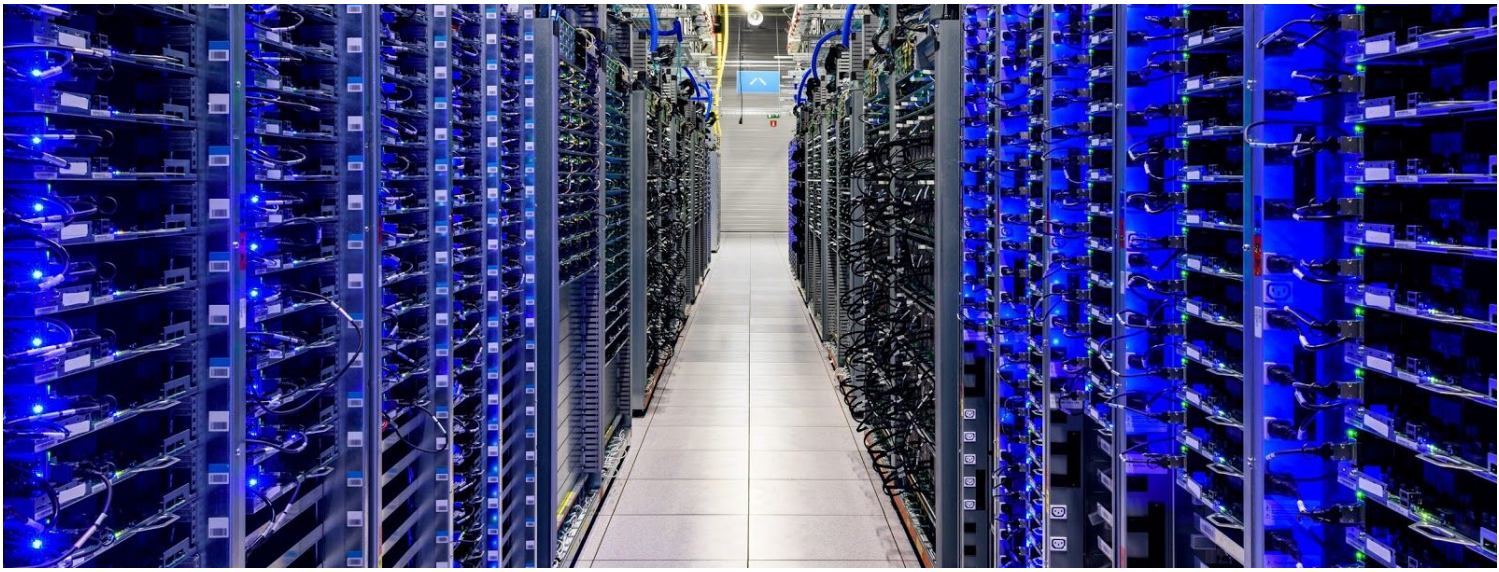
- **Tienes el control de tus datos.** Los Datos de tus Clientes[2] son de tu propiedad, no de Google. A la hora de tratar tus datos, seguimos estrictamente los contratos que hemos firmado contigo.
- **Nunca utilizamos tus datos para segmentar anuncios.** No tratamos los datos de tus clientes ni de tus servicios con fines publicitarios ni para mejorar los productos de Google Ads.
- **Somos transparentes sobre cómo recogemos y usamos los datos.** Nos comprometemos a ser transparentes, cumplir normativas como el RGPD y seguir prácticas recomendadas sobre privacidad.
- **Nunca vendemos datos de clientes o servicios.** Nunca vendemos datos de clientes ni de servicios[3] a terceros.
- **La seguridad y la privacidad son criterios de diseño primordiales en todos nuestros productos.** Dar prioridad a la privacidad de nuestros clientes implica proteger los datos que nos confías. Para ello, integramos las tecnologías de seguridad más potentes en nuestros productos.

Google diseñó Google Workspace cumpliendo unos estándares muy estrictos de privacidad y seguridad, según las prácticas recomendadas del sector.[4] Además de establecer severos compromisos contractuales relativos a la propiedad y el uso de los datos, la seguridad, la transparencia y la responsabilidad, te proporcionamos las herramientas necesarias para que puedas satisfacer los requisitos de elaboración de informes y cumplimiento de normas de tu organización. Puedes ver más información al respecto en el Apéndice 1. Nuestros principios de confianza, por otra parte, son claros en lo que concierne a nuestros compromisos en materia de privacidad y en cuanto a lo que puedes esperar a la hora de proteger y gestionar tus datos en la nube.

La transparencia forma parte del ADN de Google y resulta clave en nuestros esfuerzos por lograr y mantener la confianza de los clientes. En Google Cloud tenemos la firme convicción de que la confianza se cimenta en la transparencia. Por eso, queremos dejar claros nuestros compromisos y las expectativas que puedes tener sobre nuestra responsabilidad compartida a la hora de proteger y gestionar tus datos en la nube. Nos esforzamos por crear un ecosistema de confianza, centrándonos en tres áreas clave: velar por la privacidad y la seguridad de los datos de nuestros clientes, asegurar la fiabilidad de nuestros servicios y establecer, así como mantener, los más altos estándares del sector en transparencia y seguridad.

Todo ello sin olvidarnos de proteger los datos de los servicios; es decir, la información que Google recoge o genera mientras proporciona o administra los servicios de Google Workspace, y que es esencial para asegurar la fiabilidad y la seguridad de esos servicios. Los datos de los servicios no incluyen Datos de los Clientes, sino la información sobre la configuración de seguridad, los detalles

operativos y la información de facturación. Tratamos estos datos de servicios con diversos fines, como hacer recomendaciones para optimizar el uso de Google Workspace o mejorar su rendimiento y funcionalidad. Estos fines se detallan en la nueva versión del Aviso de Privacidad de Google Cloud que



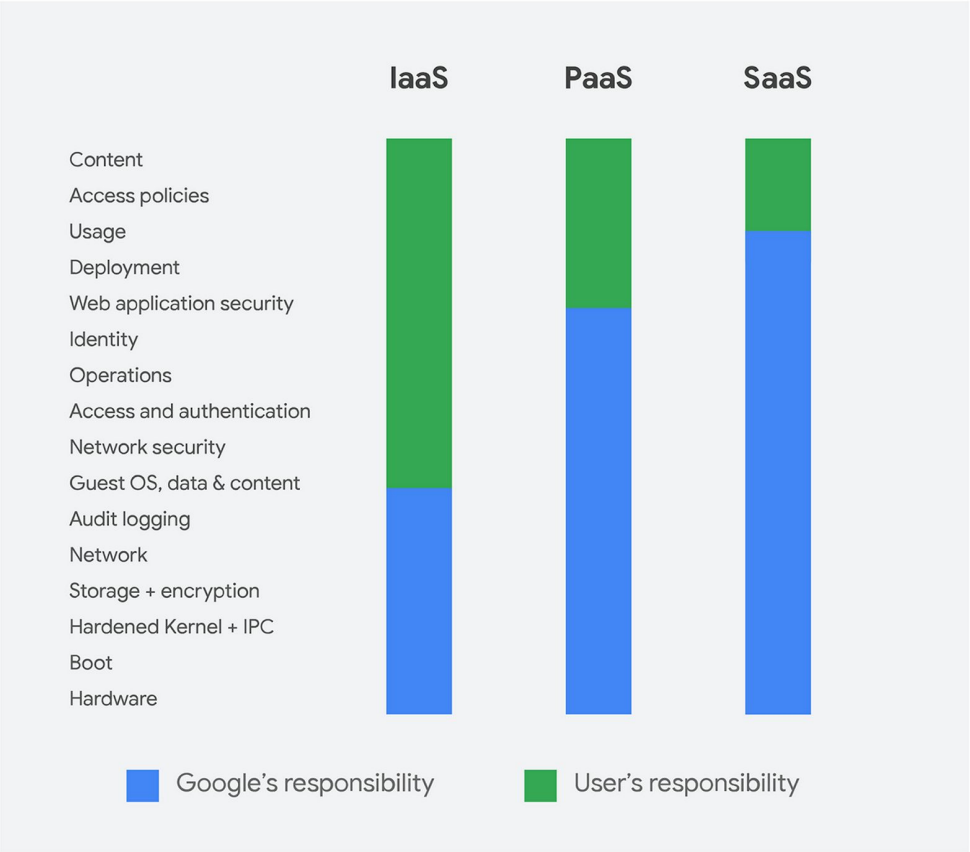
acabamos de publicar.

Modelo de Responsabilidad Compartida de Google

La protección de los datos no es solo responsabilidad de las empresas que utilizan los servicios de Google Workspace ni solo de Google como proveedor de esos servicios. Proteger los datos en la nube es, de hecho, una responsabilidad compartida, una colaboración entre el cliente y el proveedor de servicios en la nube.

En el Modelo de Responsabilidad Compartida de Google se describen visualmente las diversas responsabilidades relacionadas con la seguridad de la que somos conjuntamente responsables nosotros y nuestros clientes. Google Workspace es una solución de software como servicio (SaaS) en la que prácticamente todo, excepto el contenido y su política de acceso, es responsabilidad de los proveedores de servicios en la nube. En el modelo SaaS, estos proveedores gestionan toda la infraestructura física y virtual, así como la plataforma, a la vez que proporcionan las aplicaciones y los servicios basados en la nube que consumen los clientes. Las aplicaciones de Internet que se ejecutan directamente en un navegador web o en aplicaciones móviles son ejemplos de aplicaciones SaaS. Con este modelo, los clientes no tienen que instalar ni actualizar aplicaciones, como tampoco dar asistencia sobre ellas; únicamente gestionan las políticas de acceso al sistema y a los datos.

Importante: Como cliente de Google Workspace, tienes la responsabilidad de proteger los elementos que tú proporcionas o controlas, como el contenido que publicas en los servicios de Google Workspace, así como de controlar el acceso de tus usuarios.



Puedes usar el Modelo de Responsabilidad Compartida como guía para proteger los Datos de tus Clientes en Google Workspace. Según se determina en diversos reglamentos de protección de datos, tienes la responsabilidad de establecer los controles de seguridad que deben proteger los Datos Personales de los Clientes que obren en tu poder y, asimismo, tienes la responsabilidad de supervisar el tratamiento de esos Datos Personales, supervisar el acceso a los datos, asegurar su precisión y gestionar su ciclo de vida.

