Google Cloud

Enmienda de procesamiento de datos al Espacio de trabajo de Google y / o Acuerdo de producto complementario

Última modificación: 27 de mayo de 2021

El cliente que acepta estos términos (" **Cliente** ") y Google LLC, Google Ireland Limited, Google Asia Pacific Pte. Ltd., o cualquier otra entidad que controle directa o indirectamente, esté controlada por, o esté bajo control común con Google LLC (según corresponda, " **Google** "), haya celebrado uno o más acuerdos de espacio de trabajo de Google (como se define a continuación) y / o Acuerdos de productos complementarios (como se definen a continuación) (cada uno, con las enmiendas periódicas, un " **Acuerdo** ").

1. **Inicio**

   Esta Enmienda de procesamiento de datos al Espacio de trabajo de Google y / o Acuerdo de producto complementario, incluidos sus apéndices (la " **Enmienda de procesamiento de datos** ") entrará en vigencia y reemplazará cualquier procesamiento de datos y términos de seguridad previamente aplicables a partir de la Fecha de vigencia de la Enmienda (como se define a continuación).

   Esta Enmienda de procesamiento de datos complementa el Acuerdo aplicable. Cuando ese Acuerdo se celebró fuera de línea con Google Ireland Limited, esta Enmienda de procesamiento de datos reemplaza la Cláusula de "Privacidad" en el Acuerdo (si corresponde).

2. **Definiciones**

   2.1 Los términos en mayúscula definidos en el Acuerdo aplicable se aplican a esta Enmienda de procesamiento de datos. Además, en esta Enmienda de procesamiento de datos:

   " **Productos adicionales** " hace referencia a productos, servicios y aplicaciones que no forman parte de los Servicios pero que pueden ser accesibles, a través de la Consola de administración o de otro modo, para su uso con los Servicios.

   " **Controles de seguridad adicionales** " significa recursos de seguridad, características, funcionalidad y / o controles que el Cliente puede usar a su opción y / o según lo determine, incluida la Consola de administración, encriptación, registro y monitoreo, administración de identidad y acceso, escaneo de seguridad y cortafuegos.

   " **Publicidad** " se refiere a los anuncios en línea que Google muestra a los Usuarios finales, excluyendo cualquier anuncio que el Cliente elija expresamente que Google o cualquiera de sus Afiliados se muestre en relación con los Servicios en virtud de un acuerdo separado (por ejemplo, anuncios de Google AdSense implementados por el Cliente en un sitio web creado por el Cliente utilizando cualquier funcionalidad de Google Sites dentro de los Servicios).

   " **Límite de responsabilidad acordado** " significa el monto máximo monetario o basado en pagos al que se limita la responsabilidad de una parte en virtud del Acuerdo aplicable.

   " **Solución de transferencia alternativa** " significa una solución, distinta de las Cláusulas contractuales modelo, que permite la transferencia legal de datos personales a un tercer

país de acuerdo con la Ley europea de protección de datos.

" **Fecha de vigencia de la enmienda** " significa la fecha en la que el Cliente aceptó, o las partes acordaron de otro modo, esta Enmienda de procesamiento de datos.

" **Servicios auditados** " significa:

una. aquellos Servicios centrales de Google Workspace indicados como incluidos en el alcance de la certificación o informe correspondiente en https://cloud.google.com/security/compliance/services-in-scope/ , siempre que Google solo pueda eliminar un Servicio central de Google Workspace de dicha URL interrumpiendo ese Servicio de acuerdo con el Acuerdo aplicable; y

B. todos los demás Servicios, a menos que el Resumen de servicios de Google Workspace o el Resumen de servicios de productos complementarios indiquen lo contrario o las partes acuerden expresamente lo contrario por escrito.

" **Acuerdo de producto complementario** " significa: un Acuerdo de identidad en la nube u otro acuerdo en virtud del cual Google acepta proporcionar servicios de identidad como tales al Cliente u otro acuerdo que incorpore esta Enmienda de procesamiento de datos por referencia o establezca que se aplicará si el Cliente lo acepta.

“ **Resumen de servicios de productos complementarios** ” significa la descripción vigente en ese momento de los servicios prestados en virtud de un Acuerdo de producto complementario, según se establece en el Acuerdo aplicable.

" **Datos del cliente** " se refiere a los datos enviados, almacenados, enviados o recibidos a través de los Servicios por el Cliente o los Usuarios finales.

" **Datos personales del cliente** " se refiere a los datos personales contenidos en los Datos del cliente.

“ **Incidente de datos** ” significa una violación de la seguridad de Google que conduce a la destrucción, pérdida, alteración, divulgación no autorizada o acceso a los Datos del cliente en sistemas administrados o controlados por Google de manera accidental o ilegal.

“ **EEE** ” significa el Espacio Económico Europeo.

“ **Fecha de activación completa** ” significa: (a) si esta Enmienda de procesamiento de datos se incorpora automáticamente al Acuerdo aplicable, la Fecha de vigencia de la Enmienda; o (b) si el Cliente aceptó o las partes acordaron de otro modo esta Enmienda de procesamiento de datos, el octavo día después de la Fecha de vigencia de la Enmienda.

" **RGPD UE** " hace referencia al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas con respecto al tratamiento de datos personales y sobre la libre circulación de dichos datos, y por la que se deroga la Directiva. 95/46 / CE.

“ **Ley europea de protección de datos** ” significa, según corresponda: (a) el RGPD; y / o (b) la Ley Federal de Protección de Datos de 19 de junio de 1992 (Suiza).

" **Legislación europea o nacional** " significa, según corresponda: (a) la legislación de la UE o de los Estados miembros de la UE (si el RGPD de la UE se aplica al procesamiento de datos personales del cliente); y / o (b) la legislación del Reino Unido o una parte de el Reino Unido (si el RGPD del Reino Unido se aplica al procesamiento de datos personales del cliente).

" **RGPD** " significa, según corresponda: (a) el RGPD de la UE; y / o (b) el RGPD del Reino Unido.

" **Auditor** externo de Google" hace referencia a un **auditor externo** calificado, independiente y designado por Google, cuya identidad actual en ese momento Google revelará al Cliente.

" **Acuerdo de espacio de trabajo de Google** " hace referencia a un Acuerdo de espacio de trabajo de Google; un Acuerdo de Google Workspace for Education; un acuerdo maestro de Google Cloud con el programa de servicios del espacio de trabajo de Google; o cualquier otro acuerdo en virtud del cual Google acepta proporcionar al Cliente los servicios descritos en el Resumen de servicios del espacio de trabajo de Google.

" **Resumen de servicios de Google Workspace** " hace referencia a la descripción vigente en ese momento de los servicios de Google Workspace (incluidas las ediciones relacionadas), según se establece en https://workspace.google.com/terms/user_features.html (según puede actualizar Google desde de vez en cuando de acuerdo con el Acuerdo de espacio de trabajo de Google).

