Anexo de Tratamiento de Datos de Cloud (clientes)

Este Anexo de Tratamiento de Datos de Cloud (incluidos sus apéndices, el "*Anexo*") se incorpora al Acuerdo (según se define a continuación) entre Google y el Cliente. Este Anexo se conocía anteriormente como las "Condiciones de Seguridad y Tratamiento de Datos" en virtud de un Acuerdo para Google Cloud Platform, Looker (original), Servicios de Google SecOps o Google Cloud Skills Boost para Organizaciones; la "Modificación de Tratamiento de Datos" en virtud de un Acuerdo para Google Workspace o Cloud Identity; y el "Anexo de Tratamiento de Datos" en virtud de un Acuerdo para Servicios de Mandiant Consulting y Servicios Administrados.

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 tratamiento y la seguridad de los Datos del Cliente (según se define a continuación). Este Anexo entrará en vigor en la Fecha de Entrada en Vigor del Anexo (según se define a continuación) y reemplazará las condiciones previamente aplicables al tratamiento y la seguridad de los Datos del Cliente. Los términos con mayúscula inicial que se usan en este Anexo, pero que no se definen en el presente documento, tienen el significado establecido en el Acuerdo.

2. Definiciones

2.1 En este Anexo:

- "*Fecha de Entrada en Vigor del Anexo*" significa la fecha en la que el Cliente aceptó este Anexo o en la que las partes lo acordaron de otra forma.
- "*Controles de Seguridad Adicionales*" significa los recursos, las características, las funciones y los controles de seguridad que el Cliente puede usar si lo desea o según su criterio, incluidos la Consola del Administrador, la encriptación, los registros y 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 prestar los Servicios aplicables al Cliente.
- "*Ley de Privacidad Aplicable*" significa, en relación con el tratamiento de los Datos Personales del Cliente, a cualquier ley o reglamentación de privacidad, seguridad o protección de datos, ya 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 correspondiente.

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

- "*Datos del Cliente*", si no se define en el Acuerdo, tiene el significado que se le da en el Apéndice 4 (Productos Específicos).

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

- "*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 Cliente, 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 Cliente); (b) a la ley del Reino Unido o de una parte del Reino Unido (si se aplica el RGPD del Reino Unido al tratamiento de los Datos Personales del Cliente); o (c) a la ley de Suiza (si se aplica la FADP de Suiza al tratamiento de los Datos Personales del Cliente).

- "*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 Cliente en su momento.

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

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

- "*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 correspondientes 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 Cliente y brindar partes de los Servicios y los TSS (si corresponde).

- "*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 y 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 modificó 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 exista 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 aplicable haya terminado o vencido, este Anexo permanecerá vigente hasta que Google borre todos los Datos del Cliente según se describe en el presente documento y vencerá de manera automática en ese momento.

4. Funciones y Cumplimiento Legal

4.1 *Funciones de las Partes.* Google es un encargado del tratamiento de datos y el Cliente es un responsable o encargado, según corresponda, del tratamiento de los Datos Personales del Cliente.

4.2 *Resumen del Tratamiento de Datos.* El objeto y los detalles del tratamiento de los Datos Personales del Cliente se describen en el Apéndice 1 (Objeto 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 Cliente conforme a la Ley de Privacidad Aplicable.

4.4 *Condiciones Legales Adicionales*. En la medida en que el tratamiento de los Datos Personales del Cliente esté sujeto a la Ley de Privacidad Aplicable descrita en el Apéndice 3 (Leyes de Privacidad Específicas), se aplicarán las condiciones correspondientes 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 *Clientes Encargados del Tratamiento de Datos*. Si el Cliente es un encargado del tratamiento de datos:

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

i. las Instrucciones

ii. la contratación de Google por parte del Cliente como otro encargado 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 Cliente enviará al responsable del tratamiento de datos pertinente, de forma inmediata y sin demoras indebidas, cualquier aviso proporcionado por Google en virtud de las Secciones 7.2.1 (Notificación de Incidentes), 9.2.1 (Responsabilidad por las Solicitudes) u 11.4 (Oportunidad de Oponerse a los Subencargados del Tratamiento de Datos).

c. El Cliente puede poner a disposición del responsable del tratamiento de datos pertinente cualquier otra información que Google ponga a su disposición en virtud de este Anexo relacionada con 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 Cliente*. El Cliente le indica a Google que trate los Datos del Cliente de conformidad con el Acuerdo aplicable (incluido este Anexo) solo como se estipula a continuación:

a. para prestar, proteger y supervisar los Servicios y los TSS (si corresponde)

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

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

ii. cualquier otra instrucción que el Cliente 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 Cliente*. Google permitirá que el Cliente borre los Datos del Cliente durante la Vigencia en concordancia con la funcionalidad de los Servicios. Si el Cliente utiliza los Servicios para borrar Datos del Cliente durante la Vigencia y no es posible recuperar esos Datos del Cliente, este uso constituirá una Instrucción para que Google borre los Datos del Cliente 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 Cliente quiere retener Datos del Cliente después del término de la Vigencia, puede indicar a Google, de acuerdo con la Sección 9.1 (Acceso, Rectificaciones, Procesamiento Restringido y Portabilidad) que devuelva esos datos durante la Vigencia. Sujeto a la Sección 6.3 (Instrucción de Eliminación Aplazada), el Cliente indica a Google borrar todos los Datos del Cliente restantes (incluidas las copias existentes) de los sistemas de Google cuando finalice la Vigencia. Después 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).

6.3. *Instrucción de Eliminación Aplazada*. En la medida en que Datos del Cliente que estén cubiertos por la instrucción de eliminación descrita en la Sección 6.2 (Devolución o Eliminación al Término de la Vigencia) también sean objeto de tratamiento, cuando venza la Vigencia aplicable en virtud de la Sección 6.2, en relación con un Acuerdo con un Período que siga vigente, esa instrucción de eliminación se aplicará con respecto a dichos Datos del Cliente solo cuando venza dicho Período. Para mayor claridad, este Anexo seguirá aplicándose a dichos Datos del Cliente hasta que Google los borre.

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 Cliente contra la destrucción, pérdida, alteración, divulgación o acceso no autorizados accidentales o ilícitos, según se describe en el Apéndice 2 (Medidas de Seguridad) **(**las **"*Medidas de Seguridad*")**. Las Medidas de Seguridad incluyen medidas para encriptar los Datos del Cliente; para ayudar a garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de Google de forma continua; para ayudar a restablecer el acceso oportuno a los Datos del Cliente 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 provoquen una reducción significativa en la seguridad de los Servicios.

