Anexo de Tratamiento de Datos de Cloud (Socios)

Este Anexo de Tratamiento de Datos de Cloud (incluidos sus apéndices, el "*Anexo*") se incorpora al Acuerdo (como se define más adelante) entre Google y el Socio. Este Anexo se conocía anteriormente como las "Condiciones de Seguridad y Tratamiento de Datos" de Google Cloud Platform y como el "Anexo de Tratamiento de Datos" o las "Condiciones de Seguridad y Tratamiento de Datos" de Looker (original) o de los Servicios de Google SecOps.

Condiciones Generales

1. Descripción General

En este Anexo, se describen las obligaciones de las partes, incluidas las obligaciones en virtud de las leyes aplicables de privacidad y seguridad y protección de datos, con respecto al procesamiento y la seguridad de los Datos del Socio. Este Anexo entrará en vigor en la Fecha de Entrada en Vigor del Anexo (como se define más adelante) y reemplazará las condiciones previamente aplicables al tratamiento y la seguridad de los Datos del Socio. Los términos con mayúscula inicial que se usan en este Anexo, pero que no se definen en el presente documento, tienen el significado que se les atribuye en el Acuerdo.

2. Definiciones

2.1 En este Anexo:

- "*Fecha de Entrada en Vigor del Anexo*" significa la fecha en la que el Socio aceptó este Anexo o en la que las partes lo hayan acordado de otra forma.
- "*Controles de Seguridad Adicionales*" significa los recursos, las características, las funciones y los controles que el Socio podrá usar si lo desea y a su discreción, incluidos la Consola del Administrador, la encriptación, los registros, la supervisión, la administración de identidades y accesos, los análisis de seguridad y los firewalls.
- "*Acuerdo*" significa el contrato en virtud del cual Google aceptó prestarle los Servicios aplicables al Socio.
- "*Ley de Privacidad Aplicable*" significa, según corresponda al tratamiento de los Datos Personales del Socio, a cualquier ley o reglamentación de privacidad o seguridad o protección de datos, sea nacional, federal, de la Unión Europea, estatal, provincial o de otra índole.

- "*Servicios Auditados*" significa los Servicios entonces vigentes que se indica que están dentro del alcance de la certificación o del informe pertinentes en https://cloud.google.com/security/compliance/services-in-scope. Google no podrá quitar ningún Servicio de esta URL, a menos que este se haya descontinuado de conformidad con el Acuerdo.

- "*Certificaciones de Cumplimiento*" tiene el significado que se le atribuye en la Sección 7.4 (Certificaciones de Cumplimiento e Informes SOC).

- "*Incidente de Datos*" significa una violación de la seguridad de Google que puede causar, de forma accidental o ilegal, la destrucción, pérdida, alteración o divulgación no autorizada de los Datos del Socio, o el acceso a ellos, en sistemas administrados o de otra manera controlados por Google.

- "*EMEA*" significa Europa, Oriente Medio y África.

- "*RGPD de la UE*" significa el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE.

- "*Ley Europea de Protección de Datos*" significa, según corresponda, (a) al RGPD o (b) a la FADP de Suiza.

- "*Ley Europea*" significa, según corresponda, (a) a la ley de la UE o de un Estado Miembro de la UE (si se aplica el RGPD de la UE al tratamiento de los Datos Personales del Socio); (b) a la ley del Reino Unido o de parte del Reino Unido (si se aplica el RGPD del Reino Unido al tratamiento de los Datos Personales del Socio), o (c) a la ley de Suiza (si se aplica la FADP de Suiza al tratamiento de los Datos Personales del Socio).

- "*RGPD*" significa, según corresponda, (a) al RGPD de la UE o (b) al RGPD del Reino Unido.

- "*Auditor Externo de Google*" significa un auditor externo independiente y calificado designado por Google, cuya identidad Google divulgará al Socio en su momento.

- "*Instrucciones*" tiene el significado que se le atribuye en la Sección 5.2 (Cumplimiento de las Instrucciones del Socio).

- "*Dirección de Correo Electrónico de Notificación*" significa las direcciones de correo electrónicas designadas por el Socio en la Consola del Administrador o el Formulario de Pedido para recibir determinadas notificaciones de Google.

- "*Usuarios Finales del Socio*" tiene el significado que se le atribuye en el Acuerdo. En caso de que no haya tal atribución, tiene el significado correspondiente a "Usuarios Finales" en el Acuerdo.

- "*Datos Personales del Socio*" significa los datos personales presentes en los Datos del Socio, incluida cualquier categoría especial de datos personales o sensibles que se defina en virtud de la Ley de Privacidad Aplicable.

- "*Documentación de Seguridad*" significa las Certificaciones de Cumplimiento y los Informes SOC.

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

- "*Servicios*" significa los servicios aplicables descritos en el Apéndice 4 (Productos Específicos).

- "*Informes SOC*" tiene el significado que se le atribuye en la Sección 7.4 (Certificaciones de Cumplimiento e Informes SOC).

- "*Subencargado del Tratamiento de Datos*" significa un tercero autorizado como otro encargado del tratamiento de datos en virtud de este Anexo para tratar los Datos del Socio y brindar partes de los Servicios y los TSS.

- "*Autoridad Supervisora*" significa, según corresponda, (a) a una "autoridad supervisora", según se define en el RGPD de la UE, o (b) al "Comisionado", según se define en el RGPD del Reino Unido o la FADP de Suiza.

- "*FADP de Suiza*" significa, según corresponda, a la Ley Federal de Protección de Datos del 19 de junio de 1992 (Suiza) (con la Ordenanza de la Ley Federal de Protección de Datos del 14 de junio de 1993) o a la Ley Federal de Protección de Datos revisada del 25 de septiembre de 2020 (Suiza) (con la Ordenanza de la Ley Federal de Protección de Datos del 31 de agosto de 2022).

- "*Vigencia*" significa el tiempo entre la Fecha de Entrada en Vigor del Anexo y el final de la prestación de los Servicios por parte de Google, incluido, si corresponde, cualquier período durante el cual se suspenda la prestación de los Servicios y cualquier período posterior a la finalización durante el cual Google siga prestando los Servicios con fines de transición.

- "*RGPD del Reino Unido*" significa el RGPD de la UE tal como se enmendó y se incorporó a la legislación del Reino Unido en virtud de la Ley del 2018 sobre la salida del Reino Unido de la Unión Europea y, además, a la legislación secundaria aplicable conforme a esa Ley.

2.2 Los términos "datos personales", "sujeto", "tratamiento", "responsable del tratamiento de datos" y "encargado del tratamiento de datos", en la forma en que se usan en este Anexo, tienen los significados que se les atribuye en la Ley de Privacidad Aplicable. En caso de que no haya tal ley o atribución, tendrán el significado que se les atribuye en el RGPD de la UE.

2.3 Los términos "sujeto", "responsable del tratamiento de datos" y "encargado del tratamiento de datos" incluyen "consumidor", "empresa" y "proveedor de servicios", respectivamente, según lo exija la Ley de Privacidad Aplicable.

3. Duración

Sin importar si el Acuerdo se termina o vence, este Anexo permanecerá vigente hasta que Google borre todos los Datos del Socio según se describe en el presente y vencerá de manera automática en ese momento.

4. Funciones y Cumplimiento Legal

4.1 *Funciones de las Partes.* Con respecto a los Datos Personales del Socio, Google es encargado del tratamiento de datos y el Socio es responsable o encargado del tratamiento de datos, según corresponda.

4.2 *Resumen del Tratamiento de Datos.* La cuestión y los detalles del tratamiento de los Datos Personales del Socio se describen en el Apéndice 1 (Cuestión y Detalles del Tratamiento de Datos).

4.3 *Cumplimiento de las Leyes.* Cada parte cumplirá con sus obligaciones en relación con el tratamiento de los Datos Personales del Socio conforme a la Ley de Privacidad Aplicable.

4.4 *Condiciones Legales Adicionales*. En la medida en que el tratamiento de los Datos Personales del Socio esté sujeto a la Ley de Privacidad Aplicable descrita en el Apéndice 3 (Leyes de Privacidad Específicas), se aplicarán las condiciones del Apéndice 3 además de estas Condiciones Generales y prevalecerán según se describe en la Sección 14.1 (Prioridad).

5. Tratamiento de Datos

5.1 *Socios Encargados del Tratamiento de Datos*. Si un Socio es encargado del tratamiento de datos:

a. El Socio garantiza de forma continua que el Cliente y responsable del tratamiento de datos pertinente autorizó lo siguiente:

i. las Instrucciones;

ii. la contratación por parte del Socio de Google como encargado adicional del tratamiento de datos;

iii. la contratación por parte de Google de Subencargados del Tratamiento de Datos, según se describe en la Sección 11 (Subencargados del Tratamiento de Datos);

b. El Socio reenviará al Cliente y responsable del tratamiento de datos pertinente, de forma inmediata y sin demoras indebidas, cualquier aviso que le proporcione Google en virtud de las Secciones 7.2.1 (Notificación de Incidentes), 9.2.1 (Responsabilidad por las Solicitudes) o 11.4 (Oportunidad de Objetar a Subencargados del Tratamiento de Datos); y

c. El Socio podrá poner a disposición del Cliente y responsable del tratamiento de datos pertinente cualquier otra información que le brinde Google en virtud de este Anexo sobre las ubicaciones de los centros de datos de Google o los nombres, las ubicaciones y las actividades de los Subencargados del Tratamiento de Datos.

5.2 *Cumplimiento de las Instrucciones del Socio*. El Socio le indica a Google que trate los Datos del Socio de conformidad con el Acuerdo (incluido este Anexo) solo en estas circunstancias:

a. para prestar, proteger y supervisar los Servicios y los TSS; y

b. en las circunstancias que se especifiquen adicionalmente a través de:

i. el uso que haga el Socio de los Servicios (incluso a través de la Consola del Administrador) y los TSS; y

ii. cualquier otra instrucción que el Socio proporcione por escrito y que Google reconozca como tal en virtud de este Anexo;

(en conjunto, las "*Instrucciones*")

Google cumplirá con las Instrucciones, a menos que lo prohíba la Ley Europea (en los casos en los que rija la Ley Europea de Protección de Datos) o la ley aplicable (en los casos en los que rija otra Ley de Privacidad Aplicable).

6. Eliminación de Datos

6.1 *Eliminación por Parte del Socio*. Google permitirá que el Socio borre los Datos del Socio durante la Vigencia de forma coherente con la funcionalidad de los Servicios. Si el Socio usa los Servicios para borrar Datos del Socio durante la Vigencia de un modo que no pueda recuperarlos, esto constituirá una Instrucción a Google para que éste borre los Datos del Socio pertinentes de los sistemas de Google. Google cumplirá con esta Instrucción en cuanto sea razonablemente factible y en un plazo máximo de 180 días, a menos que se exija su almacenamiento según la Ley Europea (en los casos en los que rija la Ley Europea de Protección de Datos) o una ley aplicable (en los casos en los que rija otra Ley de Privacidad Aplicable).