" **Cláusulas contractuales modelo** " o "MCC" se refieren a cláusulas estándar de protección de datos para la transferencia de datos personales a procesadores establecidos en terceros países que no garantizan un nivel adecuado de protección de datos, como se describe en el artículo 46 del RGPD de la UE y se establece en https://workspace.google.com/terms/mcc_terms.html .

“ **Ley de protección de datos no europea** ” hace referencia a las leyes de privacidad o protección de datos vigentes fuera del EEE, Suiza y el Reino Unido.

" **Dirección de correo electrónico de notificación** " hace referencia a las direcciones de correo electrónico designadas por el Cliente en la Consola de administración, o en el Formulario de pedido (según corresponda), para recibir determinadas notificaciones de Google. El cliente es responsable de utilizar la Consola de administración para asegurarse de que su dirección de correo electrónico de notificación se mantenga actualizada y válida.

“ **Documentación de seguridad** ” hace referencia a todos los documentos e información que Google pone a disposición en la Sección 7.5.1 (Revisiones de la documentación de seguridad).

" **Medidas de seguridad** " tiene el significado que se le da en la Sección 7.1.1 (Medidas de seguridad de Google).

" **Condiciones específicas del servicio** " tiene el significado que se le da en el Acuerdo de espacio de trabajo de Google o en el Acuerdo de producto complementario, según corresponda, o, si el Acuerdo de espacio de trabajo de Google del cliente no define "Condiciones específicas del servicio", significa las condiciones vigentes específicas de uno o más Servicios. establecido en https://workspace.google.com/terms/service-terms/ .

" **Servicios** " significa los siguientes servicios, según corresponda:

una. los Servicios Principales para Google Workspace, como se describe en el Resumen de Servicios de Google Workspace;

B. los Otros servicios para Google Workspace, como se describe en el Resumen de servicios de Google Workspace; y / o

C. los servicios descritos en el Resumen de servicios de productos complementarios.

“ **Subprocesador** ” significa un tercero autorizado como otro procesador en virtud de esta Enmienda de procesamiento de datos para tener acceso lógico y procesar los Datos del cliente con el fin de proporcionar partes de los Servicios y TSS.

" **Autoridad supervisora** " significa, según corresponda: (a) una "autoridad supervisora" según se define en el RGPD de la UE; y / o (b) el "Comisionado" según se define en el RGPD del Reino Unido.

" **Término** " significa el período desde la Fecha de vigencia de la Enmienda hasta el final de la prestación de los Servicios por parte de Google en virtud del Acuerdo aplicable, incluido, si corresponde, cualquier período durante el cual la prestación de los Servicios puede suspenderse y cualquier período posterior a la rescisión durante el cual Google puede continuar brindando los Servicios con fines de transición.

“ **RGPD del Reino Unido** ” hace referencia al RGPD de la UE en su forma enmendada e incorporada a la ley del Reino Unido en virtud de la Ley de la Unión Europea (Retirada) de 2018 del Reino Unido, si está en vigor.

2.2. Los términos "datos personales", "sujeto de datos", "procesamiento", "controlador" y "procesador", tal como se utilizan en esta Enmienda de procesamiento de datos, tienen los significados dados en el RGPD, independientemente de si la ley europea de protección de datos o datos no europeos Se aplica la Ley de Protección.

3. **Duración**

Esta Enmienda de procesamiento de datos, a pesar de la expiración del Plazo, permanecerá en vigencia hasta que Google elimine todos los Datos del cliente, y expirará automáticamente, como se describe en esta Enmienda de procesamiento de datos.

4. **Alcance de la ley de protección de datos**

4.1 Aplicación de la legislación europea . Las partes reconocen que la Ley Europea de Protección de Datos se aplicará al procesamiento de los Datos Personales del Cliente si, por ejemplo:

una. el procesamiento se lleva a cabo en el contexto de las actividades de un establecimiento del Cliente en el territorio del EEE o el Reino Unido; y / o

B. los Datos personales del cliente son datos personales relacionados con sujetos de datos que se encuentran en el EEE o el Reino Unido y el procesamiento se relaciona con la oferta de bienes o servicios en el EEE o el Reino Unido, o el monitoreo de su comportamiento en el EEE o el REINO UNIDO.

4.2 Aplicación de la legislación extraeuropea . Las partes reconocen que la ley de protección de datos no europea también puede aplicarse al procesamiento de los datos personales del cliente.

4.3 Aplicación de la Enmienda de Procesamiento de Datos . Excepto en la medida en que esta Enmienda de procesamiento de datos establezca lo contrario, los términos de esta Enmienda de procesamiento de datos se aplicarán independientemente de si la Ley europea de protección de datos o la Ley de protección de datos no europea se aplica al procesamiento de los Datos personales del cliente.

5. **Procesamiento de datos**

5.1 **Funciones y cumplimiento normativo; Autorización** .

5.1.1. Responsabilidades del procesador y del controlador . Si la ley europea de protección de datos se aplica al procesamiento de datos personales del cliente:

una. el tema y los detalles del procesamiento se describen en el Apéndice 1;

B. Google es un procesador de los Datos personales del cliente según la Ley europea de protección de datos;

C. El Cliente es un controlador o procesador, según corresponda, de los Datos personales del Cliente según la Ley europea de protección de datos; y

D. cada parte cumplirá con las obligaciones que le son aplicables en virtud de la Ley europea de protección de datos con respecto al procesamiento de los Datos personales del cliente.

5.1.2. Autorización por parte del controlador externo . Si la Ley Europea de Protección de Datos se aplica al procesamiento de Datos Personales del Cliente y el Cliente es un procesador, el Cliente garantiza que sus instrucciones y acciones con respecto a esos Datos Personales del Cliente, incluida su designación de Google como otro procesador, han sido autorizadas por el controlador correspondiente. .

5.1.3. Responsabilidades bajo la ley no europea . Si la Ley de protección de datos no europea se aplica al procesamiento de los Datos personales del cliente por cualquiera de las partes, la parte correspondiente cumplirá con las obligaciones que le sean aplicables en virtud de esa ley con respecto al procesamiento de esos Datos personales del cliente.

5.2 **Alcance del procesamiento** .

5.2.1 Instrucciones del cliente . El Cliente indica a Google que procese los Datos personales del Cliente solo de acuerdo con la ley aplicable: (a) para proporcionar los Servicios y TSS; (b) según se especifique más a través del uso de los Servicios por parte del Cliente y los Usuarios finales (incluida la Consola de administración y otras funciones de los Servicios) y TSS; (c) según se documente en la forma del Acuerdo aplicable, incluida esta Enmienda de procesamiento de datos; y (d) según se documente con más detalle en cualquier otra instrucción escrita proporcionada por el Cliente y reconocida por Google como instrucciones para los fines de esta Enmienda de procesamiento de datos.