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

a. Autorizará a sus empleados, contratistas y Subencargados del Tratamiento de Datos a acceder a los Datos del Cliente solo en la medida que sea estrictamente necesario 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 Cliente 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 al Cliente tomar medidas para proteger los Datos del Cliente

b. proporcionarle al Cliente información para proteger los Datos del Cliente, 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 Cliente y la información disponible para Google) asistirá al Cliente para garantizar el cumplimiento de sus obligaciones (o, en los casos en los que el Cliente sea el 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 correspondiente (incluido este Anexo)

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

7.2 *Incidentes de Datos*.

7.2.1 *Notificación de Incidentes*. Google notificará al Cliente, 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 Cliente.

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 Cliente 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 Cliente 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 Cliente por parte de Google*. Google no tiene la obligación de evaluar los Datos del Cliente para identificar información que esté sujeta a requisitos legales específicos.

7.2.4 *Inexistencia de Reconocimiento de Culpa 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 ningún error o ninguna responsabilidad con respecto al Incidente de Datos.

7.3 *Responsabilidades y Evaluación de la 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 de lo dispuesto en el Acuerdo correspondiente, el Cliente es responsable del uso de los Servicios y su almacenamiento, así como del almacenamiento de cualquier copia de los Datos del Cliente 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 Cliente

b. proteger las credenciales, los sistemas y los dispositivos de autenticación de cuentas que usa el Cliente para acceder a los Servicios

c. crear copias de seguridad o retener copias de sus Datos del Cliente según sea adecuado

7.3.2 *Evaluación de Seguridad por parte del Cliente*. El Cliente 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 Cliente (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 Cliente, así como los riesgos para las 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*")

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, una vez cada 12 meses (los "*Informes SOC*")

Google puede agregar estándares en cualquier momento. Además, Google puede 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 Cliente la revise y, si el Cliente es encargado del tratamiento de datos, permitirá que el Cliente solicite acceso a los Informes SOC para el 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 Cliente*.

a. *Auditoría del Cliente*. Si lo exige la Ley de Privacidad Aplicable, Google permitirá que el Cliente 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 Cliente o su auditor según se describe en esta Sección 7.5 (Revisiones y Auditorías de Cumplimiento).

b. *Revisión Independiente del Cliente*. El Cliente podrá realizar una auditoría para verificar que Google cumpla con 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 Cliente debe comunicarse con el Equipo de Protección de Datos de Cloud de Google 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)

ii. o bien, una auditoría en virtud de la Sección 7.5.2(a) (Auditoría del Cliente)

b. Luego de una solicitud del Cliente en virtud de la Sección 7.5.3(a), Google y el Cliente 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)

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 Cliente)

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 Cliente). Google le brindará al Cliente más detalles sobre cualquier tarifa correspondiente, además del criterio del cálculo, antes de cualquier auditoría. El Cliente será responsable de las tarifas que cobre cualquier auditor que haya designado para ejecutar esa auditoría.

d. Google podrá objetar por escrito a cualquier auditor designado por el Cliente para que realice una auditoría en virtud de la Sección 7.5.2(a) (Auditoría del Cliente) 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 Cliente designe a otro auditor o realice la auditoría por sí mismo.

e. Cualquier solicitud por parte del Cliente 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 Cliente para garantizar el cumplimiento de sus obligaciones (o, en los casos en los que el Cliente 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 correspondiente (incluido este Anexo)

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

9. Acceso, Derechos de los Titulares y Exportación de Datos

9.1 *Acceso, Rectificaciones, Tratamiento Restringido y Portabilidad*. Durante la Vigencia, Google permitirá que el Cliente, de forma coherente con la funcionalidad de los Servicios, acceda a los Datos del Cliente, los rectifique y restrinja su tratamiento, incluso a través de la función de eliminación que ofrece Google según lo descrito en la Sección 6.1 (Eliminación por Parte del Cliente), y también permitirá que exporte los Datos del Cliente. Si el Cliente se da cuenta de que hay Datos Personales del Cliente que son inexactos o están obsoletos, el Cliente será responsable de usar dicha funcionalidad para rectificar o borrar esos datos si así lo requiere 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 Cloud de Google recibe una solicitud de parte de un sujeto en relación con Datos Personales del Cliente en la que se identifique al Cliente, Google hará lo siguiente:

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

b. Notificará de inmediato al Cliente.

c. No responderá de otra forma a esa solicitud del sujeto sin la autorización del Cliente.

El Cliente 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 para las Solicitudes de los Titulares*. Google (tomando en cuenta la naturaleza del tratamiento de los Datos Personales del Cliente) asistirá al Cliente para permitir que cumpla sus obligaciones (o, en los casos en los que el Cliente 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 titulares 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, Tratamiento 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 Cliente (o el responsable del tratamiento de datos pertinente) con la finalidad de cumplir las obligaciones mencionadas, si el Cliente lo solicita, brindándole al Cliente la cooperación y asistencia adicionales que resulten razonables

10. Ubicaciones del Tratamiento de Datos

10.1 *Instalaciones para el Almacenamiento y el 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 Cliente podrán tratarse 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 Cliente 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 Oponerse a Subencargados del Tratamiento de Datos), el Cliente 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 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 Cliente 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 aplicable (incluido este Anexo)

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 Oponerse a Subencargados del Tratamiento de Datos*.

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

b. El Cliente podrá, en un plazo de 90 días después de recibir la notificación de la contratación de un Nuevo Subencargado del Tratamiento de Datos, objetar poniendo fin inmediatamente por conveniencia al Acuerdo aplicable de una de las siguientes formas:

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

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 Cliente relacionada con el tratamiento de los Datos del Cliente en virtud del Acuerdo aplicable. Se podrá establecer contacto con él según se describe en la Sección Avisos del Acuerdo aplicable 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 relacionada con el Cliente, el Cliente usará la Consola del Administrador, o bien otros medios identificados en el Apéndice 4 (Productos Específicos) para suministrar dicha información y mantener su exactitud y vigencia. 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 Cliente, Google le indicará a dicho tercero que se comunique con el Cliente.

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 Cliente 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.

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

Para mayor claridad, si el Cliente tiene más de un Acuerdo, este Anexo modificará cada uno de los Acuerdos por separado.

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

Apéndice 1: Objeto y Detalles del Tratamiento de Datos

Objeto

La prestación de los Servicios y los TSS (si corresponde) por parte de Google al Cliente.

