ACUERDO DE TRATAMIENTO DE DATOS

El presente Acuerdo de tratamiento de datos **("ATD")** contiene el acuerdo entre las partes con respecto a los términos que rigen el Tratamiento de Datos Personales en nombre del Cliente en virtud de cualquier contrato escrito aplicable entre el Cliente y Dynatrace que regule el uso de las Ofertas de Dynatrace (de pago o de otro tipo), y de cualquier Formularios u Ordenes de Pedido, anexos y documentos de trabajo que estén relacionados con el mismo (colectivamente, el **"Contrato").** Este ATD entra en vigor a partir de la fecha en que ambas partes lo ejecuten (la **"Fecha Efectiva").**

El presente ATD está sujeto a los términos del Contrato, y se incorpora al mismo como si a letra estuviese insertado, plenamente formando parte del mismo. Este ATD sustituirá cualquier acuerdo de tratamiento de datos existente a la fecha, a menos que se indique explícitamente lo contrario en el presente documento. En caso de que surja algún conflicto entre el contenido de este ATD y cualquier otra disposición del Contrato con respecto a los datos personales, regirán y serán de aplicación los términos del presente ATD. Los términos en mayúscula usados en el presente, pero no definidos en este ATD tendrán el mismo significado que se establece en el Contrato de Suscripción disponible en https://assets.dynatrace.com/global/legal/Online-SA-April-2023-Spanish.pdf.

1. Definiciones.

(a) "**APPI**" se refiere a la Ley japonesa sobre protección de información personal [Act on the Protection of Personal Information] (Ley n.º 57 de 2003, según lo modificado en 2016).

(b) "**Ley de Protección de Datos**" se refiere a todas las leyes y reglamentos en materia de protección de datos y de privacidad de datos que resulten aplicables al Tratamiento de los Datos personales del Cliente por parte de Dynatrace en virtud del Contrato.

(c) "**Responsable del Tratamiento**" tiene el mismo significado que el otorgado en la Ley de protección de datos correspondiente e incluye el término "Propietario de base de datos" conforme a la Ley de protección de la privacidad de Israel y el término "Empresa" conforme a la correspondiente Ley de privacidad estatal de EE. UU.

(d) "**Datos Personales del Cliente**" se refiere a cualquier Dato personal enviado, almacenado, publicado, mostrado o transmitido en general por o en nombre del Cliente en el transcurso del uso de las Ofertas de Dynatrace; y excluye los Datos personales (como Información restringida) enviados, almacenados, publicados, mostrados o transmitidos en general por o en nombre del Cliente en violación de cualquier disposición del Contrato y/o de este ATD.

(e) "**Grupo Dynatrace**" se refiere a una o más entidades de Dynatrace LLC, una sociedad de responsabilidad limitada de Delaware, junto con sus Filiales que puedan ayudar a Dynatrace a proporcionar las Ofertas de Dynatrace, y/o el soporte o servicios relacionados, en virtud del Contrato y de este ATD.

(f) "**Europa**" se refiere a la Unión Europea, el Espacio Económico Europeo ("EEE") y/o sus estados miembros, Suiza y el Reino Unido.

(g) "**RGPD**" se refiere al Reglamento 2016/679 del Parlamento Europeo y del Consejo sobre la protección de las personas físicas con respecto al tratamiento de datos personales y a la libre circulación de dichos datos (Reglamento General de Protección de Datos).

(h) "**LGPD**" se refiere a la Lei Geral de Proteção de Dados Pessoais (Ley General de Protección de Datos Personales en Brasil).

(i) "**Violación de la Seguridad de los Datos Personales**" se refiere a una violación de la seguridad que conduce a la destrucción, pérdida, alteración o divulgación accidental o ilícita de, o al acceso no autorizado a, Datos Personales del Cliente mientras Dynatrace los transmite, almacena o trata en general.

(j) "**PIPL**" se refiere a la Ley de Protección de Información Personal de China [Personal Information Protection Law].

(k) "**Datos Personales**" se refiere a "Datos Personales" o "Información Personal," según se define en las Leyes de Protección de Datos correspondientes, que Dynatrace recopila o recibe en nombre del Cliente. Los Datos Personales no incluyen información que Dynatrace obtenga o trate independientemente del cumplimiento de sus respectivas obligaciones en virtud del Contrato con el Cliente.

(l) "**Encargado del Tratamiento**" tiene el mismo significado que el otorgado en la Ley de Protección de Datos correspondiente e incluye "Titular" conforme se define en la Ley de protección de la privacidad de Israel, y "Proveedor de Servicios" conforme a la correspondiente Ley de privacidad estatal de EE. UU.

(m) "**Cláusulas Contractuales Tipo**" se refiere a las Cláusulas Contractuales Tipo promulgadas por la Decisión de la Comisión Europea 2021/914/UE e incorporadas en el presente documento mediante referencia, en cada caso conforme se hayan modificado o sustituido en ese momento.

(n) "**Subencargado" o "Subencargado del Tratamiento**" se refiere a los Encargados del tratamiento contratados por Dynatrace o miembros del Grupo Dynatrace para permitir que Dynatrace entregue/suministre las Ofertas de Dynatrace en virtud de los términos del Contrato o de este ATD.

(o) "**Autoridad de Control**" se refiere a la agencia, departamento u otra organización pública competente con autoridad respecto del tratamiento de Datos personales relevantes para este ATD.

(p) "**Anexo del Reino Unido**" se refiere al Anexo de Transferencia Internacional de Datos a las Cláusulas contractuales tipo de la Comisión de la UE, emitido por la oficina del Comisionado de Información del Reino Unido en virtud de la Ley de Protección de Datos de 2018 S119A (1), y conforme se actualice, modifique o sustituya en cada momento.

(q) **"Empresa",** "**Responsable del Tratamiento**", "**Consumidor",** "**Encargado del Tratamiento**", "**Proveedor de Servicios**", "**Titular**", **"Venta",** y "**Tratamiento**" (y "**tratar**") tendrán los significados que se les otorguen en virtud de la Ley de protección de datos correspondiente.

2. Aplicabilidad del ATD y funciones de las partes

(a) Este ATD aplicará al Tratamiento de Datos Personales del Cliente por parte de Dynatrace, en nombre del Cliente, para cumplir con sus obligaciones y ejercer sus derechos en virtud del Contrato y de este ATD. Para evitar dudas, este ATD no aplica al Tratamiento de Datos Personales del Cliente por parte de Dynatrace como Responsable del Tratamiento.

(b) El Cliente es considerado como Responsable del Tratamiento o un Encargado del Tratamiento, mientras que Dynatrace es el Encargado del Tratamiento. En la medida en que resulte aplicable bajo la Ley de Protección de Datos, el Cliente designa a Dynatrace como Encargado del Tratamiento para tratar los Datos personales del Cliente, en nombre de este último.

3. Tratamiento de Datos Personales del Cliente

(a) La naturaleza y el alcance del Tratamiento de los Datos Personales del Cliente por Dynatrace, para prestar las Ofertas de Dynatrace, es determinado y controlado por el Cliente, complementándose con el Anexo A. La naturaleza, el propósito y la duración del Tratamiento, así como los tipos de Datos Personales recopilados y las categorías de Titulares cuyos Datos Personales puede, ser tratados por Dynatrace, se describen en el **Anexo A** de este ATD. El Cliente reconoce que Dynatrace no tiene conocimiento de los datos reales ni de los tipos de Datos Personales contenidos en los Datos del Cliente. Las partes acuerdan que las instrucciones completas y finales del Cliente sobre la naturaleza y el propósito del Tratamiento en conexión con las Ofertas de Dynatrace se encuentran establecidas en el Contrato y en este ATD.

