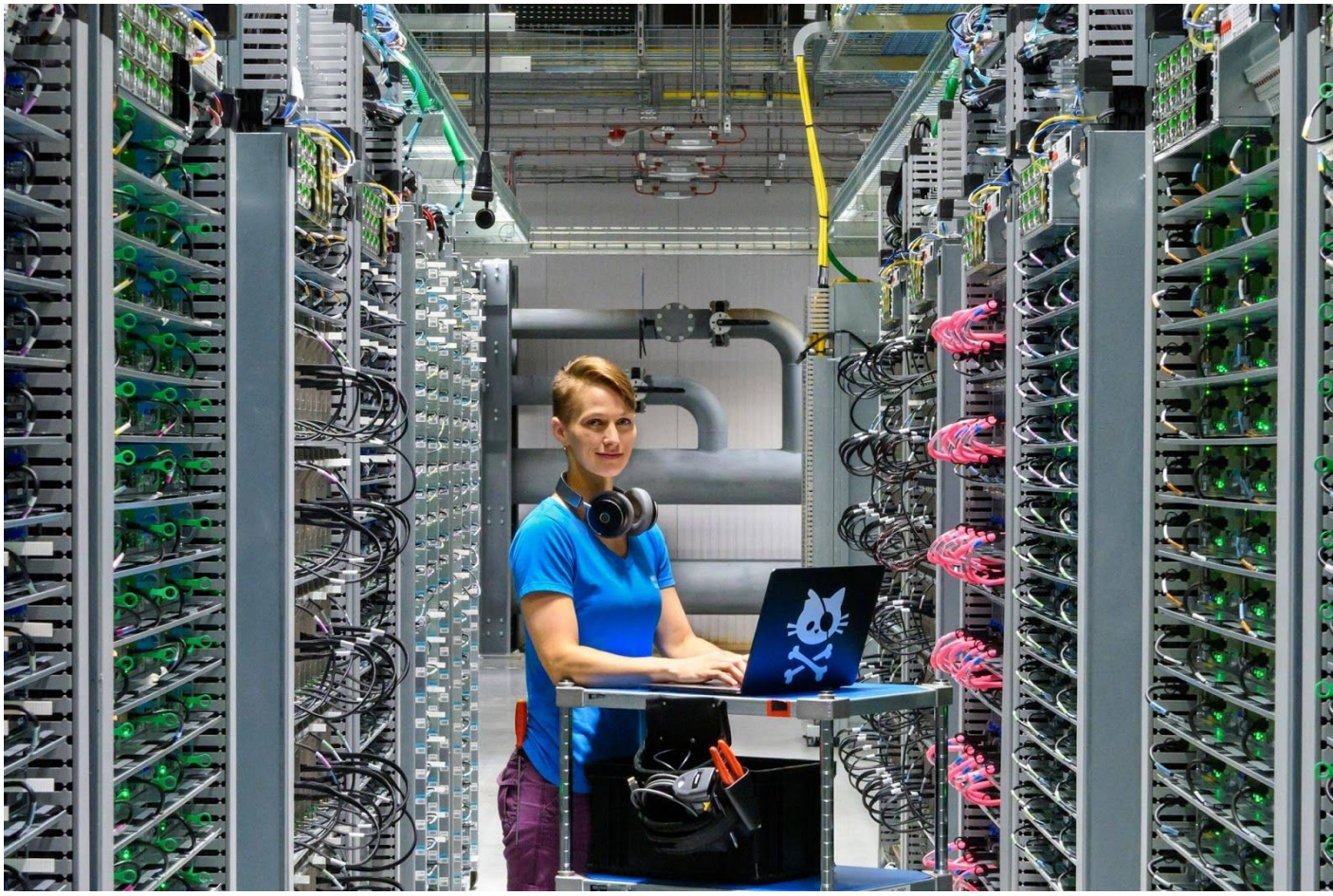
Google Workspace

Informe sobre seguridad de Google Workspace



Google Cloud

Google Workspace

Contenido

Introducción

Los servicios de cloud computing han cambiado la forma de hacer negocios de las empresas en la actualidad. Las organizaciones recurren principalmente a la nube pública para gestionar la infraestructura, las operaciones y la prestación de servicios, ya que se han dado cuenta de que los proveedores pueden invertir más en sus empleados y procesos para conseguir una infraestructura segura y que cumpla las normativas.

Google es una empresa pionera en los servicios en la nube y, por eso, comprende las implicaciones de seguridad de este modelo de nube. Por eso, nuestros servicios en la nube están diseñados para ofrecer más seguridad que muchas soluciones on-premise tradicionales. La seguridad es una prioridad a la hora de proteger nuestras operaciones y, dado que Google se ejecuta en la misma infraestructura que ponemos a disposición de nuestros clientes, tu organización puede beneficiarse directamente de estas medidas de protección.

La seguridad y la protección de los datos impulsan, no solo nuestra estructura organizativa, sino también nuestras prioridades de formación y nuestros procesos de contratación. Estos principios dan forma a las operaciones de nuestros centros de datos y a la tecnología que albergan. Resultan fundamentales tanto para nuestras operaciones diarias como para planificar la recuperación tras fallos, incluida la forma en que abordamos las amenazas, y les damos total prioridad a la hora de gestionar los datos de los clientes. Además, son la piedra angular sobre la que se fundamentan nuestros controles de cuentas, nuestras auditorías de cumplimiento y las certificaciones que ofrecemos a nuestros clientes. En los principios de confianza de Google Cloud resumimos nuestro compromiso con las empresas y los datos de los clientes, y explicamos cómo protegemos su privacidad cada vez que usan Google Workspace y Google Cloud Platform.

En este informe se describe la filosofía de Google sobre seguridad y cumplimiento en lo que respecta a Google Workspace, nuestro paquete de herramientas de productividad basado en la nube. Ya son más de cinco millones de empresas de todo el mundo, desde grandes bancos y comercios con cientos de miles de empleados hasta empresas emergentes que crecen rápidamente, las que disfrutan de las herramientas de colaboración y productividad de Google Workspace y G Suite for Education. Ambos servicios se han diseñado para ofrecer a los equipos otras formas más eficientes de colaborar de manera segura, independientemente de dónde se encuentren sus miembros o del dispositivo que usen. Gmail, por ejemplo, analiza más de 300.000 millones de archivos adjuntos para comprobar si contienen software malicioso y evita que los usuarios reciban el 99,9 % del spam, los mensajes de phishing y el software malicioso que se envían.[1] Nos comprometemos a proteger a los usuarios frente a las amenazas de seguridad de todo tipo. Para ello, ofrecemos herramientas de seguridad innovadoras para los usuarios y administradores, y proporcionamos un servicio seguro en la nube a nuestros clientes.

Nota: En los próximos meses, pondremos Google Workspace a disposición de los clientes de instituciones educativas y organizaciones sin ánimo de lucro. Los clientes de instituciones educativas pueden seguir disfrutando de nuestras herramientas a través de G Suite for Education, que incluye Classroom, Tareas, Gmail, Calendar, Drive, Documentos, Hojas de cálculo, Presentaciones y Meet. G Suite para Organizaciones sin Ánimo de Lucro seguirá estando disponible para las organizaciones que cumplan los requisitos del programa Google para Organizaciones sin Ánimo de Lucro. A menos que se indique lo contrario, este documento hace referencia a Google Workspace y G Suite for Education.

[1] Datos de abril del 2020

Renuncia de responsabilidad

El contenido de este documento es correcto en octubre del 2020 y representa la situación en el momento en que se redactó. Las políticas y los sistemas de seguridad de Google Cloud pueden cambiar en el futuro, ya que mejoramos día tras día la protección que proporcionamos a nuestros clientes.

Cultura centrada en la privacidad y la seguridad de Google

Google ha creado una cultura de privacidad y seguridad dinámica e inclusiva para todos sus empleados. La influencia de esta cultura siempre es palpable: durante el proceso de contratación, cuando se incorporan los empleados, a lo largo de su proceso continuo de formación y en los eventos que involucran a toda la empresa para concienciar al personal sobre alguna causa.

Comprobaciones de antecedentes de los empleados

Antes de unirse a nuestro personal, Google verifica la formación de cada candidato, así como sus puestos de trabajo anteriores, y contacta con sus referencias internas y externas. Siempre que la legislación laboral local o las disposiciones legales lo permitan, y en función del puesto, Google también puede comprobar la identidad de los candidatos, sus antecedentes penales, estado financiero y condición migratoria o de residencia.

Formación en seguridad para todos los empleados

Todos los empleados de Google reciben formación en seguridad como parte del proceso de orientación y también de forma continua a lo largo de su trayectoria en Google. Durante la orientación, los nuevos empleados aceptan nuestro código de conducta, donde se destaca nuestro compromiso de mantener la información del cliente segura y protegida.

En función de su puesto, los empleados también pueden recibir formación adicional sobre otros aspectos de seguridad específicos. Por ejemplo, el equipo de seguridad de la información instruye a los nuevos ingenieros en ámbitos como prácticas de programación segura, diseño de productos y herramientas de pruebas de vulnerabilidad automatizadas. Los ingenieros también asisten a presentaciones técnicas sobre temas relacionados con la seguridad y reciben un boletín con información sobre nuevas amenazas, patrones de ataque y técnicas de mitigación, entre otros aspectos.

Entorno seguro

Google sigue una estrategia de confianza cero por la que se aplican controles de acceso de nivel crítico según la información que obtenga sobre el dispositivo, el estado, el usuario asociado y el contexto. De acuerdo con esta estrategia, de forma predeterminada, ni las redes internas ni las externas son de confianza, lo que da lugar al concepto de "conformidad sin límites". Esto quiere decir que exigimos y aplicamos niveles de acceso en la capa de las aplicaciones de forma dinámica. Gracias a ello, los equipos de seguridad y cumplimiento de Google gozan de los mismos niveles de seguridad y eficacia durante una emergencia que en cualquier otro momento.

El COVID-19 no solo ha cambiado nuestra forma de trabajar, sino desde dónde lo hacemos, y ha creado la necesidad de contar con nuevas soluciones que aún así satisfagan los requisitos de cumplimiento del sector. Con nuestro enfoque de confianza cero, puedes ofrecer una solución de teletrabajo segura y escalable a tus empleados y al personal externo sin depender de una VPN ni de requisitos de ubicación.