Google protege la infraestructura subyacente en Google Workspace en todo el ciclo de vida de tratamiento de la información. La seguridad está presente en todas las capas: la de hardware, la de comunicación entre los servicios, la de gestión del acceso entre los servicios, la del almacenamiento de datos, la de la comunicación en Internet y la del área operativa. Para obtener más información sobre este tema, consulta el informe sobre el diseño de la seguridad en la infraestructura de Google.

Servicios de Google

En esta sección, te ofrecemos una visión general de algunos de los servicios que Google te proporciona, incluidos los Servicios Principales de Google Workspace, funciones integradas, Servicios Adicionales, Cuenta de Google gestionada por la organización y servicios de asistencia técnica.

- **Servicios Principales de Google Workspace**: servicios incluidos y descritos en el resumen de servicios
- **Funciones Integradas en los Servicios Principales de Google**: incluidas en los Servicios Principales de Google Workspace y disponibles de forma automática para todos los usuarios de Google Workspace
- **Comentarios**: las correcciones ortográficas y gramaticales sugeridas y los comentarios incluidos en los productos están sujetos a la Política de Privacidad de Google
- **Servicios Adicionales**: no se venden como parte de la oferta de Google Workspace, y pueden ser cualquier servicio de Google que se pueda utilizar en una Cuenta de Google gestionada por una organización. Puedes consultar una lista no exhaustiva de los Servicios Adicionales de Google aquí
- **Cuenta de Google gestionada por la organización**: para usar Google Workspace, necesitas una Cuenta de Google gestionada por tu organización (distinta de tu Cuenta de Google personal) y que será gestionada por un administrador
- **Servicios de Asistencia Técnica**: los administradores de Google Workspace pueden ponerse en contacto con Google para recibir servicios de asistencia técnica por teléfono, correo electrónico o chat

Servicios Principales de Google Workspace

Los Servicios Principales de Google Workspace son aquellos incluidos y descritos en el resumen de servicios de los Términos del Servicio de Google Workspace, como Gmail, Documentos, Hojas de cálculo y Presentaciones. Esos servicios son los que se proporcionan a los clientes con Contrato de Google Workspace.[5]

La Adenda sobre Tratamiento de Datos de Google Workspace determina, según corresponda[6], cómo trata Google los Datos de los Clientes en los Servicios Principales. Los Datos de los Clientes son aquellos que las organizaciones y sus usuarios proporcionan a Google para su tratamiento en los Servicios Principales de Google Workspace, incluidos los Datos Personales de los Clientes, según se definen en la Adenda sobre Tratamiento de Datos. Como cliente, puedes aceptar la Adenda sobre Tratamiento de Datos en la consola de administración de Google si estás fuera de Europa y consideras que satisface los requisitos que debes cumplir.

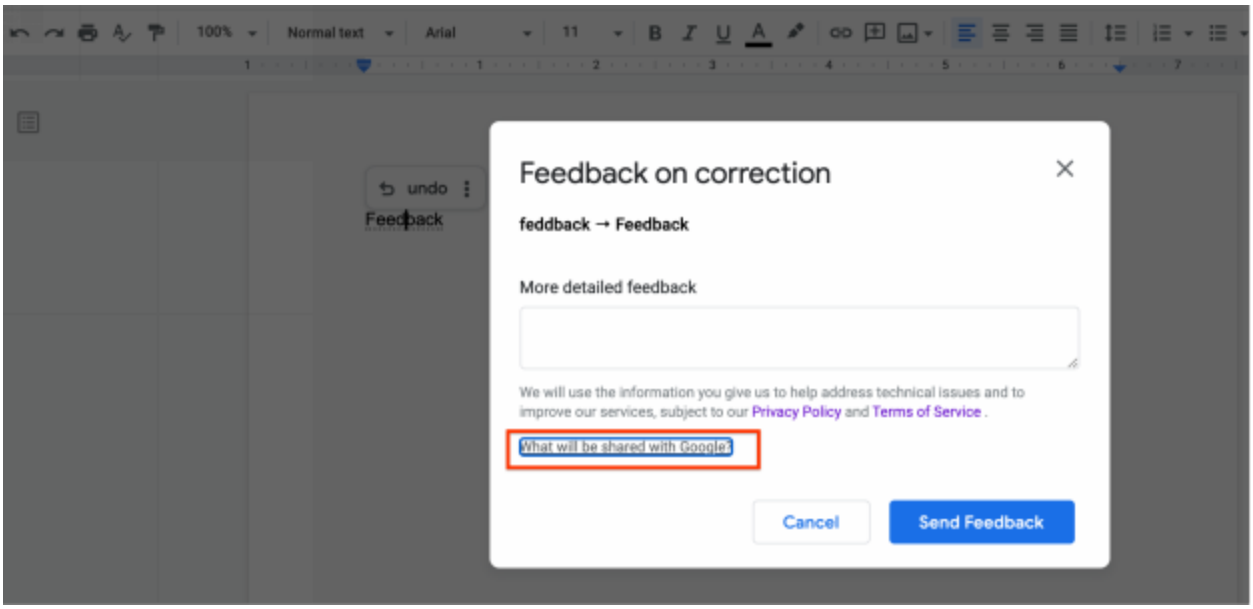
Funciones integradas en los Servicios Principales de Google Workspace

Los Servicios Principales incluyen diversas funciones, como la revisión ortográfica y gramatical, Explorar, la integración de la ubicación geográfica en el calendario y el Traductor. Estas funciones están integradas en los Servicios Principales de Google Workspace y todos los usuarios de esta solución pueden hacer uso de ellas directamente. Google se encarga del tratamiento de los Datos Personales de Clientes que se reciben por medio de las funciones integradas en los Servicios Principales de Google Workspace. Estas funciones se rigen por la Adenda sobre Tratamiento de Datos de Google Workspace cuando se usan en combinación con los Servicios Principales de esta solución.

Los usuarios pueden desactivar algunas funciones integradas; por ejemplo, pueden desactivar la corrección automática y las sugerencias en la revisión ortográfica y gramatical de Documentos de Google y Gmail. También pueden decidir que no quieren usar las funciones integradas, como "Traducir documento" y Explorar. Ten en cuenta que, si se usa Explorar para desplazarse a un sitio web de terceros, el uso de este sitio web no está sujeto a las protecciones de la Adenda sobre Tratamiento de Datos de Google Workspace.

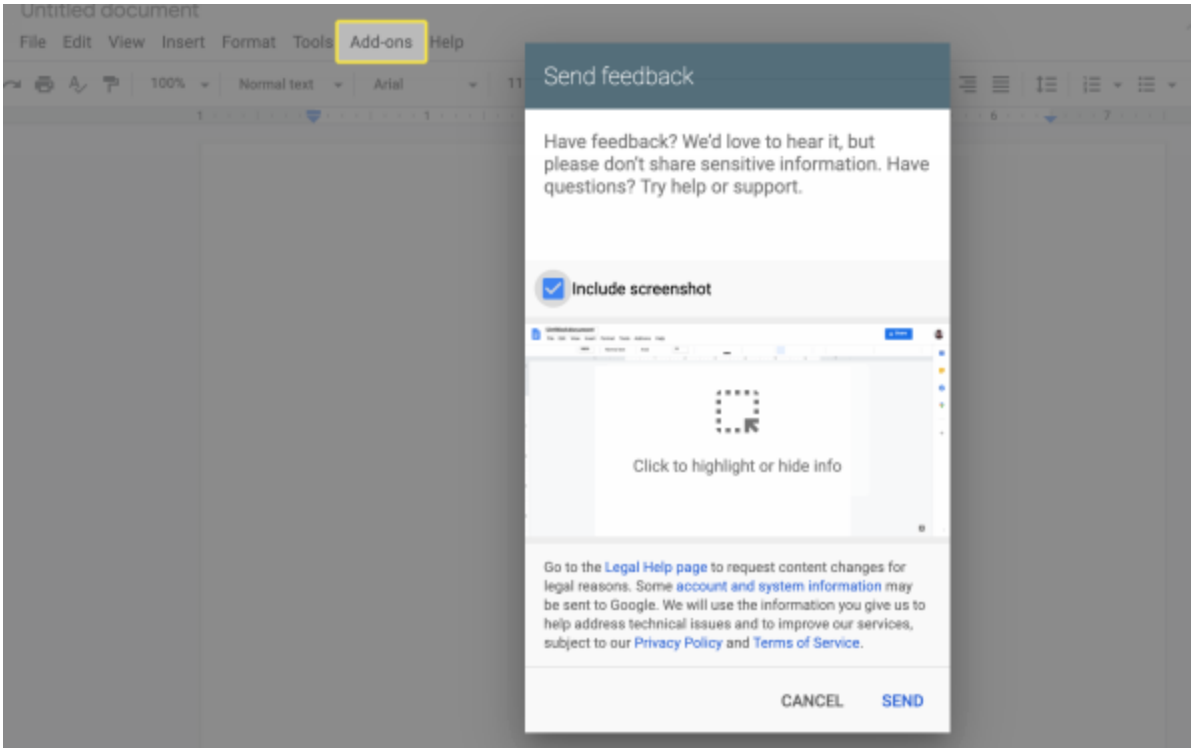
Comentarios

Los usuarios pueden aportar comentarios sobre las correcciones ortográficas y gramaticales que se sugieren, como puedes ver en el ejemplo siguiente. Es importante señalar que los Datos de Clientes no se usan para mejorar los servicios de ortografía y gramática de otras cuentas de clientes.



Los usuarios también tienen la opción de aportar comentarios en el producto e incluir capturas de pantalla relacionadas con un problema que se encuentren. En este caso, disponen de una herramienta

para ocultar la información sensible. **Ten en cuenta que cualquier comentario que se aporte voluntariamente por medio de nuestras herramientas de sugerencias se tratará de acuerdo con la Política de Privacidad de Google. Los usuarios verán un aviso de estos términos en cada punto donde puedan introducir comentarios.** Google actúa como controlador de la información que recoge a través de los comentarios sobre correcciones de ortografía y gramática y de los comentarios incluidos en los productos.



Servicios Adicionales

Los Servicios Adicionales no se venden como parte de la oferta de Google Workspace; cualquier servicio de Google que se pueda usar con una Cuenta de Google gestionada por una organización puede ser un servicio adicional. Tienes una lista no exhaustiva de estos Servicios Adicionales de Google en el artículo Servicios adicionales de Google. **Dado que estos servicios y productos no forman parte de la oferta de Google Workspace, no están sujetos al Contrato ni a la Adenda sobre Tratamiento de Datos de esta solución.**

Para que los clientes de Google Workspace disfruten de una experiencia fluida, pueden acceder a los Servicios Adicionales de Google con su Cuenta de Google gestionada por la organización. Tal y como se describe en la página de Servicios Adicionales, la mayoría de estos servicios se rigen por los Términos del Servicio de Google y su Política de Privacidad. Además, algunos Servicios Adicionales también están sujetos a términos propios. Para revisar estos términos, consulta la sección "Servicios con control de activación o desactivación propio" del artículo Servicios adicionales de Google.