(b) Todo cambio o modificación a las instrucciones, tendrá que ser comunicado por escrito y reconocido por ambas partes. Dynatrace tendrá la obligación de informar al Cliente si, en su opinión razonable, existe alguna posibilidad de que las instrucciones de tratamiento del Cliente puedan infringir alguna Ley de Protección de Datos que resulte aplicable; en tal caso, Dynatrace tendrá derecho a rechazar el Tratamiento de los Datos Personales del Cliente que considere que infrinjan alguna Ley de Protección de Datos que resulte aplicable, hasta que el Cliente modifique sus instrucciones de forma que no haya infracción.

(c) En la medida en que la configuración del Cliente de las Ofertas de Dynatrace resulte en que Dynatrace capture Datos Personales del Cliente, el Cliente declara y garantiza que cumplirá, en todo momento, con todas las Leyes de Protección de Datos que resulten aplicables. Entre el Cliente y Dynatrace, el Cliente es responsable de: (i) proteger los Datos Personales del Cliente mientras utiliza Dynatrace, ajustando las Configuraciones de Privacidad de Datos de Dynatrace tal como se describe en ttps://docs.dynatrace.com/docs/manage/data-privacy-and-security (instrucciones de Dynatrace sobre cómo ajustar las configuraciones de privacidad de datos) para controlar granularmente el alcance de los Datos Personales del Cliente que vayan a ser capturados por las Ofertas de Dynatrace; (ii) la exactitud, calidad y legalidad de los Datos Personales del Cliente, y los medios a través de los cuales el Cliente o cualquier tercero pertinente, adquirió los Datos Personales.

(d) Si el Cliente es un Encargado del Tratamiento que actúa en nombre de un tercero Responsable del Tratamiento, el Cliente garantiza a Dynatrace que las instrucciones del Cliente y las acciones con respecto a los Datos personales del Cliente, incluyendo el hecho de nombrar a Dynatrace como otro Encargado del Tratamiento, hayan sido autorizadas por el Responsable del Tratamiento pertinente.

(e) El Cliente declara y garantiza que: (i) informará a sus Titulares de acuerdo con lo requerido legalmente sobre su uso de Encargados del Tratamiento para tratar los Datos Personales del Cliente, incluido Dynatrace, e incluyendo cuando sea necesario notificar a los Interesados acerca del uso de las Ofertas de Dynatrace; (ii) ha obtenido, y sigue teniendo, durante el periodo de vigencia, todos los derechos necesarios, la base jurídica, las autorizaciones y/o los consentimientos válidos, inclusive de los Interesados, para el Tratamiento de Datos Personales del Cliente por parte de Dynatrace, según lo contemplado en el Contrato; (iii) el uso del Cliente de las Ofertas Dynatrace no le ocasionará a Dynatrace, ni causará que Dynatrace infrinja cualquier Ley de Protección de Datos, o cualquier otra ley o regulación que resulte aplicable, ni de ningún contrato u obligación entre el Cliente y cualquier tercero.

(f) El Cliente proporcionará a Dynatrace únicamente los Datos Personales del Cliente que sean necesarios para que Dynatrace cumpla con sus obligaciones en virtud del Contrato, con respecto a las Ofertas de Dynatrace y a cualquier servicio relacionado. El Cliente reconoce que el uso de las Ofertas de Dynatrace no requiere, ni es adecuado para, el Tratamiento de Información Restringida y no proporcionará, durante de su uso de las Ofertas de Dynatrace, ninguna Información Restringida para tratamiento por parte de Dynatrace.

4. Solicitudes de Terceros.

(a) Las Ofertas de Dynatrace proporcionan al Cliente con la funcionalidad de acceder Datos Personales del Cliente con el objeto de asistir a los Clientes con las solicitudes de Interesados que estén ejerciendo sus derechos otorgados en virtud de la Ley de Protección de Datos (“Solicitudes de Interesados”) o solicitudes de órganos reguladores o entidades judiciales relacionados con el Tratamiento de Datos Personales del Cliente. En la medida de que el Cliente no le sea posible acceder a los Datos Personales del Cliente pertinentes dentro de las Ofertas de Dynatrace, o que el acceso a los Datos Personales del Cliente no le proporcione asistencia suficiente para contestar a dichas solicitudes de conformidad con la Ley de Protección de Datos, y cuando así lo requiera la Ley de Protección de Datos aplicable, Dynatrace está de acuerdo con, a petición del Cliente, proporcionar asistencia razonable al Cliente para permitirle que este conteste las Solicitudes de Interesados, o las solicitudes de órganos reguladores o entidades judiciales relacionados con el Tratamiento de Datos personales del Cliente en virtud del Contrato. Si alguna solicitud es realizada directamente a Dynatrace en relación a Datos Personales del Cliente respecto de los cuales

Dynatrace puede identificar al Cliente como Responsable del Tratamiento, Dynatrace remitirá dicha comunicación al Cliente sin demora indebida, y no responderá a esa solicitud sin la autorización expresa del Cliente. Lo anterior no es una prohibición a Dynatrace de comunicarse con un Interesado o un órgano regulador o entidad judicial si en la comunicación no queda claro, o no resulta evidente, dentro de lo razonable, que dicha solicitud incumbe al Cliente, o en el caso de que Dynatrace tenga la obligación legal de responder directamente.

(b) En el caso que Dynatrace se vea obligado a divulgar Datos Personales respecto a los cuales el Cliente es el Responsable del Tratamiento como consecuencia de una solicitud de una agencia del orden público u organismo encargado del cumplimiento de la ley u otro tercero, Dynatrace notificará al Cliente de dicha solicitud antes de conceder acceso y/o proporcionar Datos Personales, para permitirle al Cliente que interponga medidas cautelaros o cualquier otro recurso adecuado. Si Dynatrace tiene legalmente prohibido informar al Cliente, Dynatrace entonces adoptará medidas para proteger los Datos Personales contra la divulgación indebida, como si fuera la propia Información Confidencial de Dynatrace la que se solicita.

5. **Asistencia y Cooperación.** Sujeto a la naturaleza del tratamiento y a los Datos Personales disponibles para Dynatrace, y cuando sea requerido por la Ley de Protección de Datos aplicable, Dynatrace, a petición por escrito del Cliente, proporcionará asistencia e información al Cliente, dentro de lo razonable, en el supuesto de que, a juicio del Cliente, el tipo de tratamiento realizado por Dynatrace requiera una evaluación de impacto de protección de datos y/o una consulta previa con las autoridades/agencia de protección de datos pertinentes, y proporcionará asistencia al Cliente, dentro de lo razonable, para cumplir con sus demás obligaciones en virtud de la Ley de Protección de Datos aplicable en relación con la seguridad de los datos y las notificaciones de Violación de la Seguridad de los Datos Personales, en la medida de lo aplicable al Tratamiento de Datos Personales del Cliente. El Cliente reembolsará a Dynatrace todos los costos notables en que incurra Dynatrace con vistas a cumplir sus obligaciones en virtud de esta sección.

6. **Cumplimiento Demostrable.** Dynatrace acepta proporcionarle al Cliente la información necesaria para demostrar el cumplimiento de este ATD luego de que este envíe una solicitud razonable.

7. **Auditorías y Evaluaciones.**

(a) Donde la Ley de Protección de Datos aplicables le otorgue al Cliente un derecho a efectuar auditorías o evaluaciones, y con sujeción al alcance de dicho derecho, el Cliente podrá llevar a cabo, previa solicitud escrita del Cliente y con una frecuencia de una vez al año, una auditoría o evaluación de las políticas, procesos y registros de Dynatrace relevantes al Tratamiento de los Datos Personales del Cliente, de acuerdo con la Ley de Protección de Datos aplicable.