Duración del Tratamiento de Datos

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

Naturaleza y Propósito del Tratamiento de Datos

Google tratará los Datos Personales del Cliente con el fin de proporcionar al Cliente los Servicios y los TSS (si corresponde) de acuerdo con este Anexo.

Categorías de Datos

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

Titulares

Los Sujetos incluyen a las personas físicas cuyos datos el Cliente o sus Usuarios Finales (o alguna otra parte en representación de estas) suministren 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 son físicamente seguros.

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 han documentado procedimientos de

mantenimiento preventivo en los que se detallan el proceso y la frecuencia de rendimiento según las especificaciones internas o del fabricante. El mantenimiento preventivo y correctivo del equipo del centro de datos se programa a través de un proceso de cambio estándar de acuerdo con los procedimientos documentados.

Alimentación. Los sistemas de alimentación eléctrica de los centros de datos se diseñaron para ser redundantes y poder mantenerse sin afectar la continuidad de las operaciones las 24 horas, todos los días. En la mayoría de los casos, se proporcionan una fuente de alimentación principal y una alternativa, cada una con la misma capacidad, para los componentes de la infraestructura crítica del centro de datos. La alimentación de respaldo se proporciona a través de diversos mecanismos, como baterías de sistemas de alimentación ininterrumpida (UPS), 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 la energía eléctrica, 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 utiliza un proceso de revisión de código para aumentar la seguridad del código utilizado para proporcionar los Servicios y potenciar los productos de seguridad en los entornos de producción.

Continuidad Empresarial. Además de haber diseñado sus programas de continuidad empresarial y de recuperación ante desastres, Google los planifica y prueba de forma periódica.

(*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 firmemente el tamaño y la composición de la superficie de ataque de Google a través de la aplicación de 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 el impacto de una clave comprometida o de una ruptura criptográfica.

2. Controles de Sitios y Accesos

(a) Controles de sitios.

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 las funciones de seguridad física de los centros de datos las 24 horas, todos los días. El personal de operaciones de seguridad en las instalaciones supervisa las cámaras de TV de circuito cerrado (CCTV) y todos los sistemas de alarma. El personal de operaciones de seguridad en las instalaciones 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 encuentran 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 en un 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 solicitando la aprobación del supervisor del solicitante y del director del centro de datos. Toda otra persona que vaya a ingresar al centro de datos y requiera acceso temporal debe: (i) obtener aprobación previa de los administradores de centros de datos para las áreas internas y los centros de datos específicos que deseen visitar; (ii) registrarse en las operaciones de seguridad en las instalaciones; y (iii) referirse a un registro de acceso al centro de datos aprobado que identifique a la persona física como 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, así como cuándo accede a puertas perimetrales, a las zonas de envíos y recibos, y 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 que funcionan tanto dentro como fuera de los centros de datos. El posicionamiento de las cámaras se diseñó para cubrir áreas estratégicas, incluidas, entre otras, el perímetro, las puertas 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 realizan grabaciones del sitio con grabadoras de video digitales 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 exige una capacitación en materia de seguridad como parte del paquete de formación de su personal. 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 Cliente 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 impedir que personas o sistemas no autorizados accedan a los sistemas que se usan en el tratamiento de los Datos del Cliente. Google diseña sus sistemas de manera que (i) permitan que solo las personas autorizadas para acceder a determinados datos puedan hacerlo; y (ii) garanticen que los Datos del Cliente no se puedan leer, copiar, modificar ni quitar sin autorización durante el tratamiento y el uso, y después del registro. Los sistemas están diseñados 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 del personal autorizados. 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 requiere 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., el acceso a estaciones de trabajo), se implementan políticas de contraseña que siguen las prácticas estándar de la industria, como mínimo. Estos estándares incluyen restricciones relativas a la reutilización de

contraseñas y a la elección de contraseñas lo suficientemente seguras. 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 Cliente entre múltiples centros de datos geográficamente dispersos. Google también aísla lógicamente los Datos del Cliente. El Cliente tendrá control sobre las políticas específicas del uso compartido de datos. Esas políticas, de conformidad con la funcionalidad de los Servicios, permitirán que el Cliente determine la configuración de uso compartido de los productos que resulte aplicable a sus Usuarios Finales para fines específicos. El Cliente 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*. Es posible que los discos que puedan presentar problemas de rendimiento, errores o fallas de hardware se retiren ("Disco Retirado"). Todos los Discos Retirados atraviesan una serie de procesos de destrucción de datos (la "Política de Borrado de Datos en Discos") antes de salir de las instalaciones de Google para su reutilización o destrucción. Los Discos Retirados se borran en un proceso de varios pasos que al menos dos validadores independientes verifican que se hayan completado. El número de serie del Disco Retirado registra los resultados del borrado para realizar un 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 Datos en 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 Cliente debe cumplir requisitos adicionales adecuados a su función (p. ej., certificaciones). El personal de Google no tratará los Datos del Cliente 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 suscriba las condiciones contractuales adecuadas en materia de seguridad, confidencialidad y privacidad.

Anexo 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 Cliente.

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

(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 permite la transferencia legal 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 proporcionan una protección adecuada.

- "*SCC del Cliente*" 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 Cliente 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 Cliente) ni de ningún otro derecho ni otra obligación de cualquiera de las partes en virtud del Acuerdo aplicable, Google notificará de inmediato al Cliente 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. O bien, 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 Cliente es un 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 Cliente. Google permitirá que el Cliente o un auditor independiente que este designe realicen auditorías (incluidas inspecciones) tal como se describe en la Sección 7.5.2(a) (Auditoría del Cliente). Durante dicha auditoría, Google pondrá a disposición toda la información necesaria para demostrar el cumplimiento de sus obligaciones en virtud de este Anexo y colaborará con 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 Cliente se traten en un País con Nivel Adecuado de Protección o sean transferidos a este. Si los Datos Personales del Cliente se transfieren a algún otro país y la Ley Europea de Protección de Datos se aplica a las transferencias (según lo certifique el Cliente en virtud de la Sección 4.2 [Certificación por Parte de Clientes 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 Cliente 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 Cliente 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.

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

ii. O bien, 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 Cliente es un responsable o encargado del tratamiento de datos, con respecto a las Transferencias Restringidas entre Google y el Cliente.

4.2 *Certificación por parte de Clientes no Pertenecientes a EMEA*. En caso de que la dirección de facturación del Cliente se encuentre fuera de EMEA, y el tratamiento de los Datos Personales del Cliente 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 Cliente 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 Cliente 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 SCC del Cliente 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 Cliente (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 Cliente le reenviará al responsable del tratamiento de datos pertinente, de forma inmediata y sin demoras indebidas, cualquier aviso que se refiera a alguna SCC.