Importante: Por motivos de cumplimiento, es posible que los administradores de Google Workspace deban impedir que sus usuarios accedan a los Servicios Adicionales cuando hayan iniciado sesión con su Cuenta de Google gestionada por la organización.

Los administradores pueden controlar los Servicios Adicionales a los que tendrán acceso los usuarios cuando hayan iniciado sesión con su Cuenta de Google gestionada por la organización. Solo tienen que activar o desactivar cada servicio para esos usuarios en la consola de administración de Google. Estos ajustes se pueden definir antes de que el administrador aprovisione las cuentas de usuario. Para saber cómo hacerlo, consulta la sección "Activar o desactivar servicios en cuentas de usuario" del artículo Servicios adicionales de Google. Además de gestionar individualmente Google Workspace y otros servicios de Google con un control de activación o desactivación en la consola de administración, los administradores pueden gestionar el acceso a otros servicios de Google que no están incluidos en la lista y no disponen de este control, como Chromecast y Google Surveys. Puedes consultar los detalles sobre cómo activar o desactivar estos servicios en el artículo sobre cómo gestionar los servicios que no se pueden controlar individualmente.

Nota: Aunque un administrador de Google Workspace haya inhabilitado el acceso a los Servicios Adicionales de los usuarios que hayan iniciado sesión, estos podrán acceder y usarlos igualmente si no se identifican. Por ejemplo, si el administrador ha inhabilitado YouTube en la organización desde la consola de administración, los usuarios que no inicien sesión podrán usar el servicio. Sin embargo, los que inicien sesión con su Cuenta de Google gestionada por la organización no podrán usarlo. En ese caso, Google no tratará los datos que puedan vincularse a la Cuenta de Google gestionada por la organización del usuario.

Te recomendamos que el Asesor Legal, el Delegado de Protección de Datos o la persona que ocupe el cargo equivalente lleve a cabo, si procede, una evaluación del impacto que supone el tratamiento de Datos Personales de Clientes con estos productos, para determinar si tu organización puede cumplir con sus obligaciones como responsable o encargada del tratamiento de datos, según corresponda, de cada uno de estos productos y, en caso afirmativo, cómo puede hacerlo.

Cuenta de Google gestionada por la organización

Para que los miembros de tu organización utilicen los servicios de Google Workspace que hayas habilitado, debes proporcionar a cada persona una cuenta de usuario. Con las Cuentas de Google gestionadas por la organización, los usuarios tendrán un nombre y una contraseña para iniciar sesión en los servicios de Google, así como una dirección de correo electrónico de tu dominio y un perfil. Los usuarios pueden proporcionar información directamente, como cuando indican un nombre y eligen una imagen de perfil, o indirectamente, como cuando Google recoge información sobre el inicio de sesión de un usuario: el momento en que lo hace, con qué finalidad y en qué contexto (aplicación o Web, plataforma y dispositivo). Cuando un usuario inicia sesión en la nueva Cuenta de Google gestionada por la organización que has creado, recibe un aviso en el que se le explica cómo se recogen sus datos y cómo su administrador accede a ellos. También se le indica que el uso que haga de los Servicios Principales de Google Workspace está sujeto a los términos de Google Workspace de la organización. El usuario deberá aceptar el aviso antes de usar una Cuenta de Google gestionada por la organización. En el aviso se explica que el uso de los Servicios Adicionales cuando se utiliza la Cuenta de Google gestionada por la organización se regirá por la Política de Privacidad de Google, los Términos del

Servicio de Google y los términos específicos del servicio correspondiente. Para obtener más información sobre la creación de las Cuentas de Google gestionadas por una organización, consulta Opciones para añadir usuarios.

Servicios de Asistencia Técnica

Los administradores de Google Workspace disponen de asistencia online, por chat y por teléfono. Los datos que se recogen y se tratan como parte de los servicios de asistencia técnica relacionados con el uso de los Servicios Principales de Google Workspace están sujetos a las Directrices de los Servicios de Asistencia Técnica de Google Workspace y al Aviso de Privacidad de Google Cloud . Google recoge y trata los datos para ofrecer los servicios de ayuda que se describen en esas Directrices y para mantener estos Servicios. Según lo establecido en el contrato o en las Directrices de los Servicios de Asistencia Técnica de Google Workspace, Google no tiene ninguna obligación de ofrecer asistencia para los Servicios Adicionales.

Prácticas recomendadas sobre privacidad

En esta sección te ofrecemos algunas prácticas recomendadas que puedes aplicar para personalizar los servicios de Google Workspace, de modo que puedas cumplir con los requisitos de protección de datos de tu organización. Ten en cuenta que esta no es una lista completa ni detallada de todas las prácticas posibles. La información incluida en esta guía no constituye ningún asesoramiento de carácter jurídico, por lo que te recomendamos que recurras a una persona experta en cuestiones legales o al delegado de protección de datos de tu organización para que te orienten sobre los requisitos específicos aplicables a tu organización.

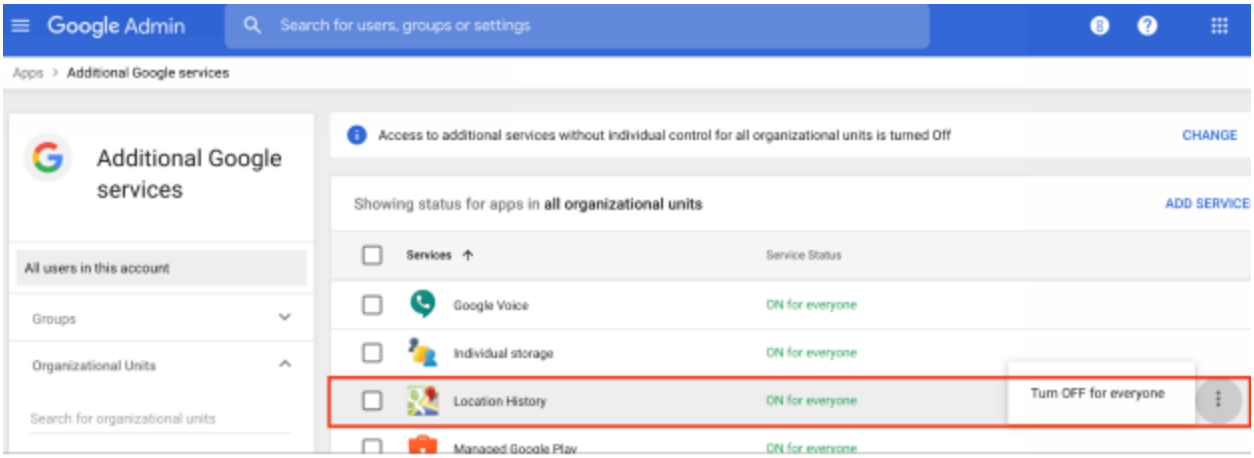
Decide qué Servicios Adicionales habilitas para tus usuarios

Los Servicios Adicionales no forman parte de la oferta de Google Workspace ni están sujetos al Contrato ni a la Adenda sobre Tratamiento de Datos de Google Workspace. Todos los Servicios Adicionales están habilitados de manera predeterminada en la consola de administración. Te recomendamos que elijas detenidamente qué Servicios Adicionales (por ejemplo, YouTube, Maps y Blogger) activarás o desactivarás como administrador para tus usuarios, en especial si se aplican restricciones de edad o si se ocupan de datos sensibles o sujetos a normativas (por ejemplo, datos del sector financiero, sanitario o gubernamental). Consulta la sección "Servicios Adicionales" de esta guía para obtener más información.

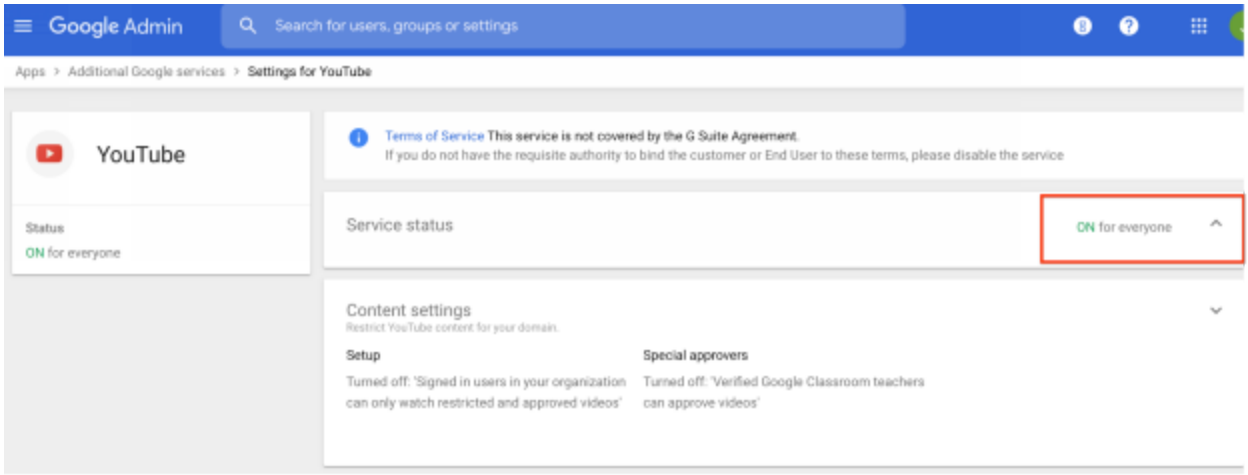
Ayuda a tus usuarios con sus controles de la actividad de privacidad

Recomienda a los usuarios que acepten los controles de la actividad que satisfagan las políticas de privacidad de la empresa y sus necesidades personales. Si no quieren que Google almacene el historial de su actividad y les ofrezca una experiencia de usuario personalizada en la Cuenta de Google gestionada por la organización, indícales que desactiven determinados ajustes de la página Controles de la actividad de tu cuenta. Para obtener más información, consulta las instrucciones y directrices que se indican a continuación.