5.2.2 Cumplimiento de las instrucciones por parte de Google . A partir de la Fecha de activación completa (a más tardar), Google cumplirá con las instrucciones descritas en la Sección 5.2.1 (Instrucciones del cliente) (incluso con respecto a las transferencias de datos) a menos que la legislación europea o nacional a la que esté sujeto Google requiera otro procesamiento de Datos personales del cliente de Google, en cuyo caso Google notificará al Cliente (a menos que la ley prohíba a Google hacerlo por motivos importantes de interés público) antes de dicho otro procesamiento. Para mayor claridad, Google no procesará los Datos personales del cliente con fines publicitarios ni ofrecerá publicidad en los Servicios.

5.3. **Productos adicionales**. Si Google, a su criterio, pone a disposición del Cliente productos adicionales de acuerdo con las Condiciones de productos adicionales, y si el Cliente opta por instalar o utilizar esos Productos adicionales, los Servicios pueden permitir que esos Productos adicionales accedan a los Datos personales del Cliente según sea necesario para la interoperación de los Productos Adicionales con los Servicios. Para mayor claridad, esta Enmienda de procesamiento de datos no se aplica al procesamiento de datos personales en relación con la provisión de Productos adicionales instalados o utilizados por el Cliente, incluidos los datos personales transmitidos hacia o desde dichos Productos adicionales. El Cliente puede usar la funcionalidad de los Servicios para habilitar o deshabilitar Productos Adicionales,

6. **Eliminación de datos**

6.1 **Eliminación durante el período**. Google permitirá que el Cliente y los Usuarios finales eliminen los Datos del cliente durante el Período aplicable de manera coherente con la funcionalidad de los Servicios. Si el Cliente o un Usuario final utiliza los Servicios para eliminar los Datos del cliente durante el Plazo aplicable y el Cliente o un Usuario final no pueden recuperar los Datos del cliente (por ejemplo, de la "papelera"), este uso constituirá una instrucción para Google para eliminar los Datos del cliente relevantes de los sistemas de Google de acuerdo con la ley aplicable. Google cumplirá con esta instrucción tan pronto como sea

razonablemente posible y dentro de un período máximo de 180 días, a menos que la legislación europea o nacional exija su almacenamiento.

6.2 **Eliminación al expirar el plazo** . Sujeto a la Sección 6.3 (Instrucción de Eliminación Diferida), al expirar el Plazo aplicable, el Cliente indica a Google que elimine todos los Datos del Cliente (incluidas las copias existentes) de los sistemas de Google de acuerdo con la ley aplicable. Google cumplirá con esta instrucción tan pronto como sea razonablemente posible y dentro de un período máximo de 180 días, a menos que la legislación europea o nacional requiera almacenamiento. Sin perjuicio de la Sección 9.1 (Acceso; Rectificación; Procesamiento restringido; Portabilidad), el Cliente es responsable de exportar, antes de que expire el Plazo aplicable, cualquier Dato del Cliente que desee retener.

6.3 **Instrucción de eliminación diferida** . En la medida en que los Datos del Cliente cubiertos por la instrucción de eliminación descrita en la Sección 6.2 (Eliminación por Vencimiento del Término) también se procesan, cuando el Término aplicable bajo la Sección 6.2 expire, en relación con un Acuerdo con un Término continuo, dicha instrucción de eliminación solo tomará efecto con respecto a dichos Datos del Cliente cuando expire el Período de vigencia. Para mayor claridad, esta Enmienda de procesamiento de datos seguirá aplicándose a dichos Datos del cliente hasta que Google la elimine.

7. **Seguridad de los datos**

7.1 **Medidas de seguridad, controles y asistencia de Google** .

7.1.1 Medidas de seguridad de Google . Google implementará y mantendrá medidas técnicas y organizativas para proteger los Datos del cliente contra la destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilegal, como se describe en el Apéndice 2 (las " **Medidas de seguridad**"). Las Medidas de Seguridad incluyen medidas para encriptar datos personales; para ayudar a garantizar la confidencialidad, integridad, disponibilidad y resistencia continuas de los sistemas y servicios de Google; para ayudar a restaurar el acceso oportuno a los datos personales después de un incidente; y para pruebas periódicas de eficacia. Google puede actualizar las Medidas de seguridad de vez en cuando, siempre que dichas actualizaciones no den como resultado la degradación de la seguridad general de los Servicios.

7.1.2 Cumplimiento de seguridad por parte del personal de Google . Google: (a) tomará las medidas adecuadas para garantizar el cumplimiento de las Medidas de seguridad por parte de sus empleados, contratistas y subprocesadores en la medida que sea aplicable a su alcance de desempeño, y (b) se asegurará de que todas las personas autorizadas para procesar los Datos personales del cliente estén bajo un obligación de confidencialidad.

7.1.3 Controles de seguridad adicionales . Google pondrá a disposición Controles de seguridad adicionales para: (a) permitir que el Cliente tome medidas para proteger los Datos del Cliente; y (b) proporcionar al Cliente información sobre cómo proteger, acceder y utilizar los Datos del Cliente.

7.1.4 Asistencia de seguridad de Google . Google (teniendo en cuenta la naturaleza del procesamiento de los Datos personales del cliente y la información disponible para Google) ayudará al Cliente a garantizar el cumplimiento de sus obligaciones de conformidad con los artículos 32 a 34 del RGPD mediante:

una. implementar y mantener las Medidas de seguridad de acuerdo con la Sección 7.1.1 (Medidas de seguridad de Google);

B. poner Controles de seguridad adicionales a disposición del Cliente de acuerdo con la Sección 7.1.3 (Controles de seguridad adicionales);

C. cumplir con los términos de la Sección 7.2 (Incidentes de datos);

D. proporcionar al Cliente la Documentación de seguridad de acuerdo con la Sección 7.5.1 (Revisiones de la Documentación de seguridad) y la información contenida en el Acuerdo aplicable, incluida esta Enmienda de procesamiento de datos; y

mi. si las subsecciones (a) - (d) anteriores son insuficientes para que el Cliente cumpla con dichas obligaciones, a solicitud del Cliente, brindando asistencia adicional razonable.

7.2 **Incidentes de datos** .

7.2.1 Notificación de incidentes . Google notificará al Cliente de inmediato y sin demoras indebidas después de tener conocimiento de un Incidente de datos y tomará las medidas razonables para minimizar el daño y proteger los Datos del cliente.

7.2.2 Detalles del incidente de datos . La notificación de Google de un Incidente de datos describirá, en la medida de lo posible, la naturaleza del Incidente de datos, las medidas tomadas para mitigar los riesgos potenciales y las medidas que Google recomienda que el Cliente tome para abordar el Incidente de datos.

7.2.3 Entrega de notificación . Las notificaciones de cualquier incidente de datos se enviarán a la dirección de correo electrónico de notificación o, a discreción de Google, mediante comunicación directa (por ejemplo, por llamada telefónica o una reunión en persona).

7.2.4 No evaluación de los datos del cliente por parte de Google . Google no tiene la obligación de evaluar los Datos del cliente para identificar la información sujeta a requisitos legales específicos.

