HITACHI
Inspire the Next

# ACUERDO DE PROTECCIÓN DE DATOS

## 1. Introducción

Este Acuerdo de Protección de Datos (el "**DPA**", por sus siglas en inglés) refleja el acuerdo de las Partes respecto del Procesamiento de los Datos Personales de Hitachi por parte del Proveedor en virtud del [ACUERDO MAESTRO], incluyendo cualquier SOW (en conjunto, el "**Acuerdo Maestro**"). Cada Parte acuerda que posee la capacidad y plena autoridad legal para cumplir con sus obligaciones en virtud de este DPA.

## 2. Definiciones

A menos se defina expresamente en este DPA, todos los términos en mayúscula tendrán el mismo significado que se les asigna en el Acuerdo Maestro. En este DPA, los siguientes términos tendrán el siguiente significado:

**País Adecuado:** un país u organización internacional determinada por la Comisión Europea, a través de un acto de aplicación, que garantice un nivel adecuado de protección de acuerdo con las Leyes de Protección de Datos, incluyendo el Artículo 45 de la Regulación General de Protección de Datos.

**Leyes de Protección de Datos:** las leyes y regulaciones de protección de datos de tanto en tanto vigentes en cada jurisdicción donde el Proveedor Procese los Datos Personales.

**Autoridades de Protección de Datos:** la autoridad legal pertinente en cada jurisdicción donde el Proveedor Procese los Datos Personales.

**Descubrimiento:** cuando una Parte toma por primera vez conocimiento de un evento o circunstancia.

**Fecha de Vigencia:** la fecha de vigencia del Acuerdo Maestro.

**Medidas Mínimas de Protección:** se refiere a las medidas técnicas y organizativas especificadas en el Anexo 2 de este DPA (Requerimientos de Seguridad de la Información).

**Datos Personales:** información personal acerca de una persona natural identificada o identificable, Procesada por el Proveedor para o en nombre de Hitachi para el cumplimiento del Propósito.

**Procesamiento:** toda operación o conjunto de operaciones realizadas sobre los Datos Personales, ya sea a través de un medio automático o no, como la recolección, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación mediante transmisión, difusión o puesta a disposición de otro modo, alineación o combinación, restricción, eliminación o destrucción.

**Propósito:** cumplimiento de las obligaciones de las Partes de acuerdo con el Acuerdo Maestro.

**Infracción de Seguridad:** todo acceso accidental o no autorizado, destrucción, modificación, comunicación o transferencia de Datos Personales no autorizada.

**Venta:** vender, alquilar, publicar, divulgar, diseminar, poner a disposición, transferir o comunicar de otra manera en forma oral, escrita o medio electrónico o de otra naturaleza, información personal a un tercero a cambio de una retribución monetaria o de otra índole.

**Cláusulas Contractuales Estándares:** plantilla adjunta al presenta como Anexo 1 a este DPA.

**Subprocessador:** cualquier tercero contratado por el Proveedor o el contratista del Proveedor o agente, que Procesa Datos Personales de Hitachi para o en nombre del Proveedor para el Propósito.

**Término:** comienza en la Fecha de Vigencia y permanece vigente de manera permanente hasta: (i) la terminación o vencimiento del Acuerdo Maestro; (ii) dicho tiempo en que el Proveedor deje de estar autorizado por Hitachi para Procesar Datos Personales; o (iii) dicho tiempo en que el Proveedor (o su Subprocessador) deja de Procesar Información Personal, lo que ocurra en último lugar.

## 3. Obligaciones del Proveedor

(a) En todo momento, el Proveedor deberá tratar a los Datos Personales con carácter de Información Confidencial y deberá requerir que todo su Personal y los Subprocesadores con acceso a los Datos Personales actúen del mismo modo.

(b) En todo momento, el Proveedor deberá cumplir con: las Leyes de Protección de Datos en la mayor medida aplicable a dichos Datos Personales y las obligaciones impuestas para sí en este DPA. En la medida en que el Proveedor obtenga el o los consentimientos para el Procesamiento de los Datos Personales, el Proveedor deberá entregarlos junto con toda documentación pertinente, solicitada de manera razonable por Hitachi, dentro del término de 72 horas desde que recibiera la solicitud de Hitachi.

(c) El Proveedor será, en todo momento, el controlador de los Datos Personales que el Proveedor entregue a Hitachi. El Proveedor es responsable de cumplir con sus obligaciones en su carácter de controlador de datos en virtud de las Leyes de Protección de Datos.

(d) El Proveedor solo deberá Procesar los Datos Personales para el Propósito y solo de conformidad con las instrucciones de Hitachi, que incluirán el Acuerdo Maestro y este DPA. El Proveedor se deberá de abstener de Procesar los Datos Personales para finalidades distintas a las instruidas por Hitachi.

(e) En relación con las Partes, todos los Datos Personales y sus derivaciones, sean o no identificadas, anónimas o colectivas, serán en todo momento propiedad de Hitachi.