Eventos internos sobre privacidad y seguridad

La seguridad y la privacidad son áreas en continuo desarrollo, y Google sabe que el compromiso de los empleados es un factor decisivo para concienciar sobre estos ámbitos. Por ello, en Google se llevan a cabo convenciones internas para todos los empleados de forma habitual que pretenden favorecer la innovación en el campo de la seguridad y de la privacidad de los datos, así como concienciar al público al respecto. También se celebran charlas sobre tecnología que, con frecuencia, se centran en temas relacionados con la seguridad y la privacidad. Un buen ejemplo de esto es la Semana de la Privacidad, durante la cual Google organiza eventos en sus oficinas de todo el mundo para concienciar sobre la privacidad en todas sus facetas, desde el desarrollo de software y la gestión de datos hasta la implementación de políticas.

Nuestro equipo de seguridad específico

Google cuenta con un equipo a tiempo completo dedicado a la seguridad y la privacidad que forma parte de nuestra división de Ingeniería y Operaciones de Software. Entre sus miembros se encuentran algunos de los mayores expertos del mundo en materia de seguridad de la información, de las aplicaciones y de las redes. Este equipo se dedica a mantener nuestros sistemas de defensa y, para ello, desarrolla los procesos de evaluación, crea la infraestructura e implementa las políticas que velan por la seguridad de la empresa. Además, busca constantemente amenazas de seguridad utilizando herramientas comerciales y personalizadas, pruebas de penetración, procesos de control de calidad y revisiones de seguridad del software.

Dentro de Google, el equipo de seguridad de la información presta numerosos servicios esenciales: revisa los planes de seguridad de todas las redes, sistemas y servicios de la empresa; ofrece servicios de consultoría específicos de cada proyecto a los equipos de productos e ingeniería; monitoriza la actividad en las redes de Google y detecta los comportamientos sospechosos; se ocupa de las amenazas de seguridad de la información; lleva a cabo evaluaciones y auditorías rutinarias de seguridad; y colabora con expertos externos que realizan evaluaciones periódicas de seguridad. Además, Google ha creado un equipo específico a tiempo completo, denominado Project Zero, que tiene como objetivo evitar ataques dirigidos informando a los proveedores de software de los errores que encuentran y archivándolos en una base de datos externa.

Pero ahí no acaba la cosa. El equipo de seguridad también participa en actividades de investigación y divulgación para proteger a los usuarios de Internet en general, no solo a aquellos que eligen las soluciones de Google. Además, publica documentos de investigación disponibles para todo el mundo y organiza proyectos de software libre y convenciones académicas, en los que también participa.

Nuestros equipos de privacidad

Los equipos de privacidad de Google son un pilar fundamental a la hora de lanzar productos y cuentan con un conjunto de herramientas de monitorización automatizadas para asegurarse de que los servicios que tratan la información personal de los usuarios funcionan de la manera prevista y de acuerdo con nuestros compromisos de protección de

datos. También revisan la documentación del diseño y las auditorías del código para asegurarse de que se cumplen los requisitos de privacidad.

Gracias a nuestros equipos multifuncionales, podemos lanzar productos que reflejen estándares de privacidad sólidos; es decir, somos capaces de ofrecer una recogida de datos de usuario transparente y poner a disposición de usuarios y administradores unas opciones de configuración de privacidad eficaces, a la vez que gestionamos de forma adecuada la información almacenada en nuestra plataforma. Tras lanzar los productos, los programas de cumplimiento y privacidad de Google supervisan los procesos automatizados que realizan auditorías sobre el tráfico de datos para verificar que el uso de datos es adecuado. Además, seguimos investigando sobre asuntos relacionados para que nuestras tecnologías emergentes y sus prácticas recomendadas se encuentren en la vanguardia en el ámbito de la privacidad.

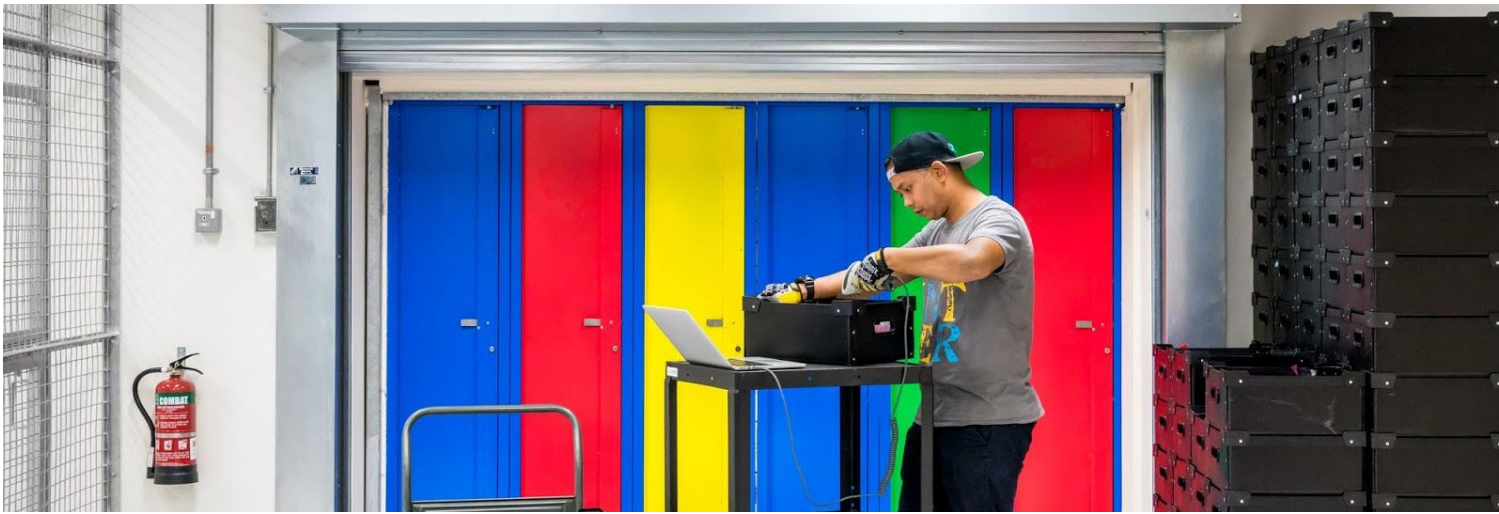
Especialistas en auditorías internas y en cumplimiento

Las normativas de protección de datos subrayan la importancia de que las empresas sepan cómo se están tratando sus datos, quién tiene acceso a ellos y cómo se gestionan los incidentes de seguridad. Contamos con equipos dedicados de ingenieros y expertos en cumplimiento que ayudan a nuestros clientes a satisfacer sus obligaciones de cumplimiento normativo y gestión de riesgos. Como parte de nuestra estrategia, colaboramos con los clientes para conocer las normativas pertinentes y ayudarlos a cumplirlas. Cuando se crean estándares de auditoría, el equipo determina los controles, procesos y sistemas necesarios para cumplirlos, al tiempo que ayuda a realizar las auditorías y evaluaciones independientes de terceros. En determinadas circunstancias, los clientes también pueden llevar a cabo auditorías para validar los controles de seguridad y cumplimiento de Google.

Colaboración con la comunidad de investigación sobre seguridad

Google mantiene, desde hace mucho tiempo, una estrecha relación con la comunidad que investiga cuestiones de seguridad, y agradecemos su ayuda a la hora de identificar las vulnerabilidades de Google Workspace y de otros productos de Google. Hemos desarrollado el programa Vulnerability Reward Program porque valoramos todas las contribuciones externas que ayudan a proteger a nuestros usuarios. Este programa anima a los investigadores a informar sobre problemas relacionados con el diseño y la implementación que pueden afectar a la confidencialidad o integridad de los datos de los usuarios, o poner en peligro los datos de los clientes. A cambio de su ayuda, ofrecemos recompensas que pueden llegar a las decenas de miles de dólares.

A raíz de esta colaboración con la comunidad de investigación, en el 2019 pagamos más de 6,5 millones de dólares en recompensas, una cifra que duplica lo que habíamos llegado a pagar hasta entonces en todo un año. Agradecemos públicamente el esfuerzo de estas personas y las incluimos como colaboradores de nuestros productos y servicios.



Seguridad operativa

En Google, la seguridad está constantemente en nuestras mentes; no se trata de un tema que abordemos con iniciativas ocasionales. Es una parte esencial de nuestras operaciones.

Gestión de las vulnerabilidades

Mediante el proceso de gestión de vulnerabilidades de Google, buscamos constantemente amenazas de seguridad. Para ello, utilizamos herramientas de terceros disponibles en el mercado y diseñamos otras de manera interna según nuestras necesidades; también empleamos estrategias intensivas de penetración manual y automatizada, así como procesos de control de calidad, revisiones de seguridad del software y auditorías externas. Cuando se identifica alguna vulnerabilidad que se debe solventar, se registra, se le otorga prioridad en función de la gravedad y se asigna a un propietario. El equipo monitoriza cada una de las vulnerabilidades hasta poder verificar que los problemas se han solucionado.

Google también se relaciona y se comunica de manera frecuente con los miembros de la comunidad de investigación de seguridad para hacer un seguimiento de las incidencias que atañen a sus servicios y a las herramientas de software libre. Puedes encontrar más información sobre cómo denunciar un problema de seguridad en Seguridad para aplicaciones de Google.

Prevención del software malicioso

Un ataque eficaz de software malicioso puede poner en peligro la seguridad de las cuentas, dar pie al robo datos y hasta conceder acceso adicional a una red. En Google, extremamos las precauciones ante este tipo de amenazas a nuestras redes y a nuestros clientes. Por ello, utilizamos distintos métodos para evitar, detectar y erradicar el software malicioso.

Esta clase de software puede estar presente en sitios web y en los archivos adjuntos de los correos electrónicos y se puede instalar en los dispositivos de los usuarios para robar información privada, realizar robos de identidad o atacar a otros ordenadores. Cuando los usuarios visitan esos sitios, se descarga automáticamente el software que se hace con el control del ordenador sin que ellos lo sepan. La estrategia de Google contra el software malicioso comienza con la prevención de infecciones, gracias a una serie de análisis manuales y automatizados que exploran el índice de búsquedas de Google para hallar cualquier sitio web que pueda incluir software malicioso o que facilite la suplantación de identidad. Además, uno de nuestros principales sistemas de protección se dedica a buscar software malicioso en archivos adjuntos, y procesa más de 300.000 millones de archivos adjuntos a la semana para bloquear el contenido dañino. El 63 % de los documentos maliciosos que bloqueamos varía de un día para otro. Para ir siempre un paso por delante de esta amenaza que evoluciona constantemente, acabamos de añadir una nueva generación de sistemas de análisis de documentos que mejoran nuestras capacidades de detección mediante el aprendizaje profundo.