6.2 *Devolución o Eliminación al Término de la Vigencia*. Si el Socio desea conservar Datos del Socio luego del término de la Vigencia, podrá indicarle a Google, de conformidad con la Sección 9.1 (Acceso, Rectificación, Tratamiento Restringido y Portabilidad) que devuelva los datos durante la Vigencia. El Socio le indica a Google que borre todos los Datos del Socio restantes (incluidas las copias existentes) de los sistemas de Google al finalizar la Vigencia. Luego de un período de recuperación de hasta 30 días contados a partir de esa fecha, Google cumplirá con esta Instrucción en cuanto sea razonablemente factible y en un plazo máximo de 180 días, a menos que se exija su almacenamiento según la Ley Europea (en los casos en los que rija la Ley Europea de Protección de Datos) o una ley aplicable (en los casos en los que rija otra Ley de Privacidad Aplicable).

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, organizativas y físicas para proteger los Datos del Socio contra casos accidentales o ilegales de destrucción, pérdida, alteración o divulgación o acceso no autorizados, según se describe en el Apéndice 2, Medidas de Seguridad. (las "*Medidas de Seguridad*"). Las Medidas de Seguridad incluyen las acciones necesarias para encriptar los Datos del Socio; para ayudar a garantizar la confidencialidad, la integridad, la disponibilidad y la resiliencia de los sistemas y servicios de Google de forma continua; para ayudar a restablecer el acceso oportuno a los Datos del Socio después de un

incidente, y para realizar pruebas de eficacia periódicas. Google podrá actualizar las Medidas de Seguridad ocasionalmente, siempre y cuando estas actualizaciones no disminuyan significativamente la seguridad de los Servicios.

7.1.2 *Acceso y Cumplimiento*. Google realizará lo siguiente:

a. Autorizará a sus empleados, contratistas y Subencargados del Tratamiento de Datos a acceder a los Datos del Socio solo en la medida que sea estrictamente necesaria para cumplir con las Instrucciones.

b. Tomará las medidas apropiadas para garantizar el cumplimiento de las Medidas de Seguridad por parte de sus empleados, contratistas y Subencargados del Tratamiento de Datos en la medida que resulte aplicable al alcance de su cumplimiento.

c. Se asegurará de que todas las personas autorizadas para tratar los Datos del Socio estén sujetas a una obligación de confidencialidad.

7.1.3 *Controles de Seguridad Adicionales*. Google ofrecerá Controles de Seguridad Adicionales para lo siguiente:

a. permitir que el Socio tome medidas para proteger los Datos del Socio; y

b. proporcionarle al Socio información para proteger los Datos del Socio, acceder a ellos y utilizarlos.

7.1.4 *Asistencia de Seguridad de Google*. Google (tomando en cuenta la naturaleza del tratamiento de los Datos Personales del Socio y la información disponible para Google) asistirá al Socio para garantizar el cumplimiento de sus obligaciones (o, en los casos en los que el Socio sea encargado del tratamiento de datos, el cumplimiento de las obligaciones del responsable del tratamiento de datos pertinente) en relación con la seguridad y las violaciones de la seguridad de los datos personales en virtud de la Ley de Privacidad Aplicable de las siguientes maneras:

a. implementando y manteniendo Medidas de Seguridad conforme a la Sección 7.1.1 (Medidas de Seguridad de Google);

b. ofreciendo Controles de Seguridad Adicionales conforme a la Sección 7.1.3 (Controles de Seguridad Adicionales);

c. cumpliendo con las condiciones de la Sección 7.2 (Incidentes de Datos);

d. ofreciendo la Documentación de Seguridad conforme a la Sección 7.5.1 (Revisiones de la Documentación de Seguridad) y proporcionando la información contenida en el Acuerdo (incluido este Anexo); y

e. en caso de que las subsecciones (a) a (d) anteriores resulten insuficientes para el Socio (o el responsable del tratamiento de datos pertinente) a fin de cumplir las obligaciones mencionadas, si el Socio lo solicita, brindándole al Socio la cooperación y asistencia adicionales que resulten razonables

7.2 *Incidentes de Datos*

7.2.1 *Notificación de Incidentes*. Google notificará al Socio, de forma inmediata y sin demoras indebidas, cuando tenga conocimiento de un Incidente de Datos y tomará inmediatamente las medidas razonables para minimizar los daños y proteger los Datos del Socio.

7.2.2 *Detalles de los Incidentes de Datos*. En la notificación por parte de Google sobre un Incidente de Datos, se describirá: la naturaleza del Incidente de Datos, incluidos los recursos del Socio afectados; las medidas que Google haya tomado o tenga previsto tomar para responder al Incidente de Datos y mitigar su riesgo potencial; las medidas, si las hubiera, que Google le recomienda al Socio en respuesta al Incidente de Datos, y los detalles de un punto de contacto para obtener más información. Si no es posible proporcionar toda la información mencionada al mismo tiempo, la notificación inicial de Google contendrá la información disponible en el momento y se brindará más información sin demoras indebidas a medida que esté disponible.

7.2.3 *Inexistencia de Evaluación de los Datos del Socio por Parte de Google*. Google no tiene la obligación de evaluar los Datos del Socio para identificar la información sujeta a requisitos legales específicos.

7.2.4 *Inexistencia de Reconocimiento de Fallas por Parte de Google*. La notificación o la respuesta de Google ante un Incidente de Datos en virtud de esta Sección 7.2 (Incidentes de Datos) no constituirá un reconocimiento por parte de Google de cualquier culpa o responsabilidad con respecto al Incidente de Datos.

7.3 *Responsabilidades y Evaluación del Socio con Respecto a la Seguridad*

7.3.1 *Responsabilidades del Socio con Respecto a la Seguridad*. 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 de lo dispuesto en el Acuerdo, entre Google y el Socio, este último es responsable del uso de los Servicios por parte suya y de sus Clientes, así como del almacenamiento de cualquier copia de los Datos del Socio fuera de los sistemas de Google o de los Subencargados del Tratamiento de Datos de Google. Esto incluye lo siguiente:

a. usar los Servicios y los Controles de Seguridad Adicionales para garantizar un nivel de seguridad adecuado al riesgo de los Datos del Socio

b. proteger las credenciales, los sistemas y los dispositivos de autenticación de cuentas que usan el Socio y sus Clientes para acceder a los Servicios

c. crear copias de seguridad de los Datos del Socio según corresponda

7.3.2 *Evaluación de la Seguridad por Parte del Socio*. El Socio acepta 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) proporcionan un nivel de seguridad adecuado para el riesgo de los Datos del Socio (tomando en cuenta la tecnología de vanguardia, los costos de la implementación y la índole, el alcance, el contexto y los fines del tratamiento de los Datos del Socio, así como los riesgos para personas físicas).

7.4 *Certificaciones de Cumplimiento e Informes SOC*. Google mantendrá, como mínimo, lo siguiente en relación con los Servicios Auditados para verificar la eficacia continua de las Medidas de Seguridad:

a. certificados de cumplimiento de la norma ISO 27001 y cualquier certificación adicional que se describa en el Apéndice 4 (Productos Específicos) (las "*Certificaciones de Cumplimiento*"); y

b. informes SOC 2 y SOC 3 producidos por el Auditor Externo de Google y actualizados anualmente a partir de una auditoría realizada, al menos, cada 12 meses (los "*Informes SOC*")

En cualquier momento, Google puede agregar estándares o reemplazar una Certificación de Cumplimiento o un Informe SOC por una alternativa equivalente o mejorada.

7.5 *Revisiones y Auditorías de Cumplimiento*

7.5.1 *Revisiones de la Documentación de Seguridad*. Para demostrar el cumplimiento de Google con respecto a sus obligaciones en virtud de este Anexo, Google pondrá a disposición la Documentación de Seguridad para que el Socio la revise y, si el Socio es encargado del tratamiento de datos, permitirá que el Socio solicite acceso a los Informes SOC para el Cliente y responsable del tratamiento de datos pertinente de conformidad con la Sección 7.5.3 (Condiciones Empresariales Adicionales para Revisiones y Auditorías).

7.5.2 *Derechos de Auditoría del Socio*

a. *Auditoría del Socio*. Si lo exige la Ley de Privacidad Aplicable, Google permitirá que el Socio o un auditor independiente que este designe realicen auditorías (incluidas inspecciones) para verificar el cumplimiento por parte de Google de sus obligaciones en virtud de este Anexo, de conformidad con la Sección 7.5.3 (Condiciones Empresariales Adicionales para Revisiones y Auditorías). Durante una auditoría, Google cooperará de manera razonable con el Socio o su auditor según se describe en esta Sección 7.5 (Revisiones y Auditorías de Cumplimiento).

b. *Revisión Independiente del Socio*. El Socio podrá realizar una auditoría para verificar el cumplimiento por parte de Google de sus obligaciones en virtud de este Anexo a través de una revisión de la Documentación de Seguridad (que refleja el resultado de las auditorías realizadas por el Auditor Externo de Google).

7.5.3 *Condiciones Empresariales Adicionales para Revisiones y Auditorías*

a. El Socio debe comunicarse con el Equipo de Protección de Datos de Google Cloud para solicitar lo siguiente:

i. acceso a los Informes SOC para un responsable del tratamiento de datos pertinente en virtud de la Sección 7.5.1 (Revisiones de la Documentación de Seguridad); o

ii. una auditoría en virtud de la Sección 7.5.2(a) (Auditoría del Socio)

b. Luego de una solicitud del Socio en virtud de la Sección 7.5.3(a), Google y el Socio analizarán y acordarán por adelantado lo siguiente:

i. los controles de seguridad y confidencialidad aplicables a cualquier acceso a los Informes SOC por parte de un responsable del tratamiento de datos pertinente en virtud de la Sección 7.5.1 (Revisiones de la Documentación de Seguridad); y

ii. la fecha de inicio, el alcance y la duración razonables, y los controles de seguridad y confidencialidad aplicables a cualquier auditoría en virtud de la Sección 7.5.2(a) (Auditoría del Socio)

c. Google podrá cobrar una tarifa (basada en los costos razonables de Google) por cualquier auditoría en virtud de la Sección 7.5.2(a) (Auditoría del Socio). Google le brindará al Socio más detalles sobre cualquier tarifa aplicable, además del criterio del cálculo, antes de la auditoría correspondiente. El Socio será responsable de las tarifas que cobre cualquier auditor designado por el Socio para llevar a cabo dicha auditoría.

d. Google podrá objetar por escrito a cualquier auditor designado por el Socio para que realice una auditoría en virtud de la Sección 7.5.2(a) (Auditoría del Socio) si el auditor, según la opinión razonable de Google, carece de las calificaciones o la independencia adecuadas, es competidor de Google o resulta claramente inadecuado por otros motivos. Cualquier objeción de Google requerirá que el Socio designe a otro auditor o realice la auditoría por sí mismo.

e. Cualquier solicitud por parte del Socio en virtud del Apéndice 3 (Leyes de Privacidad Específicas) o del Apéndice 4 (Productos Específicos) para que un responsable del tratamiento de datos pertinente tenga acceso a un informe SOC o para realizar auditorías también estará sujeta a esta Sección 7.5.3 (Condiciones Empresariales Adicionales para Revisiones y Auditorías).