(b) Para solicitar una auditoría, el Cliente debe enviar a Dynatrace un plan de auditoría detallado al menos con cuatro (4) semanas de antelación a la fecha de auditoría propuesta a Dynatrace, y dicho plan deberá describir el alcance propuesto, la duración y la fecha de inicio de la auditoría. Dynatrace revisará el plan de auditoría y le remitirá al Cliente cualquier duda o pregunta. Antes del inicio de cualquier auditoría, las partes acordarán un plan de auditoría detallado, incluyendo costos, horarios, alcance de los controles, evidencias a ser producidas y duración. Si el alcance de la auditoría solicitada hubiese sido abordado en un informe de auditoría similar dentro de los doce meses anteriores, y Dynatrace confirma que no han habido cambios sustanciales en los controles auditados, el Cliente acuerda en aceptar las conclusiones de dicho informe previo, en lugar de solicitar una nueva auditoría sobre los controles ya cubiertos por el informe previo.

(c) Toda auditoría o evaluación debe: (i) realizarse durante el horario laboral normal de Dynatrace; (ii) estar sujeta a obligaciones de confidencialidad entre las partes. Si la auditoría fuese realizada por una tercera parte, esta tercera parte no podrá ser competidor de Dynatrace, y dicha tercera parte estará sujeta al consentimiento previo de Dynatrace, teniendo la obligación, además, de firmar un acuerdo de confidencialidad por escrito con todas las partes antes de realizar la auditoría.

(d) El costo de todas las auditorías será cubierto completamente por el Cliente. Cualquier solicitud enviada a Dynatrace para que proporcione asistencia con una auditoría, será considerada como un servicio

independiente si dicha asistencia a la auditoría requiere el uso de recursos diferentes de, o a mayores de, los necesarios para la prestación de las Ofertas de Dynatrace. Dynatrace solicitará la confirmación escrita al Cliente de que el Cliente pagará cualquier costo aplicable o correspondiente, antes de realizar dicha asistencia de auditoría.

8. **Confidencialidad.** Dynatrace tiene la obligación de asegurarse de que toda persona a la que autorice a tratar Datos Personales del Cliente (incluidos su personal, agentes y subcontratistas) esté sujeta a obligaciones vinculantes de confidencialidad ya sea de carácter contractual, establecidas por ley o de otro tipo.

9. **Seguridad**

(a) **Medidas de seguridad.** Tomando en cuenta los últimos avances de la tecnología, los costos de implementación y la naturaleza, el alcance, el contexto y los fines del Tratamiento, así como el riesgo de probabilidad variables y gravedad para los derechos y libertades de las personas naturales, Dynatrace ha implementado, y mantendrá implantadas, medidas apropiadas de tipo técnico y organizativas, diseñadas para proporcionar un nivel de seguridad adecuado frente al riesgo del Tratamiento de Datos Personales del Cliente **("Medidas de Seguridad").** El Cliente confirma la implementación, por parte de Dynatrace, de las Medidas de Seguridad identificadas en el **Anexo B** adjunto al presente instrumento**,** son suficientes para cumplir con sus obligaciones en virtud del presente ATD. Sin perjuicio de lo anterior, el Cliente reconoce, acuerda y acepta que es responsable de su propio uso seguro de las Ofertas de Dynatrace.

(b) **Violación a la Seguridad de los Datos Personales.**, Dynatrace le notificará al Cliente, sin demora indebida y a más tardar cuando le sea requerido por la Ley de Protección de Datos aplicable, después de que tenga conocimiento de alguna Violación a la Seguridad de los Datos Personales. Dynatrace, sin demora, iniciará una investigación en cuanto a las circunstancias que rodean la Violación a la Seguridad de los Datos Personales y pondrá a disposición del Cliente los resultados de la misma. Dynatrace se esforzará por tomar todas las medidas requeridas por la Ley de Protección de Datos aplicable para mitigar los efectos de dicha Violación a la Seguridad de los Datos Personales. A petición del Cliente y tomando en cuenta la naturaleza del Tratamiento, y la información que este disponible para Dynatrace, Dynatrace adoptará medidas comercialmente razonables para asistir al Cliente en el cumplimiento de sus obligaciones necesarias para habilitar al Cliente de modo que pueda notificar las Violaciones a la Seguridad de los Datos Personales relevantes a las autoridades competentes y/o a los Interesados afectados, en caso de que al Cliente se le requiera hacerlo en virtud de la Ley de Protección de Datos aplicable. La notificación de una Violación a la Seguridad de los Datos Personales se entregará a uno, o más, de los administradores del Cliente por cualquier medio que Dynatrace seleccione, incluido por correo electrónico. Es responsabilidad exclusiva del Cliente asegurarse de que los administradores del Cliente mantengan información de contacto precisa en el portal en línea o de cualquier otra forma según lo exija Dynatrace mediante notificación por escrito al/a los administradores(es) del Cliente. La obligación de Dynatrace de reportar o responder a una Violación a la Seguridad de los Datos Personales en virtud de esta Sección, no constituye un reconocimiento por parte de Dynatrace de falta alguna o responsabilidad con respecto a la Violación a la Seguridad de los Datos Personales.

10. **Subtratamiento**

(a) El Cliente otorga su autorización general para nombrar a miembros del Grupo Dynatrace como subencargados en virtud de este ATD, y autoriza a Dynatrace y a los miembros del Grupo Dynatrace a contratar a otros Subencargados adicionales. La lista actualizada de los Subencargados del tratamiento a la fecha del presente para las Ofertas de Dynatrace puede ser encontrada en https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatrace-services/. Para recibir notificaciones de Subencargados nuevos o cambios en la lista de los Subencargados, el Cliente debe registrarse en la página web https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatrace-services/ ("**Avisos de protección de datos")** para la recepción de notificaciones que estén disponibles. Dynatrace actualizará la Lista de Subencargados para reflejar cualquier cambio en la lista o la incorporación de nuevos Subencargados del tratamiento tercerizados, con no menos de treinta (30) días previo a la fecha de entrada en vigor de dicho cambio. Los Clientes que se

hayan suscrito para recibir actualizaciones a la Lista de Subencargados del tratamiento, serán notificados de dicho cambio.

(b) En la medida en que así lo requiera la Ley de Protección de Datos aplicable, el Cliente puede oponerse u objetar al tratamiento de los Datos Personales del Cliente por parte de cualquier Subencargado recién designado por motivos razonables relacionados con la protección de Datos Personales del Cliente, y deberá de informar a Dynatrace de su oposición por escrito, en un plazo dentro de quince (15) días después de ser notificado de los cambios efectuados en la Lista de Subencargados, estableciendo los motivos específicos de su objeción. La objeción del Cliente debe ser por escrito y debe proporcionar una justificación comercialmente razonable para tal objeción, basándose en preocupaciones razonables relativas a las prácticas del Subencargado propuesto en cuanto a protección de datos. Tras una objeción u oposición del Cliente, las partes trabajarán conjuntamente y de buena fe, para abordar las objeciones razonables del Cliente y proceder al cambio de Subencargado. Si las partes no logran llegar a un acuerdo dentro de un plazo de quince (15) días posteriores a la fecha en que el Cliente envío la objeción, Dynatrace, a su discreción tendrá las siguientes opciones: (a) Dynatrace dará instrucciones al Subencargado de que no trate los Datos Personales del Cliente, lo cual puede resultar en la suspensión de alguna característica de las Ofertas de Dynatrace dando lugar a que no esté disponible para el Cliente; o, (b) el Cliente podrá rescindir inmediatamente este ATD y el Contrato, y Dynatrace reembolsará lo antes posible una porción prorrateada de la cuota prepagada correspondiente al periodo posterior a dicha fecha de suspensión o rescisión. Si Dynatrace no recibe ninguna objeción dentro del plazo especificado anteriormente, se considerará que el Cliente ha aprobado el uso del Subencargado nuevo.