(f) El Proveedor deberá asegurar que todo su Personal o los Subprocesadores obligados en virtud de este DPA: (i) completen la capacitación anual sobre protección de datos y (ii) estén sujetos a los términos contractuales que contengan como mínimo el mismo grado de protección hacia los Datos Personales que aquellos términos de este DPA.

(g) El Proveedor deberá asegurar que el acceso a los Datos Personales se limita al Personal o al Subprocessador del Proveedor quién requiera acceso para el Propósito. Dicho acceso se limitará en alcance a la cantidad mínima de Datos Personales necesaria para el Propósito y por un período acotado de tiempo necesario para el cumplimiento del Propósito.

(h) El Proveedor deberá implementar medidas técnicas, físicas y organizativas apropiadas a fin de proteger los Datos Personales, incluyendo medidas contra una Infracción de Seguridad. Por el plazo más prolongado que resulte entre (i) el Término de este DPA; o (ii) cualquier período de tiempo para el cual el Proveedor procese, controle o posea Datos Personales de Hitachi; dichas medidas deberán ser como mínimo tan protectoras como las Medidas Mínimas de Protección.

(i) El Proveedor no deberá, directa o indirectamente: divulgar, dar a conocer o de otro modo divulgar Datos Personales a ningún tercero, salvo después de obtener el consentimiento expreso escrito de Hitachi. En la medida en que lo permita la ley aplicable, Hitachi se reserve el derecho, a su exclusivo criterio, de condicionar dicho consentimiento a la aceptación de términos adicionales por parte del Proveedor.

(j) El Proveedor no recibirá ni transferirá ningún Dato Personal fuera del AEE a menos que: (i) el territorio receptor sea un País Adecuado; (ii) el Proveedor haya celebrado Cláusulas Contractuales Estándares suficientes para permitir dicha transferencia; (iii) la parte receptora posea normas corporativas vinculantes; (iv) la parte receptora posea certificación bajo el Marco de Escudo de Privacidad entre la Unión Europea y los Estados Unidos y mantenga dicha información vigente a lo largo del Término del Acuerdo; o (v) cuando así lo requiera la autoridad competente.

(k) El Proveedor deberá notificar a Hitachi sin demora infundada tan pronto descubra que el Proveedor o su Subprocessador no ha cumplido o de otro modo se vea incapaz de cumplir con una o más de sus obligaciones en virtud de este DPA. En caso de dicho incumplimiento y sin limitar cualquier otro recurso disponible para Hitachi en virtud de este DPA, Hitachi podrá indicar al Proveedor que cese de Procesar los Datos Personales y el Proveedor deberá cumplir con las indicaciones razonables de Hitachi respecto de los Datos Personales en posesión o control del Proveedor.

(l) El Proveedor deberá, de inmediato y en todo caso dentro del término de cuarenta y ocho (48) horas del Descubrimiento por parte del Proveedor, notificar a Hitachi de cualquier petición, investigación, reclamación o demanda efectuada por terceros (incluyendo a las Autoridades de Protección de Datos) en relación con los Datos Personales. El Proveedor deberá colaborar de manera razonable con Hitachi tal como sea necesario para que Hitachi responda ante dichos terceros.

(m) El Proveedor deberá cumplir con las decisiones aplicables de las Autoridades de Protección de Datos, árbitros o tribunales en relación con el Procesamiento de Datos Personales.

(n) En la medida que la Ley de Privacidad del Consumidor de California de 2018, codificada en el Código Civil de California §1798.100 *et seq*. aplique, el Proveedor afirma que no deberá: (i) Vender Datos Personales; (ii) retener, usar o divulgar Datos Personales para ningún fin, ya sea comercial o no, que no sea el cumplimiento de sus obligaciones en virtud del Acuerdo Maestro; ni (iii) retener, usar o divulgar Datos Personales fuera de la relación comercial directa entre Hitachi y el Proveedor. Mediante la celebración del Acuerdo Maestro, el Proveedor certifica que comprende y que cumplirá con los términos de este Artículo 3(m).

(o) El Proveedor deberá suprimir los Datos Personales una vez cumplida la relación jurídica con Hitachi o por instrucciones de Hitachi, siempre y cuando no exista una previsión legal que exija la conservación de los Datos Personales.

**4. Solicitudes de la Persona a la que se Refieren los Datos**

(a) En caso de que el Proveedor reciba una solicitud del interesado en relación con los Datos Personales, el Proveedor deberá enviar todos los detalles relacionados con dicha solicitud a Hitachi a privacy@hitachivantara.com dentro del plazo de cuarenta y ocho (48) horas desde el momento en que reciba dicha solicitud. El Proveedor no deberá responder a ninguna solicitud del interesado en relación con los Datos Personales.