Cada día, protegemos más de 4000 millones de dispositivos con la Navegación segura de Google. Gracias a esta tecnología, todos los días descubrimos miles de sitios que no son seguros, muchos de los cuales son sitios web legítimos que han sufrido algún ataque. Si encontramos un sitio que no es seguro, mostramos advertencias en la Búsqueda de Google y en los navegadores web.

Además de nuestra solución Navegación segura, Google ofrece VirusTotal, un servicio online que analiza archivos y URLs, lo que permite la identificación de virus, gusanos, troyanos y demás contenido malicioso que se puede detectar a través de los motores antivirus y los sistemas de análisis de sitios web. Sus objetivos son ayudar a mejorar el sector de

la seguridad y los antivirus, y hacer de Internet un lugar más seguro mediante el desarrollo de herramientas y servicios gratuitos. Google utiliza varios motores antivirus en Gmail, en Drive, en servidores y en estaciones de trabajo para ayudar a identificar el software malicioso que las firmas de antivirus pueden pasar por alto.

Monitorización

El programa de monitorización de seguridad de Google se centra en la información recogida del tráfico de la red interna, de las acciones que realizan los empleados en los sistemas y del conocimiento externo de las vulnerabilidades. El tráfico interno se supervisa en muchos puntos de nuestra red mundial para detectar posibles actividades sospechosas como, por ejemplo, la presencia de tráfico indicativo de conexiones con redes de robots. Este proceso se lleva a cabo mediante una combinación de herramientas comerciales y de software libre para capturar y analizar tráfico.

Además, complementamos el análisis de red con un sistema de correlación propio que utiliza la tecnología de Google y con un examen de los registros del sistema para identificar comportamientos inusuales, como un intento por acceder a los datos de los clientes. Los ingenieros de seguridad de Google implementan alertas de búsqueda permanentes en los repositorios de datos públicos para detectar incidentes de seguridad que puedan afectar a la infraestructura de la empresa. También revisan constantemente los informes de seguridad que llegan y monitorizan las listas de distribución, las entradas de los blogs y las wikis públicas. El análisis automático de la red permite identificar amenazas desconocidas e informar de ello al personal de seguridad de Google, y se conjuga con el análisis automático de los registros del sistema.

Google Workspace

Gestión de incidentes

La respuesta ante incidentes es uno de los aspectos clave del programa general de seguridad y privacidad de Google. Seguimos un proceso muy riguroso a la hora de gestionar los incidentes de datos. En este proceso se definen las acciones que se deben llevar a cabo, a quién derivar el problema y cuáles son las estrategias para mitigar, resolver y notificar cualquier incidente que pueda afectar a la confidencialidad, integridad o disponibilidad de los datos de los clientes. La gestión del programa de respuesta ante incidentes de Google recae sobre equipos de expertos en la materia de distintas funciones especializadas. De esta manera, nos aseguramos de ofrecer medidas específicas para los desafíos que supone cada incidente.

Los expertos de estos equipos participan en el proceso de distintas formas. Por ejemplo, los líderes de incidentes se encargan de evaluar la naturaleza de estos y de coordinar las respuestas ante ellos, que consisten en completar la valoración del incidente, ajustar su gravedad si es necesario y poner en marcha al equipo de respuesta ante incidentes pertinente con los jefes operativos y técnicos que correspondan, quienes revisan los hechos e identifican aspectos clave que se deben investigar. Como parte del proceso de resolución, el equipo de análisis forense digital se encarga de detectar los ataques que están teniendo lugar y lleva a cabo investigaciones forenses. Los ingenieros de productos tratan de limitar el impacto sobre las operaciones de los clientes y ofrecen soluciones para resolver los problemas de los productos afectados. El equipo legal trabaja con miembros de seguridad y privacidad correspondientes para recoger pruebas según la estrategia de Google, colaborar con los servicios policiales y órganos reguladores de las administraciones públicas, y ofrecer asesoría sobre asuntos y requisitos legales. El personal de asistencia gestiona las notificaciones de los clientes y responde a sus solicitudes y peticiones para ofrecerles más información y prestarles la ayuda necesaria.

Una vez que un incidente de datos se soluciona y se resuelve correctamente, el equipo de respuesta ante incidentes lo evalúa para extraer información que pueda ser útil en el futuro. Si un incidente da lugar a problemas críticos, el responsable a cargo del incidente puede iniciar un análisis posterior. A lo largo de este proceso, el equipo de respuesta ante incidentes analiza las causas y la respuesta de Google para ver en qué ámbitos clave se debe mejorar. En algunos casos, puede que sea necesario ponerse en contacto con distintos equipos de productos, ingeniería y operaciones, así como realizar tareas de mejora de productos. Si hay que llevar a cabo algún trabajo de seguimiento, el equipo de respuesta ante incidentes traza un plan de acción y asigna a gestores de proyectos para encargarse de esa labor a largo plazo. Cuando la solución se da por concluida, se cierra el incidente.

Tecnología con la seguridad como elemento fundamental

Google, como empresa innovadora en tecnologías de hardware, software, redes y gestión de sistemas, usó el principio de defensa reforzada para crear una infraestructura de TI más segura y fácil de gestionar que las tecnologías más tradicionales. Nos encargamos de diseñar nuestros servidores, nuestro sistema operativo propio y nuestros centros de datos, que están distribuidos geográficamente. De esta forma, nos aseguramos de que Google Workspace se ejecuta en una plataforma tecnológica que se ha concebido, diseñado y desarrollado para funcionar de forma segura.

Centros de datos de última generación

La filosofía de Google en materia de seguridad y protección de datos se encuentra entre nuestros principales criterios de diseño. La seguridad física de nuestros centros de datos cuenta con un modelo de seguridad por capas que incluye medidas de protección como tarjetas de acceso electrónicas con un diseño personalizado, alarmas, barreras en los accesos para vehículos, cercado perimetral, detectores de metales, escáneres de datos biométricos y un sistema de detección de intrusos mediante rayos láser en varias plantas.

Nuestros centros de datos están vigilados las 24 horas con cámaras interiores y exteriores de alta resolución que detectan y siguen a los posibles intrusos. Si se produce algún incidente, se pueden consultar los registros de acceso, los informes de actividad y las imágenes de las cámaras. Además, los centros de datos disponen de guardias de seguridad experimentados que han superado rigurosas comprobaciones de antecedentes y han recibido la formación adecuada para patrullar las instalaciones de forma regular.

Conforme nos acercamos a las plantas de los centros de datos, las medidas de seguridad son cada vez más estrictas. De hecho, menos del 1 % de los empleados de Google pisarán alguno de nuestros centros de datos durante su paso por la empresa. Solo lo hacen aquellos que tienen puestos específicos y han recibido su aprobación. Además, solo es posible acceder a través de un pasillo de seguridad que cuenta con un control de acceso que combina varios factores mediante el uso de distintivos de seguridad y autenticación biométrica.

Energía para nuestros centros de datos

Para que todos los servicios estén en orden y funcionen las 24 horas, los centros de datos de Google cuentan con sistemas de alimentación redundantes y controles medioambientales. Los sistemas de refrigeración preservan los servidores y otros tipos de hardware a una temperatura de funcionamiento constante, lo que reduce el riesgo de suspensión del servicio. Los componentes más importantes disponen de una fuente de energía principal y de otra alternativa, ambas con la misma potencia, por si se produce alguna incidencia. Nuestros generadores de respaldo con motores diésel proporcionan suficiente energía eléctrica de emergencia para que todos los centros de datos funcionen a plena capacidad. Los equipos de detección y extinción de incendios, incluidos los detectores de calor, fuego y humo, activan alarmas sonoras y visibles en las áreas afectadas, que aparecen en las consolas de operaciones de seguridad y en los servicios de supervisión remota, para prevenir que el hardware sufra posibles daños.

Impacto ambiental

En Google, nos preocupamos tanto por minimizar el impacto ambiental de nuestros centros de datos que incluso diseñamos y construimos nuestras instalaciones con lo último en tecnología ecológica. Instalamos controles de temperatura inteligentes, utilizamos técnicas de enfriamiento gratuito, cómo aprovechar el aire de fuera o el agua reutilizada, y rediseñamos la forma en que se distribuye la energía para que no se pierda de forma innecesaria. Para comprobar si vamos por el buen camino, calculamos el rendimiento de cada instalación utilizando mediciones de eficiencia integrales.

Nos enorgullece ser la primera empresa importante de servicios de Internet en obtener certificaciones externas por nuestros elevados estándares en gestión energética, seguridad en el lugar de trabajo y cuidado del medioambiente en todos nuestros centros de datos. En concreto, hemos recibido las certificaciones voluntarias ISO 14001, OHSAS 18001 e ISO 50001, que se basan en un concepto muy sencillo: decir lo que vas a hacer, hacer lo que has dicho y seguir mejorando.

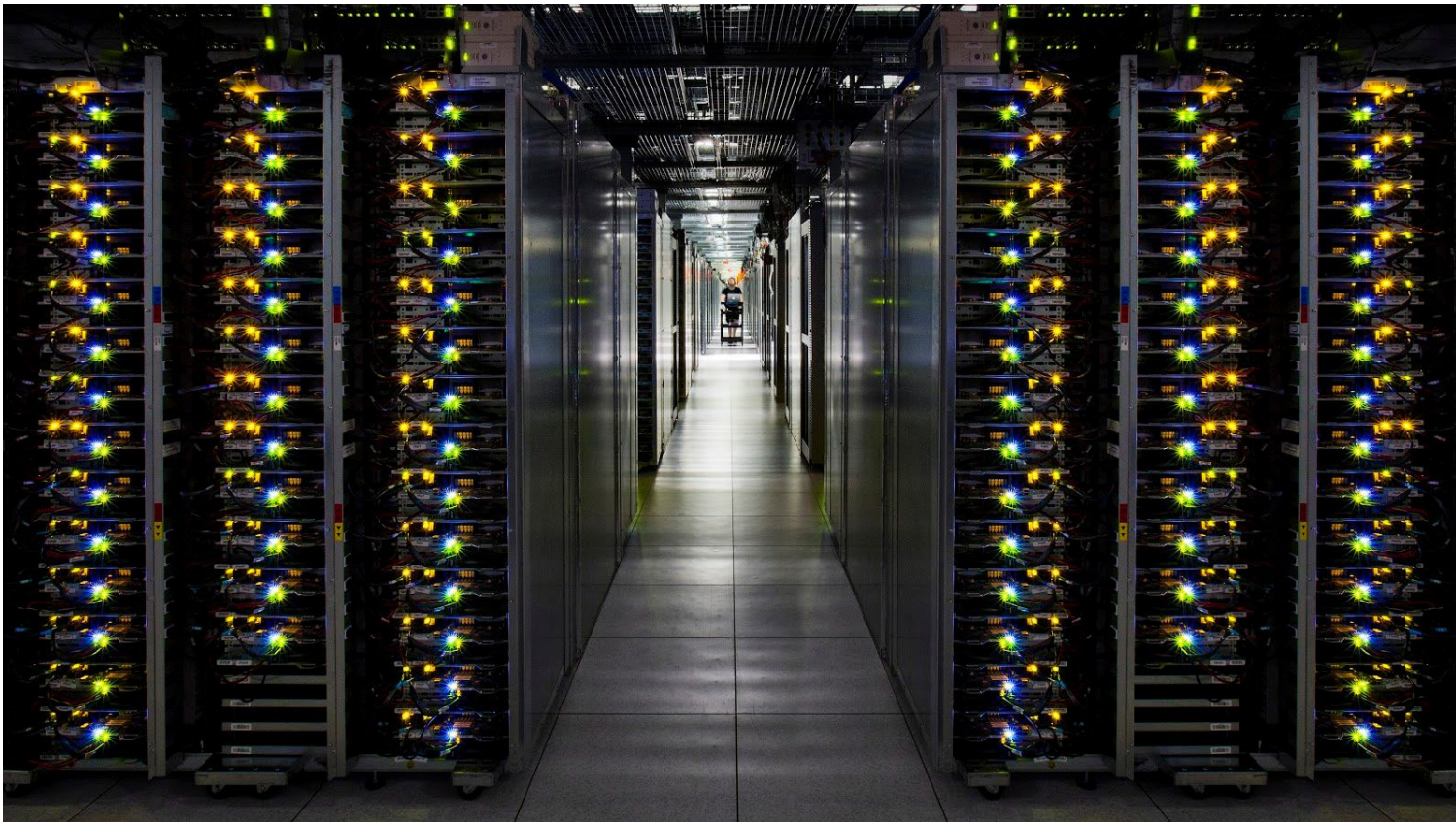
Hardware y software personalizados para los servidores