(c) Dynatrace tendrá la obligación de: (i) celebrar un acuerdo por escrito con cada Subencargado, el cual contendrá obligaciones de protección de datos con disposiciones y obligaciones contractuales apropiadas y sustancialmente similares a, más de ninguna forma, menos restrictivas que, las establecidas en este ATD, en la medida apropiada respecto de la naturaleza del servicio prestado por dicho Subencargado; y, (ii) seguir siendo responsable del cumplimiento de dicho Subencargado, con las obligaciones de este ATD y de cualquier acto u omisión de dicho Subencargado que cause que Dynatrace infrinja cualquiera de sus obligaciones bajo este ATD.

11. Eliminación de Datos del Cliente al Momento de la Rescisión. Posteriormente a la rescisión o terminación del Contrato, los Datos Personales del Cliente serán eliminados dentro de un plazo de treinta (30) días, o, si así lo prefiere el Cliente, serán devueltos, excepto en los casos en que la legislación aplicable requiera su conservación durante un plazo determinado, o en la medida en que se archiven en sistemas de copia de seguridad, en cuyo caso los términos de este ATD continuarán vigentes.

12. Transferencias internacionales de datos

(a) El Cliente autoriza a Dynatrace y a sus Subencargados del tratamiento a transferir Datos Personales del Cliente a través de fronteras internacionales, incluidos, de forma enunciativa mas no limitativa, desde el EEE, el Reino Unido y/o Suiza, Israel y China a los Estados Unidos. Si los Datos Personales del Cliente que se originan en el EEE o Suiza se transfieren a un país que carece de un nivel adecuado de protección en virtud de la Ley de Protección de datos aplicable ("**Transferencia Restringida**"), las partes acuerdan que esa transferencia se regirá por las Cláusulas Contractuales Tipo que se incorporan por este medio, por referencia, a este ATD de la manera como se indica a continuación. Las firmas de este ATD o del Contrato constituyen la firma de las Cláusulas Contractuales Tipo, así como de cualquier anexo adjunto al mismo. Cuando la transferencia de Datos personales del Cliente sea de origen en dicho Cliente ("**Exportador de Datos**") y su destino sea Dynatrace ("**Importador de Datos**"), sea una Transferencia Restringida y las Leyes de Protección de Datos requieran que se establezca un mecanismo de transferencia válido, las transferencias estarán sujetas a las Cláusulas contractuales tipo.

(b) Las Cláusulas Contractuales Tipo se completarán de la siguiente manera:

i. Se aplicará el módulo dos (según corresponda);

ii. En la Cláusula 7 (Adhesión), aplicará la cláusula de adhesión opcional;

iii. En la Cláusula 8.5 y la Cláusula 16 (d), la certificación de supresión se proporcionará a petición por escrito del Exportador de Datos;

iv. En la Cláusula 8.9, el derecho de auditoría se llevará a cabo de acuerdo con la Sección 7 del presente ATD;

v. En la Cláusula 9 (Uso de Subencargados), aplicará la opción 2 "Autorización General por Escrito" para los Subencargados del tratamiento y el periodo de tiempo para la notificación previa será el establecido en la Sección 11 del presente ATD;

vi. En la Cláusula 11 (Reparación), no aplicará el texto opcional;

vii. En la Cláusula 13 (Supervisión), la autoridad de control competente será la Commission Nationale de l'informatique et des Libertés (CNIL).

viii. En la Cláusula 14 (f) y la Cláusula 16 (c), el derecho de rescisión se limitará a la terminación de las Cláusulas;

ix. En la Cláusula 17 (Legislación Aplicable), las Cláusulas Contractuales Tipo estarán regidas por el Derecho Francés;

x. En la Cláusula 18 (b) (Elección de foro y Jurisdicción), las partes acuerdan que las disputas serán resultas en los tribunales de Francia;

xi. El Anexo 1 de las Cláusulas Contractuales Tipo será completado con la información establecida en el Apéndice A del presente ATD;

xii. El Anexo 2 de las Cláusulas Contractuales Tipo será completado con la información establecida en el Apéndice B del presente ATD; y

xiii. Se añade una nueva Cláusula 1 (e) a las Cláusulas Contractuales Tipo que indicará lo siguiente: "En la medida en que resulte aquí aplicable, estas Cláusulas también aplican, mutatis mutandis, al Tratamiento de Datos Personales del Cliente que lleven a cabo las partes, que esté sujeto a la Ley Federal Suiza sobre Protección de datos. Donde resulte aplicable, la referencia a la legislación de los Estados miembros de la UE o a las autoridades de control de la UE se modificará para incluir la referencia correspondiente, de conformidad a la legislación suiza en lo que respecta a la transferencia de Datos Personales del Cliente que estén sujetos a la Ley Federal Suiza de Protección de Datos y al Comisionado Federal Suizo de Protección de Datos e información como autoridad de control bajo estas Cláusulas".

(c) En la medida en que la prestación de las Ofertas de Dynatrace por parte de Dynatrace involucre la transferencia de Datos Personales del Cliente originados en el Reino Unido, hacia un tercer país que haya sido designado como carente de un nivel adecuado de protección de los Datos Personales del Cliente en virtud de las Leyes aplicables en el Reino Unido, las Cláusulas Contractuales Tipo deberán: (i) usarse y completarse según se establece en la sección 13; (ii) contar con una nueva Cláusula 1(f) que será agregada en las Cláusulas Contractuales Tipo, que estipule lo siguiente: "En la medida en que resulte aquí aplicable, estas Cláusulas, tal como están complementadas por la Sección 13, también serán de aplicación mutatis mutandis al Tratamiento de los Datos Personales del Cliente, por las partes que esté sujeta a las Leyes de Protección de Datos del Reino Unido; y (iii) el Anexo del Reino Unido, que se completará de la siguiente manera:

i. La Tabla 1 del Anexo del Reino Unido se completará con la información del Apéndice A.

ii. La Tabla 2 del Anexo del Reino Unido se completará con la información que se encuentra en la Sección 13 (c) de este ATD.

iii. La Tabla 3 del Anexo del Reino Unido será completada de la siguiente manera:

1) La lista de partes se establece en el Apéndice A;

2) La descripción de la transferencia se establece en el Apéndice A;

3) La descripción de las medidas técnicas y organizativas se establecen en el Apéndice B;

4) La lista de Subencargados se encuentra en la sección 11 de este ATD;

5) A efectos de completar la Tabla 4 del Anexo del Reino Unido, tanto el importador como el exportador podrán dar por terminado el Anexo del Reino Unido conforme se establece en la Sección 19 del Anexo del Reino Unido.