4.6 *Terminación Debido al Riesgo de las Transferencias de Datos*. Si el Cliente concluye, sobre la base de su uso actual o previsto de los Servicios, que no se brindan las medidas de protección adecuadas para los Datos Personales del Cliente 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.

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 Cliente (incorporadas por referencia a este Anexo) y el resto del Acuerdo (incluido este Anexo), prevalecerán las SCC del Cliente.

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 Cliente*" 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 Cliente), con respecto al tratamiento de los Datos Personales del Cliente 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 Cliente

b. retener, usar o divulgar los Datos Personales del Cliente:

i. excepto para propósitos comerciales en virtud de la CCPA en nombre del Cliente y con el objetivo específico de ejecutar los Servicios y los TSS (si corresponde)

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

c. combinar o actualizar los Datos Personales del Cliente 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 Cliente) ni de ningún otro derecho ni otra obligación de cualquiera de las partes en virtud del Acuerdo aplicable, Google notificará al Cliente 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 del Cliente. Si Google notifica al Cliente de cualquier uso no autorizado de los Datos Personales del Cliente, incluido en virtud de la Sección 3 (Cumplimiento) de este subsección o la Sección 7.2.1 (Notificación de Incidentes), el Cliente podrá tomar las medidas razonables y apropiadas para detener o corregir dicho uso no autorizado de la siguiente manera:

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 Cliente) o 9.1 (Acceso, Rectificaciones, Tratamiento 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*. Si la dirección de facturación del Cliente se encuentra en Turquía y Google ofrece condiciones adicionales opcionales (incluidas SCC de Turquía) para que el Cliente las acepte en relación con las transferencias de los Datos Personales del Cliente 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 Personales de Turquía de conformidad con la siguiente Sección 2.2 (Notificación a la Autoridad Competente), según las pruebas que presente el Cliente a Google.

2.2 *Notificación a la Autoridad Competente*. Si el Cliente acepta las SCC de Turquía en virtud de esta Sección 2 (Transferencias de Datos), el Cliente 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 Cliente acepta las SCC de Turquía en virtud de esta Sección 2 (Transferencias de Datos), Google permitirá que el Cliente (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 Cliente concluye, sobre la base de su uso actual o previsto de los Servicios, que no se brindan las medidas de protección adecuadas para los Datos Personales del Cliente 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 Cliente 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 Cliente. Google permitirá que el Cliente o un auditor independiente que este designe realicen auditorías (incluidas inspecciones) tal como se describe en la Sección 7.5.2(a) (Auditoría del Cliente).

Anexo 4: Productos Específicos

Las condiciones de cada subsección de este Apéndice 4 se aplican únicamente con respecto al tratamiento de Datos del Cliente 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 Cliente.

- "*Datos del Cliente*", si no se define en el Acuerdo, significa los datos proporcionados a Google por el Cliente o los Usuarios Finales a través de Google Cloud Platform con la Cuenta, y los datos que el Cliente o los Usuarios Finales obtengan a partir de esos datos con el uso de Google Cloud Platform.

- "*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 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 Cliente previa solicitud.

- Se borran las siguientes condiciones:

    - De la Sección 7.1.1 (Medidas de Seguridad de Google), la frase "para encriptar los Datos del Cliente"

    - 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 Cliente que requieran lo contrario (por ejemplo, en forma de una selección de la ubicación de los datos), Google replica los Datos del Cliente 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 Cliente los revise y, si el Cliente es un encargado del tratamiento de datos, permitirá que el Cliente 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 Cliente. Sin limitar las obligaciones expresas de Google en relación con la Solución Bare Metal, el Cliente tomará las medidas razonables para proteger y mantener la seguridad de los Datos del Cliente 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

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

El Cliente 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 Cliente, el software y las aplicaciones que el Cliente use con la Solución Bare Metal, suba a esta o aloje en ella.

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 Cliente) y 6.2 (Devolución o Eliminación al Término de la Vigencia) no impedirán que Google ni los Subencargados del Tratamiento de Datos retengan 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 Cliente.

Google Distributed Cloud conectado (Google Cloud Platform)

Google Distributed Cloud conectado 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 Google Distributed Cloud conectado:

- 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 cuando Finaliza la Vigencia*. El Cliente le indica a Google que borre todos los Datos del Cliente restantes (incluidas las copias existentes) del

Equipo cuando finalice la Vigencia de conformidad con la legislación aplicable. Si el Cliente quiere retener Datos del Cliente después del término de la Vigencia, puede exportar esos datos o hacer copias de ellos antes de la finalización de 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 Cliente 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 Google Distributed Cloud conectado y mejorar los productos de seguridad en entornos de producción de Google Distributed Cloud conectado.

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 el impacto de una clave comprometida o de una ruptura criptográfica. Google también ofrece encriptación de los datos en reposo con el estándar AES128 o uno similar. Google Distributed Cloud conectado cuenta con integración de CMEK. Si desea obtener más información, consulte https://cloud.google.com/kms/docs/cmek.

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

Almacenamiento Vinculado. El almacenamiento de datos del Cliente está vinculado al 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 declaraciones 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 Google Distributed Cloud conectado.

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 Cliente 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 Cliente 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 cualquier Instrucción contraria (p. ej., en forma de una selección de la ubicación de los datos), Google replica los Datos del Cliente entre varios centros de datos geográficamente dispersos. Google también aísla lógicamente los Datos del Cliente. El Cliente tendrá control sobre las políticas específicas del uso compartido de datos. Esas políticas, de conformidad con la funcionalidad de los Servicios, permitirán que el Cliente determine la configuración de uso compartido de los productos que resulte aplicable a sus Usuarios Finales para fines específicos. El Cliente 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 Cliente los revise y, si el Cliente es encargado del tratamiento de datos, permitirá que el Cliente 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).

Google Workspace y Cloud Identity

1. Definiciones Adicionales.

- "*Cuenta*", si no se define en el Acuerdo, significa la cuenta de Google Workspace o Cloud Identity del Cliente.
- "*Cloud Identity*" cuando se adquiere en virtud de un Acuerdo independiente y no como parte de Google Cloud Platform o Google Workspace, significa los Servicios de Cloud Identity que se describen en https://cloud.google.com/terms/identity/user-features.
- "*Datos del Cliente*", si no se define en el Acuerdo, significa los datos presentados, almacenados, enviados o recibidos por el Cliente o en su nombre o el de sus Usuarios Finales a través de Google Workspace o Cloud Identity con la Cuenta.
- "*Google Workspace*" significa los servicios de Google Workspace o Google Workspace for Education que se describen en https://workspace.google.com/terms/user_features.html, según corresponda.