Los centros de datos de Google albergan servidores y equipos de red personalizados, para fines específicos y eficientes en el consumo de energía, que diseñamos y fabricamos nosotros mismos. Nuestros servidores de producción utilizan un sistema operativo (SO) de diseño personalizado basado en una versión simplificada y reforzada de Linux. En otras palabras, los servidores de Google y su SO están diseñados con el único propósito de proporcionar servicios de Google, lo que significa que, a diferencia de la mayoría del hardware del mercado, los servidores de Google no incluyen componentes innecesarios, como tarjetas de vídeo, conjuntos de chips o conectores periféricos, que pueden abrir la puerta a vulnerabilidades. Los recursos del servidor se asignan de forma dinámica, lo que proporciona la flexibilidad para crecer y la capacidad de adaptarse de manera rápida y eficiente, añadiendo o reasignando recursos en función de la demanda de los clientes. El mantenimiento de este entorno homogéneo se realiza mediante software de Google que monitoriza constantemente los sistemas para detectar la presencia de modificaciones del código binario. Si se encuentra alguna modificación que difiere de la imagen de Google estándar, el sistema recupera automáticamente su estado oficial. Estos mecanismos automatizados de resolución de incidentes se reparan por sí solos y están diseñados para permitir que Google monitorice y resuelva eventos desestabilizadores, reciba notificaciones sobre incidencias y ralentice las posibles amenazas para la red antes de que se conviertan en problemas críticos.

Monitorización y eliminación de hardware

Google utiliza códigos de barras y etiquetas de recursos para monitorizar el estado y la ubicación de los equipos de los centros de datos durante todas las etapas de su ciclo de vida, desde la adquisición hasta la instalación, la retirada y la destrucción. Además, se han implementado detectores de metales y dispositivos de videovigilancia para que ningún equipo salga del centro de datos sin autorización. Cuando un componente no pasa una prueba de rendimiento en algún punto de su ciclo de vida en el centro de datos, se quita del inventario y se retira.

Cada centro de datos se adhiere a una política de eliminación estricta y cualquier divergencia se resuelve de inmediato. A la hora de retirar una unidad de disco duro, el personal autorizado debe comprobar que el disco está vacío. Para ello, sobrescribe la unidad con ceros y lleva a cabo un proceso de verificación de varios pasos para asegurarse de que la unidad no contiene ningún dato. Si la unidad de almacenamiento no se puede borrar por algún motivo, se guarda de forma segura hasta que pueda destruirse físicamente. La destrucción física de los discos consta de múltiples etapas: comienza con una trituradora que deforma la unidad, seguida de otra que la hace añicos, que finalmente se reciclan en una instalación segura.



Una red mundial con ventajas de seguridad únicas

La red de datos IP de Google está compuesta por cables de fibra propios, cables de fibra públicos y cables submarinos. Esto nos permite ofrecer servicios con una latencia baja y una alta disponibilidad en todo el mundo.

En otros servicios en la nube y soluciones on-premise, los datos del cliente deben realizar varios trayectos entre dispositivos, que se conocen como "saltos", a través de la red de Internet pública. El número de saltos depende de la distancia entre el proveedor de Internet del cliente y el centro de datos de la solución, y cada salto supone una oportunidad para que alguien pueda atacar o interceptar dichos datos. Al estar conectada a la mayoría de los proveedores de Internet del mundo, la red global de Google refuerza la seguridad de los datos en tránsito, ya que limita los saltos por la red pública.

La defensa reforzada describe las diversas capas de protección que escudan a la red de Google frente a ataques externos. Para empezar, se utilizan cortafuegos y Listas de control de acceso (LCAs), estándares del sector para separar la red, y todo el tráfico se enruta a través de los servidores personalizados del sistema Google Front End (GFE) para detectar y detener solicitudes maliciosas y ataques de denegación de servicio distribuido (DDoS). Además, los servidores del GFE solo pueden comunicarse internamente con una lista controlada de servidores. Esta configuración de denegación predeterminada evita que dichos servidores accedan a recursos no deseados. Por último, los registros se examinan a menudo para revelar cualquier uso malintencionado de errores de programación, y solo el personal autorizado puede acceder a los dispositivos de red. Como resultado, solo pueden atravesar la red los servicios y protocolos autorizados que cumplan nuestros requisitos de seguridad. Todo lo demás se queda fuera.

Encriptado de los datos en tránsito y en reposo

El encriptado es una parte importante de la estrategia de seguridad de Google Workspace que permite proteger tus correos electrónicos, chats, videollamadas, archivos, etc. Primero, como se describe más abajo, encriptamos determinados datos que se almacenan en reposo, es decir, en un disco (incluidas las unidades de estado sólido) o en una copia de seguridad. Incluso si un atacante o alguien con acceso físico se hace con el equipo de almacenamiento de los datos, será imposible que los lea, ya que no dispondrá de las claves de encriptado necesarias. En segundo lugar, encriptamos todos los datos en tránsito de los clientes: cuando viajan por Internet y en la red de Google al transferirlos de un centro de datos a otro. Si algún atacante intercepta estas transmisiones, solo podría capturar datos encriptados. Más abajo, veremos en detalle cómo encriptamos los datos almacenados en reposo y en tránsito.

Google ha liderado el sector con el uso de Seguridad de la capa de transporte (TLS) para el enrutamiento de correo electrónico, lo que permite encriptar la comunicación entre los servidores de Google y otros externos. Al mandar un correo electrónico desde un servidor de Google a otro externo compatible con TLS, el tráfico se encripta para evitar que se intercepte de manera pasiva. Para nosotros, aumentar la adopción de TLS es tan importante para el sector que hablamos del progreso de TLS en nuestro Informe de transparencia sobre el cifrado de correo electrónico. También hemos mejorado la seguridad del correo electrónico en tránsito. Para ello, hemos desarrollado el estándar MTA-STS, con el que los dominios receptores pueden exigir que se proteja la integridad y la confidencialidad del transporte de correos electrónicos. Los clientes de Google Workspace también tienen la ventaja añadida de requerir que los correos electrónicos se transmitan solo a dominios y direcciones específicos, siempre que estén protegidos mediante TLS. Para habilitar este permiso, configura el cumplimiento de TLS.

Si quieres ampliar tus conocimientos sobre el encriptado, consulta el informe de Google Workspace al respecto.

Solución con baja latencia y alta disponibilidad

Diseñamos todos los componentes de nuestra plataforma para que sean altamente redundantes, desde el diseño de nuestros servidores y el modo en que almacenamos los datos, hasta la conectividad de la red y de Internet, pasando por los servicios de software en sí. Esta redundancia total incluye la gestión de errores desde el diseño y permite crear soluciones que no dependan de un solo servidor, centro de datos ni conexión de red.