(b) A menos que las Partes acuerden de otro modo por escrito, el Proveedor deberá, sin costo adicional para Hitachi, cumplir con las solicitudes razonables de Hitachi en relación con el cumplimiento de Hitachi de las Leyes de Protección de Datos aplicable y la manipulación de solicitudes del interesado de Hitachi en relación con los Datos Personales. Esto incluye, pero no se limita a la

cooperación del Proveedor con Hitachi para abordar reclamos de privacidad y cumplir con las solicitudes legales de aquellas personas a las que se refieren los datos en relación con los Datos Personales.

**5. Sub-Procesamiento**

(a) El Proveedor no deberá subcontratar ninguna de sus obligaciones en virtud de este DPA sin previo consentimiento escrito de Hitachi.

(b) Al menos 30 días antes de contratar a un nuevo Subprocessador, el Proveedor deberá enviar a Hitachi una "**Solicitud de subprocessador**" que describa en detalle: (i) el Subprocessador previsto, (ii) el alcance de los servicios y obligaciones a subcontratar, (iii) las categorías de Datos Personales que deberá procesar el Subprocessador previsto y (iv) el método por el cual el Subprocessador accedería o recibiría los Datos Personales. El Proveedor deberá responder de inmediato a cualquier solicitud de Hitachi de información adicional acerca del Subprocessador previsto.

(b) Hitachi podrá, dentro del término de 30 días a partir de la recepción de dicha Solicitud, notificar al Proveedor de su objeción respecto del nuevo Subprocessador. La objeción respecto de cualquier nuevo Subprocessador es por cuenta de Hitachi solamente, sin necesidad de ofrecer justificación alguna. En la medida en que Hitachi objete a un nuevo Subprocessador, las Partes deberán, de buena fe, intentar encontrar una resolución mutuamente aceptable dentro del término de 30 días a partir de la objeción de Hitachi. En caso de que Hitachi no objete al nuevo Subprocessador dentro del período de 30 días mencionado en esta Sección, el Proveedor podrá considerar que Hitachi no posee objeciones respecto del nuevo Subprocessador.

(b) En la medida en que el Proveedor contrate Subprocesadores, lo hará solo mediante acuerdo escrito con el Subprocessador en términos que no sean menos restrictivos para el Subprocessador que aquellos impuestos para el Proveedor en virtud de este DPA. En todo momento, el Proveedor será plenamente responsable ante Hitachi por el desempeño del Subprocessador.

(c) Sin perjuicio de cualquier otra disposición en este DPA, el Proveedor acuerda que no designará a ningún Subprocessador si el Proveedor no está satisfecho con motivos fundados de que el Subprocessador protege los datos Personales con medidas de seguridad técnicas y organizativas que sean tengan como mínimo una naturaleza de protección idéntica a las Medidas Mínimas de Protección. El Proveedor deberá tomar todas las medidas a fin de garantizar que el Subprocessador emplee dichas medidas de seguridad técnicas y organizativas durante cualquier Procesamiento de Datos Personales.

**6. Evento de Infracción de Seguridad**

(a) En caso de cualquier Infracción de Seguridad, el Proveedor deberá notificar a Hitachi tanto a privacy@hitachivantara.com como a cybersecurity@hitachivantara.com dentro del plazo de 24 (veinticuatro) horas del Descubrimiento de la Infracción de Seguridad, incluyendo toda información pertinente que el Proveedor conozca o deba de manera razonable conocer. Dentro del término de 5 (cinco) días hábiles desde el Descubrimiento, el Proveedor deberá entregar a Hitachi un informe escrito donde incluya como mínimo los siguientes detalles, en la medida en que el Proveedor los conozca o deba razonablemente conocer: (i) Descripción del Evento de Infracción de Seguridad y la naturaleza del incidente; (ii) fecha de ocurrencia del Evento de Infracción de Seguridad; (iii) Fecha de Descubrimiento del Evento de Infracción de Seguridad; (iv) la identidad y última dirección de correo conocida de los individuos afectados; (v) las categorías afectadas de los Datos Personales para cada individuo o categoría de Información Confidencial; (vi) una descripción de las acciones implementadas a la fecha o que de otro modo deban implementarse, para responder, manejar o de otro modo mitigar cualquier impacto del Evento de Infracción de Seguridad y los detalles de la persona o entidad que ha tomado dichas acciones, las tomará o debería hacerlo; (vii) una identificación de cualquier agencia de aplicación legal contactada acerca del Evento de Infracción de Seguridad e información de contacto de cualquier funcionario pertinente; (viii) una descripción de todas las medidas que han sido adoptadas o serán adoptadas para evitar la recurrencia y los detalles de la persona o entidad que ha tomado dichas medias, las tomará o debería hacerlo, e (ix) información de contacto del individuo responsable de responder frente al Evento de Infracción de Seguridad. El Proveedor deberá actualizar el informe escrito cada vez que Descubra alguna información nueva y relevante.

(b) En caso de que un Evento de Infracción de Seguridad resulte de los actos u omisiones del Proveedor o los actos u omisiones del personal o agentes del Proveedor, el Proveedor deberá reembolsar de inmediato a Hitachi todos los costos en los que Hitachi incurra de manera razonable en relación con el Evento de Infracción de Seguridad, incluyendo, pero no limitado a los servicios de notificación y control crediticia.