8. Evaluaciones de Impacto y Asesoramiento

Google (tomando en cuenta la naturaleza del tratamiento de los datos y la información disponible para Google) asistirá al Socio para garantizar el cumplimiento de sus obligaciones (o, en los casos en los que el Socio sea un encargado del tratamiento de datos, el cumplimiento de las obligaciones del responsable del tratamiento de datos pertinente) en relación con las evaluaciones de la protección de datos, las evaluaciones de riesgos, el asesoramiento regulatorio previo o los procedimientos equivalentes en virtud de la Ley de Privacidad Aplicable de las siguientes maneras:

a. ofreciendo Controles de Seguridad Adicionales conforme a la Sección 7.1.3 (Controles de Seguridad Adicionales) y la Documentación de Seguridad conforme a la Sección 7.5.1 (Revisiones de la Documentación de Seguridad);

b. proporcionando la información contenida en el Acuerdo (incluido este Anexo); y

c. en caso de que las subsecciones (a) y (b) anteriores resulten insuficientes para el Socio (o el responsable del tratamiento de datos pertinente) a fin de cumplir las obligaciones mencionadas, si el Socio lo solicita, brindándole al Socio la cooperación y asistencia adicionales que resulten razonables

9. Acceso y Otras Consideraciones, Derechos del Sujeto y Exportación de Datos

9.1 *Acceso, Rectificaciones, Procesamiento Restringido; Portabilidad*. Durante la Vigencia, Google permitirá que el Socio, de forma coherente con la funcionalidad de los Servicios, acceda a los Datos del Socio, los rectifique y restrinja su procesamiento, incluso a través de la función de eliminación que ofrece Google según lo descrito en la Sección 6.1 (Eliminación por Parte del Socio), y también permitirá que exporte los Datos del Socio. Si el Socio toma conocimiento de que alguna parte de los Datos Personales del Socio está incorrecta o desactualizada, el Socio será responsable de usar la

funcionalidad mencionada para rectificar o borrar esos datos si así lo exige la Ley de Privacidad Aplicable.

9.2 *Solicitudes del Sujeto*

9.2.1 *Responsabilidad por las Solicitudes*. Durante la Vigencia, si el Equipo de Protección de Datos de Google recibe una solicitud de parte de un sujeto en relación con Datos Personales del Socio en la que se identifique al Socio, Google hará lo siguiente:

a. Le indicará al sujeto que envíe su solicitud al Socio.

b. Notificará de inmediato al Socio.

c. No responderá de otra forma a la solicitud de ese sujeto sin autorización del Socio.

El Socio será responsable de responder a cualquier solicitud de este tipo, lo cual incluye, cuando sea necesario, utilizar las funciones de los Servicios.

9.2.2 *Asistencia de Google con Respecto a las Solicitudes de Sujetos*. Google (tomando en cuenta la naturaleza del tratamiento de los Datos Personales del Socio) asistirá al Socio para garantizar el cumplimiento de sus obligaciones (o, en los casos en los que el Socio sea encargado del tratamiento de datos, el cumplimiento de las obligaciones del responsable del tratamiento de datos pertinente), en virtud de la Ley de Privacidad Aplicable, de responder a las solicitudes de sujetos que deseen ejercer sus derechos de las siguientes maneras:

a. ofreciendo Controles de Seguridad Adicionales conforme a la Sección 7.1.3 (Controles de Seguridad Adicionales)

b. cumpliendo con las Secciones 9.1 (Acceso, Rectificaciones, Procesamiento Restringido y Portabilidad) y 9.2.1 (Responsabilidad por las Solicitudes)

c. en caso de que las subsecciones (a) y (b) anteriores resulten insuficientes para el Socio (o el responsable del tratamiento de datos pertinente) a fin de cumplir las obligaciones mencionadas, si el Socio lo solicita, brindándole al Socio la cooperación y asistencia adicionales que resulten razonables

10. Ubicaciones del Tratamiento de Datos

10.1 *Instalaciones de Almacenamiento y Tratamiento de Datos*. Sujeto a los compromisos de ubicación de los datos de Google en virtud de las Condiciones Específicas del Servicio y de los compromisos de transferencia de datos en virtud del Apéndice 3 (Leyes de Privacidad Específicas), si corresponde, los Datos del Socio podrán procesarse en cualquier país en el que Google o sus Subencargados del Tratamiento de Datos mantengan instalaciones.

10.2 *Información sobre los Centros de Datos*. Las ubicaciones de los centros de datos de Google se describen en el Apéndice 4 (Productos Específicos).

11. Subencargados del Tratamiento de Datos

11.1 *Consentimiento para la Contratación de Subencargados del Tratamiento de Datos*. El Socio autoriza específicamente a Google para que contrate como Subencargados del Tratamiento de Datos a las entidades divulgadas que se describen en la Sección 11.2 (Información sobre los Subencargados del Tratamiento de Datos) en la Fecha de Entrada en Vigor del Anexo. Además, sin perjuicio de lo establecido en la Sección 11.4 (Oportunidad de Objetar a Subencargados del Tratamiento de Datos), el Socio autoriza en términos generales a Google para contratar a otros terceros como Subencargados del Tratamiento de Datos ("*Nuevos Subencargados del Tratamiento de Datos*").

11.2 *Información sobre los Subencargados del Tratamiento de Datos*. Los nombres, las ubicaciones y las actividades de los Subencargados del Tratamiento de Datos se describen en el Apéndice 4 (Productos Específicos).

11.3 *Requisitos para la Contratación de Subencargados del Tratamiento de Datos*. Cuando se contrate a un Subencargado del Tratamiento de Datos, Google hará lo siguiente:

a. Se asegurará de que exista un contrato escrito en el que se especifique lo siguiente:

i. que el Subencargado del Tratamiento de Datos solo accede a los Datos del Socio y los usa en la medida que sea necesario para llevar a cabo las obligaciones por las que se lo subcontrata, y que lo hace de conformidad con el Acuerdo (incluido este Anexo); y

ii. que, si así lo exigen las Leyes de Privacidad Aplicables, las obligaciones con respecto a la protección de datos que se describen en este Anexo se le imponen al Subencargado del Tratamiento de Datos (según lo que se especifique en mayor detalle en el Apéndice 3 (Leyes de Privacidad Específicas))

b. Continuará siendo plenamente responsable de todas las obligaciones subcontratadas al Subencargado del Tratamiento de Datos, así como de todas sus acciones y omisiones.

11.4 *Oportunidad de Objetar a Subencargados del Tratamiento de Datos*

a. Cuando Google contrate a cualquier Nuevo Subencargado del Tratamiento de Datos durante la Vigencia, notificará al Socio acerca de la contratación, al menos, 30 días antes de que el Nuevo Subencargado del Tratamiento de Datos comience a procesar Datos del Socio. La notificación incluirá el nombre, la ubicación y las actividades del Nuevo Subencargado del Tratamiento de Datos.

b. El Socio podrá, en un plazo de 90 días después de que se lo notifique acerca de la contratación de un Nuevo Subencargado del Tratamiento de Datos, objetar terminación por conveniencia al Acuerdo de una de las siguientes formas:

i. de acuerdo con la disposición de terminación por conveniencia del Acuerdo; o

ii. si no existiera tal disposición, a través de una notificación a Google

12. Equipo de Protección de Datos de Cloud y Tratamiento de Registros

12.1 *Equipo de Protección de Datos de Cloud*. El Equipo de Protección de Datos de Cloud de Google proporcionará asistencia inmediata y razonable ante cualquier consulta del Socio en relación con el tratamiento de los Datos del Socio en virtud de Acuerdo, y se podrá establecer contacto con él según se describe en la Sección Avisos del Acuerdo o en el Apéndice 4 (Productos Específicos).

12.2 *Registros de Tratamiento de Datos de Google*. Google mantendrá la documentación apropiada de sus actividades de tratamiento de datos según lo exija la Ley de Privacidad Aplicable. En la medida en que alguna Ley de Privacidad Aplicable exija que Google recopile y mantenga registros de determinada información en relación con el Socio o sus Clientes, el Socio usará la Consola del Administrador, o bien otros medios identificados en el Apéndice 4 (Productos Específicos) para suministrar dicha información y mantenerla correcta y actualizada. Google podrá poner dicha información a disposición de los reguladores competentes, incluida una Autoridad Supervisora si así lo exigiera la Ley de Privacidad Aplicable.

12.3 *Solicitudes del Responsable del Tratamiento de Datos*. Durante la Vigencia, si el Equipo de Protección de Datos de Cloud de Google recibe una solicitud o instrucción de un tercero que afirme ser responsable del tratamiento de los Datos Personales del Socio, Google le indicará a dicho tercero que se comunique con el Socio.

13. Avisos

Los Avisos en virtud de este Anexo (incluidas las notificaciones sobre cualquier Incidente de Datos) se enviarán a la Dirección de Correo Electrónico de Notificación. El Socio es responsable de usar la Consola del Administrador o de notificar de otra manera a Google para asegurarse de que su Dirección de Correo Electrónico de Notificación se mantenga actualizada y sea válida.

14. Interpretación

14.1 *Prioridad*. En caso de que haya conflictos:

a. Entre el Apéndice 3 (Leyes de Privacidad Específicas) y el resto del Anexo (incluido el Apéndice 4, Productos Específicos), prevalecerá el Apéndice 3;

b. Entre el Apéndice 4 (Productos Específicos) y el resto del Anexo (sin incluir el Apéndice 3); prevalecerá el Apéndice 4; y

c. Entre este Anexo y el resto del Acuerdo, prevalecerá este Anexo.

14.2 *Referencias a Secciones*. A menos que se indique lo contrario, las referencias a secciones en cualquier Apéndice de este Anexo hacen referencia a las secciones de las Condiciones Generales del Anexo.

14.3 *Clientes*. En aras de evitar dudas, los Clientes no son terceros beneficiarios de este Anexo.

Apéndice 1: Cuestión y Detalles del Tratamiento de Datos

Cuestión

La prestación de los Servicios y los TSS por parte de Google al Socio.

Duración del Tratamiento de Datos

La Vigencia más el tiempo que transcurra entre el final de la Vigencia y la eliminación de todos los Datos del Socio por parte de Google, de conformidad con el Anexo.

Naturaleza y Propósito del Tratamiento de Datos

Google tratará los Datos Personales del Socio para prestarle los Servicios y los TSS al Socio de acuerdo con este Anexo.

Categorías de Datos

Datos relacionados con personas físicas que el Socio, sus Clientes o los Usuarios Finales del Socio (o alguna otra parte en representación de estas) suministren a Google a través de los Servicios.

Titulares

Los Sujetos incluyen a las personas físicas acerca de las cuales el Socio, sus Clientes o los Usuarios Finales del Socio (o alguna otra parte en representación de estas) suministren datos a Google a través de los Servicios.

Apéndice 2: Medidas de Seguridad

A partir de la Fecha de Entrada en Vigor del Anexo, Google implementará y mantendrá las Medidas de Seguridad que se describen en este Apéndice 2.