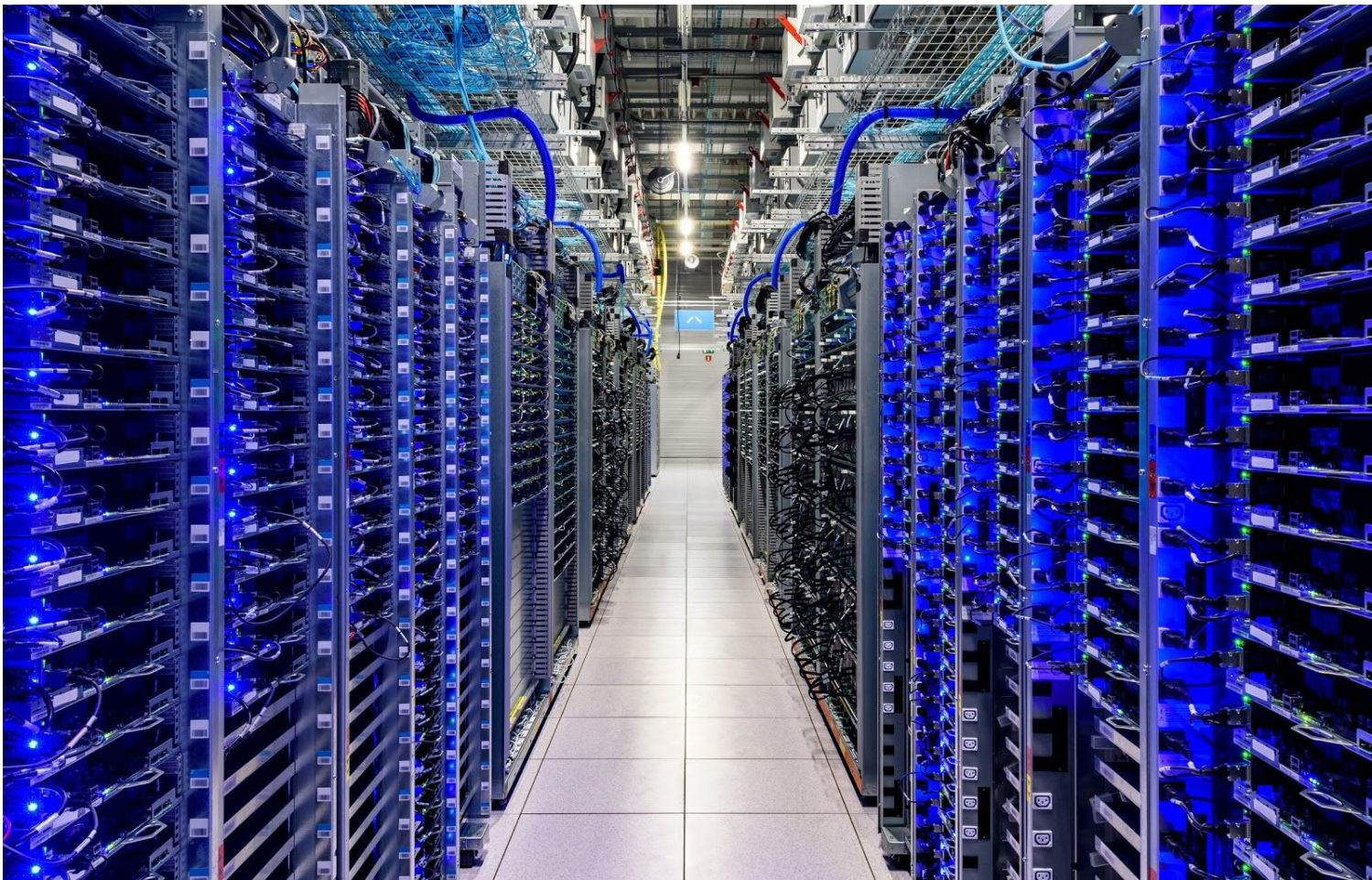
Los centros de datos de Google están distribuidos geográficamente para minimizar los efectos de las interrupciones del servicio que afectan a una región (como catástrofes naturales o problemas locales). En caso de que se produzca algún fallo en el hardware, el software o la red, los datos pasan automáticamente a otra instalación para que los clientes de Google Workspace puedan seguir trabajando sin ninguna interrupción en la mayoría de los casos. De esta forma, los clientes con una plantilla de trabajadores repartidos por todo el mundo pueden colaborar en documentos y videoconferencias, entre otros, sin necesidad de configurar nada ni gastar más para disfrutar de una experiencia de alto rendimiento y baja latencia similar a la que tendrían si trabajaran juntos en una misma red mundial.

Además, como nuestra infraestructura es altamente redundante, los clientes están a salvo de las pérdidas de datos. En el caso de Google Workspace, nuestros objetivos de punto de recuperación (RPO) y tiempo de recuperación (RTO) son cero. Queremos lograr estos objetivos mediante la replicación síncrona o en directo: las acciones del usuario en los productos de Google Workspace se replican simultáneamente en dos centros de datos, de modo que, si uno de ellos presenta un fallo, transferimos los datos al otro, que también ha estado imitando sus acciones.

Para hacerlo de una manera eficiente y segura, los datos de los clientes se dividen en fragmentos digitales con nombres de archivo aleatorios. Ni el contenido ni los nombres de archivo de estos fragmentos se almacenan en un formato legible por humanos. Por otro lado, los datos del cliente almacenados no se pueden rastrear hasta un usuario o aplicación específicos si simplemente se inspeccionan donde se encuentran almacenados. Cada fragmento se replica prácticamente en tiempo real en varios discos, servidores y centros de datos para evitar que haya un solo punto de fallo. Para estar mejor preparados para lo peor, realizamos simulacros de recuperación tras fallos como si determinados centros de datos (incluidas nuestras sedes corporativas) dejarán de estar disponibles durante 30 días.

Disponibilidad del servicio

En algunas jurisdicciones, es posible que algunos de los servicios de Google no estén disponibles ahora mismo o de forma temporal. En el Informe de transparencia de Google se muestran interrupciones del tráfico recientes y en curso que afectan a los productos de Google. Con nuestro código, podemos observar patrones de tráfico mundiales a lo largo del tiempo, lo que nos permite detectar cambios importantes. También consultamos nuestros gráficos cuando recibimos consultas de periodistas, activistas u otras personas interesadas. Proporcionamos estos datos para que el público pueda analizar y entender la disponibilidad de la información online.



Google Workspace

Cumplir los requisitos

Google se compromete a proporcionar productos y servicios seguros que satisfagan las necesidades de cumplimiento y realización de informes de los usuarios. Compartimos mucha información sobre las prácticas recomendadas y facilitamos el acceso a nuestra documentación relacionada con el cumplimiento. Google Cloud te ofrece recursos de seguridad, auditorías y certificaciones de terceros, documentación y compromisos jurídicos líderes del sector para ayudarte en el proceso de cumplimiento. Nuestros productos se someten regularmente a controles de seguridad, privacidad y cumplimiento que se verifican de forma independiente. Asimismo, obtienen certificaciones y pasan atestaciones de cumplimiento y auditorías que demuestran su conformidad con diversos estándares internacionales. Como parte de nuestro proceso de verificación independiente, nuestras prácticas de seguridad integral, incluidos los centros de datos, infraestructuras y operaciones, se someten a auditorías externas. También se han creado recursos y documentos de referencia que se ajustan a los marcos reguladores y a las leyes en aquellas áreas en las que no se aplican o no son necesarias certificaciones ni atestaciones formales. En nuestro Centro de recursos para el cumplimiento encontrarás más información sobre nuestros recursos y documentos de cumplimiento.

Trabajamos constantemente para abarcar cada vez más requisitos de cumplimiento. En Google, evaluamos las directrices proporcionadas por los principales estándares y organismos reguladores, y adaptamos nuestros programas de seguridad y privacidad a los cambios que se producen en torno al cumplimiento. Seleccionamos los programas detenidamente en función de la región y el sector para asegurarnos de que los clientes pueden aprovechar nuestros recursos de cumplimiento para tomar decisiones informadas sobre su actividad empresarial.

Si te estás planteando recurrir a Google Workspace, puedes consultar nuestras soluciones de cumplimiento para confirmar si este paquete de productos se ajusta a tus necesidades de seguridad y cumplimiento.

Cumplimiento normativo

Nuestros clientes pertenecen a sectores regulados, como el financiero, el gubernamental, el sanitario y el educativo. La forma de proporcionar productos y servicios de Google Cloud permite a los clientes cumplir numerosos requisitos específicos de su sector. Consulta más información al respecto.

Certificaciones y atestaciones externas independientes

Nuestros clientes y organismos reguladores esperan que se realice una verificación independiente de los controles de seguridad, privacidad y cumplimiento. Para estar a la altura de estas expectativas, Google se somete regularmente a diversas auditorías de terceros independientes. Algunos de los estándares internacionales clave que auditamos son:

- ISO/IEC 27001 (gestión de la seguridad de la información)
- ISO/IEC 27017 (seguridad en la nube)
- ISO/IEC 27018 (privacidad en la nube)
- ISO/IEC 27701 (privacidad)
- Informes SOC 2 y SOC 3

Google también participa en marcos reguladores específicos de diversos sectores y países, como FedRAMP (gobierno de EE. UU.), C5:2020 (Alemania), MTCS (Singapur) y muchos otros. También proporcionamos recursos y documentos de referencia que se ajustan a los marcos reguladores en aquellas áreas en las que no se aplican o no son necesarias certificaciones ni atestaciones formales.

Visita el Centro de recursos para el cumplimiento para consultar el listado completo de nuestras soluciones de cumplimiento.

Uso de datos

Nuestra filosofía

Los clientes de Google Workspace tienen la propiedad de sus datos de clientes, no Google. Los datos de los clientes que las organizaciones de Google Workspace introducen en nuestros sistemas son suyos, y no los analizamos con fines publicitarios. Ofrecemos a los clientes una Adenda sobre Tratamiento de Datos detallada en la que se describe nuestro compromiso de proteger los datos de los clientes. Por otro lado, si los clientes eliminan sus datos, nos comprometemos a hacer lo propio en nuestros sistemas en un plazo de 180 días. Por último, proporcionamos una serie de herramientas para que a los administradores de clientes les resulte más fácil llevarse los datos si eligen dejar de usar nuestros servicios, sin ningún tipo de penalización ni cargo adicional por parte de Google.

Ausencia de publicidad en Google Workspace

No mostramos publicidad en los servicios principales de Google Workspace ni tenemos previsto que esto cambie en el futuro. Google no recoge, analiza ni utiliza los datos de los servicios principales de Google Workspace con fines publicitarios. Los administradores de clientes pueden restringir el acceso a los servicios no principales desde la consola de administración de Google Workspace. Google indexa los datos de los clientes para ofrecerles servicios de gran utilidad, como el filtrado de spam, la detección de virus, el corrector ortográfico y la posibilidad de buscar correos y archivos en una cuenta concreta.

Acceso a datos y restricciones

Acceso administrativo

Al diseñar nuestros sistemas, hemos limitado el número de empleados que pueden acceder a los datos de los clientes. Además, monitorizamos de manera activa sus actividades. A los empleados de Google solo se les concede un conjunto limitado de permisos predeterminados para acceder a los recursos de la empresa. Controlamos el acceso a las herramientas de asistencia internas mediante LCAs y seguimos un proceso formal para conceder o revocar el acceso de los empleados a los recursos de Google. Por otra parte, una vez que dejan la empresa, los antiguos trabajadores pierden el acceso a ellos automáticamente. La autorización de acceso es obligatoria en todas las capas importantes del sistema. Las aprobaciones se gestionan mediante herramientas de flujo de trabajo y quedan reflejadas en los registros.

La configuración de los ajustes de autorización de los empleados se utiliza para controlar el acceso a todos los recursos, incluidos los datos y los sistemas de los productos de Google Workspace. Nuestro equipo específico de seguridad monitoriza el acceso para comprobar la eficacia de nuestros controles: presta atención a los patrones de acceso e investiga las actividades sospechosas.

Asimismo, proporcionamos la función Transparencia de acceso como parte del compromiso a largo plazo de Google con la transparencia y la confianza de los usuarios.[1] Gracias a ella, los clientes pueden consultar registros de las acciones que han llevado a cabo miembros del personal de Google al acceder a los datos específicos de los clientes. En los servicios integrados con Transparencia de Acceso, Google usa una herramienta para comprobar que la justificación empresarial presentada para respaldar el acceso es válida, y la anota en los registros de Transparencia de acceso.

Para obtener más información, consulta el informe sobre la seguridad de los datos en Google Workspace.