(d) En la medida en que la prestación de las Ofertas de Dynatrace por parte de Dynatrace implique la transferencia de Datos Personales del Cliente originados de China hacia un tercer país que haya sido designado como carente de un nivel adecuado de protección de los Datos Personales del Cliente en virtud de la Legislación aplicable en China, el Cliente será responsable de cumplir con todas las obligaciones siguientes de exportación de Datos Personales del Cliente (cuando el Cliente es el Responsable del Tratamiento) o de asegurarse que el tercero Responsable del Tratamiento pertinente haya cumplido con todas las obligaciones siguientes (cuando el Cliente sea el Encargado del Tratamiento):

i. informar a los individuos del nombre y la información de contacto de la parte destinataria en el extranjero de los Datos Personales del Cliente, el propósito y los medios del Tratamiento, las categorías de Datos Personales del Cliente y los métodos y procedimientos a través de los cuales los individuos pueden presentar solicitudes para ejercitar sus derechos sobre los Datos Personales del Cliente ante la parte receptora de los Datos Personales del Cliente en el extranjero;

ii. garantizar una base jurídica para la exportación de los Datos Personales del Cliente y, donde el consentimiento de los individuos sea la base jurídica, obtener por separado el consentimiento de los individuos;

iii. realizar una evaluación de impacto de protección de la información personal en la exportación de Datos Personales del Cliente; y

iv. adoptar las medidas de protección adecuada requeridas por la PIPL y las regulaciones administrativas que la acompañen (es decir, aprobar la evaluación de seguridad gubernamental, completar las cláusulas contractuales tipo ejecutadas u obtener la certificación) a menos que una exención resulte aplicable.

(e) Además de lo anterior, si una Autoridad de Control adopta, actualiza o reemplaza cualquier cláusula contractual tipo o mecanismos de transferencia de datos similares, Dynatrace se reserva el derecho de adoptar un estándar alternativo de cumplimiento para reemplazar o complementar las Cláusulas Contractuales Tipo o el Anexo del Reino Unido para la transferencia legal de Datos Personales, o bien añadir mecanismos nuevos de transferencia de datos para otros países, siempre y cuando que estos sean reconocidos bajo la Ley de Protección de Datos. Dynatrace notificará con treinta (30) días de antelación a los Clientes que se suscriban a Avisos de protección de datos, de la adopción del estándar de cumplimiento alternativo. La variación aplicará automáticamente conforme a lo establecido en la notificación de Dynatrace, al final del periodo de notificación.

(f) En caso de que surja algún conflicto o inconsistencia entre los documentos mencionados a continuación, el orden de prioridad será: (1) las Cláusulas Contractuales Tipo (sin embargo, siempre y cuando que, el Encargado del tratamiento podrá nombrar a Subencargados según lo establecido, y sujeto a los requisitos de la Sección 11 de este ATD) o un mecanismo similar requerido por las Leyes de Protección de Datos aplicables específicamente para las transferencias internacionales de datos; (2) este ATD; y (3) el Contrato.

(g) En la medida en que Dynatrace transfiera Datos del Cliente que se hayan originados en Brasil y que estén protegidos bajo la Ley de Protección de Datos Brasileña, Dynatrace cumplirá con los principios y derechos de los Interesados, y con las obligaciones de protección de datos previstas en la LGPD.

(h) En la medida en que Dynatrace transfiera Datos del Cliente que se hayan originados en Japón y que estén protegidos bajo la Ley de Protección de Datos Japonesa, Dynatrace cumplirá con los principios y derechos de los Interesados y con las obligaciones de protección de datos previstas en la APPI.

(i) En la medida en que la prestación de las Ofertas de Dynatrace por parte de Dynatrace involucre la transferencia de Datos Personales del Cliente originados en Israel, hacia un tercer país que haya sido

designado como carente de un nivel adecuado de protección de los Datos Personales del Cliente en virtud de las Leyes aplicables en Israel, el Cliente será responsable de asegurar una base legal para la exportación de los Datos Personales del Cliente. Para mayor claridad, este ATD constituye la obligación por escrito de Dynatrace de adoptar las medidas de protección adecuadas que requiere la Regulación de Protección de la Privacidad (Transferencia Internacional de Datos), 2001. En aras de una mayor claridad las obligaciones de este ATD son consideradas como suficientes por el Cliente para facilitar la transferencia de información fuera de Israel de conformidad con la Regulación 3 de los Regulaciones de Protección de la Privacidad (Transferencia de Datos a Bases de Datos fuera de las fronteras del país), 2001.

13. Términos específicos de las leyes de privacidad estatales de EE. UU. complementarias.

(a) La definición de "Ley de Protección de Datos aplicable" incluye las Leyes de Privacidad de los Estados de EE. UU. Las "Leyes de Privacidad de los Estados de EE. UU." significa todas las leyes estatales relacionadas con la protección y el tratamiento de datos personales que estén vigentes en los Estados Unidos de América, las cuales pueden incluir de forma enunciativa mas no limitativa, el Acto de Privacidad del Consumidor de California, modificada por el Acto de Derechos de Privacidad de California (California Consumer Privacy Act, "CCPA") así como cualquier otras legislaciones o regulaciones de privacidad del consumidor similares de otros Estados, en cada caso, tal como sean eventualmente modificadas, complementadas, o reemplazadas. .

(b) Cuando Dynatrace trate Datos Personales del Cliente sujetos a las leyes de privacidad Estatales de los EE.UU., Dynatrace será considerado como un "encargado" ("processor" en su terminología en inglés) o "proveedor de servicios" (como resulte aplicable) cuando trate Datos Personales del Cliente. El Cliente divulga o pone en general a disposición de Dynatrace Datos Personales del Cliente con el fin limitado y especifico de prestar las Ofertas de Dynatrace en virtud de lo establecido en el Contrato (el "Propósito"). Dynatrace tiene la obligación de (y exigirá lo mismo de sus Subencargados):

i. cumplir con las obligaciones que le sean aplicables en su calidad de proveedor de servicios o encargado bajo las leyes de privacidad Estatales de los EE.UU.;

ii. notificar si ya no puede cumplir con sus obligaciones en virtud de las leyes de privacidad Estatales de los EE.UU.;

iii. abstenerse de "vender" o "compartir" (tal como estos términos se encuentren definidos en la CCPA) Contenido del Cliente o de retener, usar o divulgar Datos Personales del Cliente: (1) para cualquier finalidad distinta del Propósito, incluyendo la retención, uso o divulgación de Datos Personales del Cliente para un fin comercial distinto al Propósito, o como sea permitido bajo las leyes de privacidad Estatales de los EE.U..; o, (2) fuera de la relación de negocios directa entre el Cliente y Dynatrace; o, a menos que sea permitido de otro modo por las leyes de privacidad Estatales de los EE.UU., abstenerse de combinar los Datos Personales del Cliente con Datos Personales que Dynatrace reciba de, o en nombre de otra empresa o persona, o que sean recopilados a raíz de sus propias interacciones con individuos, a menos que dicha combinación sea necesaria para llevar a cabo un fin comercial autorizado por las leyes de privacidad Estatales de los EE.UU..

iv. El Cliente debe: (1) previa notificación, tendrá derecho a tomar medidas razonables y apropiadas, acordadas entre las partes, para ayudar a asegurar que Dynatrace Trate los Datos Personales del Cliente en una forma consistente con las obligaciones del Cliente en virtud de las leyes de privacidad Estatales de los EE.UU., y detener y remediar el Tratamiento no autorizado de Datos Personales del Cliente por parte de Dynatrace; (2) notificar al Cliente si determina que ya no puede cumplir con sus obligaciones bajo las leyes de privacidad Estatales de los EE.UU. en cuanto a los Datos Personales del Cliente.

v. Dynatrace reconoce y confirma que no recibe Datos Personales del Cliente como contraprestación por ninguna Oferta que haya provista al Cliente. Dynatrace certifica que entiende y que cumplirá con sus obligaciones en virtud de las leyes de privacidad Estatales de los EE.UU.

14. Varios

(a) Con excepción de lo modificado en este ATD, el Contrato permanecerá en pleno vigor y efecto. Cualquier modificación a este ATD tendrá que ser efectuada por escrito, a través del Convenio Modificatorio correspondiente y debe estar debidamente ejecutada por los representantes legales con poderes suficientes, de las partes.