7.2.5 Sin reconocimiento de fallas por parte de Google . La notificación o respuesta de Google a un Incidente de datos en virtud de esta Sección 7.2 (Incidentes de datos) no se interpretará como un reconocimiento por parte de Google de cualquier falla o responsabilidad con respecto al Incidente de datos.

7.3. **Responsabilidades y evaluación de seguridad del cliente** .

7.3.1 Responsabilidades de seguridad del cliente . Sin perjuicio de las obligaciones de Google en virtud de las Secciones 7.1 (Medidas de seguridad, controles y asistencia de Google) y 7.2 (Incidentes de datos), y en cualquier otra parte del Acuerdo aplicable, el Cliente es responsable de su uso de los Servicios y su almacenamiento de cualquier copia de los Datos del cliente fuera de Los sistemas de Google o de los subprocesadores de Google, incluidos:

una. utilizar los Servicios y los Controles de seguridad adicionales para garantizar un nivel de seguridad adecuado al riesgo con respecto a los Datos del cliente;

B. asegurar las credenciales de autenticación de la cuenta, los sistemas y los dispositivos que utiliza el Cliente para acceder a los Servicios; y

C. conservar copias de sus Datos de cliente según corresponda.

7.3.2 Evaluación de seguridad del cliente . El Cliente acepta, en función de su uso actual y previsto de los Servicios, que los Servicios, las Medidas de seguridad, los Controles de seguridad adicionales y los compromisos de Google en virtud de esta Sección 7 (Seguridad de los datos): (a) satisfacen las necesidades del Cliente, incluso con respecto a las obligaciones de seguridad del Cliente según la Ley europea de protección de datos y / o la Ley de protección de datos no europea, según corresponda, y (b) proporcionar un nivel de seguridad adecuado al riesgo con respecto a los Datos del cliente.

7.4 **Certificaciones de cumplimiento e informes SOC** . Google mantendrá al menos lo siguiente para los Servicios auditados con el fin de evaluar la efectividad continua de las Medidas de seguridad:

una. certificados para ISO 27001, ISO 27017 e ISO 27018, y

B. Informes SOC 2 y SOC 3 elaborados por el auditor externo de Google y actualizados anualmente en base a una auditoría realizada al menos una vez cada 12 meses (los " **Informes SOC** "). Google puede agregar estándares en cualquier momento. Google puede reemplazar un Informe SOC con una alternativa equivalente o mejorada.

7.5 **Revisiones y auditorías de cumplimiento** .

7.5.1 Revisiones de la documentación de seguridad . Google pondrá los Informes SOC a disposición del Cliente para su revisión a fin de demostrar el cumplimiento por parte de Google de sus obligaciones en virtud de esta Enmienda de procesamiento de datos.

7.5.2 Derechos de auditoría del cliente .

una. Si la Ley europea de protección de datos se aplica al procesamiento de los Datos personales del cliente, Google permitirá que el Cliente o un auditor independiente designado por el Cliente realice auditorías (incluidas inspecciones) para verificar el cumplimiento de Google con sus obligaciones en virtud de esta Enmienda de procesamiento de datos de acuerdo con la Sección 7.5. 3 (Condiciones comerciales adicionales para revisiones y auditorías). Google contribuirá a dichas auditorías como se describe en la Sección 7.4 (Certificaciones de cumplimiento e informes SOC) y esta Sección 7.5 (Revisiones y auditorías de cumplimiento).

B. Si el Cliente ha celebrado las Cláusulas del contrato modelo como se describe en la Sección 10.2 (Transferencias de datos), Google permitirá al Cliente o un auditor independiente designado por el Cliente realizar auditorías como se describe en las Cláusulas del contrato modelo de acuerdo con la Sección 7.5.3 (Términos comerciales adicionales para revisiones y auditorías).

C. El Cliente puede realizar una auditoría para verificar el cumplimiento de Google con sus obligaciones en virtud de esta Enmienda de procesamiento de datos mediante la revisión de la Documentación de seguridad (que refleja el resultado de las auditorías realizadas por el Auditor externo de Google).

7.5.3 Condiciones comerciales adicionales para revisiones y auditorías .

una. El Cliente debe enviar cualquier solicitud de revisión del informe SOC 2 según la Sección 7.5.1 o auditorías según la Sección 7.5.2 (a) o 7.5.2 (b) al Equipo de Protección de Datos en la Nube de Google como se describe en la Sección 12 (Equipo de Protección de Datos en la Nube ; Procesamiento de registros).

B. Tras la recepción por parte de Google de una solicitud en virtud de la Sección 7.5.3 (a), Google y el Cliente analizarán y acordarán por adelantado: (i) las fechas razonables y los controles de seguridad y confidencialidad aplicables a cualquier revisión del SOC 2 informe según la Sección 7.5.1; y (ii) la fecha razonable de inicio, alcance y duración de los controles de seguridad y confidencialidad aplicables a cualquier auditoría bajo la Sección 7.5.2 (a) o 7.5.2 (b).

C. Google puede cobrar una tarifa (basada en los costos razonables de Google) por cualquier auditoría según la Sección 7.5.2 (a) o 7.5.2 (b). Google proporcionará al Cliente más detalles de cualquier tarifa aplicable y la base de su cálculo, antes de

dicha auditoría. El Cliente será responsable de los honorarios cobrados por cualquier auditor designado por el Cliente para ejecutar dicha auditoría.

D. Google puede oponerse por escrito a un auditor designado por el Cliente para realizar cualquier auditoría según la Sección 7.5.2 (a) o 7.5.2 (b) si el auditor, en la opinión razonable de Google, no está adecuadamente calificado o no es independiente, un competidor de Google. , o de otra manera manifiestamente inadecuada. Cualquier objeción de este tipo por parte de Google requerirá que el Cliente nombre a otro auditor o realice la auditoría él mismo.

7.5.4 Sin modificación de MCC . Nada en esta Sección 7.5 (Revisiones y auditorías de cumplimiento) varía o modifica los derechos u obligaciones del Cliente o de Google LLC en virtud de las Cláusulas de contrato modelo celebradas como se describe en la Sección 10.2 (Transferencias de datos).

8. **Evaluaciones de impacto y consultas**

Google (teniendo en cuenta la naturaleza del procesamiento y la información disponible para Google) ayudará al Cliente a garantizar el cumplimiento de sus obligaciones de conformidad con los artículos 35 y 36 del GDPR, mediante:

una. proporcionar Controles de seguridad adicionales de acuerdo con la Sección 7.1.3 (Controles de seguridad adicionales) y la Documentación de seguridad de acuerdo con la Sección 7.5.1 (Revisiones de la documentación de seguridad);

B. proporcionar la información contenida en el Acuerdo aplicable, incluida esta Enmienda de procesamiento de datos; y

C. si las subsecciones (a) y (b) anteriores son insuficientes para que el Cliente cumpla con dichas obligaciones, a solicitud del Cliente, brindando asistencia adicional razonable.

