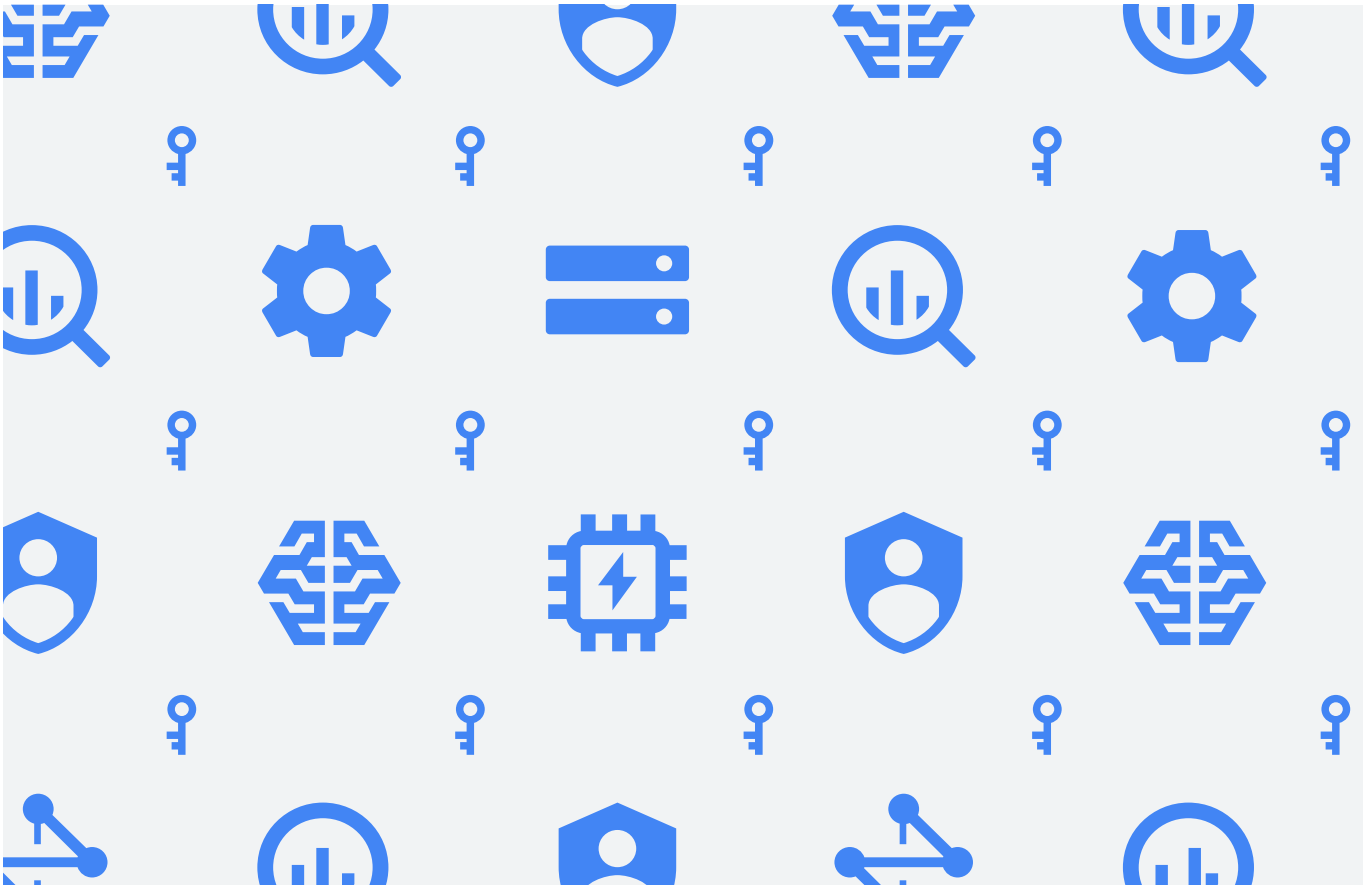
Google Cloud Whitepaper
Mayo 2018

Google Cloud y el Reglamento General de Protección de Datos (RGPD)



Google Cloud

Reglamento General de Protección de Datos (RGPD)

La normativa europea más importante en materia de protección de datos de los últimos veinte añosentrará en vigor el 25 de mayo del 2018. El Reglamento General de Protección de Datos (RGPD) reemplazará a la actual Directiva 95/46/ CE sobre la protección de los datos personales de 24 de octubre de 1995 (Directiva de Protección de Datos). El RGPD refuerza los derechos de los individuos en lo que respecta a sus datos personales y busca unificar las leyes de protección de datos en Europa con independencia del lugar en el que se procesen los datos.