(b) Sin perjuicio de cualquier disposición en contrario contenida en el Contrato o en este ATD, la responsabilidad de cada parte y de todas sus Filiales, en conjunto en el agregado, que derive de, o que esté relacionada con este ATD, con cualquier orden o con el Contrato, ya sea dicha responsabilidad de origen contractual, responsabilidad extracontractual o bajo cualquier otra teoría de responsabilidad, se verá sujeta a la cláusula o sección denominada "Limitación de Responsabilidad" contenida en el Contrato, y toda referencia en dicha sección a la responsabilidad de una parte se refiere a la responsabilidad agregada de esa parte y de todas sus Filiales en virtud del Contrato y este ATD, inclusive todos los Apéndices del presente instrumento. Dynatrace no será responsable ante el Cliente por pérdidas o daños de carácter indirecto o emergente, consecuenciales, lucro cesante, pérdida de ventas, pérdida de negocios, pérdida de ahorros previstos, pérdida o daños al fondo de comercio, o de otro modo en cada caso, ya sea directo o indirecto, que surjan de o guarden relación con este ATD. Sin limitar ninguna de las obligaciones de las partes en virtud del Contrato o de este ATD, el Cliente acepta que cualquier responsabilidad incurrida por Dynatrace en relación con los Datos Personales del Cliente y que surja como resultado de, o en relación con, el incumplimiento por parte del Cliente de sus obligaciones establecidas en este ATD o en la Ley de Protección de Datos aplicable, será descontada y reducirá el límite de responsabilidad de Dynatrace en virtud del Contrato (o, si procede, en virtud de este ATD) como si fuera responsabilidad hacia el Cliente. Sin perjuicio de cualquier disposición en contrario en este ATD (incluidas, de forma enunciativa mas no limitativa, las obligaciones de indemnización de de cada parte), ninguna de las partes será responsable de multa alguna del RGPD emitida o impuesta en virtud del artículo 83 del RGPD contra la otra parte por una autoridad reguladora o un organismo gubernamental en relación con la infracción del RGPD por la otra parte.

(c) El presente ATD se regirá y será interpretado de acuerdo con las disposiciones en cuanto a legislación aplicable y jurisdicción contenidas en el Contrato, siempre y cuando que las Cláusulas Contractuales Tipo se rijan de acuerdo a lo establecido en la sección 13 del presente ATD.

Acordado y aceptado por:	Acordado y aceptado por:
Nombre_de_entidad_del_Cliente	**Nombre_de_entidad_de_Dynatrace**
Firma autorizada	Firma autorizada
Nombre	Nombre
Cargo	Cargo
Fecha	Fecha
Dirección	Dirección
Número de empresa (si procede)	Número de empresa (si procede)

APENDICE A
DETALLES DEL TRATAMIENTO

Descripción del Exportador de Datos

El exportador de Datos es la entidad identificada como el "Cliente" o "Dynatrace", según sea el caso, en el supuesto de cualquier Subtratamiento, en el Acuerdo de Tratamiento de Datos vigente entre el Exportador de Datos y el Importador de Datos y al cual el presente Apéndice se encuentra adjunto.

Descripción del Importador de Datos

El Importador de Datos es la entidad identificada como "Dynatrace" o un Subencargado debidamente autorizado en el Acuerdo de Tratamiento de Datos vigente entre el Exportador de Datos y el Importador de Ddatos y al cual el presente Apendice se encuentra adjunto.

Objeto y Duración del Tratamiento

El objeto y la duración del Tratamiento son los siguientes:

Entre las partes, el Cliente será el Responsable del Tratamiento de determinados Datos Personales del Cliente que le hayan sido proporcionados a Dynatrace, por el Cliente, en relación con su uso de las Ofertas de Dynatrace. La duración del Tratamiento será el mismo término de la vigencia del Contrato.

Fines del Tratamiento

El Tratamiento es necesario para la siguiente finalidad:

Permitirle a Dynatrace prestar las Ofertas de Dynatrace al Cliente y ejercer sus derechos y obligaciones en virtud del Contrato.

Interesados

Los Interesados pueden incluir: (i) usuarios autorizados por el Cliente para utilizar las Ofertas de Dynatrace; y, (ii) usuarios de, o visitantes de las aplicaciones y/o sitios web monitoreadas del Cliente (incluidos, de forma enunciativa mas no limitativa, los empleados del Cliente, clientes o usuarios, agentes, contratistas y asesores) según lo determine el Cliente a su entera discreción.

Tipo de Datos Personales

Se le requiere al Cliente proporcionar ciertos Datos Personales para podrr usar las Ofertas de Dynatrace, incluyendo la dirección de IP, y el nombre y apellido si se incluyen en la dirección de correo electrónico del usuario, así como las credenciales de usuario. El Cliente puede enviar Datos Personales adicionales a las Ofertas de Dynatrace, y la medida de lo cual, y el alcance, es determinado, controlado y decidido por el Cliente a su entera discreción.

Categorías Especiales de Datos o Datos Personales Sensibles (si procede)

Los Datos Personales transferidos incumben a las siguientes categorías especiales de datos o datos personales sensibles:

No es aplicable. El Cliente no puede usar las Ofertas de Dynatrace para el tratamiento de ningún dato que sea clasificado como "datos de categoría especial" o "datos personales sensibles," a menos que se acuerde lo contrario explícitamente por escrito.

Operaciones de Tratamiento

Los Datos Personales transferidos estarán sujetos a las siguientes actividades básicas de Tratamiento:

Dynatrace Tratará los Datos Personales del Cliente únicamente como sea necesario para prestar las Ofertas de Dynatrace y ejercer sus derechos y obligaciones tal como están contenidas en los términos del

Contrato y de este Acuerdo de Tratamiento de Datos, incluyendo de forma enunciativa mas no limitativa, la habilitación del cliente, el soporte técnico, los servicios profesionales, la mejora del rendimiento y las funciones de las Ofertas de Dynatrace, la autenticación de usuarios y las comunicaciones y la administración de cuentas.

ANEXO B

MEDIDAS DE SEGURIDAD

Dynatrace (también denominado en el presente instrumento como el "Encargado del Tratamiento"), implementará, como mínimo, las medidas de seguridad técnicas y organizativas descritas a continuación con respecto a los Datos Personales del Cliente, que trate en nombre de este (también denominado en el presente documento el "Responsable del Tratamiento"). Estas medidas de seguridad serán aplicadas a todos los Datos Personales del Cliente que estén sujetos al Contrato subyacente entre el Encargado del Tratamiento y el Responsable del Tratamiento (el "Contrato"). En relación con los Subencargados tercerizados que puedan tratar Datos Personales en nombre de Dynatrace, dichos terceros tendrán sus propios requisitos de seguridad para proteger los Datos Personales.

Medidas técnicas

1.1 Autorización

(a) Un sistema de autorización será utilizado donde diferentes perfiles de autorización se utilicen para diferentes fines.

1.2 Identificación

(a) A cada Usuario Autorizado se le debe proporcionar un código de identificación que sea personal y único, para ese fin ("ID de Usuario"). No se puede asignar un ID de Usuario a una persona distinta, incluso en un momento posterior.

(b) Se mantendrá un registro actualizado de los Usuarios Autorizados, y del acceso autorizado disponible para cada uno de estos, así como se establecerán procedimientos de identificación y autenticación para todo el acceso a los sistemas de información, o para llevar a cabo cualquier Tratamiento de Datos. Conforme se usa en el presente, "Tratamiento" se refiere a cualquier operación o conjunto de operaciones que se realice en los Datos, sea o no, por medios automatizados, como, por ejemplo: recopilación, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, difusión o puesta a disposición en general, alineación o combinación, restricción, supresión o destrucción.