2. Productos Adicionales. Si Google, a su discreción, pone a disposición del Cliente Productos Adicionales para su uso con Google Workspace o Cloud Identity de conformidad con las Condiciones de los Productos Adicionales aplicables:

a. El Cliente puede habilitar o inhabilitar Productos Adicionales a través de la Consola del Administrador y no necesitará usarlos para utilizar Google Workspace o Cloud Identity.

b. Si el Cliente opta por instalar cualquier Producto Adicional o usarlo con Google Workspace o Cloud Identity, los Productos Adicionales podrán acceder a los Datos del Cliente según sea necesario para interoperar con Google Workspace o Cloud Identity, según corresponda.

Para mayor claridad, este Anexo no es aplicable al tratamiento de los datos personales en relación con el suministro de cualquier Producto Adicional instalado o utilizado por el Cliente, incluidos los datos personales transmitidos a esos Productos Adicionales o desde ellos.

3. Certificaciones de Cumplimiento. Las Certificaciones de Cumplimiento de los Servicios Auditados de Google Workspace y Cloud Identity también incluirán certificados de las normas ISO 27017 e ISO 27018.

4. Ubicaciones de los Centros de Datos. Las ubicaciones de los centros de datos de Google Workspace y Cloud Identity se describen en https://www.google.com/about/datacenters/locations/.

5. Información sobre los Subencargados del Tratamiento de Datos. Los nombres, las ubicaciones y las actividades de los Subencargados del Tratamiento de Datos para Google Workspace y Cloud Identity se describen en https://workspace.google.com/intl/en/terms/subprocessors.html.

6. Equipo de Protección de Datos de Cloud. Puede comunicarse con el Equipo de Protección de Datos para Google Workspace y Cloud Identity (si los Administradores acceden con su Cuenta de Administrador) en https://support.google.com/a/contact/googlecloud_dpr.

7. Medidas de Seguridad Adicionales. Para Google Workspace y Cloud Identity:

a. Google separa de forma lógica los datos de cada Usuario Final de los datos de los demás Usuarios Finales.

b. Los datos de un Usuario Final autenticado no se mostrarán a otro Usuario Final (a menos que el primero o un Administrador permitan que los datos se compartan).

8. 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 cloud.google.com/privacy/.

9. Anexo de Datos del Servicio. Si Google pone a disposición del Cliente un Anexo de Datos del Servicio opcional para su aceptación en relación con este Anexo, la disponibilidad de ese anexo opcional constituirá una "Actualización de la DPA" si esa condición se define en un Anexo de Datos del Servicio aceptado previamente por el Cliente.

10. Condiciones Específicas del Servicio.

AppSheet (Google Workspace)

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

- El párrafo titulado "Sistemas Operativos de Servidores" de la Sección 1(a) en el Apéndice 2 (Medidas de Seguridad) se reemplaza por lo siguiente:

    - *Sistemas Operativos de Servidores*. Los servidores de Google usan una implementación basada en Linux y personalizada para el entorno de aplicaciones.

2. Ubicaciones Adicionales de Centros de Datos. Las ubicaciones adicionales de centros de datos para AppSheet se describen en https://cloud.google.com/about/locations/.

Looker (original)

1. Definiciones Adicionales.

- "*Consola del Administrador*" significa cualquier consola del administrador aplicable a cada Instancia.

- "*Modificaciones 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 Cliente 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 Cliente 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 significar otro formulario escrito (se permiten los correos electrónicos y otros medios electrónicos), según lo autorice Google.

2. Modificaciones. 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 Cliente en el Formulario de Pedido o a través 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 de Seguridad Adicionales del Cliente. El Cliente es responsable de la seguridad de su entorno, sus bases de datos y la configuración de Looker (original), lo que excluye 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 hosting 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 hosting 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 los Clientes no Pertenecientes a EMEA. El Cliente 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 Clientes 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 modifica 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 Datos de Google. En la medida en que alguna Ley de Privacidad Aplicable exija que Google recopile y mantenga registros de determinada información relacionada con el Cliente, el Cliente suministrará dicha información a Google previa solicitud y le notificará cualquier actualización que se requiera para mantener la exactitud y vigencia de esa información, a menos que Google solicite al Cliente suministrar y actualizar esa 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 Cliente controlan el acceso a las aplicaciones por parte del personal de Google para brindar asistencia técnica a pedido del Cliente o de los Usuarios Finales del Cliente.

Servicios de SecOps

1. Definiciones Adicionales.

- "*Cuenta*", si no se define en el Acuerdo, significa la cuenta de Servicios de SecOps o de Google Cloud Platform del Cliente, según corresponda.
- "*Datos del Cliente*", si no se define en el Acuerdo, significa los datos proporcionados a Google por el Cliente o los Usuarios Finales a través de los Servicios de SecOps con la Cuenta o para los Servicios de Mandiant Consulting y los Servicios Administrados en relación con la recepción de los Servicios de SecOps.
- "*Proveedor Contratado por el Cliente*" significa un proveedor de servicios (que puede incluir a un encargado o subencargado del tratamiento de datos) contratado directamente por el Cliente en virtud de un acuerdo separado entre el Cliente y dicho proveedor.
- "*Servicios de SecOps*" significa los Servicios de SecOps que se describen en https://cloud.google.com/terms/secops/services, excepto cualquier Oferta 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 Servicios de SecOps o el Software; 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 Cliente podrá usar si lo desea o según lo determine, 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 vigentes en el momento, 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 el Acuerdo correspondiente.
- 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.
- Sección 6.1 (Eliminación por parte del Cliente) se modifica para que diga lo siguiente:
    - 6.1 **Eliminación por parte del Cliente**. Google permitirá que el Cliente borre los Datos del Cliente durante la Vigencia en concordancia con la funcionalidad de los Servicios o previa solicitud. Si el Cliente utiliza los Servicios para borrar Datos del Cliente durante la

Vigencia y no es posible recuperar esos Datos, o si el Cliente solicita la eliminación de Datos del Cliente durante la Vigencia, este uso o solicitud (según corresponda) constituirán una Instrucción para que Google borre los Datos del Cliente pertinentes de los sistemas de Google de acuerdo con la ley aplicable. 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).

- 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**").