(c) Cada Parte acuerda cooperar en cualquier investigación del Evento de Infracción de Seguridad realizada o en el que participe la otra Parte y tomar todas las medidas razonables a fin de mitigar los efectos nocivos de cualquier Evento de Infracción de Seguridad del que dicha Parte tenga conocimiento.

**7. Responsabilidad e Indemnización**

(a) El Proveedor será responsable y deberá indemnizar a Hitachi y a su personal, directores, agentes o afiliadas (en conjunto, "**Indemnización del Cliente**") respecto de cualquier responsabilidad, pérdida, daño, multas, costos, costos legales, gastos profesionales o de otra naturaleza en los que incurra un Indemnización del Cliente que surja de: (i) el incumplimiento con las

disposiciones de este DPA o (ii) incumplimiento de cualquier Ley de Protección de Datos aplicable por parte del Proveedor (o sus agentes o subprocesadores).

(b) El Proveedor será responsable y deberá indemnizar a los Indemnización del Cliente respecto de cualquier responsabilidad, daño, pérdida, multa, costos o cualquier otro gasto en lo que incurra un Indemnizado del Cliente en relación con un Evento de Infracción de Seguridad. Dicha indemnización deberá incluir, pero no se limitará al costo de notificación de la Infracción de Seguridad y a todos los servicios ofrecidos junto a la notificación de la Infracción de Seguridad.

**8. Terminación**

(a) El Proveedor deberá, a elección razonable de Hitachi, devolver o destruir de inmediato los Datos Personales Procesados en nombre de Hitachi al final del Término. En caso de que Hitachi solicite al Proveedor destruir los Datos Personales, el Proveedor deberá, dentro del período de treinta (30) días de la solicitud de Hitachi, certificar por escrito que (i) destruyó los Datos Personales de manera tal que los mismos son ilegibles y (ii) confirmó que los Subprocesadores han hecho lo mismo.

(b) A menos que se acuerde de otro modo por escrito entre las Partes, dicha devolución o destrucción deberá completarse dentro del plazo de diez (10) días a partir de la fecha de finalización del Término.

**9. Disposiciones Varias**

(a) La invalidez o inaplicabilidad de cualquier parte de este DPA por cualquier motivo no afectará la validez o aplicabilidad de las secciones restantes.

(b) Excepto tal como lo permita la Cláusula 5 de este DPA, el Proveedor no deberá transferir sus obligaciones en virtud de este DPA sin el previo consentimiento escrito de Hitachi.

(c) Este DPA, junto con el Acuerdo Maestro, constituye el acuerdo y entendimiento total entre las Partes respecto de su asunto y reemplaza todo acuerdo o entendimiento anterior entre las Partes en relación con dicho asunto. En caso de conflicto o inconsistencia entre los términos de este DPA y aquellos del Acuerdo Maestro, los términos de este DPA prevalecerán en el alcance de dicho conflicto. Este DPA no podrá modificarse excepto por escrito firmado por ambas Partes.

(d) Este DPA se celebra para el beneficio de los individuos cuyos Datos Personales sean Procesados por el Proveedor y todo dicho individuo por el presente tendrá derecho a aplicar este DPA como tercero beneficiario.

**FIRMADO A MODO DE ACUERDO:**

EN FE DE LO CUAL, las Partes han firmado este DPA a través de sus respectivos representantes autorizados a la fecha antes indicada.

| **HITACHI VANTARA S.A. de C.V.** | **PROVEEDOR** |
|---|---|
| Por | Por |
| Nombre | Nombre |
| Puesto | Puesto |
| Fecha | Fecha |

**ANEXO 1**
**AL ACUERDO DE PROTECCIÓN DE DATOS**

**Decisión de la Comisión C (2010)593**
**Cláusulas Contractuales Estándares (procesadores)**

Para los fines del Artículo 26(2) de la Directiva 95/46/EC para la transferencia de datos personales a procesadores establecidos en otros países que no garantizan un nivel adecuado de protección de datos

Nombre de la organización exportadora de datos: Hitachi Vantara S.A. de C.V.

Correo electrónico: privacy@hitachivantara.com

Otra información necesaria para identificar a la organización:

N/A
(el **exportador de datos**)

Y

Nombre de la organización importadora de datos: _____

Domicilio:.....

Tel.:.....; fax: ..... ; correo electrónico:.....

Otra información necesaria para identificar a la organización:

.....
(El **importador de datos**)

Cada una la "parte"; juntos "las partes",

HAN ACORDADO las siguientes Cláusulas Contractuales (las Cláusulas) a fin de aducir garantías adecuadas respecto de la protección de los derechos fundamentales y privacidad y las libertades de los individuos para la transferencia realizada por la exportadora de datos a la importadora de datos de los datos personales especificados en el Apéndice 1.