(c) Las contraseñas tendrán que ser modificadas periódicamente según se establece en las Políticas de Seguridad de la Información de Dynatrace.

1.3 Autenticación

(a) Los Usuarios Autorizados tendrán permitido Tratar Datos si se les proporcionan con credenciales de autenticación tales como completar con éxito un procedimiento de autenticación relacionado ya sea a una operación de Tratamiento específica o a un conjunto de operaciones de Tratamiento.

(b) La autenticación debe basarse en una contraseña secreta asociada con cada ID de usuario, y cuya contraseña solo podrá ser conocida por el Usuario Autorizado.

(c) Una o más credenciales de autenticación serán asignadas a, o serán asociadas con, un Usuario Autorizado.

(d) Debe existir un procedimiento en cuanto a la confidencialidad e integridad de la contraseña. Las contraseñas deben ser almacenadas de forma que sean ininteligibles mientras sigan siendo válidas. Debe existir un procedimiento para asignar, distribuir y almacenar contraseñas.

(e) Las contraseñas tienen que contener como mínimo doce caracteres o, si esto no es técnicamente permitido por los sistemas de información pertinentes, la contraseña contendrá el número máximo permitido de caracteres. Las contraseñas no pueden contener ningún elemento que pueda relacionarse fácilmente con el Usuario Autorizado a cargo del Tratamiento, y tienen que ser cambiadas a intervalos regulares, cuyos intervalos deben constar en el documento de seguridad. Las contraseñas serán modificadas por el Usuario Autorizado a un valor secreto conocido solo por el Usuario Autorizado cuando se utilice por primera vez y periódicamente, a partir de entonces.

(f) Además de una combinación válida de ID de Usuario y contraseña, todo acceso a datos o a los sistemas de Dynatrace debe estar asegurado por una solución de autenticación multifactor (Multi-Factor Authentication, o por sus siglas en ingles en adelante “MFA”). La solución MFA puede ser de naturaleza de software o hardware.

(g) Las credenciales de autenticación también serán desactivadas si al Usuario Autorizado se le da por terminado, es desvinculado o trasladado, o se le desautoriza el acceso a los sistemas de información o a los Datos de Tratamiento.

1.4 Controles de Acceso

(a) Solo los Usuarios Autorizados tendrán acceso a los Datos, inclusive cuando estén almacenados en un medio electrónico o portátil o cuando estos sean transmitidos. Los Usuarios Aautorizados solo tendrán acceso autorizado a dichos datos y recursos necesarios para poder desempeñar sus funciones.

(b) Un sistema que otorgue acceso a los Usuarios Autorizados a los datos designados y recursos, será utilizado.

(c) Se verificará semestralmente que los prerrequisitos para conservar o retener los perfiles de autorización pertinentes, se sigan aplicando. Esto también puede incluir la lista de Usuarios Autorizados redactada por categorías homogéneas de tareas y el perfil de autorización correspondiente.

(d) Se establecerán medidas para prevenir que un usuario obtenga acceso o uso no autorizado de los sistemas de información. En particular, se tienen que instalar sistemas de detección de intrusiones que reflejen las mejores prácticas del sector para proteger los sistemas de información contra el acceso no autorizado.

(e) Los controles de acceso al sistema operativo o a la base de datos, deben configurarse correctamente para asegurar el acceso autorizado, únicamente.

(f) Solo el personal autorizado tendrá la capacidad de conceder, alterar o cancelar el acceso de los usuarios a los sistemas de información.

1.5 Gestión de Sistemas Informáticos y Soportes Extraíbles

(a) Los sistemas de información de red y los medios físicos que almacenan Datos deben alojarse en un entorno seguro con un acceso físico restringido solo al personal autorizado a dicho acceso. Se deben mantener controles sólidos de autorización y de acceso.

(b) El software, firmware y hardware usados en los sistemas de información tendrá que ser revisado anualmente con la finalidad de detectar vulnerabilidades y defectos en los sistemas de

información y resolver dichas vulnerabilidades y defectos.

(c) Políticas y entrenamientos tendrán que ser emitidos con respecto al mantenimiento y uso de los medios/soportes en los que se almacenen los Datos, para evitar el acceso y el Tratamiento no autorizados.

(d) Cuando se vayan a eliminar o volver a usarse los medios/soportes, se tomarán medidas necesarias para prevenir cualquier recuperación posterior de los Datos y demás información almacenada previamente en ellos, o de otra manera hacer la información inteligible o se reconstruya por cualquier medio técnico antes de que se retiren del inventario. Todos los medios/soportes reutilizables que se utilicen para el almacenamiento de Datos se sobrescribirán un mínimo de tres veces con datos aleatorios antes de su eliminación o reutilización.

(e) La remoción de medios/soportes que contengan Datos de las instalaciones designadas debe estar específicamente autorizada por el Responsable del Tratamiento y ser conforme a las políticas de Dynatrace.

(f) Los medios/soportes que contengan Datos deben borrarse o hacerse ilegibles si ya no se usan, y antes de su correcta eliminación.

1.6 Distribución o Transmisión

(a) Los Datos solo deben estar disponibles para los Usuarios Autorizados.

(b) Cifrado (128 bits o más fuerte) u otra forma equivalente de protección debe ser utilizada para proteger los Datos que se transmiten electrónicamente a través de una red pública, o que se almacenan en un medio portátil, o bien cuando exista un requerimiento de almacenar o Tratar los Datos en un entorno físicamente inseguro.

(c) Cuando los Datos vayan a salir de las instalaciones designadas como resultado de operaciones de mantenimiento, tienen que tomarse las medidas necesarias para evitar cualquier recuperación no autorizada de los Datos y demás información almacenada en ellos.

(d) Donde Datos se transmitan o transfieran a través de una red de comunicaciones electrónicas, detendrá que establecerse medidas para controlar el flujo de datos y registrar el momento oportuno de la transmisión o transferencia, los Datos transmitidos o transferidos, el destino de cualquier Dato transmitido o transferido, así como los detalles del Usuario Autorizado que conduce o realiza la transmisión o transferencia.

1.7 Conservación, Copias de Seguridad (Back up) y Recuperación

(a) Deben definirse y establecerse procedimientos para hacer copias de seguridad o back up copies, y para recuperación de los Datos. Estos procedimientos deben permitir que los datos puedan ser reconstruidos en el estado en el que estaban en el momento en que se perdieron o destruyeron.

(b) Las copias de seguridad o back up copies deben realizarse al menos una vez a la semana, a menos que no se hayan actualizado Datos durante ese periodo.

(c) Una copia de seguridad o back up y los procedimientos de recuperación de datos deben ser mantenidos en una ubicación o locación diferente a la del centro de los sistemas de información que Tratan los Datos, y estos requisitos mínimos de seguridad serán aplicados a dichos back up o copias de seguridad.

1.8 Detección de intrusiones y antivirus

(a) Se debe de instalar un software antivirus y sistemas de detección de intrusiones en los sistemas de información para protegerlos contra ataques u otros actos no autorizados con respecto a los

sistemas de información. El software antivirus y los sistemas de detección de intrusiones deben ser actualizados regularmente de acuerdo con las mejores prácticas del sector para los sistemas de información en cuestión (y al menos una vez al año).

1.9 Pruebas

(a) Las pruebas previas a la implementación o modificación de los sistemas de información que tratan los Datos no podrán usar datos reales o “en vivo,” a menos que dicho uso sea necesario y no exista una alternativa razonable. Donde se utilicen datos reales o “en vivo”, se limitarán en la medida necesaria a los fines de las pruebas y se debe garantizar el nivel de seguridad correspondiente al tipo de Datos Tratados.