Puedes contar con que Google se compromete a cumplir el RGPD en los servicios de Google Cloud. También estamos comprometidos a ayudar a nuestros clientes en su camino al cumplimiento del RGPD con las robustas medidas de seguridad y privacidad que hemos integrado en nuestros servicios y en nuestros contratos a lo largo de los años.

Qué puedes hacer?

¿Cuáles son tus responsabilidades como cliente?

Los clientes de G Suite[1] y de Google Cloud Platform normalmente actúan como responsables del tratamiento de los datos de carácter personal que proporcionan a Google en conexión con su uso de los servicios. Los responsables del tratamiento determinan los fines y los medios del tratamiento de los datos de carácter personal, y los encargados del tratamiento tratan los datos en nombre de los responsables del tratamiento. Google es el encargado del tratamiento y trata los datos de carácter personal en nombre del responsable del tratamiento cuando el responsable del tratamiento utiliza G Suite o Google Cloud Platform.

Los responsables del tratamiento deben implementar las medidas técnicas y organizativas adecuadas para asegurar y demostrar que el tratamiento de los datos se realiza en cumplimiento con el RGPD. Las obligaciones de los responsables del tratamiento están relacionadas con principios como la legitimidad, equidad y transparencia, la limitación de los fines, la minimización de los datos y la exactitud, así como con facilitar los derechos de los interesados con respecto a sus datos.

Si eres un responsable del tratamiento, puedes obtener información y directrices relativas a tus responsabilidades bajo el RGPD en la página web de la autoridad nacional en materia de protección de datos o en la de la autoridad competente bajo el RGPD (según corresponda)[2], y también en las publicaciones de las asociaciones de privacidad, como la Asociación Internacional de Profesionales de la Privacidad (International Association of Privacy Professionals, IAPP).

También deberías obtener asesoramiento legal independiente en relación con tu situación y tus obligaciones bajo el RGPD, ya que solamente un abogado puede ofrecerte asesoramiento legal específico para tu situación. Por favor ten en cuenta que nada en este sitio web va dirigido a ofrecerte asesoramiento legal ni debería usarse en sustitución de éste.

[1] G Suite omvat G Suite for Business en G Suite for Education.

[2] Te recomendamos que obtengas asesoramiento legal independiente para determinar la autoridad de protección de datos nacional o competente aplicable.

¿Por dónde deberías empezar?

Si eres un cliente o un futuro cliente de Google Cloud, ahora es un buen momento para empezar a prepararte para el RGPD. Considera estos consejos:

- Familiarízate con las disposiciones del RGPD y presta especial atención a las diferencias que pueda haber con respecto a tus obligaciones de protección de datos actuales.
- Plantéate crear un inventario actualizado de los datos personales que manejas. Puedes utilizar algunas de nuestras herramientas para identificar y clasificar los datos.
- Revisa tus controles, políticas y procesos para determinar si cumplen los requisitos del RGPD y crea un plan para abordar las diferencias.
- Considera cómo puedes aprovechar las funciones de protección de datos que existen en Google Cloud en tu propio marco de cumplimiento normativo.
- Revisa las certificaciones y auditorías de terceros con los que cuenta G Suite o Google Cloud Platform para ver cómo pueden ayudarte en este ejercicio.
- Realiza un seguimiento de las nuevas directrices normativas según estén disponibles y contacta con un abogado para obtener asesoramiento legal específico que se adapte a las circunstancias de tu empresa.

Qué estamos haciendo

G Suite y Google Cloud Platform compromisos con el RGPD

Los responsables del tratamiento están obligados, entre otras cosas, a solamente utilizar encargados del tratamiento que ofrezcan suficientes garantías para implementar las medidas técnicas y organizativas apropiadas, de manera que el tratamiento cumpla con los requisitos del RGPD. A continuación encontrarás algunos aspectos a considerar a la hora de evaluar los servicios de G Suite y Google Cloud Platform.