*Cláusula 1*

***Definiciones***

Para los fines de las Cláusulas:

(a) *'datos personales', 'categorías especiales de datos', 'procesar/procesamiento', 'controlador', 'procesador', 'personas a las que se refieren los datos'* y *'autoridad de supervisión'* tendrán el mismo significado que se les asigna en la Directiva 95/46/EC del Parlamento Europeo y del Consejo del 24 de octubre de 1995 sobre la protección de los individuos respecto del procesamiento de datos personales y el movimiento libre de dichos datos[1];

(b) '*el exportador de datos'* se refiere al controlador que transfiere los datos personales;

(c) *'el importador de datos'* se refiere al procesador que acuerda recibir del exportador de datos los datos personales que se procesarán en su nombre después de la transferencia de conformidad con sus instrucciones y los términos de las Cláusulas y quién está sujeto al sistema de un país tercero asegurando la adecuada protección dentro del significado del Artículo 25(1) de la Directiva 95/46/EC;

(d) *'el subprocessador'* se refiere a cualquier procesador contratado por el importador de datos o por cualquier otro subprocessador del importador de datos que acuerda recibir del importador de datos o de cualquier otro subprocessador del importador de datos los datos personales exclusivamente diseñados para las actividades de procesamiento a ser realizadas en nombre del explorador de datos después de la transferencia de conformidad con sus instrucciones, los términos de las Cláusulas y los términos del subcontrato escrito;

(e) '*ley de protección de datos aplicable'* se refiere a ley que protege los derechos y libertades fundamentales de los individuos y, en particular, sus derechos a la privacidad con respecto al procesamiento de datos personales aplicable a un controlador de datos en los Estados Miembro en los que el exportador de datos se encuentra establecido;

(f) *"medidas de seguridad técnicas y organizativa"* se refieren a aquellas medidas tendientes a proteger los datos personales de destrucción accidental o ilegal o pérdida, alteración accidental, divulgación o acceso no autorizado, en particular cuando el procesamiento implique la transmisión de datos a través de una red y contra cualquier otra forma ilegal de procesamiento.

*Cláusula 2*

***Detalles de la transferencia***

Los detalles de la transferencia y en particular las categorías especiales de datos personales cuando corresponda se especifican en el Apéndice 1, que forma parte integral de las Cláusulas.

*Cláusula 3*

***Cláusula de tercero beneficiario***

1. La persona a la que se refiere los datos puede aplicar contra el exportador de datos esta Cláusula, la Cláusula 4(b) a (i), la Cláusula 5(a) a (e) y (g) a (j), la Cláusula 6(1) y (2), la Cláusula 7, la Cláusula 8(2) y las Cláusulas 9 a 12 como tercero beneficiario.

2. La persona a la que se refieren los datos puede aplicar contra el importador de datos esta Cláusula, la Cláusula 5(a) a (e) y (g), la Cláusula 6, la Cláusula 7, la Cláusula 8(2) y las Cláusulas 9 a 12, en casos en que el exportador de datos ha realmente desaparecido o ha dejado de existir según la ley a menos que cualquier entidad sucesoria haya asumido todas las obligaciones legales del exportador de datos mediante contrato o aplicación de la ley, como resultado de lo cual asume los derechos y las obligaciones del exportador de datos, en cuyo caso la persona a la que se refieren los datos podrá aplicarlas contra dicha entidad.

[1] Las Partes pueden reproducir las definiciones y significados contenidas en la Directiva 95/46/EC dentro de esta Cláusula en caso de que consideren que benefician la independencia del contrato.

3. La persona a la que se refieren los datos puede aplicar contra el subprocessador esta Cláusula, la Cláusula 5(a) a (e) y (g), la Cláusula 6, la Cláusula 7, la Cláusula 8(2) y las Cláusulas 9 a 12, en caso de que tanto el exportador de datos como el importador de datos hayan realmente desaparecido o dejado de existir según la ley o se hayan declarado insolvente, a menos que un sucesor haya asumido la totalidad de las obligaciones legales del exportador de datos por contrato o por ley como resultado de lo cual asume los derechos y obligaciones del exportador de datos, en cuyo caso la persona a la que se refieren los datos podrá aplicarlas contra dicha entidad. La responsabilidad civil del subprocessador se limitará a sus propias operaciones de procesamiento en virtud de las Cláusulas.

4. Las partes no se oponen a que una persona a la que se refieren los datos sea representada por una asociación u otro organismo en caso de que la persona a la que se refieren los datos así desee expresamente y en caso de que esté permitido por la ley nacional.