1.10 Auditoría

(a) Auditorías regulares de cumplimiento con estos requisitos de seguridad, deben ser realizadas al menos una vez al año.

(b) Los resultados deben proporcionar una opinión o dictamen en el grado en el cual l las medidas de seguridad y controles adoptados cumplen con estos requisitos de seguridad, identifican cualquier deficiencia y (si procede) proponer medidas correctivas o complementarias en la medida de lo necesario. También debe incluir los datos, hechos y observaciones sobre las que se basan las opiniones emitidas, y las recomendaciones propuestas.

2. Medidas Organizativas

2.1 Plan de Seguridad y documentos.

- Las medidas adoptadas para cumplir con estos requisitos de seguridad serán el objeto de las Políticas de Seguridad de la Información de la Empresa y se expondrán en un portal de seguridad, el cual tendrá que mantenerse actualizado y deberá ser revisado siempre que se realicen cambios relevantes en el/los sistema(s) de información o en las medidas técnicas u organizativas.
- Las Políticas de seguridad de la información habrán de abordar:

  (i) Medidas de seguridad relacionadas con la modificación y el mantenimiento del/de los sistema(s) usado(s) para Tratar Datos, incluyendo el desarrollo y mantenimiento de aplicaciones, soporte adecuado del proveedor y un inventario de hardware y software;

  (ii) Seguridad física, incluyendo la seguridad de los edificios o instalaciones donde ocurre el Tratamiento de datos, la seguridad de los equipos de datos e infraestructura de telecomunicaciones y los controles medioambientales; y

  (iii) Seguridad de los ordenadores y/o computadoras y sistemas de telecomunicaciones, incluidos procedimientos para gestionar copias de seguridad, procedimientos relacionados o para lidiar con viruses informáticos, procedimientos para gestionar señales/códigos, seguridad para la implementación de software, seguridad relacionada con bases de datos, seguridad para conectar sistemas a Internet, inspección de elusiones de sistema(s) de datos, mecanismos para llevar la cuenta de los intentos de infracción de la seguridad del sistema u de obtención de acceso no autorizado.

- El plan de seguridad incluirá todas las políticas de Dynatrace, según se actualicen periódicamente, incluidas, de forma limitativa mas no enunciativa:

  (i) Código de Conducta y Etica Empresarial

  (ii) Política Global de Protección de Datos

  (iii) Política de Uso Aceptable de TI de Dynatrace

  (iv) Políticas de seguridad del sistema: Política deGgestión del Control de Acceso de Dynatrace;

Norma de Conservación de Copias de Seguridad; Política de Gestión de Cambios; Política de Gestión de Cambios - Sistemas de Empresa; Política de Cumplimiento; Plan de Respuesta ante Incidentes de Seguridad Cibernética y de Datos; Política de Clasificación de Datos; Política de Prevención de Pérdida de Datos; Política de Supervisión Electrónica; Política de Cifrado; Política de seguridad de Recursos Humanos; Política de Gestión de Recursos de Información; Política de Gestión de Riesgos de la Información; Política de Operaciones de TI; Política de Dispositivos Móviles o Celulares; Política de Acceso a la Red; Política de Contraseñas de Cuentas de Red; Política de Firewall de Red; Política Medioambiental y de Seguridad Física; Política de Devolución de Activos para Empleados Cesados o Desvinculados; Política de Phishing de Seguridad; Política de Ciclo de Vida de la Cuenta de Servicio; Política de Gestión de Proveedores; Política de Gestión de Vulnerabilidades; Política de Seguridad de la Estación de Trabajo.

(v) El plan de seguridad tendrá que estar disponible para el personal que tenga acceso a los Datos y a los sistemas de información, y debe cubrir como mínimo los siguientes aspectos:

(vi) El alcance, con una especificación detallada de los recursos protegidos;

(vii) Las medidas, estándares, procedimientos, normas y reglas del código de conducta para garantizar la seguridad, incluyendo el control, la inspección y la supervisión de los sistemas de información;

(viii) Los procedimientos para informar, gestionar y responder a incidentes; y

(ix) Los procedimientos para realizar copias de seguridad/back up y recuperar Datos, incluido el miembro del personal que realizó la actividad de Tratamiento, los Datos restaurados y, según corresponda, qué datos tuvieron que introducirse manualmente en el proceso de recuperación.

2.2 Funciones y Obligaciones del Personal

- Solo los miembros del personal que tengan la necesidad operativa legítima de acceder a los sistemas de información, o llevar a cabo cualquier Tratamiento de Datos estarán autorizados a hacerlo ("**Usuarios Autorizados**").

- Tendrán que adoptarse las medidas necesarias para formar y familiarizar al personal con estos requisitos mínimos de seguridad, con cualquier política pertinente y con las leyes aplicables relativas al desempeño de sus funciones y obligaciones con respecto al Tratamiento de Datos y las consecuencias de un eventual incumplimiento de los requisitos.
- Las funciones y obligaciones del personal que tenga acceso a los Datos y a los sistemas de información, tienen que estar claramente definidas a través de los roles de seguridad de las aplicaciones.
- Los Usuarios Autorizados recibirán instrucciones al efecto de que no pueden dejar equipos electrónicos sin supervisión ni accesibles durante las sesiones de Tratamiento. El acceso físico a las zonas donde se almacenan los Datos se limitará a los Usuarios Autorizados. Las medidas disciplinarias por incumplimiento o violación del plan de seguridad tienen que estar claramente definidas, documentadas y ser comunicadas claramente al personal.

2.3 Director Ejecutivo de Seguridad

- Una persona, o personas, responsables del cumplimiento general de estos requisitos mínimos de seguridad será designado con el cargo de Director Ejecutivo de Seguridad de la Información (Chief Information Security Officer, "**CISO").** El CISO contará con la formación y experiencia adecuadas en la gestión de la seguridad de la información y deberá estar dotado de los recursos

adecuados para garantizar el cumplimiento de forma eficaz.

- Los datos de contacto del CISO serán proporcionados al Responsable del Tratamiento previa solicitud.

2.4 Mantenimiento de Registros

- Un historial de acceso a, o divulgación de, los Datos por parte del Usuario Autorizado deberá ser registrado con un registro de auditoría seguro.
- Únicamente el personal debidamente autorizado podrá tener acceso físico a las instalaciones donde se almacenan los sistemas de información y los soportes/medios que almacenan los Datos.
- Habrá un procedimiento para reportar, responder a y gestionar incidentes de seguridad tales como violaciones a la seguridad de los datos. Esto incluirá, como mínimo:
  - (i) Un procedimiento para reportar de dichos incidentes/violaciones al órgano de dirección adecuado;
  - (ii) Un equipo claramente designado para gestionar y coordinar la respuesta a un incidente, liderado por el CISO;
  - (iii) Un proceso documentado para gestionar la respuesta a un incidente, incluyendo el requisito de mantener registros de problemas y acciones adecuados, que incluirá el momento en que se produjo el incidente, la persona que reportó el incidente, a quién se le reportó y los efectos del mismo;
  - (iv) La obligación del Encargado del Tratamiento de informar al Responsable del Tratamiento sin demora indebida en cao que haya una violación de la seguridad que conduzca a la destrucción, pérdida, alteración, divulgación no autorizada o al acceso, accidental o ilícito, de los Datos transmitidos, almacenados o tratados en general por el Encargado del Tratamiento; y
  - (v) El equipo de seguridad/gestión de incidentes del Encargado del Tratamiento debe, cuando proceda, trabajar junto con los representantes de seguridad del Responsable del Tratamiento hasta que se haya resuelto satisfactoriamente el incidente o la violación.
  - (vi) El procedimiento para informar, gestionar y responder a incidentes deberá probarse al menos una vez al año.