- **Historial de ubicaciones:** Elige si activas o desactivas el historial de ubicaciones en las Cuentas de Google gestionadas por la organización de tus usuarios. De forma predeterminada, esta opción está desactivada para los usuarios. El historial de ubicaciones solo se puede activar si lo has habilitado en la consola de administración de Google y si los usuarios lo han habilitado también. En la consola de administración, ve a *Aplicaciones > Servicios adicionales de Google > Historial de ubicaciones*. Indica a tus usuarios que pueden activar o desactivar el historial de ubicaciones en su Cuenta de Google gestionada por la organización, en la página Controles de la actividad de tu cuenta. Puedes consultar las instrucciones dirigidas a los usuarios en el artículo Gestionar el historial de ubicaciones.



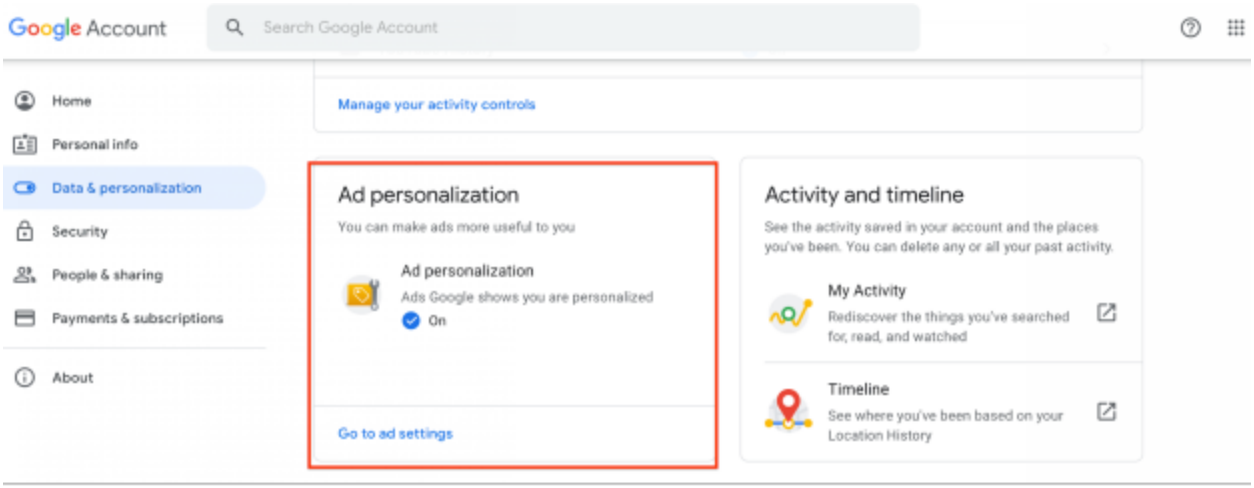
- **Historial de YouTube:** Elige si activas o desactivas YouTube para los usuarios. En la consola de administración, ve a *Aplicaciones > Servicios adicionales de Google > YouTube*. Cuando hayas activado YouTube en la consola de administración, cada usuario podrá activar o desactivar en su cuenta la opción **Historial de YouTube**, en la página Controles de la actividad de tu cuenta. Si el historial está desactivado, no se usará para mejorar las recomendaciones que se hagan a los usuarios ni se guardarán los vídeos que estos vean. Puedes consultar las instrucciones dirigidas a los usuarios en el artículo Ver, borrar o poner en pausa el historial de reproducciones.



- **Personalización de anuncios:** Los anuncios se basan en la información personal que cada usuario añade a su Cuenta de Google gestionada por la organización, en los datos de los anunciantes asociados a Google y en los intereses de usuario que determina Google. Si la opción "Personalización de Anuncios" está activada, el usuario disfruta de una experiencia de anuncios adaptada a sus intereses. Los usuarios pueden activar o desactivar este ajuste en la página Controles de la actividad de tu cuenta. Si la opción "Personalización de Anuncios" está desactivada, Google no usa la información de los usuarios para personalizar los anuncios que les muestra. Indica a los usuarios que pueden activar o desactivar la opción Personalización de

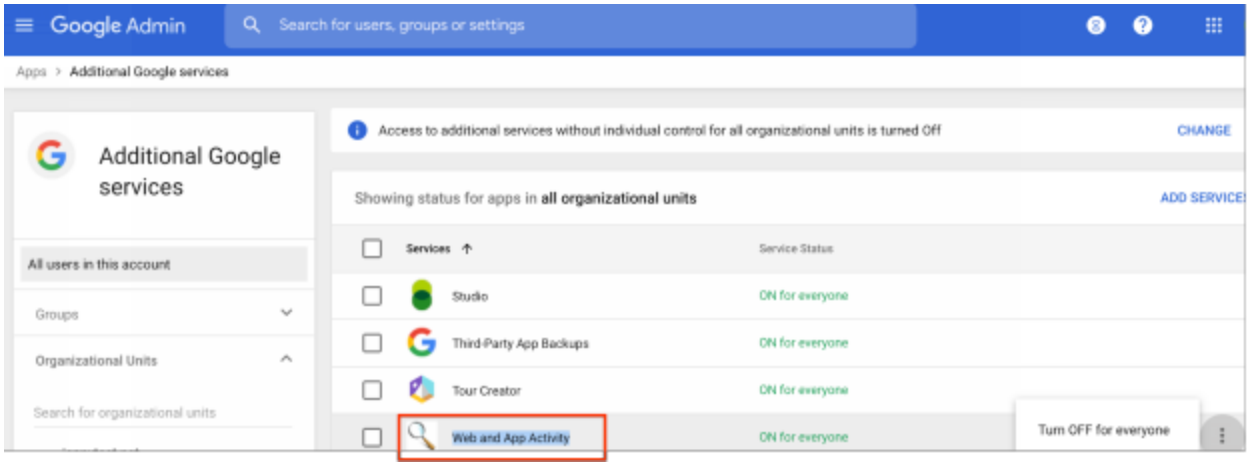
Anuncios en la página Controles de la actividad de tu cuenta.

Nota: Google Workspace no utiliza los Datos de Clientes con fines publicitarios. La personalización de anuncios solo se aplica en servicios de Google que se ofrecen fuera de Google Workspace.



- **Actividad en la Web y en Aplicaciones:** Elige si activas o desactivas esta opción para los usuarios. En la consola de administración, ve a *Aplicaciones > Servicios adicionales de Google > Actividad en la Web y en Aplicaciones*. De forma predeterminada, este control de la consola está habilitado en la organización, pero el ajuste de los usuarios finales está desactivado. Si este servicio está activado en la organización, los usuarios finales pueden activarlo o desactivarlo. Si desactivas el control del servicio en tu organización desde la consola de administración, los usuarios no podrán activarlo en sus ajustes personales.

  Si un usuario activa la opción Actividad en la Web y en Aplicaciones en sus ajustes personales, en su Cuenta de Google gestionada por la organización se guardarán tanto las búsquedas como la actividad que haga en otros servicios de Google, lo que le permitirá disfrutar de una experiencia más personalizada. Los usuarios pueden ver y eliminar su actividad en la web y en las aplicaciones desde la página Controles de la actividad de tu cuenta. Puedes consultar las instrucciones dirigidas a los usuarios en Ver y controlar los datos de Actividad en la Web y en Aplicaciones.



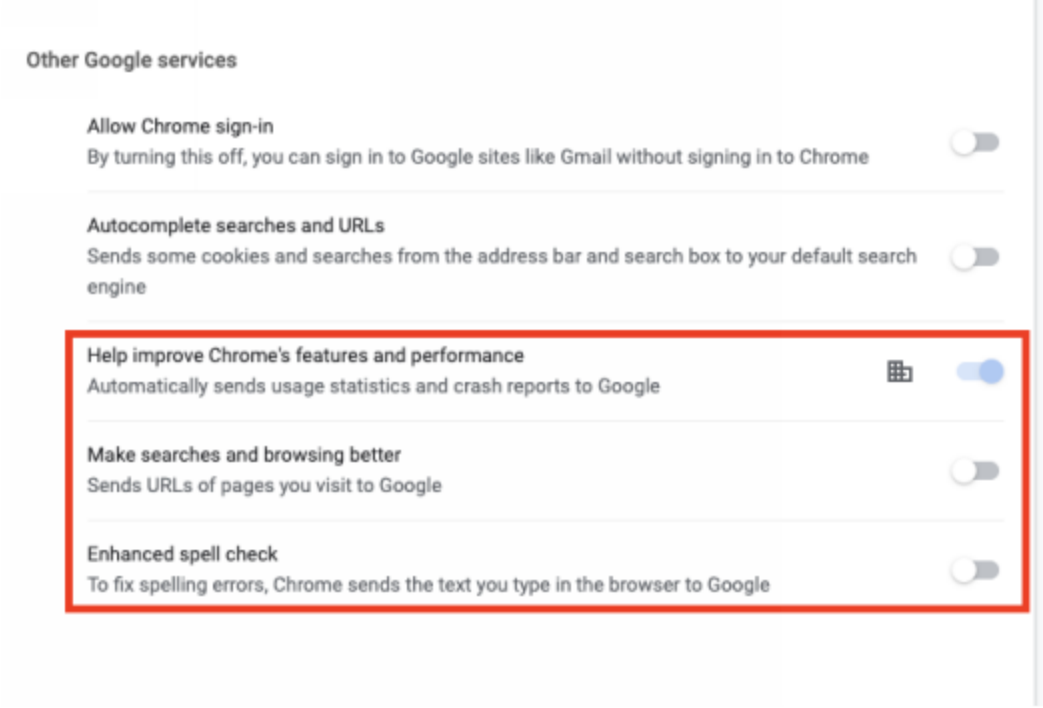
Controla qué usuarios pueden usar la sincronización de Chrome y recomienda otros ajustes de Chrome

La sincronización de Chrome permite a los usuarios guardar de forma segura los marcadores, el historial, las contraseñas y otros ajustes en las Cuentas de Google gestionadas por la organización y acceder a todo ello desde Chrome en cualquier dispositivo. Como administrador, puedes activar o desactivar la sincronización de Chrome para los usuarios. En la consola de administración, ve a *Servicios adicionales de Google > Sincronización de Google Chrome*. Si la sincronización de Chrome está activada, los usuarios pueden ver y actualizar en cualquier dispositivo la información sincronizada, como marcadores, historial, contraseñas y otros ajustes.