Los conocimientos, la fiabilidad y los recursos de un experto

Experiencia en la protección de datos

Google emplea a profesionales en el ámbito de la seguridad y de la privacidad, entre los que se encuentran algunos de los mayores expertos del mundo en materia de seguridad de la información, de aplicaciones y de redes. Este equipo se dedica a mantener los sistemas de defensa de la empresa, a desarrollar los procesos de revisión de seguridad, a crear la infraestructura de seguridad y a implementar las políticas de seguridad de Google. Google también cuenta con un extenso equipo de abogados, expertos en el cumplimiento normativoy especialistas en política pública que se encargan de preservar el cumplimiento de la privacidad y de la seguridad de Google. Estos equipos están en contacto con los clientes y partes interesadas de la industria, así como con las autoridades de supervisión con el fin de modelar nuestros servicios de G Suite y de Google Cloud Platform de forma que ayuden a nuestros clientes con sus obligaciones de cumplimiento.

Compromisos de protección de datos

Acuerdos de tratamiento de datos

Nuestros acuerdos de tratamiento de datos de G Suite y Google Cloud Platform exponen con claridad los compromisos de privacidad que hemos adquirido con nuestros clientes. Hemos desarrollado estos términos a lo largo de los años basándonos en los comentarios de nuestros clientes y organismos reguladores.Recientemente, hemos actualizado los acuerdos de tratamiento de datos de G Suite y Google Cloud Platform para que reflejen el RGPD y los hemos puesto a disposición de nuestros clientes mucho antes de que el RGPD entre en vigor para facilitar la valoración de su cumplimiento por parte de nuestros clientes y su disposición en relación con el RGPD cuando usen los servicios de Google Cloud.

Los clientes pueden aceptar ahora estos términos de tratamiento de datos actualizados a través del proceso de aceptación que se describe aquí para la adenda sobre tratamiento de datos de G Suite (G Suite Data Processing Amendment) y aquí para los términos de seguridad y de tratamiento de datos de Google Cloud Platform (GCP Data Processing and Security Terms). Los términos actualizados serán de aplicación a partir del 25 de mayo del 2018 (inclusive), cuando el RGPD entre en vigor.

Tratamiento según las instrucciones

Los datos que introducen nuestros clientes y sus usuarios en nuestros sistemas solamente serán tratados de acuerdo con sus instrucciones, tal y como se describe en nuestros términos de tratamiento de datos actualizados según el RGPD.

Compromiso de confidencialidad del personal

Todos los empleados de Google deben firmar un acuerdo de confidencialidad y realizar cursos obligatorios sobre confidencialidad y privacidad, y un curso sobre el Código de Conducta. En el Código de Conducta de Google se incluyen de forma específica las responsabilidades y el comportamiento que se espera de nuestros empleados en relación con la protección de la información.

Uso de subencargados del tratamiento

Las empresas del grupo Google llevan a cabo la mayor parte de las actividades de tratamiento de datos necesarias para poder ofrecer los servicios de G Suite y de Google Cloud Platform. No obstante, colaboramos con proveedores que ofrecen asistencia para estos servicios. Cada uno de nuestros proveedores se somete a un exigente proceso de selección para garantizar que cuenta con los conocimientos técnicos necesarios y que es capaz de ofrecer el nivel adecuado de seguridad y de privacidad. Ponemos a disposición de nuestros clientes información sobre los subencargados del tratamiento del grupo Google que ofrecen asistencia para los servicios de G Suite y Google Cloud Platform, así como sobre los proveedores subencargados del tratamiento que están involucrados en estos servicios. También incluimos compromisos relacionados con los subencargados en nuestros acuerdos actuales y actualizados de tratamiento de datos.

Seguridad de los servicios

Según el RGPD, el responsible y el encargado del tratamiento deben implementar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad acorde al riesgo. Google cuenta con una infraestructura global diseñada para ofrecer la seguridad más avanzada durante todo el ciclo de tratamiento de la información. Esta infraestructura se ha desarrollado para proveer nuestros servicios de forma segura, almacenamiento de datos seguro para salvaguardar la privacidad del usuario final, comunicaciones seguras entre servicios, comunicaciones seguras y privadas con los clientes a través de Internet y operaciones seguras de los administradores. G Suite y Google Cloud Platform están construidos en esta infraestructura.