1. Seguridad de los Centros de Datos y las Redes

(a) Centros de Datos

Infraestructura. Google mantiene centros de datos distribuidos geográficamente. Google almacena todos los datos de producción en centros de datos que cuentan con medidas de protección física.

Redundancia. Los sistemas de infraestructura se diseñaron para eliminar los puntos únicos de fallo y minimizar el impacto de los riesgos ambientales previstos. Los circuitos dobles, los interruptores, las redes y otros dispositivos necesarios ayudan a proporcionar esta redundancia. Los Servicios se diseñaron para permitir que Google realice ciertos tipos de mantenimiento preventivo y correctivo sin interrupciones. Todas las instalaciones y los equipos ambientales cuentan con procedimientos de mantenimiento preventivo documentados en los que se detallan el proceso y la frecuencia con que se llevan a cabo según las especificaciones internas o del fabricante. El mantenimiento preventivo y correctivo de los equipos de los centros de datos se programa a través de un proceso de cambio estándar según los procedimientos documentados.

Energía. Los sistemas de alimentación eléctrica de los centros de datos se diseñaron para ser redundantes y someterse a mantenimiento sin obstaculizar la continuidad de las operaciones las 24 horas, todos los días. En la mayoría de los casos, se proporcionan una fuente de energía principal y una alternativa, cada una con la misma capacidad, para los componentes de la infraestructura crítica del centro de datos. La energía de respaldo se proporciona a través de diversos mecanismos, como baterías de sistemas de alimentación ininterrumpida (UPS, por sus siglas en inglés), que proporcionan un suministro constante y confiable durante períodos de disponibilidad limitada de la red eléctrica, apagones, sobretensiones, caídas de tensión y condiciones de frecuencia fuera del rango de tolerancia. Si se interrumpe el suministro eléctrico, la alimentación 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 generadores de respaldo tomen el control. Los generadores de respaldo pueden iniciarse automáticamente en cuestión de segundos para proporcionar suficiente energía eléctrica de emergencia como para que el centro de datos funcione a plena capacidad, por lo general, durante un período de varios días.

Sistemas Operativos de Servidores. Los servidores de Google usan una implementación basada en Linux y personalizada para el entorno de aplicaciones. Los datos se almacenan con algoritmos privados para aumentar la redundancia y la seguridad de los datos.

Calidad del Código. Google emplea un proceso de revisión de código para aumentar la seguridad del código utilizado para prestar los Servicios y potenciar los productos de seguridad en los entornos de producción.

Continuidad Empresarial. Google diseñó programas de continuidad empresarial y de recuperación ante desastres, y realiza actividades de planificación y pruebas periódicamente.

(*b) Redes y Transmisión*

Transmisión de Datos. Los centros de datos suelen conectarse entre sí a través de vínculos privados de alta velocidad para proporcionar una transferencia de datos rápida y segura. Este diseño impide que los datos se lean, copien, alteren o quiten sin autorización durante la transferencia o el transporte electrónico, o mientras se registran en medios de almacenamiento de datos. Google transfiere datos a través de protocolos estándar de Internet.

Superficie de Ataque Externa. Google utiliza varias capas de dispositivos de red y detección de intrusiones para proteger la superficie de ataque externa. Google considera los posibles vectores de ataque y también incorpora tecnologías compiladas con propósitos específicos en sistemas externos.

Detección de Intrusiones. El objetivo de la detección de intrusiones es proporcionar estadísticas sobre las actividades de ataques en curso y brindar información adecuada para responder ante los incidentes. La detección de intrusiones de Google implica: (i) controlar de cerca el tamaño y la composición de la superficie de ataque de Google aplicando medidas preventivas; (ii) emplear controles de detección inteligentes en los puntos de entrada de datos, y (iii) usar tecnologías que solucionen automáticamente algunas situaciones peligrosas.

Respuesta ante Incidentes. Google supervisa varios canales de comunicación para detectar incidentes de seguridad. Además, el personal de seguridad de Google reaccionará con rapidez ante los incidentes conocidos.

Tecnologías de Encriptación. Google hace que la encriptación HTTPS (también conocida como conexión SSL o TLS) esté disponible. Los servidores de Google admiten el intercambio de claves criptográficas de la curva elíptica efímera Diffie-Hellman firmadas con RSA y ECDSA. Estos métodos de confidencialidad directa perfecta (PFS) ayudan a proteger el tráfico y minimizar las consecuencias de las vulneraciones de claves o las rupturas criptográficas.

2. Controles de Instalaciones y Accesos

(a) Controles de Instalaciones

Operaciones de Seguridad del Centro de Datos en las Instalaciones. Los centros de datos de Google mantienen operaciones de seguridad en las instalaciones que son responsables de todas sus funciones de seguridad física las 24 horas, todos los días. El personal de operaciones de seguridad en las instalaciones supervisa las cámaras de circuito cerrado de TV (CCTV) y todos los sistemas de alarma, y patrulla el interior y el exterior del centro de datos periódicamente.

Procedimientos de Acceso a los Centros de Datos. Google mantiene procedimientos de acceso formales para permitir el acceso físico a los centros de datos. Los centros de datos se alojan en instalaciones a las que solo se puede acceder con una tarjeta de clave electrónica y cuentan con alarmas vinculadas a las operaciones de seguridad en las instalaciones. Toda persona que quiera ingresar al centro de datos debe identificarse y demostrar su identidad ante los encargados de las operaciones de seguridad en las instalaciones. Solo los empleados, contratistas y visitantes autorizados tienen permitido ingresar a los centros de datos. Solo los empleados y contratistas autorizados pueden solicitar acceso a través de tarjetas de clave electrónicas para estas instalaciones. Las solicitudes de acceso con tarjetas de clave electrónicas para el centro de datos deben realizarse por correo electrónico y aprobarse por el supervisor del solicitante y el director del centro de datos. Todas las demás personas que requieran acceder temporalmente al centro de datos deben (i) obtener aprobación previa de los administradores de los centros de datos para las áreas internas y los centros de datos específicos que deseen visitar; (ii) registrarse con los encargados de las operaciones de seguridad en las instalaciones, y (iii) presentar un registro de acceso al centro de datos en el que se identifique que la persona física está aprobada.

Dispositivos de Seguridad del Centro de Datos en las Instalaciones. Los centros de datos de Google utilizan un sistema de control de acceso con doble autenticación que está vinculado a una alarma del sistema. El sistema de control de acceso supervisa y registra la tarjeta de clave electrónica de cada persona, cuando acceden a puertas perimetrales, para hacer envíos y recibir entregas, y cuando acceden a otras áreas críticas. La actividad no autorizada y los intentos de acceso fallidos se registran en el sistema de control de acceso y se investigan, según corresponda. El acceso autorizado en todas las operaciones comerciales y en los centros de datos está restringido en función de las zonas y las responsabilidades del trabajo de la persona física. Las puertas contra incendios de los centros de datos tienen alarmas. Hay cámaras de CCTV en funcionamiento tanto dentro como fuera de los centros de datos. Las cámaras se ubican para cubrir áreas estratégicas, incluidas, entre otras, el perímetro, las puertas para ingresar al edificio del centro de datos y los espacios de envíos y recepciones. El personal de operaciones de seguridad en las instalaciones administra los equipos de supervisión, grabación y control de CCTV. Los cables que conectan los equipos de CCTV del centro de datos están protegidos en toda su extensión. Las cámaras cuentan con grabadoras de video digitales que capturan lo que ocurre en las instalaciones las 24 horas, todos los días. Los registros de vigilancia se conservan durante un máximo de 30 días, según la actividad.

(b) Control de Acceso

Personal de Seguridad de la Infraestructura. Google tiene y mantiene una política de seguridad para su personal, y les exige capacitarse en materia de seguridad como parte del paquete de formación. El personal de seguridad de la infraestructura de Google es responsable de la supervisión continua de su infraestructura de seguridad, la revisión de los Servicios y la respuesta ante incidentes de seguridad.

Control de Acceso y Administración de Privilegios. Los Administradores y Usuarios Finales del Socio deben autenticarse por medio de un sistema de autenticación central o inicio de sesión único para poder usar los Servicios.

Políticas y Procesos de Acceso a los Datos Internos: Política de Acceso. Los procesos y las políticas de acceso a los datos internos de Google se diseñaron para evitar que personas o sistemas no autorizados puedan ingresar a los sistemas que se usan para tratar los Datos del Socio. Google diseña sus sistemas de modo que (i) permitan que solo las personas autorizadas para acceder a determinados datos puedan hacerlo y (ii) garanticen que los Datos del Socio no se puedan leer, copiar, alterar ni quitar sin autorización durante el tratamiento y el uso, y después del registro. Los sistemas se diseñaron para detectar cualquier acceso inapropiado. Google emplea un sistema de administración de accesos centralizado para controlar el acceso del personal a los servidores de producción, y solo proporciona acceso a una cantidad limitada de miembros autorizados del personal. Los sistemas de autenticación y autorización de Google utilizan certificados SSH y llaves de seguridad, y se diseñaron para proporcionarle a Google mecanismos de acceso seguros y flexibles. Estos mecanismos se diseñaron para otorgar únicamente derechos de acceso aprobados a los hosts, los registros, los datos y la información de configuración de las instalaciones. Google exige el uso de IDs de usuario únicos, contraseñas seguras, autenticación de dos factores y listas de acceso supervisadas rigurosamente para minimizar el uso potencial no autorizado de cuentas. El otorgamiento o la modificación de los derechos de acceso se basa en las responsabilidades laborales del personal autorizado y los requisitos del puesto necesarios para realizar tareas autorizadas, y se realiza en el caso exclusivo de que sea necesario. El otorgamiento o la modificación de los derechos de acceso también debe cumplir con las políticas y la capacitación para el acceso a los datos internos de Google. Se emplean herramientas de flujo de trabajo para administrar las aprobaciones y mantener registros de auditoría sobre todos los cambios. El acceso a los sistemas se guarda en un registro de auditoría con fines de contabilización. Cuando se emplean contraseñas para la autenticación (p. ej., acceder a estaciones de trabajo), se implementan políticas que siguen, como mínimo, las prácticas estándar de la industria, incluidas restricciones de reutilización y exigencias de seguridad. Para acceder a información extremadamente sensible (p. ej., datos de tarjetas de crédito), Google usa tokens de hardware.

3. Datos

(a) *Almacenamiento, Aislamiento y Registro de Datos*. Google almacena los datos en un entorno multiusuario en sus propios servidores. Sujeto a posibles Instrucciones que requieran lo contrario (p. ej., en forma de una selección de la ubicación de los datos), Google replica los Datos del Socio entre múltiples centros de datos geográficamente dispersos. Google también aísla lógicamente los Datos del Socio. El Socio tendrá control sobre las políticas específicas del uso compartido de datos. Dichas políticas, de conformidad con la funcionalidad de los Servicios, permitirán que el Socio determine la configuración de uso compartido de los productos que resulte aplicable a los Usuarios Finales del Socio para fines específicos. El Socio puede optar por usar la función de registros que Google ofrece a través de los Servicios.