9. **Acceso, etc .; Derechos del interesado; Exportación de datos**

9.1 **Acceso; Rectificación; Procesamiento restringido; Portabilidad** . Durante el Plazo aplicable, Google permitirá al Cliente, de una manera coherente con la funcionalidad de los Servicios, acceder, rectificar y restringir el procesamiento de los Datos del Cliente, incluso a través de la función de eliminación proporcionada por Google como se describe en la Sección 6.1 (Eliminación durante el Plazo). y para exportar datos del cliente.

9.2 **Solicitudes de sujetos de datos** .

9.2.1 Responsabilidad del cliente por las solicitudes . Durante el Plazo aplicable, si el Equipo de Protección de Datos en la Nube de Google recibe una solicitud de un interesado en relación con los Datos Personales del Cliente, y la solicitud identifica al Cliente, Google le informará al interesado que envíe su solicitud al Cliente. El Cliente será responsable de responder a dicha solicitud, incluido, cuando sea necesario, mediante el uso de la funcionalidad de los Servicios.

9.2.2 Solicitud de asistencia del sujeto de datos de Google . Google (teniendo en cuenta la naturaleza del procesamiento de los Datos personales del cliente) ayudará al Cliente a cumplir con sus obligaciones en virtud del Capítulo III del RGPD para responder a las solicitudes de ejercicio de los derechos del interesado mediante:

una. proporcionar Controles de seguridad adicionales de acuerdo con la Sección 7.1.3 (Controles de seguridad adicionales);

B. cumplir con las Secciones 9.1 (Acceso; Rectificación; Procesamiento restringido; Portabilidad) y 9.2.1 (Responsabilidad del cliente por las solicitudes); y

C. si las subsecciones (a) y (b) anteriores son insuficientes para que el Cliente cumpla con dichas obligaciones, a solicitud del Cliente, brindando asistencia

adicional razonable.

10. **Transferencias de datos**

10.1 **Instalaciones de procesamiento y almacenamiento de datos** . Google puede almacenar y procesar los Datos del Cliente en cualquier lugar donde Google o sus Subprocesadores mantengan instalaciones, sujeto a:

una. Sección 10.2 (Transferencias de datos) con respecto a las Cláusulas del contrato modelo o la Solución de transferencia alternativa; y

B. los Términos específicos del servicio aplicables (si los hubiera) con respecto a la ubicación de los datos.

10.2 **Transferencias de datos** . Si el almacenamiento y / o procesamiento de datos personales del cliente implica transferencias de datos personales del cliente desde el EEE, Suiza o el Reino Unido a cualquier tercer país que no garantice un nivel adecuado de protección según la ley europea de protección de datos, y se aplica la ley europea de protección de datos. a esas transferencias, entonces:

una. si el Cliente (como exportador de datos) entra en las Cláusulas de contrato modelo con Google LLC (como importador de datos) dentro de la Consola de administración, entonces:

I. las transferencias estarán sujetas a las Cláusulas de Contrato Modelo; y

ii. Google se asegurará de que Google LLC cumpla con sus obligaciones en virtud de las Cláusulas del contrato modelo con respecto a esas transferencias; o

B. si el Cliente no suscribe las Cláusulas del contrato modelo como se describe en la Sección 10.2 (a), entonces:

I. si Google pone a disposición una Solución de transferencia alternativa: (A) se considerará que el Cliente la está utilizando y tomará cualquier acción (que puede incluir la ejecución de documentos) estrictamente necesaria para que tenga pleno efecto; y (B) Google se asegurará de que las transferencias se realicen de acuerdo con dicha Solución de transferencia alternativa; o

ii. si Google no pone a disposición una Solución de transferencia alternativa: (A) Se considerará que el Cliente (como exportador de datos) ha suscrito las Cláusulas de contrato modelo con Google LLC (como importador de datos); (B) las transferencias estarán sujetas a las Cláusulas del Contrato Modelo; y (C) Google se asegurará de que Google LLC cumpla con sus obligaciones en virtud de las Cláusulas del contrato modelo con respecto a esas transferencias; y

C. Si el Cliente ha suscrito las Cláusulas del contrato modelo, pero posteriormente determina razonablemente que no brindan un nivel adecuado de protección, entonces:

I. si Google pone a disposición una Solución de transferencia alternativa, el Cliente puede, notificando a Google LLC a través del Equipo de protección de datos en la nube de Google de acuerdo con la Sección 12.1 (Equipo de protección de datos en la nube de Google), rescindir cualquier Cláusula de contrato modelo aplicable en virtud de la Sección 10.2 (a), de manera que se aplique la Sección 10.2 (b) (i); o

ii. Si Google no pone a disposición una Solución de transferencia alternativa, el Cliente puede rescindir el Acuerdo de inmediato notificando a Google.

10.3 **Información del centro de datos** . La información sobre las ubicaciones de los centros de datos de Google está disponible en: https://www.google.com/about/datacenters/inside/locations/index.html (según lo pueda actualizar Google de vez en cuando).

10.4 **Divulgación de información confidencial que contenga datos personales** . Si el Cliente ha celebrado Cláusulas de contrato modelo como se describe en la Sección 10.2 (Transferencias de datos), Google, sin perjuicio de cualquier término en contrario en el Acuerdo aplicable, se asegurará de que cualquier divulgación de la Información confidencial del Cliente que contenga datos personales y cualquier notificación relacionada con cualquier divulgación de este tipo se realizará de acuerdo con dichas Cláusulas de contrato modelo.

11. **Subprocesadores**

11.1 **Consentimiento para la participación del subprocesador** . El Cliente autoriza específicamente la contratación como Subencargados del tratamiento de: (a) aquellas entidades enumeradas a partir de la Fecha de entrada en vigor de la Enmienda en la URL especificada en la Sección 11.2 (Información sobre Subencargados); y (b) todos los demás afiliados de Google de vez en cuando. Además, sin perjuicio de la Sección 11.4 (Oportunidad de oponerse a los cambios del subprocesador), el Cliente generalmente autoriza la contratación como Subprocesadores de cualquier otro tercero (“ **Nuevos subprocesadores de terceros** ”). Si el Cliente ha celebrado Cláusulas de contrato modelo como se describe en la Sección 10.2 (Transferencias de datos), las autorizaciones anteriores constituyen el consentimiento previo por escrito del Cliente a la subcontratación por parte de Google LLC del procesamiento de los Datos del cliente.

11.2 **Información sobre subprocesadores** . La información sobre los subprocesadores, incluidas sus funciones y ubicaciones, está disponible en https://workspace.google.com/intl/en/terms/subprocessors.html (según pueda ser actualizado por Google de vez en cuando de acuerdo con esta Enmienda de procesamiento de datos).