Hemos diseñado la seguridad de nuestra infraestructura en capas que se sustentan recíprocamente, desde la seguridad física de los centros de datos hasta las medidas de seguridad de nuestro hardware y software,pasando por los procesos que utilizamos para aumentar la seguridad operativa. Gracias a esta protección por capas, conseguimos unos sólidos cimientos en materia de seguridad para todo lo que realizamos. Puedes encontrar una descripción detallada de nuestra Infraestructura de Seguridad en el informe técnico sobre el diseño de la infraestructura de seguridad de Google.

Disponibilidad, integridad y resistencia

Google diseña los componentes de nuestra plataforma para que sean altamente redundantes. Los centros de datos de Google están distribuidos geográficamente para minimizar los efectos de las interrupciones regionales del servicio en productos globales como desastres naturales o interrupciones locales. En caso de producirse un fallo en el hardware, software o en la red, los servicios se trasladan de una instalación a otra de forma automática e instantánea, de modo que las operaciones pueden continuar sin interrumpirse. Nuestra infraestructura altamente redundante protege a los clientes frente a las pérdidas de datos.

Pruebas

Cada año, Google realiza pruebas de recuperación de desastres con el objetivo de crear un espacio coordinado en el que los equipos de infraestructura y aplicaciones comprueben los planes de comunicación, las situaciones de conmutación por error, la transición operacional y otras respuestas de emergencia. Todos los equipos que participan en el ejercicio de recuperación tras fallos desarrollan planes de prueba y análisis posteriores, en los que se deja constancia de los resultados y de las lecciones aprendidas en las pruebas.

Encriptado

Google utiliza el encriptado para proteger los datos en tránsito y en reposo. Los datos en tránsito a G Suite están protegidos mediante HTTPS (esta opción está activada de forma predeterminada para todos los usuarios). Los servicios de G Suite y de Google Cloud Platform encriptan los datos en reposo de los clientes, sin que éstos tengan que realizar ninguna otra acción, utilizando uno o más mecanismos de encriptado. Puedes encontrar una descripción detallada de cómo encriptamos los datos en nuestro informe técnico sobre el encriptad.

Controles de acceso

Los derechos y niveles de acceso de los empleados de Google se basan en la función que desempeñan en su puesto de trabajo. Se aplican según los conceptos de asignación del menor grado de privilegios preciso y de información en el caso exclusivo de que sea necesario, de modo que los derechos de acceso se asignan en función de las responsabilidades definidas. Las peticiones para obtener más derechos de acceso siguen un proceso formal en el que es necesario que el propietario del sistema o de los datos, el administrador u otros directivos (tal y como dictan las políticas de seguridad de Google) aprueben la petición.

Administración de vulnerabilidades

Buscamos vulnerabilidades en el software mediante una combinación de herramientas comercialmente disponibles y herramientas internas específicas; pruebas de penetración exhaustivas, tanto manuales como automáticas; procesos de control de calidad; revisiones de seguridad de software y auditorías externas. También contamos con la investigación de seguridad de la comunidad y valoramos enormemente su labor a la hora de identificar vulnerabilidades en G Suite, Google Cloud Platform y otros productos de Google. Nuestro Vulnerability Reward Program anima a los investigadores a informarnos de problemas de diseño e implementación que puedan poner en peligro datos de clientes.

Seguridad de los Productos: G Suite

Los clientes de G Suite pueden utilizar las funciones y opciones de configuración de nuestros productos para aumentar la protección de sus datos personales contra un tratamiento no autorizado o ilegal:

- La verificación en 2 pasos reduce en gran medida el riesgo de acceso no autorizado al pedir una prueba de identidad adicional al iniciar sesión. El uso de la llave de seguridad añade otra capa de protección a las cuentas de los usuarios al precisar de una llave física.

- Las alertas de inicio de sesión sospechoso (Suspicious Logging Monitoring) permiten detectar inicios de sesión sospechosas mediante funciones de aprendizaje automático muy robustas.

- La seguridad aumentada para el correo electrónico require que todos los mensajes deban firmarse y encriptarse utilizando extensiones seguras multipropósito de correo de Internet (Secure/Multipurpose Internet Mail Extensions, S/MIME).

- La prevención de la pérdida de datos protege información sensible en Gmail y Drive de que pueda compartirse sin autorización. Puedes encontrar más información en nuestro informe técnico sobre la pérdida de datos.