Además, los usuarios pueden elegir qué funciones de Google quieren utilizar en Chrome, como las siguientes:

- **Ayudar a mejorar las funciones y el rendimiento de Chrome:** La transmisión a Google de los informes sobre fallos y las estadísticas de uso está habilitada de forma predeterminada, pero los usuarios pueden deshabilitarla en los ajustes de Chrome. Las estadísticas de uso contienen información como preferencias, clics en botones, estadísticas de rendimiento y uso de la memoria. En general, estas estadísticas no incluyen las URL de páginas web ni datos personales. Sin embargo, si el usuario ha activado la opción *"Mejorar las búsquedas y la navegación"* en los ajustes de Chrome, las estadísticas de uso sí incluirán información sobre las páginas web que visita y el uso que hace de esas páginas. Si la sincronización de Chrome está habilitada, también se puede combinar la información de edad y sexo indicada en la Cuenta de Google gestionada por la organización del usuario con las estadísticas, para ayudarnos a mejorar los productos que ofrecemos a los distintos grupos demográficos. Esta información no identifica de modo personal al usuario y solo se usa como dato agregado. Los informes sobre fallos contienen información del sistema recogida en el momento del bloqueo. Pueden incluir las URL de páginas web o información personal, según lo que estuviera ocurriendo en el momento de producirse el error. Puedes sugerir a los usuarios que activen o desactiven este ajuste en función de sus

necesidades personales y de la política de la empresa. Puedes consultar las instrucciones dirigidas a los usuarios en el artículo Iniciar o detener la generación automática de informes sobre errores y bloqueos.



- **Revisión ortográfica mejorada:** La revisión ortográfica básica utiliza un diccionario local, en tanto que la opción mejorada se basa en la nube y envía el texto que los usuarios escriben a Google. De forma predeterminada, está activada la revisión básica para los usuarios. Si quieren habilitar la opción mejorada, pueden hacer clic en el menú de Chrome y, a continuación, en *Configuración > Configuración avanzada > Idiomas*. Si está habilitada la revisión ortográfica mejorada, Chrome envía el contenido de los campos de texto a medida que se escribe a Google, junto con el idioma predeterminado del navegador. Ten en cuenta que esta revisión mejorada no forma parte de los Servicios Principales de Google Workspace y, por tanto, no está sujeta al Contrato ni a la Adenda sobre Tratamiento de Datos de Google Workspace. Los datos que la revisión ortográfica mejorada envía a Google se tratan de acuerdo con la Política de Privacidad de Google, los Términos del Servicio de Google y los Términos del Servicio Adicionales de Chrome y Chrome OS.

Si en tu organización es necesario establecer un control más estricto de los ajustes de Chrome y controlar los datos que se comparten con Google y con terceros mediante Chrome, puedes usar Chrome Enterprise. Con este servicio, los administradores tienen opciones para definir diversas políticas de privacidad para la organización. Por ejemplo, pueden configurar la política Informes de métricas para que los usuarios de la organización no puedan enviar a Google datos relacionados con bloqueos ni informes anónimos sobre el uso de la aplicación. Los administradores también pueden inhabilitar o habilitar los servicios de revisión ortográfica mejorada en la organización. Para obtener más

información, consulta el documento sobre gestión en la nube del navegador Chrome y la guía de configuración de la seguridad empresarial en el navegador Chrome.

Separa el acceso de los usuarios dentro del dominio

Como administrador, puedes crear unidades organizativas para gestionar el acceso de los usuarios a diferentes conjuntos de Servicios y Productos Adicionales de Google Workspace. De este modo, puedes separar en diferentes grupos a los usuarios que gestionan datos personales o sensibles y a los que no manejan este tipo de datos. Después de configurar las unidades organizativas, puedes activar o desactivar servicios o productos específicos para distintos grupos de usuarios.

Por ejemplo, el departamento de Recursos Humanos (RR. HH.) puede gestionar datos personales o sensibles, pero puede que solo algunos miembros tengan que acceder realmente a ellos. En este caso, puedes configurar una unidad organizativa de RR. HH. que incluya a los usuarios que utilizan los Servicios Principales de Google Workspace con datos personales o sensibles, en la que determinados servicios estén deshabilitados o diversos ajustes estén configurados según lo que necesites.

Recomienda a los usuarios que mantengan separadas la Cuenta de Google gestionada por la organización y su cuenta personal

Recomendamos que los usuarios mantengan separadas la Cuenta de Google gestionada por la organización y su cuenta personal de Google. Te recomendamos que, como administrador, sugieras a los usuarios que no inicien sesión simultáneamente en varias cuentas de Google desde la misma instancia del navegador Chrome. Así se reduce el riesgo de que se produzcan errores humanos que lleven a almacenar accidentalmente Datos de Clientes en la cuenta personal de un usuario o a aplicar ajustes de privacidad de una cuenta personal de Google en la cuenta de Google gestionada de la organización.

Si la organización necesita aplicar un control más estricto, puedes impedir que los usuarios inicien sesión en los servicios de Google con cuentas que no les has facilitado. Por ejemplo, puede que no quieras que los usuarios utilicen su cuenta personal de Gmail o una Cuenta de Google gestionada por la organización de otro dominio. Para obtener instrucciones, consulta Bloquear el acceso de cuentas de consumidor.[7]

También puedes gestionar de forma segura las aplicaciones y los datos de trabajo de los dispositivos Android, dejando las aplicaciones y los datos personales bajo el control del usuario. En los dispositivos Android se pueden configurar perfiles de trabajo[8] para separar las aplicaciones y los datos de trabajo de los personales. Consulta más información sobre cómo configurar el perfil de trabajo y cómo incluir las aplicaciones de trabajo preferidas en una lista de aplicaciones permitidas en dispositivos Android.

Revisa las recomendaciones sobre el estado de la seguridad

Puedes revisar las recomendaciones que se incluyen en la página sobre el estado de la seguridad de la consola de administración para mejorar la seguridad y la protección de los datos de tu organización. También puedes consultar la lista de comprobación de seguridad para medianas y grandes empresas en el Centro de Ayuda para administradores de Google Workspace.

Los administradores disponen también de muchas herramientas potentes y pueden personalizar los ajustes individuales de seguridad para adaptarlos a las necesidades de su empresa. Por ejemplo, el Centro de alertas de Google Workspace proporciona alertas y consejos sobre seguridad relacionados con la actividad en tu dominio para que puedas tomar medidas y proteger a tu organización ante las nuevas amenazas para la seguridad, como la suplantación de identidad (phishing) y la actividad sospechosa en un dispositivo. La herramienta de investigación de seguridad te permite identificar y clasificar problemas de seguridad y privacidad en tu dominio, y tomar medidas al respecto. También puedes crear reglas de actividad en la herramienta de investigación; estas reglas automatizan acciones para detectar y solucionar estos problemas de forma más rápida y eficaz. Google Vault es otra herramienta que puedes usar para conservar, bloquear, buscar y exportar datos, y responder así a las necesidades de conservación y descubrimiento electrónico de la organización. Estas y muchas otras herramientas de seguridad están disponibles y se explican en la página de seguridad de Google Workspace.

Revisa el uso que se hace en tu organización de las aplicaciones de terceros

En algunos Servicios Principales de Google Workspace, la configuración del dominio puede permitir que un usuario comparta Datos Personales de Clientes con una persona ajena a la organización o con una aplicación externa. Los clientes son responsables de asegurar que cuentan con las medidas adecuadas y válidas de protección ante terceros antes de compartir o transmitir Datos Personales de Clientes. Tu organización debe determinar si hay que aplicar otras condiciones de protección de los datos antes de compartir datos personales o sensibles con terceros por medio de los servicios de Google Workspace o de las aplicaciones que se integran con ellos.

Como administrador, dispones de tres opciones a la hora de gestionar Google Workspace Marketplace: puedes prohibir la instalación de todas las aplicaciones, dejar que se instalen solo las aplicaciones permitidas o dejar que se instale cualquier aplicación. De forma predeterminada, se permite que los usuarios de Google Workspace instalen todas las aplicaciones disponibles en Google Workspace Marketplace. Te recomendamos que revises la política de la empresa y que permitas instalar solo aplicaciones de terceros seleccionadas que puedan acceder a ámbitos de API en los servicios de Google Workspace.

Con el control de acceso de aplicaciones, puedes establecer en mayor medida qué aplicaciones de terceros y del dominio tienen acceso a los datos sensibles de Google Workspace. Al usar el control de acceso de aplicaciones, puedes hacer lo siguiente:

- Restringir el acceso a la mayoría de los servicios de Google Workspace o dejarlos sin restricciones.
- Dar permiso a aplicaciones concretas para que puedan acceder a servicios restringidos de Google Workspace.
- Dar permiso a todas las aplicaciones que pertenezcan a un dominio.

El acceso a los Datos de los Clientes está habilitado de forma predeterminada en las aplicaciones instaladas desde Marketplace. Te recomendamos que revises la política de la empresa y que cambies el ajuste para restringir o limitar el acceso a los Datos de los Clientes de Google Workspace si es necesario.

Supervisa la actividad de las cuentas

Los informes y los registros de auditoría disponibles en la consola de administración te permiten detectar fácilmente posibles riesgos para la seguridad, medir el nivel de colaboración de los usuarios, averiguar quién inicia sesión y cuándo lo hace, y analizar la actividad de los administradores, entre otras muchas acciones. Para supervisar los registros, los administradores pueden configurar notificaciones para recibir alertas cuando se detecten determinadas actividades, como intentos de inicio de sesión sospechosos, usuarios suspendidos por un administrador, nuevos usuarios añadidos, usuarios suspendidos que se han activado, usuarios eliminados, cambios de contraseña hechos por un administrador, usuarios a los que se les asigna un privilegio de administrador y usuarios a los que se les revoca ese privilegio. El administrador también puede revisar los informes y los registros de auditoría periódicamente para detectar posibles riesgos para la seguridad. Concretamente, la revisión de las tendencias clave de la sección Destacado, de la exposición a la quiebra de seguridad de los datos, de los archivos creados en la actividad de uso de las aplicaciones, de la actividad de las cuentas y de las auditorías ofrecen detalles útiles sobre los riesgos para la seguridad.

Si los registros de auditoría del administrador proporcionan información sobre las acciones hechas por los miembros de tu organización, la opción Transparencia de acceso[9] proporciona registros de las acciones efectuadas por el personal de Google. En estos registros se incluye información sobre el recurso al que se ha accedido, la acción que se ha llevado a cabo, la hora de la acción y el motivo (por ejemplo, el número de caso asociado a una solicitud al servicio de asistencia).