(b) *Discos Retirados y Política de Borrado de Datos en Discos*. Cuando los discos de datos presentan problemas de rendimiento, errores o fallas de hardware, estos se pueden retirar (cada uno se denomina "Disco Retirado"). Todos los Discos Retirados se someten a una serie de procesos de destrucción de datos (la "Política de Borrado de Discos") antes de salir de las instalaciones de Google

para reutilizarlos o destruirlos. Los Discos Retirados se borran en un proceso de múltiples pasos cuya finalización se verifica por al menos dos validadores independientes. Los resultados del borrado se registran con el número de serie del Disco Retirado con fines de seguimiento. Por último, el Disco Retirado que se borró se publica en el inventario para su reutilización y reimplementación. Si, debido a una falla en el hardware, el Disco Retirado no se puede borrar, se almacenará de forma segura hasta que se pueda destruir. Cada instalación se audita con regularidad para supervisar el cumplimiento de la Política de Borrado de Discos.

4. Seguridad del Personal

El personal de Google debe cumplir con unos lineamientos en función de los reglamentos de la empresa en cuanto a la confidencialidad, la ética empresarial, el uso adecuado y los estándares profesionales. Google realiza verificaciones de antecedentes razonablemente adecuadas en la medida en que la ley lo permita y de acuerdo con la legislación laboral local y las reglamentaciones legales aplicables.

El personal de Google debe firmar un acuerdo de confidencialidad, confirmar la recepción de las políticas de confidencialidad y privacidad de Google, y asegurar el cumplimiento de estas. El personal recibe una capacitación en seguridad. El personal que maneja los Datos del Socio debe cumplir requisitos adicionales adecuados a su función (p. ej., certificaciones). El personal de Google no tratará los Datos del Socio sin autorización.

5. Seguridad de los Subencargados del Tratamiento de Datos

Antes de capacitar a nuevos Subencargados del Tratamiento de Datos, Google lleva a cabo una auditoría de sus prácticas de seguridad y privacidad para asegurarse de que los Subencargados del Tratamiento de Datos ofrezcan un nivel de seguridad y privacidad acorde a su acceso a los datos y al alcance de los servicios para los que se los contrata. Una vez que Google evalúa los riesgos que presenta el Subencargado del Tratamiento de Datos, sujeto a los requisitos que se describen en la Sección 11.3 (Requisitos para la Contratación de Subencargados del Tratamiento de Datos), se le exige al Subencargado del Tratamiento de Datos que acepte las condiciones contractuales adecuadas en materia de seguridad, confidencialidad y privacidad.

Apéndice 3: Leyes de Privacidad Específicas

Las condiciones que se indican en cada subsección de este Apéndice 3 se aplican únicamente a los casos en que las leyes correspondientes se apliquen al tratamiento de los Datos Personales del Socio.

Ley Europea de Protección de Datos

1. Definiciones Adicionales

- "*País con Nivel Adecuado de Protección*" significa lo siguiente:

(a) en relación con los datos que se tratan sujetos al RGPD: al Espacio Económico Europeo o a un país o territorio al cual se lo reconoce por garantizar una protección adecuada en virtud del RGPD de la UE;

(b) en relación con los datos que se tratan sujetos al RGPD del Reino Unido: al Reino Unido o a un país o territorio al cual se lo reconoce por garantizar una protección adecuada en virtud del RGPD del Reino Unido y la Ley de Protección de Datos del 2018; o

(c) en relación con los datos que se tratan sujetos a la FADP de Suiza: a Suiza o a un país o territorio que: (i) está incluido en la lista de estados cuya legislación garantiza una protección adecuada, según lo publicado por el Comisionado de Información y Protección de Datos Federal Suizo, si corresponde, o (ii) es reconocido por garantizar una protección adecuada por el Consejo Federal Suizo en virtud de la FADP de Suiza

En cada caso, salvo que sea sobre la base de un marco de protección de datos opcional.

- "*Solución Alternativa de Transferencia*" significa una solución, distinta de las SCC, que haga posible la transferencia lícita de datos personales a un tercer país de conformidad con la Ley Europea de Protección de Datos; por ejemplo, un marco de protección de datos reconocido por garantizar que las entidades participantes proporcionen protección adecuada.

- "*SCC del Socio*" significa las SCC (de Responsable a Encargado del Tratamiento de Datos), las SCC (de un Encargado del Tratamiento de Datos a Otro) o las SCC (de Encargado a Responsable del Tratamiento de Datos), según corresponda.

- "*SCC*" significa las SCC del Socio o las SCC (de un Encargado del Tratamiento de Datos a Otro, Exportador de Google), según corresponda.

- "*SCC (de Responsable a Encargado del Tratamiento de Datos)*" significa las condiciones que se encuentran en https://cloud.google.com/terms/sccs/eu-c2p.

- "*SCC (de Encargado a Responsable del Tratamiento de Datos)*" significa las condiciones que se encuentran en https://cloud.google.com/terms/sccs/eu-p2c.

- "*SCC (de un Encargado del Tratamiento de Datos a Otro)*" significa las condiciones que se encuentran en https://cloud.google.com/terms/sccs/eu-p2p.

- "*SCC (de un Encargado del Tratamiento de Datos a Otro, Exportador de Google)*" significa las condiciones que se encuentran en https://cloud.google.com/terms/sccs/eu-p2p-google-exporter.

2. Notificaciones de Instrucciones. Sin perjuicio de las obligaciones de Google en virtud de la Sección 5.2 (Cumplimiento de las Instrucciones del Socio) ni de ningún otro derecho u obligación de cualquiera de las partes en virtud del Acuerdo, Google notificará de inmediato al Socio si, en opinión de Google, ocurre cualquiera de las siguientes situaciones:

a. La Ley Europea prohíbe que Google cumpla una Instrucción.

b. Una Instrucción no cumple con alguna Ley Europea de Protección de Datos.

c. Google es incapaz de cumplir una Instrucción por algún otro motivo. En cada caso, esto se hará a menos que la Ley Europea prohíba dicha notificación.

Si el Socio es encargado del tratamiento de datos, reenviará de inmediato al responsable del tratamiento de datos pertinente cualquier aviso que Google proporcione en virtud de esta sección.

3. Derechos de Auditoría del Socio. Google permitirá que el Socio o un auditor independiente que este designe realicen auditorías (incluidas inspecciones) según se describe en la Sección 7.5.2(a) (Auditoría del Socio). Durante dicha auditoría, Google pondrá a disposición toda la información necesaria para demostrar el cumplimiento de sus obligaciones en virtud de este Anexo y aportará a la auditoría según se describe en la Sección 7.5 (Revisiones y Auditorías de Cumplimiento) y en esta Sección.

4. Transferencias de Datos

4.1 *Transferencias Restringidas.* Las partes reconocen que la Ley Europea de Protección de Datos no exige SCC ni una Solución Alternativa de Transferencia para que los Datos Personales del Socio se procesen en un País Adecuado o sean transferidos a este. Si los Datos Personales del Socio se transfieren a algún otro país y la Ley Europea de Protección de Datos se aplica a las transferencias (según lo certifique el Socio en virtud de la Sección 4.2 (Certificación por Parte de Socios no Pertenecientes a EMEA) de estas condiciones sobre la Ley Europea de Protección de Datos, en caso de que su dirección de facturación se encuentre fuera de EMEA) ("*Transferencias Restringidas*"), ocurrirá lo siguiente:

a. Si Google adoptó una Solución Alternativa de Transferencia para cualquier Transferencia Restringida, Google le informará al Socio sobre la solución pertinente y se asegurará de que las Transferencias Restringidas se hagan de acuerdo con ella.

b. Si Google no adoptó una Solución Alternativa de Transferencia para cualquier Transferencia Restringida o si le informa al Socio que Google ya no adopta una Solución Alternativa de Transferencia para cualquier Transferencia Restringida (sin adoptar una Solución Alternativa de Transferencia de reemplazo):

i. En caso de que la dirección de Google se encuentre en un País Adecuado:

A. Se aplicarán las SCC (de un Encargado del Tratamiento de Datos a Otro, Exportador de Google) con respecto a dichas Transferencias Restringidas de Google a los Subencargados del Tratamiento de Datos.; y

B. Además, si la dirección de facturación del Socio no se encuentra en un País Adecuado, se aplicarán las SCC (de Encargado a Responsable del Tratamiento de Datos), sin importar si el Socio es responsable o encargado del tratamiento de datos, con respecto a dichas Transferencias Restringidas entre Google y el Socio; o

ii. En caso de que la dirección de Google no se encuentre en un País Adecuado, se aplicarán las SCC (de Responsable a Encargado del Tratamiento de Datos) o las SCC (de un Encargado del Tratamiento de Datos a Otro), según si el Socio es responsable o encargado del tratamiento de datos, con respecto a las Transferencias Restringidas entre Google y el Socio.

4.2 *Certificación por Parte de Socios no Pertenecientes a EMEA*. En caso de que la dirección de facturación del Socio se encuentre fuera de EMEA, y el tratamiento de los Datos Personales del Socio

esté sujeto a la Ley Europea de Protección de Datos, salvo que se indique lo contrario en el Apéndice 4 (Productos Específicos) de este Anexo, el Socio identificará y certificará como tal a su Autoridad Supervisora competente por medio de la Consola del Administrador en relación con los Servicios aplicables.

4.3 *Información sobre las Transferencias Restringidas*. Google le proporcionará al Socio la información pertinente sobre las Transferencias Restringidas, los Controles de Seguridad Adicionales y otras medidas de protección complementarias del siguiente modo:

a. según se describe en la Sección 7.5.1 (Revisiones de la Documentación de Seguridad)

b. en cualquier ubicación adicional descrita en el Apéndice 4 (Productos Específicos)

c. en relación con la adopción por parte de Google de una Solución Alternativa de Transferencia, como se describe en https://cloud.google.com/terms/alternative-transfer-solution

4.4 *Auditorías de las SCC*. Si se aplican las SCC del Socio según se describe en la Sección 4.1 (Transferencias Restringidas) de estas condiciones de la Ley Europea de Protección de Datos, Google permitirá que el Socio (o un auditor independiente que este designe) lleve a cabo auditorías según se describe en dichas SCC y, durante una auditoría, pondrá a disposición toda la información que se exija en esas SCC. Ambas acciones se llevarán a cabo de conformidad con la Sección 7.5.3 (Condiciones Empresariales Adicionales para Revisiones y Auditorías).

4.5 *Avisos de SCC*. El Socio le reenviará al responsable del tratamiento de datos pertinente, de forma inmediata y sin demoras indebidas, cualquier aviso referido a alguna SCC.

4.6 *Terminación Debido al Riesgo de las Transferencias de Datos*. Si el Socio concluye, con base en su uso actual o previsto de los Servicios, que no se brindan las medidas de protección adecuadas para los Datos Personales del Socio transferidos, podrá poner fin de inmediato al Acuerdo de conformidad con la disposición de terminación por conveniencia del Acuerdo o, en caso de que no exista tal disposición, por medio de una notificación a Google.

4.7 *Inexistencia de Modificaciones de las SCC*. Nada de lo dispuesto en el Acuerdo (incluido este Anexo) tiene el propósito de modificar o contradecir ninguna SCC, ni de menoscabar los derechos o libertades fundamentales de los sujetos en virtud de la Ley Europea de Protección de Datos.