- La administración de derechos de la información de Drive permite inhabilitar la descarga, la impresión y la copia de archivos desde el menú de uso compartido avanzado, así como establecer fechas de vencimiento para el acceso a los archivos.

- La gestión de dispositivos móviles ofrece una supervision continua del sistema y recepción de alertas en caso de actividad sospechosa en los dispositivos.

Para más información, visita esta página web

Sicurezza dei prodotti: GCP

I clienti di GCP possono sfruttare le funzioni e le configurazioni del prodotto per proteggere ulteriormente i dati personali da possibili elaborazioni non autorizzate o illegali:

- La verificación en 2 pasos reduce en gran medida el riesgo de acceso no autorizado al pedir una prueba de identidad adicional al iniciar sesión. El uso de la llave de seguridad añade otra capa de protección a las cuentas de los usuarios al precisar de una llave física..
- La gestión de identidad y acceso de Google Cloud (Google Cloud Identity and Access Management, Cloud IAM) te permite crear y administrar al detalle los permisos de acceso y modificación de los recursos en Google Cloud Platform.
- La API de prevención de la pérdida de datos (Data Loss Prevention API) te permite identificar y supervisar el tratamiento de categorías especiales de datos de carácter personal para implementar los controles adecuados.
- Stackdriver Logging y Stackdriver Monitoring integra el almace-namiento de registros, la supervisión, las alertas y los sistemas de detección de anomalías en Google Cloud Platform.
- Cloud Identity-Aware Proxy (Cloud IAP) controla el acceso a las aplicaciones en la nube que se ejecutan en Google Cloud Platform.
- Cloud Security Scanner busca y detecta vulnerabilidades comunes en las aplicaciones de Google App Engine.

Para más información, visita esta página web

Devolución y borrado de datos

Durante el periodo de vigencia del acuerdo, los administradores pueden exportar los datos del cliente en cualquier momento mediante la funcionalidad de los servicios de G Suite o de Google Cloud Platform. Hemos incluido, desde hace años, los compromisos relacionados con la exportación de datos, y seguiremos ofreciéndolos después de que el RGPD entre en vigor. También continuaremos trabajamos para mejorar la solidez de las funciones de exportación de datos de los servicios de G Suite, así como de cada uno de los servicios de Google Cloud Platform (consulta la documentación de Google Cloud Platform para obtener más información).

Además, la funcionalidad específica de los servicios de G Suite o Google Cloud Platform te permite eliminar los datos de clientes en cualquier momento. Cuando Google recibe una orden completa de borrado de datos por parte de un cliente (por ejemplo, cuando un mensaje de correo electrónico es eliminado y no se puede recuperar de la papelera), eliminamos todos los datos relevantes del cliente de todos nuestros sistemas en un máximo de 180 días, a menos que se apliquen obligaciones de retención de datos.

Asistencia al responsable del tratamiento

Derechos del interesado

Los responsables del tratamiento pueden utilizar las consolas de administración de G Suite o de Google Cloud Platform y la funcionalidad de los servicios, para acceder, rectificar, restringir el tratamiento de, o eliminar, los datos que ellos mismos o sus usuarios hayan introducido en nuestros sistemas. Esta funcionalidad les ayudará a cumplir con sus obligaciones de responder a solicitudes de interesados que ejercen sus derechos bajo el RGPD.

Equipo de protección de datos

Nuestros clientes de G Suite y Google Cloud Platform cuentan con un equipo dedicado al que pueden dirigir sus consultas sobre protección de datos.

Notificaciones

Desde hace años, hemos contraído compromisos contractuales relacionados con la notificación de incidentes en G Suite y Google Cloud Platform. Seguiremos informándote lo antes posible de los incidentes relacionados con tus datos de acuerdo con los términos de incidentes de datos incluidos en nuestros acuerdos actuales y en los términos actualizados que se aplicarán a partir del 25 de mayo del 2018 (inclusive), cuando el RGPD entre en vigor.

Transferencias internacionales de datos

El RGPD ofrece varios mecanismos para facilitar las transferencias de datos personales fuera de la Unión Europea (UE). Estos mecanismos se han establecido para confirmar que el nivel de protección sea el adecuado o para garantizar la implementación de las medidas de seguridad pertinentes a la hora de transferir los datos personales a países fuera de la UE.