*Cláusula 4*

***Obligaciones del exportador de datos***

El exportador de datos acuerda y garantiza:

(a) que el procesamiento, incluyendo la propia transferencia, de los datos personales ha sido y seguirá siendo llevado a cabo de conformidad con las disposiciones pertinentes de la ley de protección de datos aplicable (y, cuando corresponda, ha sido notificado a las autoridades pertinentes de los Estados Miembro donde el exportador de datos se encuentra establecido) y no viola las disposiciones pertinentes del Estado;

(b) que ha instruido y a lo largo de la duración de los servicios de procesamiento de datos personales instruirá al importador de datos que procese los datos personales transferidos solo en nombre del exportador de datos y de conformidad con la ley de protección de datos y las Cláusulas aplicables;

(c) que el importador de datos brindará garantías suficientes respecto de las medidas de seguridad técnica y organizativa especificada en el Apéndice 2 de este contrato;

(d) que después de la evaluación de los requerimientos de la ley de protección de datos aplicable, las medidas de seguridad resultan apropiadas para proteger los datos personales contra la destrucción accidental o ilegal, o la pérdida accidental, alteración, divulgación o acceso no autorizado, en particular cuando el procesamiento implique la transmisión de datos a través de una red y contra toda otra forma ilícita de procesamiento y que estas medidas garantizan un nivel de seguridad apropiado según los riesgos presentados por el procesamiento y la naturaleza de los datos a proteger teniendo en cuenta las posibilidades técnicas más recientes y el costo de su implementación;

(e) que asegurará el cumplimiento de las medidas de seguridad;

(f) que, en caso de que la transferencia incluya categorías especiales de datos, el sujeto al que pertenecen los datos ha sido informado o será informado antes, o tan pronto sea posible después de la transferencia que sus datos podrían transmitirse a otro país que no ofrece una protección adecuada dentro del significado de la Directiva 95/46/EC;

(g) enviar cualquier notificación que reciba del importador de datos o de cualquier subprocessador de conformidad con la Cláusula 5(b) y la Cláusula 8(3) a la autoridad supervisora de protección de datos en caso de que el exportador de datos decida continuar la transferencia o levantar la suspensión;

(h) poner a disposición de las personas a las que se refieren los datos, previa solicitud, una copia de las Cláusulas con las excepciones establecidas en el Apéndice 2 y una breve descripción de las medidas de seguridad, así como también una copia de cualquier contrato para servicios de subprocesamiento que se haya celebrado de conformidad con las Cláusulas a menos que las cláusulas o el contrato contengan información comercial, en cuyo caso se puede eliminar dicha información comercial;

(i) que, en caso de subprocesamiento, la actividad de procesamiento se lleva a cabo de conformidad con la Cláusula 11 a través de un subprocessador que brinde como mínimo el mismo nivel de protección para los datos personales y los derechos de la persona a la que se refieren los datos que el importador de datos en virtud de las Cláusulas y

(j) que asegurará el cumplimiento de la Cláusula 4(a) a (i).

*Cláusula 5*

***Obligaciones del importador de datos[2]***

El importador de datos acuerda y garantiza:

(a) procesar los datos personales solo en nombre del exportador de datos y en cumplimiento con sus instrucciones y las Cláusulas; en caso de no poder ofrecer dicho cumplimiento por cualquier motivo, acuerda informar de inmediato al exportador de datos respecto de su incapacidad de cumplir, en cuyo caso el exportador de datos tendrá derecho a suspender la transferencia de datos y/o terminar el contrato;

(b) que no posee motivos para creer que la legislación aplicable impide el cumplimiento de las instrucciones recibidas del exportador de datos y sus obligaciones en virtud del contrato y que en caso de un cambio en esta legislación que probablemente tenga un efecto adverso importante sobre las garantías y obligaciones estipuladas en las Cláusulas, notificará de inmediato el cambio al exportador de datos tan pronto tome conocimiento del mismo, en cuyo caso el exportador de datos tendrá la facultad de suspender la transferencia de datos y/o terminar el contrato;

(c) que ha implementado las medidas de seguridad técnicas y organizativas especificadas en el Apéndice 2 antes de procesar los datos personales transferidos;

(d) que notificará de inmediato al exportador:

(i) cualquier solicitud jurídicamente vinculante de divulgación de los datos personales por parte de una autoridad de aplicación a menos que de otro modo esté prohibido, tal como una prohibición de acuerdo con el derecho penal de preservar la confidencialidad de una investigación de cumplimiento con la ley,

(ii) cualquier acceso accidental o no autorizado, y

(iii) cualquier solicitud que reciba directamente de las personas a las que se refieran los datos sin responder a dicha solicitud, a menos que esté de otro modo autorizado a hacerlo;

(e) dar inmediata y adecuada respuesta a todas las consultas del exportador de datos en relación con su procesamiento de los datos personales a transferir y cumplir con la recomendación de la autoridad de supervisión respecto del procesamiento de los datos transferidos;

(f) a solicitud del exportador de datos someter sus instalaciones de procesamiento de datos a auditoría de las actividades de procesamiento contempladas en las cláusulas, la cual la llevará a cabo el exportador de datos o un organismo de inspección compuesto por miembros independientes y que posea calificaciones profesionales obligados al deber de confidencialidad, seleccionado por el exportador de datos, cuando corresponda, en acuerdo con la autoridad de supervisión;