4.8 *Prioridad de las SCC*. En caso de que haya conflictos o discrepancias entre alguna de las SCC del Socio (incorporadas por referencia a este Anexo) y el resto del Acuerdo (incluido este Anexo), prevalecerán las SCC del Socio.

5. Requisitos para la Contratación de Subencargados del Tratamiento de Datos. La Ley Europea de Protección de Datos exige que Google garantice, por medio de un contrato por escrito, que las obligaciones de protección de datos descritas en este Anexo, según se hace referencia a ellas en el Artículo 28(3) del RGPD, si corresponde, se impongan a cualquier Subencargado del Tratamiento de Datos que Google contrate.

CCPA

1. Definiciones Adicionales

- "*CCPA*" significa la Ley de Privacidad del Consumidor de California del 2018, con sus modificaciones, incluidas las modificaciones de la Ley de Derechos de Privacidad de California del 2020, junto con todas las reglamentaciones de su implementación.

- "*Datos Personales del Socio*" incluye "información personal".

- Los términos "empresa", "propósito comercial", "consumidor", "información personal", "tratamiento de datos", "venta", "vender", "proveedor de servicios" y "compartir" tendrán los significados que se les atribuyen en la CCPA.

2. Prohibiciones. Sin perjuicio de las obligaciones de Google en virtud de la Sección 5.2 (Cumplimiento de las Instrucciones del Socio), con respecto al tratamiento de los Datos Personales del Socio de acuerdo con la CCPA, Google no realizará las siguientes acciones, salvo que estén permitidas de otra forma en virtud de la CCPA:

a. vender o compartir los Datos Personales del Socio;

b. retener, usar o divulgar los Datos Personales del Socio;

i. excepto para propósitos comerciales en virtud de la CCPA en nombre del Socio y con el objetivo específico de ejecutar los Servicios y los TSS

ii. fuera de la relación comercial directa entre Google y el Socio

c. combinar ni actualizar los Datos Personales del Socio con información personal que Google reciba de un tercero o en representación de este, ni con información personal que recopile a partir de sus propias interacciones con el consumidor

3. Cumplimiento. Sin perjuicio de las obligaciones de Google en virtud de la Sección 5.2 (Cumplimiento de las Instrucciones del Socio) ni de ningún otro derecho u obligación de cualquiera de las partes en virtud del Acuerdo, Google notificará al Socio si, en opinión de Google, no puede cumplir sus obligaciones en virtud de la CCPA, a menos que dicho aviso esté prohibido por la ley aplicable.

4. Intervención por Parte del Socio. Si Google notifica al Socio de algún uso no autorizado de los Datos Personales del Socio, lo cual incluye los casos contemplados en la Sección 3 (Cumplimiento) de esta subsección o en la Sección 7.2.1 (Notificación de Incidentes), el Socio podrá tomar las medidas razonables y apropiadas para detener o remediar el uso no autorizado de las siguientes formas:

a. tomando las medidas que recomiende Google en relación con la Sección 7.2.2 (Detalles de los Incidentes de Datos), si corresponde

b. ejerciendo sus derechos en virtud de las Secciones 7.5.2(a) (Auditoría del Socio) o 9.1 (Acceso, Rectificaciones, Procesamiento Restringido y Portabilidad)

Turquía

1. Definiciones Adicionales

- "*Ley Turca de Protección de Datos*" significa la Ley de Protección de Datos Personales núm. 6698 de Turquía, del 7 de abril de 2016.

- "*Agencia de Protección de Datos Personales de Turquía*" significa la Kişisel Verileri Koruma Kurumu.

- "*SCC de Turquía*" significa las cláusulas de contrato estándar en virtud de la Ley Turca de Protección de Datos.

2. Transferencias de Datos

2.1 *Condiciones Complementarias*. En caso de que la dirección de facturación del Socio se encuentre en Turquía y Google ofrezca condiciones adicionales opcionales (incluidas SCC de Turquía) para que el Socio las acepte en relación con las transferencias de los Datos Personales del Socio en virtud de la Ley Turca de Protección de Datos, dichas condiciones complementarán este Anexo a partir de la fecha en que se notifiquen a la Agencia de Protección de Datos de Turquía de conformidad con la siguiente Sección 2.2 (Notificación a la Autoridad Competente), según las pruebas que presente el Socio a Google.

2.2 *Notificación a la Autoridad Competente*. Si el Socio acepta las SCC de Turquía en virtud de esta Sección 2 (Transferencias de Datos), el Socio será responsable de notificar a la Agencia de Protección de Datos Personales de Turquía sobre el uso de las SCC de Turquía en un plazo de cinco (5) días hábiles contados a partir de la firma de las SCC de Turquía, según lo exige la Ley Turca de Protección de Datos.

2.3 *Auditorías de las SCC*. Si el Socio acepta las SCC de Turquía en virtud de esta Sección 2 (Transferencias de Datos), Google permitirá que el Socio (o un auditor independiente que este designe) realice auditorías según se describe en dichas SCC y, durante una auditoría, Google pondrá a disposición toda la información exigida por dichas SCC, todo ello de conformidad con la Sección 7.5.3 (Condiciones Empresariales Adicionales para Revisiones y Auditorías).

2.4 *Terminación Debido al Riesgo de las Transferencias de Datos*. Si el Socio concluye, con base en su uso actual o previsto de los Servicios, que no se brindan las medidas de protección adecuadas para los Datos Personales del Socio transferidos, podrá poner fin de inmediato al Acuerdo aplicable de conformidad con la disposición de terminación por conveniencia de ese Acuerdo o, en caso de que no exista tal disposición, por medio de una notificación a Google.

2.5 *Inexistencia de Modificaciones de las SCC de Turquía*. Nada de lo dispuesto en el Acuerdo (incluido este Anexo) tiene el propósito de modificar o contradecir las SCC de Turquía, ni de menoscabar los derechos o libertades fundamentales de los sujetos en virtud de la Ley Turca de Protección de Datos.

2.6 *Prioridad de las SCC*. En caso de que haya conflictos o discrepancias entre las SCC de Turquía (que se incorporarán por referencia a este Anexo si el Socio las acepta) y el resto del Acuerdo (incluido este Anexo), prevalecerán las SCC de Turquía.

Israel

1. Definición Adicional

- "*Ley Israelí de Protección de la Privacidad*" significa la Ley de Protección de la Privacidad de Israel de 1981 y a todas las reglamentaciones promulgadas en virtud de esta.

2. Términos Equivalentes. Los términos equivalentes a "responsable del tratamiento de datos", "datos personales", "tratamiento de datos" y "encargado del tratamiento de datos" que se usan en este Anexo tienen los mismos significados que se les atribuye en la Ley Israelí de Protección de la Privacidad.

3. Derechos de Auditoría del Socio. Google permitirá que el Socio o un auditor independiente que este designe realicen auditorías (incluidas inspecciones) según se describe en la Sección 7.5.2(a) (Auditoría del Socio).

Apéndice 4: Productos Específicos

Las condiciones de cada subsección de este Apéndice 4 se aplican únicamente con respecto al tratamiento de Datos del Socio por parte de los Servicios correspondientes.

Google Cloud Platform

1. Definiciones Adicionales

- "*Cuenta*", si no se define en el Acuerdo, significa la cuenta de Google Cloud Platform del Socio.
- "*Google Cloud Platform*" significa los servicios de Google Cloud Platform que se describen en https://cloud.google.com/terms/services, sin incluir ninguna de las Ofertas de Terceros.
- "*Ofertas de Terceros*", si no se define en el Acuerdo, significa (a) los servicios, el software, los productos y demás ofertas de terceros que no estén incorporados en Google Cloud Platform o el Software; (b) las ofertas identificadas en la Sección "Condiciones de Terceros" de las Condiciones Específicas del Servicio del Acuerdo, y (c) los sistemas operativos de terceros.

2. Certificaciones de Cumplimiento. Las Certificaciones de Cumplimiento de los Servicios Auditados de Google Cloud Platform también incluirán certificados de las normas ISO 27017 e ISO 27018, así como una Certificación de Cumplimiento de PCI DSS.

3. Ubicaciones de los Centros de Datos. Las ubicaciones de los centros de datos de Google Cloud Platform se describen en https://cloud.google.com/about/locations/.

4. Información sobre los Subencargados del Tratamiento de Datos. Los nombres, las ubicaciones y las actividades de los Subencargados del Tratamiento de Datos de Google Cloud Platform se describen en https://cloud.google.com/terms/subprocessors.

5. Equipo de Protección de Datos de Cloud. Puede comunicarse con el Equipo de Protección de Datos de Google Cloud Platform en https://support.google.com/cloud/contact/dpo.

6. Información sobre las Transferencias Restringidas. Encontrará más información pertinente sobre las Transferencias Restringidas, los Controles de Seguridad Adicionales y otras medidas de protección complementarias en https://cloud.google.com/privacy.

7. Condiciones Específicas del Servicio

Solución Bare Metal (Google Cloud Platform)

La Solución Bare Metal ofrece acceso no virtualizado a los recursos de infraestructura subyacentes y, por su diseño, cuenta con determinadas características distintivas.

1. Modificaciones. Este Anexo se modifica de la siguiente manera con respecto a la Solución Bare Metal:

- La definición de "Auditor Externo de Google" se reemplaza por lo siguiente:
    - "*Auditor Externo de Google*" significa un auditor externo independiente y calificado designado por Google o un Subencargado del Tratamiento de Datos de la Solución Bare Metal, cuya identidad actual Google divulgará al Socio a pedido.
- Se borran las siguientes condiciones:
    - De la Sección 7.1.1 (Medidas de Seguridad de Google), la frase "para encriptar los Datos del Socio"
    - Del Apéndice 2 (Medidas de Seguridad), las subsecciones de la Sección 1(a) titulados "Sistemas Operativos de Servidores" y "Continuidad Empresarial"
    - Del Apéndice 2, las subsecciones de la Sección 1(b) titulados "Superficie de Ataque Externa", "Detección de Intrusiones" y "Tecnologías de Encriptación"
    - Del Apéndice 2, las siguientes oraciones de la Sección 3(a):
        - Google almacena los datos en un entorno multiusuario en sus propios servidores. Sujeto a posibles instrucciones del Socio que requieran lo contrario (por ejemplo, en forma de una selección de la ubicación de los datos), Google replica los Datos del Socio entre múltiples centros de datos geográficamente dispersos.

2. Certificaciones de Cumplimiento e Informes SOC. Google o su Subencargado del Tratamiento de Datos mantendrán, como mínimo, lo siguiente (o una alternativa equivalente o mejor) en relación con la Solución Bare Metal para verificar la eficacia continua de las Medidas de Seguridad:

a. un certificado de la norma ISO 27001 y una Certificación de Cumplimiento de PCI DSS (las "*Certificaciones de Cumplimiento de BMS*")

b. informes SOC 1 y SOC 2 actualizados anualmente sobre la base de una auditoría realizada, al menos, una vez cada 12 meses (los "*Informes SOC de BMS*")

3. Revisiones de la Documentación de Seguridad. Para demostrar el cumplimiento de Google con respecto a sus obligaciones en virtud de este Anexo, Google pondrá a disposición las Certificaciones de Cumplimiento de BMS y los Informes SOC de BMS para que el Socio los revise y, si el Socio es un

encargado del tratamiento de datos, permitirá que el Socio solicite acceso a los Informes de SOC de BMS para el responsable del tratamiento de datos pertinente, de conformidad con la Sección 7.5.3 (Condiciones Empresariales Adicionales para Revisiones y Auditorías).