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

- La Sección 9.1 (Acceso, Rectificación, Tratamiento de Datos Restringido y Portabilidad) se modifica para que diga lo siguiente:

9.1 **Acceso, Rectificaciones, Tratamiento Restringido y Portabilidad**. Durante la Vigencia, Google permitirá que el Cliente, de forma coherente con la funcionalidad de los Servicios, acceda a los Datos del Cliente, los rectifique y restrinja su tratamiento, incluso según lo descrito en la Sección 6.1 (Eliminación por Parte del Cliente), y también permitirá que exporte los Datos del Cliente previa solicitud. Si el Cliente se da cuenta de que hay Datos Personales del Cliente que son inexactos o están obsoletos, el Cliente será responsable de notificarlo a Google. Google ayudará al Cliente a rectificar los datos si así lo requiere la Ley de Privacidad Aplicable.

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

4. Inexistencia de Certificaciones por parte de los Clientes no Pertenecientes a EMEA. El Cliente 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 Clientes 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 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 a través de otros medios que Google pueda ofrecer ocasionalmente).

7. Registros de Tratamiento de Datos de Google. En la medida en que alguna Ley de Privacidad Aplicable exija que Google recopile y mantenga registros de determinada información relacionada con el Cliente, el Cliente suministrará dicha información a Google previa solicitud y le notificará cualquier actualización que se requiera para mantener la exactitud y vigencia de esa información, a menos que Google solicite al Cliente suministrar y actualizar esa información por otros medios.

8. Condiciones Específicas del Servicio.

Servicios de Mandiant Consulting y Servicios Administrados

Los Servicios de Mandiant Consulting y Servicios Administrados proporcionan servicios de implementación y asesoría (incluidas respuesta ante incidentes, preparación estratégica y garantía técnica para mitigar amenazas y reducir los riesgos relacionados con incidentes), y servicios de detección y respuesta administradas. Además, por diseño tienen ciertas características distintivas.

1. Modificaciones. El Anexo se modifica de la siguiente manera solo con respecto a los Servicios de Mandiant Consulting y los Servicios Administrados:

- La definición de "Incidente de Datos" se complementa con lo siguiente:
    - Para mayor claridad, un Incidente de Datos excluye los incidentes que son objeto de los Servicios de Mandiant Consulting y los Servicios Administrados, según corresponda.
- La Sección 5.2(b)(i) (Cumplimiento de las Instrucciones del Cliente) se reemplaza por lo siguiente:
    - i. Uso de los Servicios por parte del Cliente
- La segunda oración de la Sección 7.1.1 (Medidas de Seguridad de Google) se modifica para que diga lo siguiente:
    - Las Medidas de Seguridad pueden incluir (según corresponda) medidas para encriptar los Datos del Cliente; para ayudar a garantizar la confidencialidad, la integridad, la disponibilidad y la resiliencia continuas de los sistemas y servicios de Google; para ayudar a restablecer el acceso oportuno a los Datos del Cliente después de un incidente; y para comprobar la eficacia de forma periódica.
- La Sección 7.3.1(b) se modifica para que diga lo siguiente:
    - b. la administración y la gestión del acceso y la protección de las credenciales de autenticación de las cuentas, los sistemas, el software, las redes y los dispositivos que el Cliente usa para recibir o autorizar el acceso a Google para proporcionar los Servicios de Mandiant Consulting o los Servicios Administrados, según corresponda

- Se agregan nuevas Secciones 7.3.1(d) y (e) de la siguiente manera:
    - d. minimizar la cantidad de Datos del Cliente proporcionados por el Cliente, o en su nombre, a Google
    - e. en la medida en que el acceso a los Datos del Cliente de Google se encuentra dentro del control del Cliente, revocar ese acceso cuando Google completa los Servicios de Mandiant Consulting y los Servicios Administrados, según corresponda
- El Apéndice 2 (Medidas de Seguridad) se reemplaza por lo siguiente:
    - Apéndice 2: Medidas Técnicas y Organizacionales Adicionales

1. Entorno Controlado por el Cliente. Google solo accederá y tratará los Datos del Cliente proporcionados por el Cliente, o en su nombre, a Google a través de un entorno o una cuenta controlados o aprobados por el Cliente.

2. Políticas y Procesos de Acceso a los Datos: Política de Acceso. Los procesos y las políticas de acceso a los datos de Google se diseñaron para evitar que personas o sistemas no autorizados accedan a los sistemas que se usan en el tratamiento de los Datos del Cliente. Google (i) solo permite que las personas autorizadas para acceder a los datos puedan hacerlo; y (ii) toma medidas para garantizar que los datos personales no se puedan leer, copiar, modificar ni quitar sin autorización durante el tratamiento y el uso. El otorgamiento de los derechos de acceso o su modificación por parte de Google se basa en el otorgamiento a Google por parte del Cliente de acceso de usuario final a su cuenta o entorno.

3. 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 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 Cliente debe cumplir requisitos adicionales adecuados a su función (p. ej., certificaciones). El personal de Google no tratará los Datos del Cliente sin autorización.

4. Medidas de Seguridad Adicionales. Google y el Cliente pueden acordar medidas de seguridad adicionales en el Formulario de Pedido correspondiente, incluida cualquier Declaración de Trabajo adjunta, para los Servicios de Mandiant Consulting o los Servicios Administrados, según corresponda.

2. Proveedor Contratado por el Cliente. Para mayor claridad y sin limitarse a ello, las obligaciones de Google en virtud de la Sección 7 (Seguridad de los Datos) o la Sección 11 (Subencargados del Tratamiento de Datos), Apéndice 2 (Medidas de Seguridad) no describen las medidas de seguridad ni los controles implementados o proporcionados por el Cliente o los Proveedores Contratados por el Cliente.

Servicios de implementación

1. Definiciones Adicionales.

- "*Datos del Cliente*" significa los datos para los que el Cliente autoriza el acceso al Personal de Google en los Sistemas Administrados por el Cliente.

- "*Sistemas Administrados por el Cliente*" significa lo siguiente, según lo use el Cliente para recibir los Servicios de Implementación: (a) instancias administradas por el Cliente de Servicios de Google Cloud o servicios de nube de terceros; y (b) cualquier hardware o software alojado o administrado en el entorno local del Cliente.

- "*Servicios de Google Cloud*" significa los Servicios descritos en este Apéndice 4 (Productos Específicos), distintos de los Servicios de Implementación, los Servicios de Mandiant Consulting y los Servicios Administrados de Mandiant.

- "*Personal de Google*" significa los empleados y contratistas de Google contratados para proporcionar los Servicios de Implementación.