(g) poner a disposición de la persona a la que se refieren los datos, previa solicitud, una copia de las cláusulas, o cualquier contrato existente de subprocesamiento, a menos que las Cláusulas o el contrato contengan información comercial, en cuyo caso se podrá eliminar dicha información comercial, con excepción del Apéndice 2 que será reemplazado por una breve descripción de las medidas de seguridad en aquellos casos en los que la persona a la que se refieren los datos no pueda obtener una copia del exportador de datos;

(h) que, en caso de subprocesamiento, ha informado previamente al exportador de datos y ha obtenido su consentimiento previo escrito;

(i) que los servicios de procesamiento prestados por el subprocessador se llevarán a cabo en virtud de la Cláusula 11;

(j) que enviará de inmediato copia de cualquier acuerdo de subprocesamiento que incluya en virtud de las Cláusulas al exportador de datos.

---

[2] Los requerimientos obligatorios de la legislación nacional aplicables al importador de datos que no exceden lo que es necesario en una sociedad democrática en base a uno de los intereses enumerados en el Artículo 13(1) de la Directiva 95/46/EC, que es, en caso de constituir una medida necesaria para salvaguardar la seguridad nacional, la defense, la seguridad pública, la prevención, la investigación, detección y procesamiento de acciones penales o de incumplimientos con la ética de profesiones reguladas, un importante interés económico o financiero del Estado o la protección de los sujetos a los que pertenecen los datos o los derechos y libertades de otros, no contradigan las cláusulas contractuales estándares. Algunos ejemplos de dichos requerimientos obligatorios que no exceden lo necesario en una sociedad democrática son sanciones de reconocimiento internacional, requerimientos de informes impositivos y requerimientos de informes de eventos contra el lavado de dinero.

*Cláusula 6*

***Responsabilidad***

1. Las partes acuerdan que toda persona a la que pertenecen los datos, que haya sufrido algún daño como resultado de cualquier violación a las obligaciones a las que se refiere la Cláusula 3 o la Cláusula 11 debido a cualquiera de las partes o al subprocessador tendrá derecho de recibir una compensación del exportador de datos por el daño sufrido.

2. En caso de que la persona a la que se refieren los datos no sea capaz de entablar una demanda de compensación de conformidad con el párrafo 1 contra el exportador de datos, que surja de un incumplimiento del importador de datos o su subprocessador de cualquiera de sus obligaciones detalladas en la Cláusula 3 o en la Cláusula 11, debido a que el exportador de datos ha realmente desaparecido o ha cesado de existir jurídicamente o ser insolvente, el importador de datos acuerda que la persona a la que se refieren los datos podrá entablar una demanda en su contra como si fuera el exportador de datos, a menos que cualquier entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos en virtud de contrato o por ley, en cuyo caso la persona a la que se refieren los datos podrá exigir sus derechos a dicha entidad.

   El importador de datos no podrá basarse en el incumplimiento de las obligaciones de un subprocessador a fin de eludir sus propias responsabilidades.

3. En caso de que la persona a la que pertenecen los datos no pueda interponer contra el exportador de datos o el importador de datos la demanda a que se refieren los apartados 1 y 2, por incumplimiento por parte del subprocessador de sus obligaciones impuestas en la cláusula 3 o en la cláusula 11, por haber desaparecido de facto, cesado de existir jurídicamente o ser insolventes ambos, tanto el exportador de datos como el importador de datos, el subprocessador acepta que la persona a la que pertenecen los datos podrá demandarlo en cuanto a sus propias operaciones de tratamiento de datos como si fuera el exportador de datos o del importador de datos, a menos que cualquier entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos o del importador de datos en virtud de contrato o por ley, en cuyo caso la persona a la que pertenecen los datos podrá exigir sus derechos a dicha entidad. La responsabilidad del subprocessador se limitará a sus propias operaciones de tratamiento de datos de acuerdo con las presentes cláusulas.

*Cláusula 7*

***Mediación y jurisdicción***

1. El importador de datos acuerda que, si la parte a la que pertenecen los datos invoca en su contra derechos de tercero beneficiario o reclama una indemnización por daños y perjuicios de acuerdo con las cláusulas, aceptará la decisión de la dicha parte de:

   a) someter el conflicto a mediación mediante una persona independiente o, si procede, la autoridad de control;

   b) someter el conflicto a los tribunales del Estado miembro donde el exportador de datos se encuentra establecido.

2. Las partes acuerdan que las opciones de la persona a la que pertenecen los datos no obstaculizarán sus derechos sustantivos o de procedimiento a obtener reparación de conformidad con otras disposiciones de Derecho nacional o internacional.

*Cláusula 8*

***Cooperación con autoridades de control***

1. El exportador de datos acuerda depositar una copia del presente contrato ante la autoridad de control si así lo requiere o si el depósito es exigido por la legislación de protección de datos aplicable.

2. Las partes acuerdan que la autoridad de control está facultada para auditar al importador de datos, o a cualquier subprocessador, que tenga la misma medida y condiciones en que lo haría respecto del exportador de datos conforme a la legislación de protección de datos aplicable.