4. Obligaciones del Socio. Sin limitar las obligaciones expresas de Google en relación con la Solución Bare Metal, el Socio tomará las medidas razonables para proteger y mantener la seguridad de los Datos del Socio y de cualquier otro contenido que se almacene o trate en la Solución Bare Metal.

5. Exención de Responsabilidad. Sin perjuicio de ninguna disposición en contrario en el Acuerdo (incluido este Anexo), Google no es responsable de ninguno de los siguientes aspectos en relación con la Solución Bare Metal:

a. la seguridad no física, como los controles de acceso, la encriptación, los firewalls, la protección con antivirus, la detección de amenazas y los análisis de seguridad;

b. los registros y la supervisión;

c. el mantenimiento o la asistencia no relacionados con el hardware;

d. la creación de copias de seguridad de los datos, incluida cualquier configuración de redundancia o alta disponibilidad; y

e. las políticas o los procedimientos de continuidad empresarial y recuperación ante desastres;

El Socio es el único responsable de la protección (más allá de la seguridad física de los servidores de la Solución Bare Metal), los registros y la supervisión, el mantenimiento y la asistencia, y las copias de seguridad en relación con los Sistemas Operativos, los Datos del Socio, el software y las aplicaciones que el Socio use con la Solución Bare Metal, suba a esta o aloje en esta.

Cloud NGFW (Google Cloud Platform)

La edición de Cloud NGFW titulada "Cloud NGFW Enterprise" ("CNE") está diseñada para mitigar los riesgos de ciberseguridad y, por tanto, tiene determinadas características distintivas.

1. Modificaciones. El Anexo se modifica de la siguiente manera con respecto a CNE:

- Las Secciones 6.1 (Eliminación por Parte del Socio) y 6.2 (Devolución o Eliminación al Término de la Vigencia) no impedirán que Google ni los Subencargados del Tratamiento de Datos conserven archivos o capturas de paquetes del tráfico de red que se envíen para los TSS y que CNE designe como amenaza de seguridad, siempre que el archivo o la captura de paquetes del tráfico de red no incluya Datos Personales del Socio.

Google Distributed Cloud Edge (Google Cloud Platform)

Google Distributed Cloud Edge ("*GDCE*") no se implementa en un centro de datos de Google y, por su diseño, tiene determinadas características distintivas.

1. Modificaciones. Este Anexo se modifica de la siguiente manera con respecto a GDCE:

- Las referencias a “los sistemas de Google” se reemplazan por “los Equipos”.
- La Sección 6.2 (Devolución o Eliminación al Término de la Vigencia) se reemplaza por lo siguiente:
    - 6.2 *Devolución o Eliminación al Término de la Vigencia*. El Socio le indica a Google que borre todos los Datos del Socio restantes (incluidas las copias existentes) de los Equipos al finalizar la Vigencia, de conformidad con las leyes aplicables. Si el socio desea conservar Datos del Socio luego del término de la Vigencia, podrá exportar los datos o crear copias de estos antes de que termine la Vigencia. Google cumplirá con la Instrucción de esta Sección 6.2 en cuanto sea razonablemente factible y en un plazo máximo de 180 días, a menos que se exija el almacenamiento según la Ley Europea (en los casos en los que rija la Ley Europea de Protección de Datos) o la ley aplicable (en los casos en los que rija otra Ley de Privacidad Aplicable).
- Se agregan las siguientes palabras al final de la Sección 10.1 (Instalaciones de Almacenamiento y Tratamiento de Datos): “o donde sea que se encuentre la Ubicación del Cliente”.
- La Sección 1 (Seguridad de los Centros de Datos y las Redes) del Apéndice 2 (Medidas de Seguridad) se reemplaza por lo siguiente:
    - **1. Máquinas Locales y Seguridad de las Redes**

Máquinas Locales. Los Datos del Socio se almacenan únicamente en los Equipos para implementarse en una Ubicación del Cliente.

Sistemas Operativos de Servidores. Los servidores de Google usan una implementación basada en Linux y personalizada para el entorno de aplicaciones. Google emplea un proceso de revisión de código para aumentar la seguridad del código utilizado para ofrecer GDCE y mejorar los productos de seguridad en los entornos de producción de GDCE.

Tecnologías de Encriptación. Google ofrece encriptación HTTPS (también denominada conexión SSL o TLS) y permite la encriptación de los datos en tránsito. Los servidores de Google admiten el intercambio de claves criptográficas de la curva elíptica efímera Diffie-Hellman firmadas con RSA y ECDSA. Estos métodos de confidencialidad directa perfecta (PFS) ayudan a proteger el tráfico y minimizar las consecuencias de las vulneraciones de claves o las rupturas criptográficas. Google también ofrece encriptación de los datos en reposo con el estándar AES128 o uno similar. GDCE cuenta con integración de CMEK; para obtener más información, consulte https://cloud.google.com/kms/docs/cmek.

Conexión a Cloud VPN. Google permite que el Socio habilite y configure una interconexión sólida y encriptada entre los Equipos y la Nube Privada Virtual del Socio con Cloud VPN a través de una conexión de VPN IPsec.

Almacenamiento Delimitado. El almacenamiento de datos del Socio está delimitado dentro del servidor. Si se roba un disco o se copia en reposo, su contenido será irrecuperable fuera del servidor.

- Se borran las Secciones 2 (Controles de Sitios y Accesos) y 3 (Datos) del Apéndice 2 (Medidas de Seguridad).

2. Disposiciones Inaplicables. Cualquier obligación de Google mencionada en el Acuerdo (incluido este Anexo) o en afirmaciones dentro la documentación de seguridad asociada (incluidos los informes) que dependa de la operación por parte de Google de un centro de datos de Google no se aplica a GDCE.

Servicios de Múltiples Nubes Administrados por Google (Google Cloud Platform)

Los Servicios de Múltiples Nubes Administrados por Google involucran la infraestructura de terceros y, por su diseño, tienen determinadas características distintivas.

1. Definición Adicional

- "*Modificación de Tratamiento de Datos de MCS Administrados por Google*" significa las condiciones que se encuentran en https://cloud.google.com/terms/mcs-data-processing-terms.

2. Condiciones del Tratamiento de Datos en Múltiples Nubes. La Modificación de Tratamiento de Datos de MCS Administrados por Google complementa y modifica este Anexo con respecto a los Servicios de Múltiples Nubes Administrados por Google para Google Cloud Platform.

Google Cloud VMware Engine (Google Cloud Platform)

Google no podrá acceder al entorno de VMware del Socio ni encriptar los datos personales que se encuentren en él.

NetApp Volumes (Google Cloud Platform)

1. Modificaciones. Este Anexo se modifica de la siguiente manera con respecto a NetApp Volumes:

- La definición de "Auditor Externo de Google" se reemplaza por lo siguiente:
    - "*Auditor Externo de Google*" significa un auditor externo independiente y calificado designado por Google o un Subencargado del Tratamiento de Datos de NetApp Volumes, cuya identidad actual Google divulgará al Socio previa solicitud.
- La Sección 3(a) (Almacenamiento, Aislamiento y Registro de Datos) del Apéndice 2 (Medidas de Seguridad) se reemplaza por lo siguiente:
    - (a) *Almacenamiento, Aislamiento y Registro de Datos*. Google almacena los datos en un entorno multiusuario o servidores que son propiedad de NetApp, Inc. Sujeto a posibles Instrucciones que requieran lo contrario (p. ej., en forma de una selección de la ubicación de los datos), Google replica los Datos del Socio entre múltiples centros de datos geográficamente dispersos. Google también aísla lógicamente los Datos del Socio. El Socio tendrá control sobre las políticas específicas del uso compartido de datos. Dichas políticas, de conformidad con la funcionalidad de los Servicios,

permitirán que el Socio determine la configuración de uso compartido de los productos que resulte aplicable a los Usuarios Finales del Socio para fines específicos. El Socio puede optar por usar la función de registros que Google ofrece a través de los Servicios.

2. Certificaciones de Cumplimiento e Informes SOC. Google o su Subencargado del Tratamiento de Datos obtendrán, como mínimo, lo siguiente (o una alternativa equivalente o mejor) en relación con NetApp Volumes:

a. un certificado de la norma ISO 27001 y una Certificación de Cumplimiento de PCI DSS (las "*Certificaciones de Cumplimiento de NetApp*")

b. informes SOC 1 y SOC 2 actualizados anualmente sobre la base de una auditoría realizada, al menos, una vez cada 12 meses (los "*Informes SOC de NetApp*")

3. Revisiones de la Documentación de Seguridad. Para demostrar el cumplimiento de Google con respecto a sus obligaciones en virtud de este Anexo, Google pondrá a disposición las Certificaciones de Cumplimiento de NetApp y los Informes SOC de NetApp para que el Socio los revise y, si el Socio es encargado del tratamiento de datos, permitirá que el Socio solicite acceso a los Informes de SOC de NetApp para el responsable del tratamiento de datos pertinente, de conformidad con la Sección 7.5.3 (Condiciones Empresariales Adicionales para Revisiones y Auditorías).

Looker (original)

1. Definiciones Adicionales

- "*Consola del Administrador*" significa cualquier consola del administrador aplicable a cada Instancia.
- "*Modificación de Tratamiento de Datos de MCS Administrados por Google*" significa, si corresponde, a las condiciones que se encuentran en https://cloud.google.com/terms/mcs-data-processing-terms.
- "*Servicios de Múltiples Nubes Administrados por Google*" significa, si corresponde, a los servicios, los productos y las funciones de Google especificados que se alojan en la infraestructura de un proveedor de servicios en la nube externo.
- "*Looker (original)*" significa una plataforma integrada (que incluye la infraestructura basada en la nube, si corresponde, y los componentes de software, incluidas las APIs asociadas) que permite que las empresas analicen datos y definan métricas empresariales en varias fuentes de datos que Google pone a disposición del Socio en virtud del Acuerdo. Looker (original) excluye las Ofertas de Terceros.
- "*Proveedor Externo de Servicios de Múltiples Nubes*" tiene el significado que se le atribuye en la Modificación de Tratamiento de Datos de MCS Administrados por Google.
- "*Formulario de Pedido*" tiene el significado que se le atribuye en el Acuerdo, a menos que el Socio haya realizado la compra por medio de un revendedor o en un mercado en línea, o que

use Looker solo con fines de prueba y evaluación en virtud de un acuerdo de prueba o evaluación, en cuyo caso "Formulario de Pedido" podría hacer referencia a otro formulario escrito (se permiten los correos electrónicos y otros medios electrónicos), según lo autorice Google.