Las medidas de seguridad adecuadas pueden alcanzarse mediante las cláusulas contractuales tipo. También puede confirmarse un nivel de protección adecuado mediante decisiones de constatación como las del marco Escudo de privacidad UE-EE.UU.

Nosotros nos comprometemos en nuestros acuerdos para el tratamiento de datos a mantener un mecanismo que facilite la transferencia de datos fuera de la UE como se requiere en la Directiva de Protección de Datos, y ofreceremos el compromiso correspondiente desde el 25 de mayo del 2018, cuando el RGPD entra en vigor.

La certificación de Google conforme al marco Escudo de privacidad UE-EE.UU. y Suiza-EE.UU. incluye G Suite y Google Cloud Platform. También contamos con una confirmación de cumplimiento de las autoridades de protección de datos europeas de nuestras cláusulas contractuales tipo, afirmando que nuestros compromisos contractuales actuales de G Suite y de Google Cloud Platform cumplen con la Directiva de Protección de Datos y ofrecen un marco legal para las transferencias de datos personales desde la UE a otros lugares del mundo.

Estándares y certificaciones

ISO 27001 (Information Security Management)

ISO 27001 es uno de los estándares de seguridad independientes más reconocidos y aceptados internacionalmente. Google ha obtenido la certificación ISO 27001 para los sistemas, las aplicaciones, las personas, la tecnología, los procesos y los centros de datos que componen nuestra infraestructura común compartida (Common Infrastructure), así como para G Suite y Google Cloud Platform.

ISO 27017 (Cloud Security)

ISO 27017 es un estándar internacional de prácticas para llevar a cabo tareas de control relacionadas con la seguridad de la información. Se basa en ISO/IEC 27002, específico para Cloud Services. Google ha obtenido la certificación ISO 27017 para G Suite y para Google Cloud Platform.

ISO 27018 (Cloud Privacy)

ISO 27018 es un estándar internacional de prácticas relacionadas con la protección de información personal identificable (PII) en los servicios de la nube pública. Google ha obtenido la certificación ISO 27018 para G Suite y para Google Cloud Platform.

SSAE16 / ISAE 3402 (SOC 2/3)

El American Institute of Certified Public Accountants (AICPA) SOC 2 (Service Organization Controls) y SOC 3 Los marcos de trabajo de auditoría SOC 2 (controles de organizaciones de servicios) y SOC 3 definen los principios de confianza (Trust Principles) y los criterios para la seguridad, la disponibilidad, la integridad del tratamiento y la confidencialidad. Google cuenta con los informes SOC 2 y SOC 3, tanto para Google Cloud Platform como para G Suite.

Domande frequenti

1 ¿Qué es el RGPD?

El Reglamento General de Protección de Datos es la nueva normativa en materia de protección de datos la UE que sustituirá a la Directiva 95/46/CE sobre la protección de los datos personales de 24 de octubre de 1995.

2 ¿Cuándo entrará en vigor el RGPD?

El Reglamento General de Protección de Datos será directamente aplicable en todos los estados miembros de la Unión Europea desde el 25 de mayo del 2018.

3 ¿Requiere el RGPD almacenar los datos personales en la ue?

No. Como la Directiva 95/46/CE sobre la protección de los datos personales de 24 de octubre de 1995, el RGPD establece ciertas condiciones para la transferencia de datos personales a países fuera de la UE. Dichas condiciones pueden cumplirse mediante mecanismos como las cláusulas contractuales tipo.

4 ¿Establece el RGPD el derecho de los clientes a auditar google cloud?

Según el RGPD, el acuerdo de tratamiento de datos personales entre el responsable y el encargado del tratamiento debe incluir los derechos de auditoría. Elacuerdo actualizado de tratamiento de datos aplicable a partir del 25 de mayo del 2018, incluye derechos de auditoría en beneficio de nuestros clientes.

5 ¿Cuál es la función de los informes externos iso 27001, ISO 27017, iso 27018 y soc 2/3 en el cumplimiento del RGPD?

Nuestros clientes pueden utilizar las certificaciones ISO y los informes de auditoría SOC 2/3 que hemos obtenido de entidades externas, para llevar a cabo sus evaluaciones de riesgos y determinar las medidas técnicas y organizativas que deben llevarse a cabo.

6 ¿Qué otra información ofrece google sobre el RGPD?

Consulta la página de Empresas y Datos de Google.