Establece políticas de privacidad para los nombres de archivo y de ruta

Como medida de seguridad adicional para restringir que se compartan Datos Personales de Clientes, te recomendamos que establezcas políticas para impedir que los usuarios incluyan información sensible

al asignar nombres a los archivos y organizarlos en los Servicios Principales de Google Workspace (por ejemplo, Documentos, Hojas de cálculo, Presentaciones, Formularios, Drive, Gmail), o bien al asignar un nombre que utilice información personal sensible a una sala de Google Chat o una invitación de Meet. Entre los Datos Personales de Clientes sensibles se encuentran el nombre completo, la dirección de correo electrónico, la dirección postal o el número de teléfono de una persona, o bien los identificadores de cuenta únicos, como el ID de cliente, el ID de proyecto y el nombre de pantalla.

También puedes aprovechar las funciones de Prevención de la pérdida de datos (DLP) que se incluyen en Google Workspace para inspeccionar, clasificar y desidentificar datos sensibles, contribuyendo así a limitar la exposición a los riesgos. Consulta Evitar la pérdida de datos con la nueva versión de DLP de Drive y Analizar el tráfico de correo electrónico con reglas de Prevención de la pérdida de datos. Ponemos a tu disposición una biblioteca de detectores de contenido predefinidos que te ayudarán con la configuración. Por ejemplo, una vez que se defina la política de DLP, Gmail puede comprobar automáticamente todo el correo saliente en busca de información sensible y actuar directamente para evitar la filtración de datos: puede poner en cuarentena el correo electrónico para que se revise, pedir a los usuarios que modifiquen información o evitar que se envíen mensajes e informar de ello al remitente. Las reglas fáciles de configurar y el reconocimiento óptico de caracteres (OCR) del contenido almacenado en imágenes de DLP para Drive permiten a los administradores auditar con facilidad los archivos que incluyen contenido sensible o configurar reglas para advertir a los usuarios de posibles riesgos y para impedirles compartir datos confidenciales con personas ajenas a la organización. Si quieres obtener más información sobre el tema, consulta el informe sobre DLP.

Recursos adicionales

Queremos facilitar a nuestros clientes sus labores de cumplimiento y generación de informes relacionados con la privacidad, por lo que ponemos a su disposición instrucciones y prácticas recomendadas sobre privacidad y ofrecemos un acceso sencillo a documentación que trata estas cuestiones. Nuestros productos se someten regularmente a controles independientes de seguridad, privacidad y cumplimiento, lo que nos permite obtener certificaciones que demuestran su conformidad con diversos estándares internacionales que nos hacen merecedores de tu confianza. Puedes consultar una lista de los estándares, las normativas y las certificaciones de Google Workspace en nuestro Centro de recursos para el cumplimiento.

Puedes acceder en todo momento y de forma sencilla a estos recursos esenciales sobre cumplimiento desde el Administrador de informes de cumplimiento, sin coste adicional. Entre los recursos clave se incluyen nuestros últimos certificados ISO/IEC, los informes sobre los estándares de cumplimiento y los autodiagnósticos. Es posible que tengas que iniciar sesión con tu cuenta de Google Cloud Platform o Google Workspace para acceder a algunos recursos.

Para obtener más información sobre cómo se han diseñado los servicios de Google Workspace teniendo presentes la privacidad, la confidencialidad, la integridad y la disponibilidad de los datos, consulta los siguientes recursos:

- **Privacidad de Google Cloud**: Incluye la lista de principios de confianza de Google Cloud.
- **Página Seguridad de Google Workspace**: Esta página principal de la seguridad de Google Cloud incluye enlaces a informes sobre la seguridad y otros recursos sobre productos relacionados con la privacidad, la transparencia, la infraestructura y la seguridad.
- **Centro de Ayuda para administradores de Google Workspace**: Esta página principal incluye enlaces a las instrucciones y la documentación técnica relacionada con los productos y las funciones de seguridad de Google Workspace.
- **Centro de recursos sobre el RGPD**: Incluye información sobre normativas, cumplimiento y productos que te puede ayudar a cumplir con el RGPD.
- **Centro de recursos de seguridad**: Incluye informes, vídeos, artículos, entradas de blog y documentación sobre cuestiones relacionadas con la privacidad y la seguridad.

Apéndice 1: Asignación de controles de privacidad

Esta asignación de controles de privacidad es una forma rápida de evaluar qué necesitas para cumplir con los requisitos de las diversas normativas de privacidad cuando usas Google Workspace. Ten en cuenta que esta no es una lista completa de todos los controles de privacidad, sino que está pensada para ofrecer una perspectiva general. La información incluida en esta guía no constituye ningún asesoramiento de carácter jurídico, por lo que te recomendamos que recurras a una persona experta en cuestiones legales para que te oriente sobre los requisitos que se aplican específicamente a tu organización.

Consideraciones sobre el responsable de tratamiento de datos

Controles habituales de privacidad	Responsabilidad del cliente	Funciones de apoyo en Google Workspace
Conocer la organización y su contexto	La organización tiene que determinar su rol, bien como responsable del tratamiento de la información personal identificable (IPI), bien como encargada del tratamiento de la IPI para identificar los requisitos que debe cumplir (normativos, etc.) al tratar Datos Personales de Clientes.	Consulta los roles y las responsabilidades del tratamiento de los Datos de los Clientes en la sección 5 de la Adenda sobre Tratamiento de Datos de Google Workspace.
Determinar si se debe obtener consentimiento de los usuarios y registrarlo	El cliente debe conocer los requisitos legales y normativos para obtener el consentimiento de las personas antes de tratar los Datos Personales de Clientes y debe registrar ese consentimiento cuando se necesite.	Google no ofrece opciones para obtener o registrar el consentimiento de los usuarios en todas las actividades. Cuando los usuarios inician sesión en la Cuenta de Google gestionada por la organización que has creado, reciben un aviso donde se les explica cómo se recogen sus datos y cómo el administrador puede acceder a ellos.
Identificar las bases jurídicas que legitiman el tratamiento de datos y documentar la finalidad	El cliente debe conocer los requisitos exigidos para que el tratamiento de datos sea legítimo; por ejemplo, si es necesario obtener antes el consentimiento del usuario. Además, debe documentar con qué finalidad se tratan los Datos	Google no ofrece ninguna opción para cumplir con las condiciones legales necesarias para tratar datos en todas las actividades. Si quieres conocer las actividades de tratamiento de datos que Google lleva a cabo y las finalidades de ese tratamiento, consulta los Términos del

	Personales de Clientes.	Servicio de Google Workspace y la Adenda sobre Tratamiento de Datos.
Contratos con los encargados del tratamiento de la IPI	El cliente debe asegurarse de que sus contratos con los encargados del tratamiento de la IPI incluyen los requisitos necesarios para cumplir con las obligaciones legales o normativas de tratamiento y protección de los Datos Personales de Clientes.	En su función como encargado del tratamiento de datos, Google te ayudará a cumplir con tus obligaciones (teniendo en cuenta la naturaleza del tratamiento de los Datos Personales de los Clientes y la información a disposición de Google), de acuerdo con la Adenda sobre Tratamiento de Datos. Consulta las secciones 7.1.4 (asistencia con la seguridad), 9.2.2 (asistencia con los derechos de los interesados) y 8.1 (asistencia con la EIPD) de la adenda para obtener más información.
Limitar la recogida y el tratamiento de los datos	El cliente debe conocer los requisitos sobre los límites en la recogida y el tratamiento de los Datos Personales de Clientes, como que la recogida y el tratamiento deben limitarse a los datos necesarios para la finalidad indicada.	Si quieres conocer las actividades de tratamiento de datos que Google lleva a cabo y las finalidades de ese tratamiento, consulta los Términos del Servicio de Google Workspace y la Adenda sobre Tratamiento de Datos.
Registros relacionados con el tratamiento de la IPI	El cliente debe mantener todos los registros obligatorios y necesarios relacionados con el tratamiento de los Datos Personales de Clientes.	Google Workspace ofrece registros de auditoría que dan visibilidad a las cuestiones relacionadas con el acceso a los datos y te ayudan a responder preguntas sobre quién hizo qué, dónde y cuándo. Entre los registros de auditoría disponibles tienes los registros de actividad de los administradores (registro de auditoría de la consola de administración), los registros de seguridad (inicio de sesión, SAML y Transparencia de acceso) y los registros sobre los servicios y las cuentas de los usuarios (búsqueda en el registro de correo electrónico y registro de auditoría de Drive). Para obtener más información sobre los registros de auditoría, consulta el artículo Registros de auditoría disponibles. Por lo general, los registros de auditoría se conservan durante seis meses; consulta los detalles en Plazos de conservación y periodos de retraso de los datos. Puedes personalizar la información que revisas en los registros de auditoría desde la consola de administración de Google; puedes filtrar los datos por usuario o actividad, unidad organizativa o fecha. También puedes configurar alertas para determinadas actividades.

Política y evaluación de la protección de los datos de la organización

Controles habituales de privacidad	Responsabilidad del cliente	Funciones de apoyo en Google Workspace
Revisión independiente de la seguridad de la información	El cliente debe poner en práctica un proceso de evaluación de los riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de la confidencialidad, la integridad y la disponibilidad de los datos. Este proceso puede incluir auditorías internas o externas, u otras medidas para evaluar la seguridad del tratamiento de los datos. Si una persona ajena a la organización u otra organización se ocupa de todo o parte del tratamiento de los datos, deberá poner en práctica también esas evaluaciones. El cliente, por su parte, deberá recoger la información sobre ellas.	Eres responsable del uso que haces de los servicios y del almacenamiento de las copias de los Datos de los Clientes que hagas fuera de los sistemas de Google o de los sistemas de los subencargados del tratamiento de Google. Google se somete de forma periódica a un número cada vez mayor de auditorías externas. En todas ellas, un auditor independiente examina nuestros centros de datos, infraestructura y operaciones. Se hacen auditorías periódicas para certificar nuestro cumplimiento de las normas ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701 y SOC 2. Si quieres conocer la lista completa de certificaciones, consulta el Centro de recursos de cumplimiento de Google Cloud. Según los términos de tu contrato con Google como cliente de Google Workspace, Google puede permitir que lleves a cabo (o lo haga un auditor independiente que hayas designado) auditorías o inspecciones para verificar el cumplimiento por parte de Google de sus obligaciones, de acuerdo con la sección 7.5 (revisiones y auditorías de cumplimiento) de la Adenda sobre Tratamiento de Datos.
Evaluación de impacto relativa a la protección de datos (EIPD)	El cliente debe conocer los requisitos necesarios para llevar a cabo una evaluación de impacto relativa a la protección de datos: cuándo debe hacerse, qué debe incluir la evaluación y quién debe	En su función como encargado del tratamiento de datos, Google te ayudará a cumplir con las obligaciones sobre esta evaluación (teniendo en cuenta la naturaleza del tratamiento de los datos personales y la información a disposición