Para administradores de clientes

Los clientes pueden controlar el acceso a los datos y servicios de Google Workspace para asegurarse de que sus datos están protegidos de conformidad con la configuración elegida por la organización. Con los controles de acceso basados en roles, los clientes pueden nombrar administradores para concederles acceso a la consola de administración de Google Workspace, donde podrán realizar ciertas tareas. Puedes convertir a un usuario en superadministrador para que pueda hacer todas las tareas disponibles en la consola de administración o asignarle un rol que limite las tareas que puede realizar el administrador, como solo crear grupos, gestionar la configuración de servicios o cambiar la contraseña de los usuarios.

Solicitudes de datos por parte de las autoridades competentes

El cliente, como propietario de los datos, es el principal responsable a la hora de responder ante las autoridades competentes en lo que a sus datos se refiere. Además, de acuerdo con nuestra política, cuando un organismo gubernamental nos solicita tal información, lo remitimos directamente al cliente en cuestión. Sin embargo, al igual que otras empresas de tecnología y de comunicación, Google puede recibir solicitudes directas por parte de gobiernos y tribunales de todo el mundo para que proporcionemos datos sobre el uso que ha hecho una persona de los servicios que ofrece la empresa. Tomamos medidas para proteger la privacidad de los clientes y limitar las solicitudes excesivas, a

[1] La función Transparencia de acceso solo está disponible con Google Workspace Enterprise y G Suite Enterprise for Education.

la vez que cumplimos nuestras obligaciones legales. Por eso, tenemos el respeto por la privacidad y la seguridad de los datos que se almacenan con Google en mente a la hora de cumplir dichas obligaciones.

Puedes consultar información detallada sobre las solicitudes de datos y la respuesta de Google en nuestro Informe de transparencia. Para entrar más en materia, también puedes leer nuestro informe sobre la seguridad de los datos en Google Workspace.

Proveedores externos

Google realiza directamente casi todas las actividades de tratamiento de datos para prestar sus servicios. No obstante, también puede contratar a proveedores externos para que presten servicios relacionados con Google Workspace, como servicios de asistencia técnica o de otros tipos. Antes de incorporar proveedores externos, Google evalúa sus prácticas de seguridad y privacidad para asegurarse de que están acordes con el acceso que tendrán a los datos y al alcance de los servicios que se comprometen a prestar. Cuando Google ha sopesado los riesgos que presenta el proveedor externo, este debe suscribir las condiciones del contrato adecuadas en materia de seguridad, confidencialidad y privacidad.

Google Workspace

Dotar de medios a usuarios y administradores para mejorar la seguridad y el cumplimiento

Google integra controles de seguridad en la infraestructura, la tecnología, las operaciones y el tratamiento de los datos de los clientes. De manera predeterminada, todos los clientes de Google Workspace se benefician de nuestros sólidos sistemas e infraestructura de seguridad. A partir de ahí, ponemos activamente distintos recursos a disposición de los usuarios para que mejoren y personalicen sus ajustes concretos de seguridad para adaptarlos a las necesidades de su empresa mediante paneles de control y asistentes de seguridad de cuentas.

Google Workspace también ofrece a los administradores un control total a la hora de configurar la infraestructura, las aplicaciones y las integraciones de los sistemas en un único panel de control mediante nuestra consola de administración, sea cual sea el tamaño de la organización. Esto simplifica la administración y configuración. Pongamos como ejemplo la implementación de DKIM (un método de prevención contra el phishing) en un sistema de correo electrónico on-premise. Normalmente, los administradores tendrían que aplicar parches y configurar cada servidor por separado, y cualquier error de configuración provocaría una interrupción del servicio. Al usar nuestra consola de administración, en cambio, se puede configurar DKIM en cuestión de minutos en cientos de miles de cuentas con total tranquilidad sin que se produzca ninguna interrupción del servicio ni haya ventanas de mantenimiento.

Esto es solo un ejemplo, pero los administradores tienen muchas herramientas útiles a su alcance que pueden usar para cumplir sus requisitos de seguridad e integración de sistemas, incluidas funciones de autenticación como la verificación en dos pasos y el inicio de sesión único, o políticas de seguridad del correo electrónico como el cumplimiento obligatorio del protocolo TLS.

Acceso y autenticación

Verificación en dos pasos y llaves de seguridad

Para reforzar la seguridad de su cuenta, los clientes pueden usar la verificación en dos pasos y las llaves de seguridad,[1] que pueden ayudarles a mitigar riesgos como la configuración incorrecta de los controles de acceso de empleados o la aparición de atacantes que aprovechen las cuentas vulneradas.[2] Con el Programa de Protección Avanzada para empresas, podemos implementar una selección de políticas de seguridad eficaces en las cuentas de los usuarios registrados. Por ejemplo, se puede exigir el uso obligatorio de llaves de seguridad, bloquear el acceso a aplicaciones que no sean de confianza y disfrutar de análisis avanzados para detectar amenazas relacionadas con el correo electrónico.

Inicio de sesión único (SAML 2.0)

Google Workspace ofrece a los clientes el inicio de sesión único (SSO) para que puedan acceder a varios servicios desde la misma página y con las mismas credenciales de autenticación. Está basado en SAML 2.0, un estándar XML con el que los dominios web seguros pueden intercambiar datos de autenticación y autorización de los usuarios. Para mayor seguridad, el SSO acepta claves públicas y certificados generados tanto con el algoritmo RSA como con el DSA. Las organizaciones de clientes pueden usar el servicio SSO para integrar el inicio de sesión único de Google Workspace en su sistema LDAP o en cualquier otro del SSO.

OAuth 2.0 y OpenID Connect

Google Workspace es compatible con OAuth 2.0 y con OpenID Connect, un protocolo abierto de autenticación y autorización con el que los clientes pueden configurar un servicio SSO para varias soluciones en la nube. Los usuarios pueden iniciar sesión en aplicaciones de terceros mediante Google Workspace (y viceversa) sin tener que volver a introducir sus credenciales ni compartir información sensible sobre su contraseña.

Gestión de los derechos de la información (IRM)

La mayoría de las organizaciones también tienen políticas internas que rigen el **tratamiento de los datos sensibles**. Para ayudar a los administradores de Google Workspace a mantener el control sobre este tipo de datos, ofrecemos la función de **gestión de los derechos de la información (IRM)** de Drive. Tanto administradores como usuarios pueden aprovechar los permisos de acceso de Google Drive para proteger el contenido sensible y evitar que un archivo se vuelva a compartir, se descargue, se imprima o se copie, o bien que se cambien los permisos.

Entrega de correos electrónicos restringida

De manera predeterminada, los usuarios con cuentas de Gmail de tu dominio pueden intercambiar correos electrónicos con cualquier dirección. Pero, en algunos casos, puede que los administradores quieran restringir las direcciones de correo electrónico con las que pueden hacerlo. Por ejemplo, es probable que un centro educativo permita que los alumnos se escriban con los profesores y con otros alumnos, pero no con nadie ajeno al centro.

---

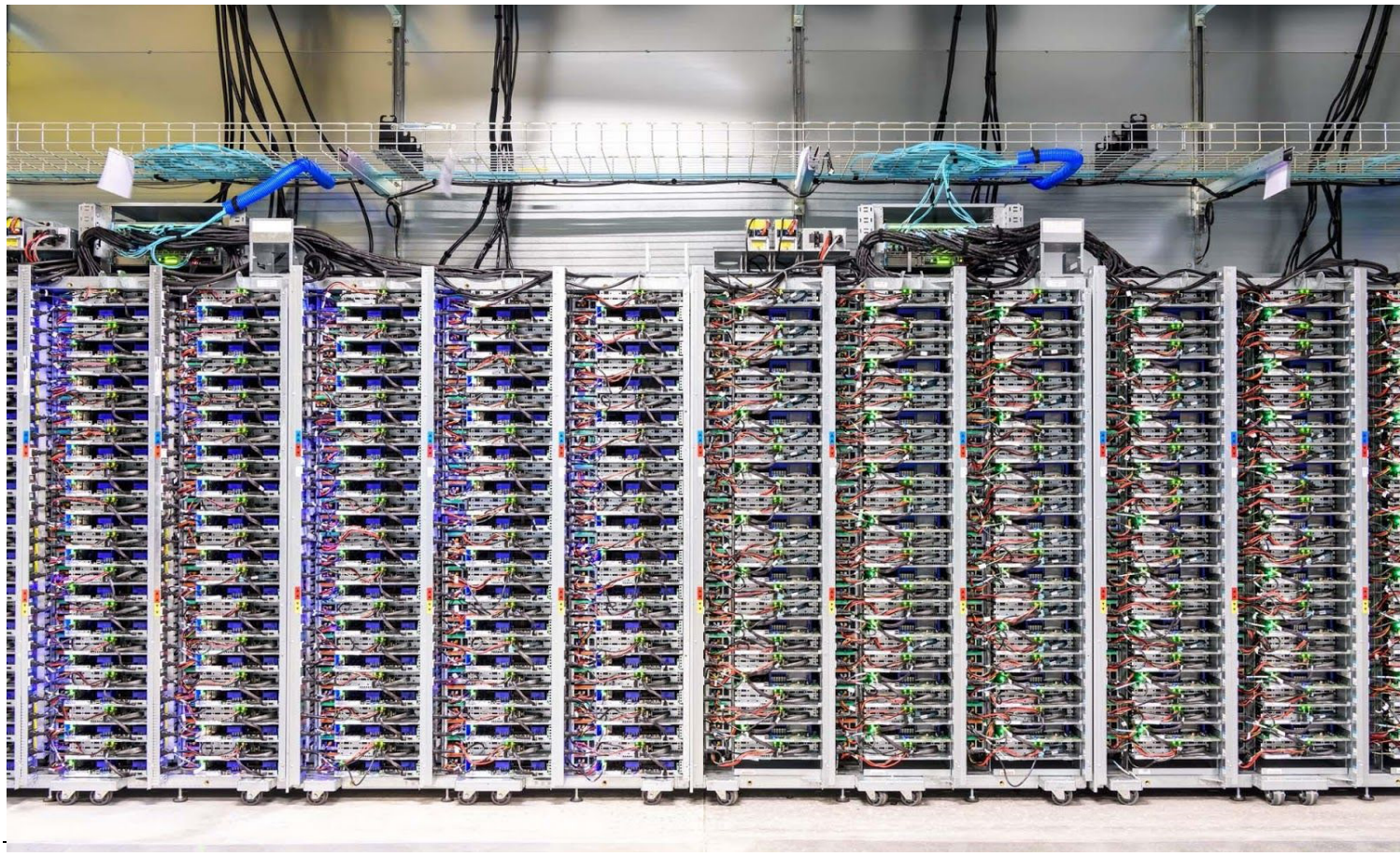
[1] Puedes informarte sobre cómo implementar la verificación en dos pasos en nuestro Centro de Ayuda.