11.3 **Requisitos para la contratación del subprocesador** . Al contratar cualquier subprocesador, Google:

una. garantizar mediante un contrato escrito que:

I. el Subprocesador solo accede y utiliza los Datos del Cliente en la medida necesaria para cumplir con las obligaciones subcontratadas, y lo hace de acuerdo con el Acuerdo (incluida esta Enmienda de procesamiento de datos) y las Cláusulas del contrato modelo o Solución de transferencia alternativa, según corresponda en la Sección 10.2 (Transferencias de datos); y

ii. si el RGPD se aplica al procesamiento de Datos personales del cliente, las obligaciones de protección de datos descritas en el Artículo 28 (3) del RGPD, como se describe en esta Enmienda de procesamiento de datos, se imponen al Subencargado del tratamiento; y

B. seguirá siendo plenamente responsable de todas las obligaciones subcontratadas y de todos los actos y omisiones del Subprocesador.

11.4 **Oportunidad de oponerse a los cambios del subprocesador** .

una. Cuando se contrata a un nuevo subprocesador de terceros durante el período aplicable, Google, al menos 30 días antes de que el nuevo subprocesador de terceros comience a procesar los datos del cliente, notificará al cliente sobre el compromiso (incluido el nombre y la ubicación del subprocesador correspondiente y las actividades). funcionará).

B. El Cliente puede, dentro de los 90 días posteriores a la notificación de la contratación de un nuevo subprocesador externo, objetar rescindiendo el Acuerdo aplicable inmediatamente notificando a Google. Este derecho de rescisión es el único y exclusivo recurso del Cliente si el Cliente se opone a cualquier nuevo subprocesador de terceros.

12. **Equipo de protección de datos en la nube; Procesamiento de registros**

12.1 **Equipo de protección de datos en la nube de Google** . Los administradores del cliente pueden ponerse en contacto con el equipo de protección de datos en la nube de Google en https://support.google.com/a/contact/googlecloud_dpr (mientras los administradores hayan iniciado sesión en su cuenta de administrador) y / o por el cliente proporcionando un aviso a Google como descrito en el Acuerdo aplicable.

12.2. **Registros de procesamiento de Google** . En la medida en que el GDPR requiera que Google recopile y mantenga registros de cierta información relacionada con el Cliente, el Cliente, cuando se le solicite, utilizará la Consola de administración para proporcionar dicha información y mantenerla precisa y actualizada. Google puede poner dicha información a disposición de las autoridades supervisoras si así lo requiere el RGPD.

13. **Responsabilidad**

13.1 Límite de **responsabilidad** . Si las Cláusulas del contrato modelo se han celebrado como se describe en la Sección 10.2 (Transferencias de datos), entonces, sujeto a la Sección 13.2 (Exclusiones del límite de responsabilidad), la responsabilidad total combinada de cualquiera de las partes y sus Afiliadas hacia la otra parte y sus Afiliadas bajo o en relación con el Acuerdo aplicable y dichas Cláusulas de contrato modelo combinadas se limitarán al Límite de responsabilidad acordado para la parte correspondiente.

13.2 **Exclusiones del** límite de **responsabilidad** . Nada en la Sección 13.1 (Límite de responsabilidad) afectará los términos restantes del Acuerdo aplicable relacionados con la responsabilidad (incluidas las exclusiones específicas de cualquier limitación de responsabilidad).

14. **Tercero beneficiario**

Sin perjuicio de cualquier disposición en contrario en el Acuerdo aplicable, cuando Google LLC no sea parte de dicho Acuerdo, Google LLC será un tercero beneficiario de las Secciones 7.5 (Revisiones y auditorías de cumplimiento), 10.2 (Transferencias de datos), 11.1 (Consentimiento para Contratación del subprocesador) y 13 (Responsabilidad).

15. **Efecto de la enmienda**

Sin perjuicio de cualquier disposición en contrario en el Acuerdo aplicable, en la medida de cualquier conflicto o incoherencia entre los términos de esta Enmienda de procesamiento de datos y el resto del Acuerdo aplicable, prevalecerá esta Enmienda de procesamiento de datos. Para mayor claridad, si el Cliente ha celebrado más de un Acuerdo, esta Enmienda de procesamiento de datos modificará cada uno de los Acuerdos por separado.

Apéndice 1: Asunto y detalles del procesamiento de datos

Tema en cuestion

Prestación de los Servicios y TSS por parte de Google al Cliente.

Duración del procesamiento

El Plazo aplicable más el período desde la expiración de dicho Plazo hasta la eliminación de todos los Datos del Cliente por parte de Google de acuerdo con la Enmienda de Procesamiento de Datos.

Naturaleza y finalidad del tratamiento

Google procesará los Datos personales del cliente con el fin de proporcionar los Servicios y TSS al Cliente de acuerdo con la Enmienda de procesamiento de datos.

Categorías de datos

Datos relacionados con individuos proporcionados a Google a través de los Servicios, por (o bajo la dirección de) el Cliente o los Usuarios finales.

Sujetos de los datos

Los sujetos de los datos incluyen las personas sobre las que se proporcionan datos a Google a través de los Servicios por (o bajo la dirección de) el Cliente o los Usuarios finales.

Apéndice 2: Medidas de seguridad

A partir de la Fecha de entrada en vigor de la Enmienda, Google implementará y mantendrá las Medidas de seguridad descritas en este Apéndice 2.

1. **Centro de datos y seguridad de la red**

    (a) Centros de datos.

    Infraestructura . Google mantiene centros de datos distribuidos geográficamente. Google almacena todos los datos de producción en centros de datos físicamente seguros.

    Redundancia. Los sistemas de infraestructura se han diseñado para eliminar puntos únicos de falla y minimizar el impacto de los riesgos ambientales anticipados. Los circuitos duales, conmutadores, redes u otros dispositivos necesarios ayudan a proporcionar esta redundancia. Los Servicios están diseñados para permitir que Google realice ciertos tipos de mantenimiento preventivo y correctivo sin interrupción. Todos los equipos e instalaciones ambientales tienen procedimientos de mantenimiento preventivo documentados que detallan el proceso y la frecuencia de desempeño de acuerdo con las especificaciones internas o del fabricante.

    Energía. Los sistemas de energía eléctrica del centro de datos están diseñados para ser redundantes y fáciles de mantener sin afectar las operaciones continuas, las 24 horas del día, los 7 días de la semana. En la mayoría de los casos, se proporciona una fuente de energía primaria y otra alternativa, cada una con la misma capacidad, para los componentes de infraestructura críticos en el centro de datos. La energía de respaldo es proporcionada por varios mecanismos, como las baterías de fuentes de alimentación ininterrumpida (UPS), que brindan protección de energía confiable y constante durante caídas de tensión, apagones, sobrevoltaje, bajo voltaje y condiciones de frecuencia fuera de tolerancia. Si se interrumpe el suministro eléctrico, La energía de respaldo está diseñada para proporcionar energía transitoria al centro de datos, a plena capacidad, durante un máximo de 10 minutos hasta que los sistemas de generadores diésel se hagan cargo. Los generadores diésel son capaces de arrancar automáticamente en cuestión de segundos para proporcionar suficiente energía eléctrica de emergencia para hacer funcionar el centro de datos a plena capacidad, normalmente durante varios días.