	hacerla, entre otros aspectos.	de Google), de acuerdo con la sección 8 de la Adenda sobre Tratamiento de Datos.
Determinar el alcance del sistema de gestión de la seguridad de la información	Los programas generales sobre seguridad y privacidad que desarrollen los clientes tienen que incluir el tratamiento de los Datos Personales de Clientes y los requisitos relacionados con él. Las políticas para el diseño y el desarrollo de esos sistemas deben incluir indicaciones sobre el tratamiento de la IPI por parte de la organización, en función de las obligaciones de los partícipes de la IPI, de la legislación o normativa aplicable y de los tipos de tratamiento que lleva a cabo la organización.	Google no ofrece asistencia para los procesos internos de los clientes. Te recomendamos que elabores, al menos una vez al año, políticas de privacidad y materiales de formación asociados para los usuarios y los grupos encargados de la privacidad en tu organización. Google ofrece opciones de servicios profesionales de asesoría para formar a los usuarios sobre temas de seguridad y privacidad en la nube incluida, entre otras, la evaluación de seguridad de Google Workspace.
Políticas de seguridad de la información	El cliente debe añadir a las políticas de seguridad de la información que ya tenga otras que protejan los Datos Personales de Clientes, incluidas las políticas necesarias para cumplir con la legislación aplicable. También debe determinar quién tiene la responsabilidad de proporcionar la formación necesaria sobre la protección de los Datos Personales de Clientes y asignar esa responsabilidad.	Google no ofrece asistencia para los procesos internos de los clientes. Puedes desarrollar una política de evaluación y autorización de la seguridad y la privacidad de los datos en toda la organización que defina los procedimientos y los requisitos de implementación de las evaluaciones de privacidad, los controles de privacidad y los controles de autorización.
Consideraciones sobre cómo debe organizar la seguridad de la información el cliente	El cliente debe definir las responsabilidades relacionadas con la seguridad y la protección de los Datos Personales de Clientes dentro de la organización. Entre ellas puede incluirse establecer roles específicos para supervisar las cuestiones sobre privacidad, como el delegado de protección de datos. Además, estos roles deben recibir la asistencia en la gestión y la formación necesarias	Google no ofrece asistencia para los procesos internos de los clientes. Puedes designar a una o varias personas como responsables de desarrollar, implementar, mantener y supervisar un programa global de control y privacidad en la organización para asegurar el cumplimiento de la legislación y las normativas aplicables sobre el tratamiento de la IPI.

	para cumplir sus objetivos.	Puedes designar al delegado de protección de datos y representante de la UE en la opción **Configuración de la cuenta > Información legal y de cumplimiento** de la consola de administración. Hemos designado a un delegado de protección de datos para que actúe por cuenta de Google LLC y sus filiales en lo que respecta al tratamiento de datos amparado por diversas normativas de privacidad.
Clasificación de información	El cliente debe mencionar explícitamente el uso que hace de la IPI como parte de un esquema de clasificación de los datos.	Google no ofrece asistencia para los procesos internos de los clientes. El sistema de clasificación de la información que utilices tiene que mencionar explícitamente el uso de la IPI como parte del esquema que pongas en práctica. Tener en cuenta la IPI dentro del sistema de clasificación global es esencial para comprender qué tipos o categorías especiales de IPI tratas, dónde se almacena esta IPI y por qué sistemas puede moverse esta información. El sistema de clasificación de datos debe describir cómo clasificas los datos en cuanto a su grado de sensibilidad y a la posibilidad de que sirvan como elementos de identificación. Los propietarios de los datos son los responsables de determinar la clasificación adecuada para ellos, en función de quién necesita acceder a esos datos y con qué fin, los posibles riesgos y daños si los datos se ven sometidos a un acceso no autorizado, y el contexto general de los datos.
Gestión de incidentes relacionados con la seguridad de la información	El cliente debe tener procesos para determinar si se ha producido una quiebra en la seguridad de los Datos Personales de Clientes.	Te recomendamos que establezcas una política de respuesta ante incidentes en tu organización, que incluya procedimientos para facilitar y poner en práctica controles de respuesta a

	El cliente debe conocer y documentar las responsabilidades implicadas en una quiebra de la seguridad de los datos u otros incidentes relacionados con la seguridad de los Datos Personales de Clientes. Entre estas responsabilidades se puede incluir notificar a las partes interesadas o comunicarse con los encargados del tratamiento u otras personas ajenas a la organización, así como otras responsabilidades dentro de la organización del cliente.	incidentes, y que crees grupos de seguridad para los equipos y los responsables de las respuestas a los incidentes de tu organización. También te recomendamos que desarrolles un plan de prueba, procedimientos, listas de comprobación, requisitos y puntos de referencia de respuesta a incidentes para asegurar su éxito. Puedes especificar clases de incidentes que deberá reconocer la organización y describir las acciones asociadas que se harán como respuesta a esos incidentes. Además, puedes definir las acciones específicas que deberá llevar a cabo el personal autorizado en caso de que se produzca un incidente, como los pasos para gestionar vertidos de información, vulnerabilidades de ciberseguridad y ataques. No olvides aprovechar las funciones de Google Workspace para analizar y poner en cuarentena los mensajes de correo electrónico, bloquear los intentos de suplantación de la identidad (phishing) y definir restricciones sobre los archivos adjuntos. Puedes usar también la Prevención de la pérdida de datos (DLP) para inspeccionar, clasificar y desidentificar datos sensibles, contribuyendo así a limitar la exposición a los riesgos. Consulta Evitar la pérdida de datos con la nueva versión de DLP de Drive, Analizar el tráfico de correo electrónico con reglas de Prevención de la pérdida de datos y el informe sobre DLP. Como eres cliente de Google, te avisaremos cuanto antes si advertimos un Incidente de Datos y tomaremos medidas razonables al momento para minimizar los daños y proteger los Datos

		de los Clientes. Consulta nuestro compromiso en la sección 7.2 (Incidentes de Datos) de la Adenda sobre Tratamiento de Datos. Consulta también nuestro proceso de respuesta ante incidentes de datos.
Copia de seguridad de la información	El cliente debe tener una política que establezca los requisitos para la copia de seguridad, recuperación y restauración de la IPI, que puede formar parte de una política de copia de seguridad de la información global. También debe establecer otros requisitos que puedan ser necesarios, por motivos contractuales o legales por ejemplo, para el borrado de la IPI presente en los datos que se conservan debido a los requisitos de copia de seguridad.	Te recomendamos que desarrolles un plan de contingencia que defina los procedimientos y los requisitos para la implementación de controles de planificación de contingencias en tu organización. También te recomendamos que identifiques al personal clave, los roles y las responsabilidades en caso de contingencias en los elementos de la organización. Además, debes señalar qué operaciones del sistema de información son esenciales para los objetivos y el negocio dentro de la organización. Describe los objetivos de tiempo de recuperación (RTO) y de punto de recuperación (RPO) para reanudar las operaciones esenciales cuando se haya activado el plan de contingencia. Documenta los sistemas de información críticos y el software asociado. Identifica la información adicional relacionada con la seguridad y aporta orientaciones y requisitos para almacenar copias de seguridad de componentes y datos esenciales de los sistemas. Los centros de datos que Google tiene en todo el mundo ayudan a mantener Internet en funcionamiento de manera ininterrumpida y proporcionan redundancia y resiliencia a nuestros clientes. También puedes utilizar opciones para la copia de seguridad y sincronización de tus archivos locales en Google Drive.

Configuración de la protección y la seguridad de los datos

Controles habituales de privacidad	Responsabilidad del cliente	Funciones de apoyo en Google Workspace
Gestión del acceso de los usuarios, incluido el aprovisionamiento del acceso y la gestión del acceso con privilegios	El cliente debe saber cuáles son sus responsabilidades en el control de acceso al servicio que usan y debe ocuparse de estas responsabilidades de manera adecuada con las herramientas disponibles.	Te recomendamos que desarrolles una política de control de acceso en la organización que actúe sobre las cuentas del sistema de información en la nube y que definas los parámetros y procedimientos que se utilizarán para crear, habilitar, modificar, inhabilitar y eliminar información de las cuentas del sistema. La consola de administración de Google te ofrece funciones de administración centralizada con las que podrás configurar y gestionar las opciones de manera más eficaz. Puedes proteger tu organización con los análisis de seguridad y las prácticas recomendadas que te ofrece el Centro de seguridad. También puedes usar la gestión de identidades y accesos de Cloud Identity para asignar roles y permisos a grupos administrativos, siguiendo la metodología del mínimo acceso y la separación de funciones. Consulta cómo añadir Cloud Identity a tu cuenta de Google Workspace.
Procedimientos seguros para el inicio de sesión	El cliente debe ofrecer procedimientos seguros para el inicio de sesión con las cuentas de usuario que estén bajo su control.	Como cliente de Google Workspace, puedes usar las funciones integradas de Cloud Identity para gestionar usuarios y configurar opciones de seguridad, como la verificación en dos pasos y las llaves de seguridad. La verificación en dos pasos te permite añadir un nivel más de seguridad en las cuentas de Google Workspace; con esta opción, los usuarios deben introducir un código de verificación, además de su nombre de usuario y contraseña, cuando inician sesión.