[2] Consulta las listas de comprobación de seguridad para ver prácticas recomendadas al respecto.

Con el ajuste Restricción de envío, los administradores pueden especificar con qué direcciones y dominios pueden intercambiar correos electrónicos los usuarios. Al hacerlo, los usuarios solo pueden comunicarse con las partes autorizadas. Si intentan mandar un correo electrónico a un dominio que no lo esté, les aparecerá un mensaje indicándoles la política que prohíbe mandar correos electrónicos a esa dirección y se les confirmará que el mensaje no se ha enviado. Asimismo, los usuarios solo recibirán mensajes autenticados de los dominios autorizados. Los mensajes que se envíen desde dominios no autorizados (o desde dominios autorizados que no se puedan verificar mediante los registros DKIM o SPF) se devolverán al remitente con un mensaje con información sobre esta política.

Acceso a las aplicaciones según el contexto del usuario

Para facilitar el acceso de los usuarios y proteger al mismo tiempo la seguridad de sus datos, Google ha desarrollado el acceso contextual.[1] Proporciona controles granulares de las aplicaciones de Google Workspace según la identidad del usuario y el contexto de la solicitud (como el estado de seguridad del dispositivo o la dirección IP). Gracias al modelo de seguridad BeyondCorp desarrollado por Google, los usuarios pueden acceder a las aplicaciones web y a los recursos de la infraestructura desde prácticamente cualquier dispositivo y lugar, sin tener que recurrir a las pasarelas VPN de acceso remoto, a la vez que los administradores pueden implementar controles en el dispositivo. Además, puedes seguir creando y aplicando políticas de acceso, como la verificación en dos pasos, a todos los miembros de una unidad organizativa o un grupo.



[1] Integrado con Cloud Identity. Para proteger el acceso a las aplicaciones de Google Workspace con las funciones de acceso contextual, se necesita una licencia de Cloud Identity Premium o Google Workspace Enterprise.

Protección de recursos

Protección contra el spam, el phishing y el software malicioso

Gmail protege el correo entrante contra el spam, los intentos de phishing y el software malicioso. Nuestros modelos de aprendizaje automático son muy eficaces en este sentido y, junto con el resto de nuestras protecciones, ayudan a bloquear más del 99,9 % de las amenazas para impedir que lleguen a las bandejas de entrada de Gmail. Uno de nuestros principales sistemas de protección se dedica a analizar software malicioso y procesa más de 300.000 millones de archivos adjuntos a la semana para bloquear el contenido dañino.[1] El 63 % de los documentos maliciosos que bloqueamos varía de un día para otro.[2] Además, Gmail puede analizar o ejecutar los archivos adjuntos en un entorno virtual al que nos referimos como la zona de pruebas de seguridad. Si los considera una amenaza, se dirigen a las carpetas de spam de los usuarios o se ponen en cuarentena.

Estamos mejorando continuamente la precisión con la que detectamos el spam, y para ello contamos con la detección temprana de phishing, un modelo de aprendizaje automático específico que retarda los mensajes de forma selectiva (de media, menos del 0,05 % de los mensajes) para realizar rigurosos análisis de phishing y proteger aún más los datos de los usuarios.

Nuestros modelos de detección se integran con las tecnologías de aprendizaje automático de Navegación segura de Google para detectar URLs sospechosas y de phishing, e informar al respecto. Estos modelos nuevos combinan diversas técnicas, como el análisis de la similitud y reputación de las URLs, y nos permiten generar advertencias al hacer clic en los enlaces de phishing y software malicioso. A medida que detectamos nuevos patrones, nuestros modelos se perfeccionan y se adaptan más rápido de lo que podría esperarse de cualquier sistema manual.

Prevención de spoofing

A veces, los distribuidores de spam pueden falsificar la dirección del remitente en los correos electrónicos para que parezcan provenir del dominio de una organización respetable. Para ayudar a evitar el spoofing, Google participa en el programa DMARC, que permite a los propietarios de dominios indicar a los proveedores de correo electrónico qué hacer con los mensajes no autenticados de su dominio. Para utilizar DMARC, los clientes de Google Workspace deben crear un registro DMARC en su configuración de administrador e implementar un registro SPF y claves DKIM en todo el correo saliente.

Advertencias para que los empleados eviten la pérdida de datos

Cuando dotamos de medios a los empleados para que tomen las decisiones adecuadas para proteger los datos, la estrategia de seguridad de una empresa puede mejorar considerablemente. Para ponerlo más fácil, Gmail muestra advertencias de respuestas externas no intencionadas a los usuarios para ayudarles a evitar la pérdida de datos. Si intentas responder a alguien fuera del dominio de tu empresa, recibirás una pequeña advertencia para comprobar que de verdad quieres mandar ese correo electrónico. Y como Gmail se sirve de la inteligencia contextual, sabe si el destinatario es uno de tus contactos o alguien con quien interactúas con frecuencia. Así, evitamos mostrar estas advertencias si no es necesario.

---

[1] En febrero del 2020.

[2] En febrero del 2020.

S/MIME alojado para una mayor seguridad

Con la solución de S/MIME alojado de Google, al recibir un correo electrónico encriptado con S/MIME, se almacena usando el encriptado de Google. Esto implica que el correo se procesa de la forma habitual. Esto incluye las protecciones exhaustivas contra el spam, el phishing y el software malicioso, así como servicios de administración (como reglas de enrutamiento de correo electrónico, auditoría y conservación de Vault) y funciones muy útiles para el usuario final, como la categorización del correo electrónico, la búsqueda avanzada y la Respuesta inteligente. Esta es la solución más segura para la gran mayoría de los correos electrónicos, ya que aporta las ventajas de las políticas sólidas de autenticación y encriptado en tránsito sin renunciar a la seguridad ni a las funciones del procesamiento de Google.

Modo confidencial de Gmail

El modo confidencial puede ayudar a los usuarios de Gmail a evitar que personas no autorizadas accedan a información sensible. Cuando se activa esta función, los destinatarios no pueden reenviar, copiar, imprimir ni descargar mensajes ni archivos adjuntos. Los remitentes pueden fijar fechas de vencimiento de los correos, revocar el acceso a ellos en cualquier momento u obligar a que se introduzca un código de verificación que se envía por SMS para poder acceder a los mensajes.

Prevención de la pérdida de datos (DLP) en Gmail y Drive

La prevención de la pérdida de datos (DLP)[1] añade un nivel adicional de protección para impedir que se filtre a miembros ajenos a la organización la información confidencial o privada, como los números de las tarjetas de pago, los números de identificación nacional o información médica protegida. Con DLP, los clientes pueden auditar el uso de contenido sensible en su empresa o activar advertencias y bloquear acciones para evitar que los usuarios **envíen datos confidenciales**. Para ello, proporciona detectores de contenido predefinidos, entre los que se incluyen la detección de identificadores mundiales y regionales, información médica y credenciales. Los clientes también pueden definir sus propios detectores personalizados según las necesidades de su empresa. Para los archivos adjuntos y los documentos basados en imágenes, DLP usa el reconocimiento óptico de caracteres de Google para mejorar la calidad y el alcance de la detección. Consulta más información sobre DLP de Gmail. También se puede usar para impedir que los usuarios compartan contenido sensible en Google Drive o en una unidad compartida con alguien ajeno a la organización. Además, los clientes pueden automatizar los controles de IRM y la clasificación de las reglas avanzadas de DLP para los archivos de Drive.

Configurar los ajustes de seguridad de Google Workspace

Gestión de alertas y seguridad

Las organizaciones suelen tener en marcha varios controles de seguridad y privacidad, por lo que **necesitan una ubicación centralizada desde la que evitar, detectar y neutralizar las amenazas.** En el centro de seguridad de Google Workspace[2] puedes consultar analíticas e información de seguridad avanzadas, así como supervisar y controlar problemas que podrían estar afectando a tu dominio en este sentido.[3] En él puedes encontrar analíticas de seguridad,

[1] Disponible solo para los clientes de Google Workspace Enterprise y G Suite Enterprise for Education.

[2] Incluido con Google Workspace Enterprise y G Suite Enterprise for Education.

[3] Si quieres acceder al centro de seguridad, necesitas una cuenta de administrador con licencia de Google Workspace Enterprise, G Suite Enterprise for Education, Drive Enterprise o Cloud Identity Premium Edition. En estos dos últimos servicios, los administradores cuentan con un subconjunto de informes del centro de seguridad en el panel de control de seguridad.

información útil y prácticas recomendadas por Google que te permitirán proteger la organización, los datos y a los usuarios. Como administrador, puedes usar el panel de control de seguridad para tener una perspectiva general de los diferentes informes del centro de seguridad. En la página sobre el estado de la seguridad puedes ver de forma clara los ajustes de la consola de administración, lo que te permite comprender y gestionar mejor los distintos riesgos de seguridad. También puedes usar la herramienta de investigación de seguridad para identificar y clasificar problemas de seguridad y privacidad en tu dominio, y tomar medidas al respecto. Los administradores pueden crear reglas de actividad para automatizar acciones en esta herramienta y así detectar y solucionar este tipo de problemas de un modo más rápido y eficiente. Por ejemplo, puedes crear una regla para que se envíen notificaciones por correo electrónico a determinados administradores cuando se compartan documentos de Drive con usuarios ajenos a la empresa.

Si eres cliente de Google Workspace, su Centro de alertas te proporciona alertas y datos sobre seguridad relacionados con la actividad en tu dominio para que puedas tomar medidas y proteger tu organización ante las nuevas amenazas, como el phishing, el software malicioso, las cuentas sospechosas y la actividad cuestionable en un dispositivo. También puedes usar la API del Centro de alertas para exportarlas a tus plataformas de gestión de incidencias o de eventos e información de seguridad (SIEM).

Dominios de confianza para compartir contenido de Drive

Los administradores pueden controlar cómo comparten los usuarios de su organización archivos y carpetas en Google Drive. Por ejemplo, deciden si se pueden compartir archivos con personas ajenas a la organización o si se limita el intercambio de contenido a los dominios de confianza.[1] También se pueden definir unas alertas para recordar a los usuarios que comprueben que los archivos no son confidenciales antes de compartirlos con alguien ajeno a la organización.

Seguridad durante las videollamadas

Google Meet aprovecha la misma infraestructura segura desde el diseño, la protección integrada y la red global que utiliza Google para salvaguardar tu información y privacidad. Nuestras medidas de protección contra el uso inadecuado, entre las que se incluyen controles antihackers, tanto en videoconferencias como en llamadas telefónicas, están activadas de forma predeterminada para que puedas reunirte virtualmente de forma segura.