2. Modificación. Este Anexo se modifica de la siguiente manera con respecto a Looker (original):

- La definición de "Dirección de Correo Electrónico de Notificación" se reemplaza por lo siguiente:
    - "*Dirección de Correo Electrónico de Notificación*" significa las direcciones de correo electrónico designadas por el Socio en el Formulario de Pedido o por medio de Looker (según corresponda) para recibir determinadas notificaciones de Google.
- Las definiciones de "SCC (de Responsable a Encargado del Tratamiento de Datos)", "SCC (de Encargado a Responsable del Tratamiento de Datos)", "SCC (de un Encargado del Tratamiento de Datos a Otro)" y "SCC (de un Encargado del Tratamiento de Datos a Otro, Exportador de Google)" en el Apéndice 3 (Leyes de Privacidad Específicas) se reemplazan por lo siguiente:
    - "*SCC (de Responsable a Encargado del Tratamiento de Datos)*" significa las condiciones que se encuentran en https://cloud.google.com/terms/looker/legal/sccs/eu-c2p.
    - "*SCC (de Encargado a Responsable del Tratamiento de Datos)*" significa las condiciones que se encuentran en https://cloud.google.com/terms/looker/legal/sccs/eu-p2c.
    - "*SCC (de un Encargado del Tratamiento de Datos a Otro)*" significa las condiciones que se encuentran en https://cloud.google.com/terms/looker/legal/sccs/eu-p2p.
    - "*SCC (de un Encargado del Tratamiento de Datos a Otro, Exportador de Google)*" significa las condiciones que se encuentran en https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group.
- Se agregan las siguientes palabras al final de la Sección 10.1 (Instalaciones de Almacenamiento y Tratamiento de Datos): "o donde sea que tenga instalaciones cualquier Proveedor Externo de Servicios de Múltiples Nubes".

3. Responsabilidades Adicionales del Socio con Respecto a la Seguridad. El Socio es responsable de la seguridad del entorno del Socio, sus bases de datos y la configuración de Looker (original), excepto por los sistemas administrados y controlados por Google.

4. Certificaciones de Cumplimiento e Informes SOC. Las Certificaciones de Cumplimiento y los Informes SOC correspondientes a los Servicios Auditados de Looker (original) pueden variar según el entorno de alojamiento en el que se utilicen los Servicios pertinentes. Google proporcionará detalles de las Certificaciones de Cumplimiento y los Informes SOC disponibles en relación con distintos entornos de alojamiento previa solicitud.

5. Ubicaciones de los Centros de Datos. Las ubicaciones de los centros de datos de Looker (original) se describirán en el Formulario de Pedido aplicable, o bien Google las identificará de otra forma.

6. Inexistencia de Certificaciones por Parte de Socios no Pertenecientes a EMEA. El Socio no tiene la obligación de certificar ni identificar a su Autoridad Supervisora competente según lo descrito en la Sección 4.2 (Certificación por Parte de Socios no Pertenecientes a EMEA) de las condiciones de Protección de Datos para Europa en el Apéndice 3 (Leyes de Privacidad Específicas) en relación con Looker (original).

7. Información sobre las Transferencias Restringidas. Encontrará más información pertinente sobre las Transferencias Restringidas, los Controles de Seguridad Adicionales y otras medidas de protección complementarias relativas a Looker (original) en https://docs.looker.com.

8. Información sobre los Subencargados del Tratamiento de Datos. Los nombres, las ubicaciones y las actividades de los Subencargados del Tratamiento de Datos de Looker (original) se describen en:

a. https://cloud.google.com/terms/looker/privacy/lookeroriginal-subprocessors

b. https://cloud.google.com/terms/subprocessors

9. Servicios de Múltiples Nubes Administrados por Google (Looker (original))

Los Servicios de Múltiples Nubes Administrados por Google involucran la infraestructura de terceros y, por su diseño, tienen determinadas características distintivas.

9.1 *Condiciones del Tratamiento de Datos en Múltiples Nubes*. La Modificación de Tratamiento de Datos de MCS Administrados por Google complementa y modificación este Anexo con respecto a los Servicios de Múltiples Nubes Administrados por Google para Looker (original).

10. Equipo de Protección de Datos de Cloud. Puede comunicarse con el Equipo de Protección de Datos de Looker (original) en https://support.google.com/cloud/contact/dpo.

11. Registros de Tratamiento de Google. En la medida en que alguna Ley de Privacidad Aplicable exija que Google recopile y mantenga registros de determinada información en relación con el Socio o sus Clientes, el Socio suministrará dicha información a Google cuando este lo solicite y notificará a Google acerca de cualquier actualización necesaria para que la información se mantenga correcta y actualizada, a menos que Google solicite que el socio suministre la información por otros medios.

12. Medidas de Seguridad Adicionales para las Aplicaciones. Google implementará y mantendrá las Medidas de Seguridad adicionales que se describen a continuación para Looker (original):

a. Google sigue, como mínimo, las prácticas estándar de la industria con respecto a la arquitectura de seguridad. Los servidores proxy que se usan para las aplicaciones de Google ayudan a acceder de forma segura a Looker proporcionando un único punto para filtrar ataques por medio de listas de bloqueo de IP y límites de frecuencia de conexión.

b. Los administradores del Socio controlan el acceso a las aplicaciones por parte del personal de Google para brindar asistencia técnica a pedido del Socio o de los Usuarios Finales del Socio.

Servicios de SecOps

1. Definiciones Adicionales

- "*Cuenta*", si no se define en el Acuerdo, significa la cuenta de Servicios de SecOps del Socio o su cuenta de Google Cloud Platform, según corresponda.

- "*Servicios de SecOps*" significa Chronicle SIEM, Chronicle SOAR y Mandiant Solutions, cada uno según se describe en https://cloud.google.com/terms/secops/services, con la exclusión de cualquier Oferta de Terceros. En aras de evitar dudas, Servicios de SecOps excluye los Servicios Administrados de Mandiant y los Servicios de Asesoramiento de Mandiant.

- "*Ofertas de Terceros*", si no se define en el Acuerdo, significa (a) los servicios, el software, los productos y demás ofertas de terceros que no estén incorporados en los Servicios o el Software de SecOps, y (b) los sistemas operativos de terceros.

2. Modificaciones. Este Anexo se modifica de la siguiente manera con respecto a los Servicios de SecOps:

- La definición de "Controles de Seguridad Adicionales" se reemplaza por lo siguiente:

    - *"Controles de Seguridad Adicionales"* significa los recursos, las características, las funciones o los controles (si los hubiera) que el Socio podrá usar si lo desea o según su criterio, incluidos (si los hubiera) la encriptación, los registros, la supervisión, la administración de identidades y accesos, y los análisis de seguridad.

- La definición de "Servicios Auditados" se reemplaza por lo siguiente:

    - "*Servicios Auditados*" significa los Servicios de SecOps entonces vigentes que se indica que están dentro del alcance de la certificación o del informe pertinentes en https://cloud.google.com/security/compliance/secops/services-in-scope. Google no podrá quitar ningún Servicio de SecOps de esta URL, a menos que este se haya descontinuado de conformidad con este Acuerdo.

- Las definiciones de "SCC (de Responsable a Encargado del Tratamiento de Datos)", "SCC (de Encargado a Responsable del Tratamiento de Datos)", "SCC (de un Encargado del Tratamiento de Datos a Otro)" y "SCC (de un Encargado del Tratamiento de Datos a Otro, Exportador de Google)" en el Apéndice 3 (Leyes de Privacidad Específicas) se reemplazan por lo siguiente:

    - "*SCC (de Responsable a Encargado del Tratamiento de Datos)*" significa las condiciones que se encuentran en https://cloud.google.com/terms/secops/sccs/eu-c2p.

    - "*SCC (de Encargado a Responsable del Tratamiento de Datos)*" significa las condiciones que se encuentran en https://cloud.google.com/terms/secops/sccs/eu-p2c.

    - "*SCC (de un Encargado del Tratamiento de Datos a Otro)*" significa las condiciones que se encuentran en https://cloud.google.com/terms/secops/sccs/eu-p2p.

- *"SCC (de un Encargado del Tratamiento de Datos a Otro, Exportador de Google)"* significa las condiciones que se encuentran en https://cloud.google.com/terms/secops/sccs/eu-p2p-google-exporter.

- La Sección 7.4 (Certificaciones de Cumplimiento e Informes SOC) del Anexo se modifica para que diga lo siguiente:

  - 7.4 *Certificaciones de Cumplimiento e Informes SOC*. Google mantendrá, como mínimo, las certificaciones y los informes que se identifican en https://cloud.google.com/security/compliance/secops/services-in-scope en relación con los Servicios Auditados para verificar la eficacia continua de las Medidas de Seguridad (las "Certificaciones de Cumplimiento" y los "Informes SOC").

En cualquier momento, Google puede agregar estándares o reemplazar una Certificación de Cumplimiento o un Informe SOC por una alternativa equivalente o mejorada.

3. Ubicaciones de los Centros de Datos. Las ubicaciones de los centros de datos de Servicios de SecOps se describen en https://cloud.google.com/terms/secops/data-residency.

4. Inexistencia de Certificaciones por Parte de Socios no Pertenecientes a EMEA. El Socio no tiene la obligación de certificar ni identificar a su Autoridad Supervisora competente según lo descrito en la Sección 4.2 (Certificación por Parte de Socios no Pertenecientes a EMEA) de las condiciones de Protección de Datos para Europa en el Apéndice 3 (Leyes de Privacidad Específicas) en relación con los Servicios de SecOps.

5. Información sobre los Subencargados del Tratamiento de Datos. Los nombres, las ubicaciones y las actividades de todos los Subencargados del Tratamiento de Datos para los Servicios de SecOps se describen en https://cloud.google.com/terms/secops/subprocessors.

6. Equipo de Protección de Datos de Cloud. Puede comunicarse con el Equipo de Protección de Datos de Servicios de SecOps en https://support.google.com/cloud/contact/dpo (o utilizando los medios alternativos que Google pueda ofrecer ocasionalmente).

7. Registros de Tratamiento de Google. En la medida en que alguna Ley de Privacidad Aplicable exija que Google recopile y mantenga registros de determinada información en relación con el Socio, el Socio suministrará dicha información a Google cuando este lo solicite y notificará a Google acerca de cualquier actualización necesaria para que la información se mantenga correcta y actualizada, a menos que Google solicite que el socio suministre la información por otros medios.

Versiones Anteriores de las Condiciones de Seguridad y Tratamiento de Datos (Socios):

30 de junio de 2022 24 de septiembre de 2021 20 de agosto de 2020 10 de agosto de 2020 17 de julio de 2020 1 de octubre de 2019 28 de febrero de 2019 25 de mayo de 2018 13 de marzo de 2018

Versiones Anteriores de las DPST de Servicios de SecOps (Socios):

6 de febrero de 2023 31 de octubre de 2022 27 de septiembre de 2021

Versiones anteriores *(última modificación: 30 de octubre de 2024)*

15 de octubre de 2024 26 de septiembre de 2024 9 de septiembre de 2024 9 de abril de 2024 8 de noviembre de 2023 15 de agosto de 2023 20 de septiembre de 2022