- "*Servicios de Implementación*" significa los servicios de implementación, asesoría y consultoría proporcionados por los empleados y contratistas de Google en apoyo a los Servicios de Google Cloud, tal como se describe en el Acuerdo, incluido un Formulario de Pedido o una Declaración de Trabajo.

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

- La definición de "Controles de Seguridad Adicionales" se borró.

- La definición de "Incidente de Datos" se reemplaza por lo siguiente:

    - "*Incidente de Datos*" significa un incumplimiento de la Sección 7.1 (Medidas de Seguridad, Controles y Asistencia de Google) por parte del Personal de Google, que lleva, de forma accidental o ilegal, a la destrucción, pérdida, modificación o divulgación no autorizada de los Datos Personales del Cliente, o al acceso a ellos.

- Sujeto al resto de esta Sección, el término "Datos del Cliente" se reemplaza por "Datos Personales del Cliente" cuando se utiliza (a) en la Sección 2 (Definiciones) en la definición de "Subencargado del Tratamiento de Datos", y (b) en otras secciones de este Anexo. Para mayor claridad, otras definiciones en la Sección 2 (Definiciones) permanecen sin cambios.

- La Sección 3 (Duración) se reemplaza por lo siguiente:

    - **3. Duración**. Sin importar si el Acuerdo aplicable se termina o vence, este Anexo permanecerá vigente hasta que Google ya no tenga acceso a los Datos Personales del Cliente y vencerá de manera automática en ese momento.

- La Sección 6 (Eliminación de Datos) se reemplaza por lo siguiente:

    - **6. Eliminación de Datos.** Cuando finalice la Vigencia, el Cliente (a) determinará si desea borrar los Datos Personales del Cliente y (b) será responsable de cualquier eliminación.

- La segunda oración de la Sección 7.1.1 (Medidas de Seguridad de Google) se reemplaza por lo siguiente:

    - "Las Medidas de Seguridad pueden incluir (según corresponda) medidas para encriptar los Datos del Cliente; para ayudar a garantizar la confidencialidad, la integridad la disponibilidad y la resiliencia continuas de los sistemas y servicios de Google; para ayudar a restablecer el acceso oportuno a los Datos del Cliente después de un incidente; y para comprobar la eficacia de forma periódica".

- La Sección 7.1.3 (Controles de Seguridad Adicionales) se borra junto con cualquier otra referencia a esa Sección.

- La Sección 9.1 (Acceso, Rectificaciones, Tratamiento Restringido y Portabilidad) se reemplaza por lo siguiente:

    - 9.1 *Acceso, Rectificaciones, Tratamiento Restringido y Portabilidad*. El Cliente será responsable de usar las funciones de los Sistemas Administrados por el Cliente para acceder a los Datos Personales del Cliente, rectificarlos y restringir su tratamiento, incluso si el Cliente se da cuenta de que algunos de los Datos Personales del Cliente son inexactos o están obsoletos y la Ley de Privacidad Aplicable exige la rectificación o eliminación de esos datos.

- La Sección 11.4 (Oportunidad de Oponerse a Subencargados del Tratamiento de Datos) se reemplaza por lo siguiente:

    - 11.4 *Oportunidad de Oponerse a Subencargados del Tratamiento de Datos*. Cuando se contrate a un Nuevo Subencargado del Tratamiento de Datos durante la Vigencia, Google notificará al Cliente de su contratación antes de que este realice el tratamiento de los Datos Personales del Cliente. El Cliente puede oponerse al Nuevo Subencargado del Tratamiento de Datos con una notificación a Google y, si el Cliente lo hace, las partes trabajarán de buena fe para determinar una alternativa mutuamente aceptable.

- El Apéndice 1 (Objeto y Detalles del Tratamiento de Datos) se modifica de la siguiente manera:

    - La Sección "Duración del Tratamiento de Datos" se reemplaza por lo siguiente:

        - *"Duración del Tratamiento de Datos.* La Vigencia más (si corresponde) el tiempo que transcurra desde el final de este Período hasta el vencimiento del acceso por parte de Google a los Datos Personales del Cliente".

- Las palabras “suministren a Google a través de los Servicios” en las Secciones “Categorías de Datos” y “Sujetos de Datos” se reemplazan por “puestos a disposición de Google en relación con los Servicios”.

- El Apéndice 2 (Medidas de Seguridad) se reemplaza por lo siguiente:

    - **Apéndice 2: Medidas de Seguridad**

1. Sistemas Administrados por el Cliente. El Personal de Google solo accederá y tratará los Datos Personales del Cliente en los Sistemas Administrados por el Cliente. Si esos sistemas incluyen Servicios de Google Cloud, el uso que realice el Cliente de los Servicios de Google Cloud sigue rigiéndose por el acuerdo aplicable a esos servicios.

2. Control 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 accedan a los Servicios de Google Cloud que se usan para el tratamiento de los datos personales. Las políticas de Google (i) solo permiten que el Personal de Google acceda a datos para los que tienen acceso autorizado; y (ii) exigen que el Personal de Google no lea, copie, modifique o quite los Datos Personales del Cliente sin autorización durante el tratamiento, uso y después del registro. El Cliente controla el aprovisionamiento o la modificación de los derechos de acceso de usuario final para los Sistemas Administrados por el Cliente. Si esos sistemas incluyen Servicios de Google Cloud, en el acuerdo para los Servicios de Google Cloud correspondientes, se abordan los detalles relacionados con herramientas de flujo de trabajo que mantienen los registros de cambios de auditoría y los registros de acceso al sistema.

3. 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. También recibe una capacitación en seguridad. El Personal de Google que maneja Datos Personales del Cliente debe cumplir requisitos adicionales adecuados a su función (p. ej., certificaciones).

4. Medidas de Seguridad Adicionales. Google y el Cliente pueden acordar medidas de seguridad adicionales en el Acuerdo, incluidas en un Formulario de Pedido o una Declaración de Trabajo.

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 suscriba las condiciones contractuales adecuadas en materia de seguridad, confidencialidad y privacidad.

3. Responsabilidades de Seguridad del Cliente. Además de sus obligaciones estipuladas en la Sección 7.3.1 (Responsabilidades de Seguridad del Cliente), el Cliente es responsable de lo siguiente:

- administrar y gestionar el acceso a los Sistemas Administrados por el Cliente y su protección, lo que incluye minimizar el acceso del Personal de Google a los Datos Personales del Cliente en la medida en que sea razonablemente factible y poner fin a ese acceso una vez completados los Servicios de Implementación

- implementar las recomendaciones de seguridad que Google le proporcione por escrito al Cliente con respecto a los Sistemas Administrados por el Cliente

4. Certificación de Cumplimiento. Google mantendrá certificados para las normas ISO 27001, ISO 27017 e ISO 27018 que abarcan los Servicios de Implementación proporcionados en apoyo de Google Cloud Platform y Google Workspace (las "*Certificaciones de Cumplimiento de los Servicios de Implementación*"). Google podrá agregar estándares en cualquier momento. Google podrá reemplazar una Certificación de Cumplimiento de los Servicios de Implementación por una alternativa equivalente o mejorada.