    Sistemas operativos de servidor . Los servidores de Google utilizan una implementación basada en Linux personalizada para el entorno de la aplicación. Los datos se almacenan utilizando algoritmos patentados para aumentar la seguridad y la redundancia de los datos. Google emplea un proceso de revisión de código para aumentar la seguridad del código utilizado para proporcionar los Servicios y mejorar los productos de seguridad en los entornos de producción.

Continuidad de negocios . Google ha diseñado, planifica y prueba periódicamente sus programas de planificación de la continuidad empresarial y recuperación ante desastres.

(b) Redes y Transmisión.

Transmisión de datos . Los centros de datos suelen estar conectados a través de enlaces privados de alta velocidad para proporcionar una transferencia de datos rápida y segura entre los centros de datos. Esto está diseñado para evitar que los datos se lean, copien, alteren o eliminen sin autorización durante la transferencia o transporte electrónico o mientras se graban en medios de almacenamiento de datos. Google transfiere datos a través de protocolos estándar de Internet.

Superficie de ataque externa . Google emplea múltiples capas de dispositivos de red y detección de intrusos para proteger su superficie de ataque externa. Google considera los posibles vectores de ataque e incorpora tecnologías apropiadas diseñadas específicamente en los sistemas externos.

Detección de intrusiones . La detección de intrusiones tiene como objetivo proporcionar información sobre las actividades de ataque en curso y proporcionar información adecuada para responder a los incidentes. La detección de intrusos de Google implica:

1. controlar estrictamente el tamaño y la composición de la superficie de ataque de Google mediante medidas preventivas;
2. emplear controles de detección inteligentes en los puntos de entrada de datos; y
3. emplear tecnologías que resuelvan automáticamente determinadas situaciones peligrosas.

Respuesta a incidentes . Google monitorea una variedad de canales de comunicación para detectar incidentes de seguridad, y el personal de seguridad de Google reaccionará rápidamente a los incidentes conocidos.

Tecnologías de cifrado . Google hace que el cifrado HTTPS (también conocido como conexión SSL o TLS) esté disponible. Los servidores de Google admiten el intercambio de claves criptográficas Diffie-Hellman de curva elíptica efímera firmado con RSA y ECDSA. Estos métodos de secreto directo perfecto (PFS) ayudan a proteger el tráfico y minimizar el impacto de una clave comprometida o un avance criptográfico.

2. Controles de acceso y sitio

(a) Controles del sitio.

Operación de seguridad del centro de datos en el sitio . Los centros de datos de Google mantienen una operación de seguridad en el sitio responsable de todas las funciones de seguridad del centro de datos físico las 24 horas del día, los 7 días de la semana. El personal de operaciones de seguridad en el lugar monitorea las cámaras de circuito cerrado de TV (CCTV) y todos los sistemas de alarma. El personal de operaciones de seguridad in situ realiza patrullas internas y externas del centro de datos con regularidad.

Procedimientos de acceso al centro de datos. Google mantiene procedimientos formales de acceso para permitir el acceso físico a los centros de datos. Los centros de datos están alojados en instalaciones que requieren acceso con clave de tarjeta electrónica, con alarmas que están vinculadas a la operación de seguridad en el sitio. Todos los que ingresan al centro de datos deben identificarse y mostrar una prueba de identidad para las operaciones de seguridad en el sitio. Solo los empleados, contratistas y visitantes autorizados pueden ingresar a los centros de datos. Solo los empleados y contratistas autorizados pueden

solicitar acceso con clave de tarjeta electrónica a estas instalaciones. Las solicitudes de acceso a la clave de la tarjeta electrónica del centro de datos deben realizarse por correo electrónico, y requieren la aprobación del gerente del solicitante y del director del centro de datos. Todos los demás participantes que requieran acceso temporal al centro de datos deben: (i) obtener la aprobación previa de los gerentes del centro de datos para el centro de datos específico y las áreas internas que desean visitar; (ii) registrarse en las operaciones de seguridad en el sitio; y (iii) hacer referencia a un registro de acceso al centro de datos aprobado que identifique a la persona como aprobada. (i) obtener la aprobación previa de los gerentes del centro de datos para el centro de datos específico y las áreas internas que desean visitar; (ii) registrarse en las operaciones de seguridad en el sitio; y (iii) hacer referencia a un registro de acceso al centro de datos aprobado que identifique a la persona como aprobada. (i) obtener la aprobación previa de los gerentes del centro de datos para el centro de datos específico y las áreas internas que desean visitar; (ii) registrarse en las operaciones de seguridad en el sitio; y (iii) hacer referencia a un registro de acceso al centro de datos aprobado que identifique a la persona como aprobada.

Dispositivos de seguridad del centro de datos en el sitio. Los centros de datos de Google emplean una llave de tarjeta electrónica y un sistema de control de acceso biométrico que está vinculado a un sistema de alarma. El sistema de control de acceso monitorea y registra la llave de la tarjeta electrónica de cada individuo y cuándo acceden a las puertas perimetrales, el envío y la recepción, y otras áreas críticas. El sistema de control de acceso registra la actividad no autorizada y los intentos fallidos de acceso y los investiga, según corresponda. El acceso autorizado a todas las operaciones comerciales y los centros de datos está restringido según las zonas y las responsabilidades laborales de la persona. Las puertas cortafuegos de los centros de datos están alarmadas. Las cámaras de circuito cerrado de televisión están en funcionamiento tanto dentro como fuera de los centros de datos. El posicionamiento de las cámaras ha sido diseñado para cubrir áreas estratégicas que incluyen, entre otras, el perímetro, las puertas al edificio del centro de datos y el envío / recepción. El personal de operaciones de seguridad en el sitio administra el equipo de monitoreo, grabación y control de CCTV. Los cables seguros en todos los centros de datos conectan el equipo de CCTV. Las cámaras graban en el sitio a través de grabadoras de video digitales las 24 horas del día, los 7 días de la semana. Los registros de vigilancia se conservan hasta por 30 días según la actividad. El posicionamiento de las cámaras ha sido diseñado para cubrir áreas estratégicas que incluyen, entre otras, el perímetro, las puertas al edificio del centro de datos y el envío / recepción. El personal de operaciones de seguridad en el sitio administra el equipo de monitoreo, grabación y control de CCTV. Los cables seguros en todos los centros de datos conectan el equipo de CCTV. Las cámaras graban en el sitio a través de grabadoras de video digitales las 24 horas del día, los 7 días de la semana. Los registros de vigilancia se conservan hasta por 30 días según la actividad. El posicionamiento de las cámaras ha sido diseñado para cubrir áreas estratégicas que incluyen, entre otras, el perímetro, las puertas al edificio del centro de datos y el envío / recepción. El personal de operaciones de seguridad en el sitio administra el equipo de monitoreo, grabación y control de CCTV. Los cables seguros en todos los centros de datos conectan el equipo de CCTV. Las cámaras graban en el sitio a través de grabadoras de video digitales las 24 horas del día, los 7 días de la semana. Los registros de vigilancia se conservan hasta por 30 días según la actividad. El personal de operaciones de seguridad en el sitio administra el equipo de monitoreo, grabación y control de CCTV. Los cables seguros en todos los centros de datos conectan el equipo de CCTV. Las cámaras graban en el sitio a través de grabadoras de video digitales las 24 horas del día, los 7 días de la semana. Los registros de vigilancia se conservan hasta por 30 días según la actividad. El personal de

operaciones de seguridad en el sitio administra el equipo de monitoreo, grabación y control de CCTV. Los cables seguros en todos los centros de datos conectan el equipo de CCTV. Las cámaras graban en el sitio a través de grabadoras de video digitales las 24 horas del día, los 7 días de la semana. Los registros de vigilancia se conservan hasta por 30 días según la actividad.