		La llave de seguridad es una mejora de la verificación en dos pasos que ha desarrollado Google en colaboración con la organización de estándares FIDO Alliance. Se trata de una llave física que se utiliza para acceder a la Cuenta de Google gestionada por la organización y que envía una firma cifrada en lugar de un código, lo que ayuda a asegurar que no se puede suplantar el inicio de sesión. Si quieres conocer más detalles, consulta el artículo Utilizar una llave de seguridad para la verificación en dos pasos. Puedes consultar otras funciones relacionadas con la autenticación y la autorización de usuarios en el informe sobre seguridad y cumplimiento de Google Cloud.
Registro y protección de eventos	El cliente debe conocer las funciones de registro que ofrece el sistema y utilizarlas para asegurarse de que se pueden registrar acciones relacionadas con los Datos Personales de Clientes si lo estima necesario. Debe establecerse un procedimiento para revisar los registros de eventos, ya sea mediante procesos continuos y automáticos de supervisión y alerta o mediante un control manual en el que la revisión se hace con una periodicidad previamente especificada y documentada para identificar irregularidades y proponer soluciones.	Google Workspace ofrece registros de auditoría que ayudan a responder cuestiones como quién hizo qué, dónde y cuándo. Entre los registros de auditoría disponibles tienes los registros de actividad de los administradores (registro de auditoría de la consola de administración), los registros de seguridad (inicio de sesión, SAML y Transparencia de acceso) y los registros sobre los servicios y las cuentas de los usuarios (búsqueda en el registro de correo electrónico y registro de auditoría de Drive). Para obtener más información sobre los registros de auditoría, consulta el artículo Registros de auditoría disponibles. Por lo general, los registros de auditoría se conservan durante seis meses; consulta los detalles en Plazos de conservación y periodos de retraso de los datos. Puedes personalizar la información que revisas en los registros de auditoría desde la consola de administración de Google; puedes filtrar los datos por usuario o actividad, unidad

		organizativa o fecha. También puedes configurar alertas para determinadas actividades.
Cifrado	El cliente debe determinar qué datos deben cifrarse y si el servicio que utilizan lo permite. Debe utilizar el cifrado según sea necesario, con las herramientas que tenga disponibles.	Los Datos de los Clientes de Google Workspace se envían cifrados, están cifrados en reposo y también están cifrados en los soportes de copia de seguridad. El cifrado es un elemento importante en la estrategia de seguridad de Google Workspace y ayuda a proteger el correo electrónico, los chats, los archivos de Google Drive y otros datos. Si quieres ver información adicional sobre los mecanismos de protección de los datos cuando están en reposo, en tránsito o en un soporte de copia de seguridad, y sobre cómo se gestionan las claves de cifrado, consulta el informe sobre cifrado de Google Workspace. Como administrador, si tu organización necesita un mayor nivel de cifrado del correo saliente, puedes configurar reglas para que esos mensajes se firmen y se cifren con extensiones seguras multipropósito de correo de Internet (S/MIME). Así ayudas a que los Datos Personales de Clientes estén seguros, sigan siendo confidenciales y mantengan su integridad.

Registros de países y organizaciones a las que se puede transferir la IPI	El cliente debe saber a qué países se transfieren o se pueden transferir los Datos Personales de Clientes, y debe ser capaz de proporcionar esta información a los usuarios. Si esta transferencia puede ser hecha por un encargado del tratamiento o alguien ajeno a la organización, el cliente debe obtener de él esta información.	Google tiene y opera sus propios centros de datos en todo el mundo, para que sus productos estén operativos de forma ininterrumpida. Para obtener más información, consulta el artículo Conoce las ubicaciones de nuestros centros de datos. Puedes decidir si tus datos se almacenan en una ubicación geográfica concreta (de Estados Unidos o Europa) con una política de la región de datos. Este servicio ofrece un control más detallado de la ubicación geográfica donde se almacenarán los mensajes de correo electrónico, los documentos y otro contenido de Google Workspace. Revisa detenidamente los productos a los que se aplican políticas de región de datos y busca asesoramiento legal para comprobar si satisface los requisitos de cumplimiento específicos o las necesidades de tu empresa.
Registros de la divulgación de la IPI a terceros	El cliente debe registrar la divulgación de la IPI que hace ante terceros, como las autoridades legislativas. Debe incluir la información que se ha divulgado, a quién y cuándo se ha hecho. Cuando es un encargado del tratamiento o un tercero quien divulga los datos, el cliente debe asegurarse de que también mantendrá los registros adecuados y de que puede obtenerlos de él en caso necesario.	Google y sus entidades asociadas utilizan varios subencargados del tratamiento de datos que colaboran en la provisión de servicios. Para conocer los detalles, consulta la información sobre los subencargados del tratamiento de datos de Google Workspace. Como administrador, te recomendamos que evalúes el uso de las aplicaciones de terceros. Puedes impedir que los usuarios instalen aplicaciones de terceros, como aplicaciones de Google Drive y complementos de Documentos de Google. Te recomendamos que revises la documentación sobre seguridad que proporcionan los desarrolladores externos, así como los términos del tratamiento de datos aplicables, antes de usar esas aplicaciones con Google Drive y Documentos de Google. De acuerdo con nuestra política, si

		Google recibe una solicitud para acceder a los Datos del Cliente de Cloud por parte de una autoridad legislativa, remitimos a las autoridades a que soliciten estos datos directamente al cliente de Cloud. En Google contamos con un equipo que revisa y evalúa cada una de las solicitudes que recibimos para asegurarnos de que se ajusta a los requisitos legales. Si nos vemos obligados a comunicar los datos, avisamos a los clientes antes de divulgar ninguna información, salvo si dicha notificación se nos prohíbe por ley o en casos de emergencia que pongan vidas en peligro. En la medida en que lo permitan la ley y los términos de la solicitud, nos comprometemos a atender a las razones fundamentadas del cliente si decide ejercer su derecho de oposición a una solicitud. Puedes consultar más información en nuestro informe de transparencia y en el informe sobre solicitudes gubernamentales en Google Cloud.
Determinación de los derechos (incluidos los de acceso, corrección, borrado y exportación) de los interesados y habilitación de su ejercicio	El cliente debe conocer los requisitos relacionados con los derechos de las personas en lo que atañe al tratamiento de los Datos Personales de Clientes. Entre estos derechos se incluyen acciones como el acceso a esos datos o su corrección, borrado y exportación. Si el cliente usa un sistema externo, debe determinar qué elementos (si los hay) del sistema ofrecen herramientas relacionadas con la posibilidad de que el usuario ejerza sus derechos, como el acceso a sus datos personales. Si el sistema ofrece estas opciones, el cliente debe utilizarlas según sea necesario.	Como administrador de Google Workspace, puedes usar la consola de administración de Google para cumplir con las posibles obligaciones que tengas en lo que respecta a las Solicitudes de los Interesados. Google Workspace ofrece funciones para que tanto los administradores de Google Workspace como los interesados accedan directamente a los datos personales de los clientes desde los productos de Google y puedan exportarlos. Los administradores de Google Workspace pueden usar la herramienta de exportación de datos para exportar los datos de toda la organización y Google Vault para búsquedas y exportaciones de datos de usuarios concretos. Los interesados que sean usuarios pueden usar la interfaz de Google Takeout para

		acceder directamente a sus propios datos personales de los clientes y exportarlos. Para obtener las instrucciones, consulta la guía de respuestas a Solicitudes de los Interesados para Google Workspace.
Conservación y eliminación	La organización que trata la IPI debe asegurarse de que se deshace de ella tras el periodo especificado por la jurisdicción correspondiente.	Google seguirá las instrucciones para eliminar los Datos de los Clientes de sus sistemas que, como administrador, le indiques. Los administradores pueden gestionar las cuentas de los usuarios desde la consola de administración de Google. Esto incluye eliminar las cuentas o eliminar los datos personales de los clientes de los dispositivos móviles y los productos. Si tu organización tiene que conservar datos durante un periodo determinado, puedes configurar Vault para hacerlo, incluso si los usuarios los eliminan y vacían la papelera. Para acceder a las instrucciones sobre cómo configurar la eliminación, consulta la guía de respuestas a Solicitudes de los Interesados para Google Workspace. Consulta nuestro compromiso sobre la eliminación de datos en la sección 6 (eliminación de datos) de la Adenda sobre Tratamiento de Datos. Consulta la sección del Aviso de Privacidad de Google Cloud acerca de la eliminación y la conservación de los datos del servicio.

Gestión de puntos de conexión	El cliente debe asegurarse de que el uso de los dispositivos móviles no pone en peligro la protección de la IPI.	Al usar la gestión de puntos de conexión de Google como administrador, puedes aumentar la seguridad de los datos de tu organización en los dispositivos móviles, ordenadores, portátiles y otros puntos de conexión que utilicen tus usuarios. La gestión básica te permite configurar la implementación obligatoria de contraseñas básicas, los informes de dispositivos móviles, la protección contra accesos no autorizados, el borrado remoto de las cuentas y las auditorías y alertas de dispositivos. Con la gestión avanzada, consigues funciones adicionales de seguridad y privacidad, como la implementación obligatoria de contraseñas seguras, el bloqueo de dispositivos en riesgo de seguridad o la aprobación de dispositivos, entre otras. Para obtener más información y saber cuál es la versión adecuada para ti, consulta Comparar funciones de la gestión de dispositivos móviles. Consulta también Configurar la gestión básica de dispositivos móviles y Configurar la gestión avanzada de dispositivos móviles.

---

[1] Los Datos Personales de los Clientes son los datos personales que forman parte de los Datos de los Clientes.
[2] Los Datos de los Clientes son aquellos que tú, tu organización y tus usuarios proporcionáis a Google al acceder a Google Workspace, así como los datos que creáis cuando usáis sus servicios.
[3] Los Datos de los Servicios es la información personal que Google recoge o genera durante la provisión y administración de los Servicios de Cloud, excluyendo los Datos de los Clientes y los Datos de Partners. Los Datos de los Servicios están sujetos al Aviso de Privacidad de Google Cloud.
[4] Consulta nuestras certificaciones ISO/IEC (ISO/IEC 27001, 27017, 27701, 27018) así como nuestro informe de auditoría SOC 3, disponible en este documento. Si eres cliente nuestro y quieres informarte sobre la seguridad en Google, puedes consultar una versión detallada del informe SOC 2 en el Administrador de informes de cumplimiento. Puedes acceder a la lista completa de recursos de cumplimiento que ofrecemos en nuestro Centro de recursos de cumplimiento.
[5] G Suite para Centros Educativos se ofrece a los centros educativos bajo un contrato de G Suite para Centros Educativos independiente y (según corresponda) sujeto a la Adenda sobre Tratamiento de Datos.
[6] Si el RGPD se aplica al tratamiento que Google hace de tus datos —por ejemplo, si resides en la Unión Europea, o si resides fuera de la Unión Europea, pero ofreces productos o servicios a sujetos que se encuentran en la Unión Europea— es necesario que tu contrato con Google incluya determinados términos sobre el tratamiento de datos.

[7] Tienes que registrarte en la Gestión en la nube del navegador Chrome si quieres configurar políticas de grupo para los navegadores registrados.
[8] Tienes que usar la gestión avanzada de dispositivos móviles para configurar un perfil de trabajo. Consulta más información en Configurar la gestión avanzada de dispositivos móviles.
[9] Esta función solo está disponible con Google Workspace Enterprise Plus y G Suite Enterprise para Centros Educativos.