Los usuarios de Chrome, Firefox, Safari y la nueva versión de Edge no tienen que instalar ningún complemento ni programa de software, ya que Meet solo necesita el navegador. De este modo, se reducen la superficie de ataque de Meet y el número de parches de seguridad que se deben aplicar en los ordenadores de los usuarios finales. Si vas a usar un dispositivo móvil, te recomendamos instalar la aplicación Google Meet desde el App Store de Apple o desde Google Play Store.

Ofrecemos varias opciones prácticas y seguras de verificación en dos pasos de las cuentas, como llaves de seguridad de hardware o integradas en los teléfonos y notificaciones de Google. Además, los usuarios de Google Meet pueden registrar su cuenta en nuestro Programa de Protección Avanzada, que proporciona nuestras mejores medidas de protección contra el phishing y la interceptación de cuentas, y está diseñado específicamente para las cuentas de mayor riesgo. A día de hoy, ningún participante del programa ha sido víctima del phishing, por mucho que se le ataque repetidamente. Puedes informarte acerca de este programa en el Centro de Ayuda.

[1] Algunas funciones, como restringir el intercambio de contenido solo a los dominios incluidos en una lista blanca, están disponibles únicamente con Google Workspace Enterprise, Enterprise for Education, Drive Enterprise, Business, for Education y para Organizaciones sin Ánimo de Lucro.

Gestión de puntos finales

La protección de la información en **dispositivos móviles y de escritorio** puede ser un gran quebradero de cabeza para algunos. Los clientes de Google Workspace pueden usar la gestión de puntos finales[1] para ayudar a proteger los datos de la empresa que haya tanto en los dispositivos personales de los usuarios como en los que pertenecen a la organización. Al registrar los dispositivos para gestionarlos, los usuarios disfrutan de un acceso seguro a los servicios de Google Workspace y las organizaciones pueden definir políticas para proteger los datos y dispositivos mediante el encriptado de estos últimos, el bloqueo de la pantalla o el uso obligatorio de contraseñas. Además, si un dispositivo se roba o se pierde, es posible eliminar las cuentas de la empresa de los dispositivos móviles y cerrar la sesión de los usuarios de los dispositivos de escritorio de manera remota. Los administradores de TI también pueden gestionar y configurar dispositivos con Windows 10 mediante la consola de administración, y los usuarios pueden usar las credenciales de su cuenta de Google Workspace para iniciar sesión en los dispositivos con Windows 10 y acceder a las aplicaciones y servicios mediante el SSO.

Con los informes, los clientes pueden monitorizar el cumplimiento de las políticas y obtener información sobre los usuarios y dispositivos. Consulta más información sobre la gestión de puntos finales.

Analíticas para la creación de informes

Registros de auditoría con Google Workspace

Las empresas que almacenan sus datos en la nube quieren controlar el acceso a los datos y la actividad de la cuenta. Los registros de auditoría de Google Workspace permiten a los equipos de seguridad conservar registros de auditoría en Google Workspace y consultar información detallada sobre la actividad de administración, el acceso a los datos y los eventos del sistema. Los administradores de Google Workspace pueden usar la consola de administración para consultar estos registros, personalizarlos y exportarlos según sea necesario.

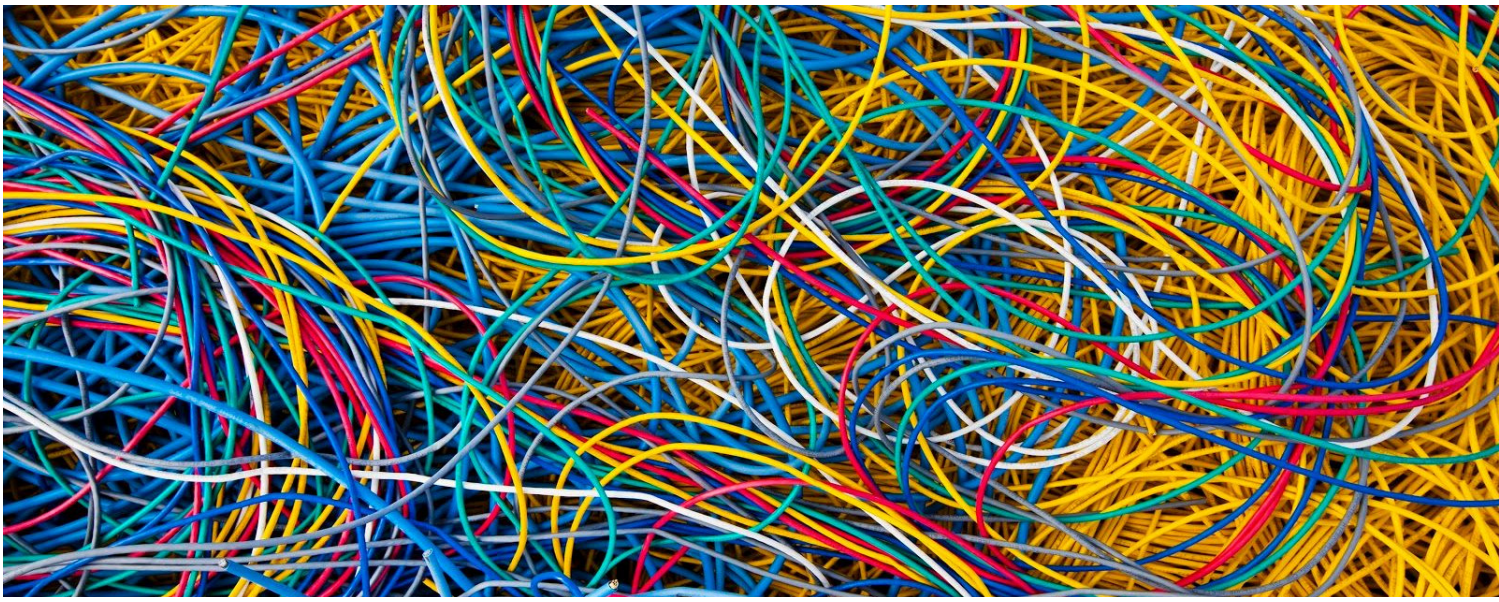
Informes de seguridad

Los administradores de Google Workspace tienen acceso a informes de seguridad que les proporcionan información esencial sobre la exposición de la organización a riesgos relacionados con los datos. Así, pueden descubrir rápidamente qué usuarios concretos pueden poner en riesgo la seguridad por omitir la verificación en dos pasos, instalar aplicaciones externas o compartir documentos de forma indiscriminada. Los administradores también pueden decidir si quieren recibir alertas cuando se detecte alguna actividad de inicio de sesión sospechosa que pueda suponer una amenaza para la seguridad.

Información valiosa con BigQuery

Los administradores de Google Workspace pueden exportar los registros de auditoría y otros datos a BigQuery. Gracias a este almacén de datos empresariales de Google pensado para las analíticas de datos a gran escala, se pueden analizar los registros de Google Workspace mediante sofisticadas consultas personalizadas que ofrecen excelentes resultados, así como aprovechar herramientas de terceros para poder ahondar más en los datos.

[1] Incluido de serie con Google Workspace.



Recuperación de datos

Restaurar usuarios eliminados recientemente

Los administradores tienen un plazo de 20 días para restaurar la cuenta de un usuario a partir del momento en que la hayan eliminado. Pasado ese tiempo, la consola de administración elimina la cuenta permanentemente, por lo que no será posible restaurarla, ni siquiera a través de la asistencia técnica de Google. Los administradores de clientes son los únicos que pueden eliminar cuentas.

Restaurar los datos de Drive o Gmail de un usuario

Los administradores tienen un plazo de 25 días para restaurar los datos de Drive o Gmail a partir del momento en que se haya vaciado la papelera, en función de las políticas de conservación que se hayan definido en Vault. Pasado ese tiempo, no es posible restaurar los datos, ni siquiera a través de la asistencia técnica de Google. Google elimina todos los datos eliminados por el cliente de todos sus sistemas lo antes posible, dentro de un plazo de 180 días como máximo.

Conservación y descubrimiento electrónico

Los administradores pueden activar Google Vault para conservar, bloquear, buscar y exportar datos, y responder así a las necesidades de conservación y descubrimiento electrónico de la organización. Vault admite datos como mensajes de Gmail, archivos de Google Drive y grabaciones de Google Meet, entre otros.

Residencia de los datos

Como administrador, puedes definir una política de región de datos para decidir la ubicación geográfica donde se van a almacenar los datos sujetos a ella: Estados Unidos o Europa. Las políticas de región de datos se aplican a los datos principales en reposo (incluidas las copias de seguridad) de estos servicios principales de Google Workspace. Entre los datos cubiertos se incluye el contenido de los archivos de Drive, los mensajes y archivos adjuntos de Google Chat y los asuntos y correos de Gmail, así como los datos de otros servicios principales.

Conclusión

La protección de tus datos es una cuestión primordial a la hora de diseñar todas las operaciones de infraestructura, productos y personal de Google. Consideramos que podemos ofrecer un nivel de protección que muy pocos proveedores de la nube pública o equipos de TI de empresas privadas pueden igualar.

Diseñamos Google Workspace para cumplir estrictos estándares de privacidad y seguridad de acuerdo con las prácticas recomendadas del sector. Además, proporcionamos unos compromisos contractuales muy estrictos sobre la propiedad y el uso de los datos, la seguridad, la transparencia y la responsabilidad. Con ellos nos aseguramos de que mantienes el control sobre tus datos y sobre cómo se tratan, para que tengas la certeza de que no se utilizarán con fines publicitarios ni para ningún otro propósito que no sea el de ofrecer los servicios de Google Cloud. Asimismo, ponemos a tu disposición todas las herramientas necesarias para que puedas satisfacer los requisitos de elaboración de informes y cumplimiento de normas pertinentes.

Y, como la protección de datos es un aspecto fundamental de Google Workspace, podemos invertir grandes cantidades en seguridad, recursos y especialización a una escala imposible para otras organizaciones. De este modo, puedes centrar toda tu atención en tu empresa y en innovar. Finalmente, gracias a nuestras operaciones y a la colaboración con la comunidad de investigación sobre seguridad, Google puede afrontar las vulnerabilidades de forma rápida o evitarlas por completo.

Por estas y otras muchas razones, más de seis millones de organizaciones de todo el mundo confían a Google su recurso más valioso: la información. Así pues, seguiremos invirtiendo en Google Workspace para que puedas aprovechar nuestros servicios de forma segura y transparente.