(b) Control de acceso.

Personal de seguridad de infraestructura . Google tiene y mantiene una política de seguridad para su personal y requiere capacitación en seguridad como parte del paquete de capacitación para su personal. El personal de seguridad de la infraestructura de Google es responsable del monitoreo continuo de la infraestructura de seguridad de Google, la revisión de los Servicios y la respuesta a los incidentes de seguridad.

Control de acceso y gestión de privilegios . Los Administradores del Cliente y los Usuarios finales deben autenticarse mediante un sistema de autenticación central o mediante un sistema de inicio de sesión único para poder utilizar los Servicios.

Procesos y políticas de acceso a datos internos - Política de acceso. Los procesos y políticas de acceso a datos internos de Google están diseñados para evitar que personas y / o sistemas no autorizados obtengan acceso a los sistemas utilizados para procesar datos personales. Google diseña sus sistemas para: (i) permitir que solo las personas autorizadas accedan a los datos a los que están autorizados a acceder; y (ii) garantizar que los datos personales no se puedan leer, copiar, alterar o eliminar sin autorización durante el procesamiento, uso y después de la grabación. Los sistemas están diseñados para detectar cualquier acceso inadecuado. Google emplea un sistema de gestión de acceso centralizado para controlar el acceso del personal a los servidores de producción. y solo proporciona acceso a un número limitado de personal autorizado. Los sistemas de autenticación y autorización de Google utilizan certificados SSH y claves de seguridad, y están diseñados para proporcionar a Google mecanismos de acceso seguros y flexibles. Estos mecanismos están diseñados para otorgar solo derechos de acceso aprobados a los hosts del sitio, los registros, los datos y la información de configuración. Google requiere el uso de ID de usuario únicos, contraseñas seguras, autenticación de dos factores y listas de acceso cuidadosamente monitoreadas para minimizar el potencial de uso no autorizado de la cuenta. La concesión o modificación de los derechos de acceso se basa en: las responsabilidades laborales del personal autorizado; requisitos de tareas laborales necesarios para realizar tareas autorizadas; y una necesidad de conocer la base. La concesión o modificación de los derechos de acceso también debe estar de acuerdo con las políticas y la formación de acceso a datos internos de Google. Las aprobaciones se gestionan mediante herramientas de flujo de trabajo que mantienen registros de auditoría de todos los cambios. El acceso a los sistemas se registra para crear una pista de auditoría para la rendición de cuentas. Cuando se emplean contraseñas para la autenticación (por ejemplo, inicio de sesión en estaciones de trabajo), se implementan políticas de contraseñas que siguen al menos las prácticas estándar de la industria. Estos estándares incluyen restricciones sobre la reutilización de contraseñas y suficiente seguridad de contraseñas.

3. Datos

(a) Almacenamiento, aislamiento y registro de datos.

Google almacena datos en un entorno de múltiples inquilinos en servidores propiedad de Google. Sujeto a las instrucciones del Cliente en sentido contrario (por ejemplo, en forma de una selección de ubicación de datos), Google replica los Datos del Cliente entre varios

centros de datos dispersos geográficamente. Google también aísla lógicamente los Datos del cliente y separa lógicamente los datos de cada Usuario final de los datos de otros Usuarios finales, y los datos de un Usuario final autenticado no se mostrarán a otro Usuario final (a menos que el Usuario final anterior o un Administrador permita que los datos ser compartido).

El cliente tendrá control sobre políticas específicas de intercambio de datos. Esas políticas, de acuerdo con la funcionalidad de los Servicios, permitirán al Cliente determinar la configuración de uso compartido de productos aplicable a los Usuarios finales para fines específicos. El Cliente puede optar por utilizar la funcionalidad de registro que Google pone a disposición a través de los Servicios.

(b) Discos retirados y política de borrado de disco.

Los discos que contienen datos pueden experimentar problemas de rendimiento, errores o fallas de hardware que los lleven a ser dados de baja ("Disco fuera de servicio"). Cada Disco retirado está sujeto a una serie de procesos de destrucción de datos (la "Política de borrado de disco") antes de salir de las instalaciones de Google para su reutilización o destrucción. Los discos dados de baja se borran en un proceso de varios pasos y se verifican completos por al menos dos validadores independientes. Los resultados del borrado se registran con el número de serie del disco retirado para su seguimiento. Finalmente, el Disco retirado borrado se libera al inventario para su reutilización y redespliegue. Si, debido a una falla de hardware, el disco retirado no se puede borrar, se almacena de forma segura hasta que se pueda destruir. Cada instalación se audita periódicamente para supervisar el cumplimiento de la Política de borrado de disco.

4. Seguridad del personal

El personal de Google debe comportarse de manera coherente con las pautas de la empresa con respecto a la confidencialidad, la ética empresarial, el uso adecuado y los estándares profesionales. Google lleva a cabo verificaciones de antecedentes razonablemente apropiadas en la medida en que lo permita la ley y de acuerdo con la legislación laboral local aplicable y las regulaciones estatutarias.

El personal debe firmar un acuerdo de confidencialidad y debe acusar recibo y cumplimiento de las políticas de privacidad y confidencialidad de Google. El personal recibe formación en seguridad. El personal que maneja los Datos del Cliente debe completar los requisitos adicionales adecuados a su función (por ejemplo, certificaciones). El personal de Google no procesará los Datos del cliente sin autorización.

5. Seguridad del subprocesador

Antes de incorporar a los subprocesadores, Google lleva a cabo una auditoría de las prácticas de seguridad y privacidad de los subprocesadores para garantizar que los subprocesadores brinden un nivel de seguridad y privacidad apropiado para su acceso a los datos y el alcance de los servicios que están contratados para brindar. Una vez que Google ha evaluado los riesgos presentados por el subprocesador, y sujeto a los requisitos descritos en la Sección 11.3 (Requisitos para la participación del subprocesador) de esta Enmienda de procesamiento de datos, el subprocesador debe suscribir los términos del contrato de seguridad, confidencialidad y privacidad adecuados.

Versión anterior

29 de octubre de 2019

25 de mayo de 2018

25 de abril de 2018

11 de julio de 2017

28 de noviembre de 2016

7 de enero de 2016

24 de abril de 2015

1 de abril de 2014

14 de noviembre de 2012

Enmienda de procesamiento de datos de productos complementarios y espacio de trabajo de Google, versión 2.3