5. Revisiones de la Certificación de Cumplimiento. Para demostrar el cumplimiento de Google con respecto a sus obligaciones en virtud de este Anexo, Google pondrá a disposición del Cliente la Certificación de Cumplimiento de los Servicios de Implementación para su revisión y, si el Cliente es encargado del tratamiento de datos, permitirá que el Cliente solicite acceso a la Certificación de Cumplimiento de los Servicios de Implementación para el responsable del tratamiento de datos pertinente.

6. Ubicaciones del Tratamiento de Datos. Los Datos Personales del Cliente pueden tratarse en cualquier país en el que Google proporcione Servicios de Implementación o en el que el Cliente mantenga Sistemas Administrados por el Cliente.

7. Inexistencia de Certificaciones por parte de los Clientes no Pertenecientes a EMEA. El Cliente 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 Clientes 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 Implementación.

8. Información sobre los Subencargados del Tratamiento de Datos. Los Subencargados del Tratamiento de Datos para los Servicios de Implementación se identificarán (como subcontratistas) en un Formulario de Pedido o Declaración de Trabajo correspondientes, o bien otra confirmación proporcionada al Cliente antes del comienzo de los Servicios de Implementación, o serán Afiliados de Google. Google también pondrá a disposición del Cliente los nombres, las ubicaciones y actividades de los Subencargados del Tratamiento de Datos para los Servicios de Implementación previa solicitud.

9. Registros de Tratamiento de Datos de Google. En la medida en que alguna Ley de Privacidad Aplicable exija que Google recopile y mantenga registros de determinada información relacionada con el Cliente, el Cliente suministrará dicha información a Google previa solicitud y le notificará cualquier actualización que se requiera para mantener la exactitud y vigencia de esa información, a menos que Google solicite al Cliente suministrar y actualizar esa información por otros medios.

Google Cloud Skills Boost para Organizaciones

1. Definiciones Adicionales.

- "*Cuenta*", si no se define en el Acuerdo, significa la Cuenta del Cliente de Google Cloud Skills Boost para Organizaciones.
- "*GCSBO*" significa los servicios educativos, de capacitación y aprendizaje y el contenido proporcionado a través de https://www.cloudskillsboost.google/ (o bien otro sitio web operado o controlado por Google y que se utilice para Google Cloud Skills Boost para Organizaciones).
- "*TSS*" significa los servicios de asistencia técnica que Google, a discreción, puede proporcionar al Cliente.

2. Modificaciones. Este Anexo se modifica de la siguiente manera con respecto a GCSBO:

- 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 Cliente podrá usar si lo desea o según lo determine, incluidos (si los hubiera) la encriptación, los registros, la supervisión, la administración de identidades y accesos, y los análisis de seguridad.
- 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/skillsboost-organizations/sccs/eu-c2p.
    - "SCC (de Encargado a Responsable del Tratamiento de Datos)" significa las condiciones que se encuentran en: https://cloud.google.com/terms/skillsboost-organizations/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/skillsboost-organizations/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/skillsboost-organizations/sccs/eu-p2p-intra-group.

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

4. Inexistencia de Certificaciones por parte de los Clientes no Pertenecientes a EMEA. El Cliente 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 Clientes no Pertenecientes a EMEA) de las condiciones de Protección de Datos para Europa en el Apéndice 3 (Leyes de Privacidad Específicas) en relación con GCSBO.

5. Información sobre los Subencargados del Tratamiento de Datos. Los nombres, las ubicaciones y las actividades de los Subencargados del Tratamiento de Datos para GCSBO se describen en:

a. https://cloud.google.com/terms/skillsboost-organizations/subprocessors

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

6. Equipo de Protección de Datos de Cloud. Puede comunicarse con el Equipo de Protección de Datos de GCSBO en https://support.google.com/qwiklabs (o a través de otros medios que Google pueda ofrecer ocasionalmente).

7. Registros de Tratamiento de Datos de Google. En la medida en que alguna Ley de Privacidad Aplicable exija que Google recopile y mantenga registros de determinada información relacionada con el Cliente, el Cliente suministrará dicha información a Google previa solicitud y le notificará cualquier actualización que se requiera para mantener la exactitud y vigencia de esa información, a menos que Google solicite al Cliente suministrar y actualizar esa información por otros medios.

Versiones anteriores de las Condiciones de Seguridad y Tratamiento de Datos:

9 de abril de 2024 30 de junio de 2022 24 de septiembre de 2021 19 de agosto de 2020 10 de agosto de 2020 17 de julio de 2020 11 de octubre de 2019 1 de octubre de 2019 25 de mayo de 2018 13 de marzo de 2018 9 de noviembre de 2017 11 de octubre de 2017 7 de febrero de 2017 6 de octubre de 2016

Versiones anteriores de la Modificación de Tratamiento de Datos:

7 de julio de 2022 24 de septiembre de 2021 27 de mayo de 2021 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

Versiones anteriores del Anexo de Tratamiento de Datos para Servicios de Looker (original) (Clientes):

14 de febrero de 2023 4 de enero de 2023 20 de septiembre de 2022 30 de junio de 2022 16 de marzo de 2022 24 de septiembre de 2021 1 de abril de 2021 15 de enero de 2021 17 de diciembre de 2020 28 de agosto de 2020 1 de junio de 2020 9 de marzo de 2020

Versiones anteriores de las DPST de los Servicios de SecOps (Clientes):

6 de febrero de 2023 28 de noviembre de 2022 27 de septiembre de 2021 1 de octubre de 2020

Versiones anteriores del Anexo de Tratamiento de Datos para Servicios de Asesoría y Servicios Administrados de SecOps:

5 de octubre de 2023 19 de septiembre de 2023 15 de junio de 2023 22 de febrero de 2023 6 de febrero de 2023

Versiones anteriores *(última modificación: 15 de octubre de 2024)*

26 de septiembre de 2024 9 de septiembre de 2024 5 de agosto de 2024 23 de mayo de 2024 9 de abril de 2024 8 de noviembre de 2023 15 de agosto de 2023 20 de septiembre de 2022