3. El importador de datos informará de inmediato al exportador de datos en caso de que la legislación existente aplicable a él o a cualquier subprocessador no permita auditar al importador de datos ni a los subprocesadores, de acuerdo con el apartado 2. En tal caso, el importador de datos estará autorizado a adoptar las medidas previstas en la cláusula 5 (b).

*Cláusula 9*

***Legislación aplicable***

Las cláusulas se regirán por las leyes del Estado Miembro donde el exportador de datos se encuentre establecido.

*Cláusula 10*

***Variación del contrato***

Las partes se comprometen a no variar ni modificar las cláusulas. Esto no excluye que las partes añadan cláusulas relacionadas con sus negocios en caso de que las mismas no contradigan a las cláusulas.

*Cláusula 11*

***Subprocesamiento***

1. El importador de datos no subcontratará ninguna de sus operaciones de procesamiento llevadas a cabo en nombre del exportador de datos de acuerdo con las cláusulas sin previo consentimiento por escrito del exportador de datos. Si el importador de datos subcontrata sus obligaciones de acuerdo con las cláusulas, con el consentimiento del exportador de datos, lo hará exclusivamente mediante un acuerdo escrito con el subprocessador, en el que se le impongan a este las mismas obligaciones impuestas al importador de datos de acuerdo con las cláusulas[3]. En los casos en que el subprocessador no pueda cumplir sus obligaciones de protección de los datos de conformidad con dicho acuerdo escrito, el importador de datos seguirá siendo plenamente responsable frente al exportador de datos del cumplimiento de las obligaciones del subprocessador según dicho acuerdo.

2. El contrato escrito previo entre el importador de datos y el subprocessador contendrá asimismo una cláusula de tercero beneficiario, tal como se establece en la cláusula 3, para los casos en que la parte a la que pertenecen los datos no pueda interponer la demanda de indemnización a que se refiere el apartado 1 de la cláusula 6 contra el exportador de datos o el importador de datos por haber estos desaparecido de facto, cesado de existir jurídicamente o ser insolventes, y ninguna entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos o del importador de datos en virtud de un contrato o por ley. Dicha responsabilidad civil del subprocessador se limitará a sus propias operaciones de tratamiento de datos de acuerdo con las cláusulas.

3. Las disposiciones relacionadas a aspectos de protección de datos en caso de subcontratación de operaciones de procesamiento a que se refiere el apartado 1 se regirán por la legislación del Estado miembro de establecimiento en el que el exportador de datos se encuentra establecido.

4. El exportador de datos deberá conservar una lista de los acuerdos de subprocesamiento celebrados en virtud de las cláusulas notificados por el importador de datos de conformidad con la Cláusula 5 (j), cuya lista se actualizará al menos una vez al año. La lista estará a disposición de la autoridad de control de protección de datos del exportador de datos.

*Cláusula 12*

***Obligación después de la terminación de la prestación de los servicios de tratamiento de datos personales***

1. Las partes acuerdan que, una vez finalizada la prestación de los servicios de tratamiento de los datos personales, el importador y el subprocessador deberán, a criterio del exportador de datos, devolver todos los datos personales transferidos y sus copias, o destruir todos los datos personales y certificar esta circunstancia al exportador de datos, a menos que la legislación aplicable al importador de datos le impida devolver o destruir total o parcialmente los datos personales transferidos. En tal caso, el importador de datos garantiza que guardará la confidencialidad de los datos personales transferidos y que no volverá a procesar los datos personales transferidos.

2. El importador de datos y el subprocessador garantizan que, a pedido del exportador de datos y/o de la autoridad de control, pondrá a disposición sus instalaciones de procesamiento de datos para que se lleve a cabo la auditoría de las medidas mencionadas en el apartado 1.

[3] Este requisito podrá cumplirse en caso de que el subprocessador sea consignatario del contrato celebrado entre el exportador de datos y el importador de datos de acuerdo con la presente Decisión.

**En nombre del exportador de datos:**

Nombre (completo):

Puesto:

Domicilio:

Otra información necesaria para la obligatoriedad del contrato (si la hubiere):

Firma……..

(sello de la entidad)

**En nombre del importador de datos:**

Nombre (completo):

Puesto:

Domicilio:

Otra información necesaria para la obligatoriedad del contrato (si la hubiere):

Firma……..

(sello de la entidad)

HITACHI
Inspire the Next

**APÉNDICE 1 A LAS CLÁUSULAS CONTRACTUALES ESTÁNDARES**

Este Apéndice forma parte de las Cláusulas y debe ser completado y firmado por las partes.

Los Estados Miembro podrán completar o especificar, de acuerdo con sus procedimientos nacionales, cualquier información adicional que deba incluirse en este Apéndice.

**Exportador de datos**
El exportador de datos es (por favor, especificar brevemente sus actividades relacionadas con la transferencia):
El exportador de datos es Hitachi Vantara LLC o su afiliada, quien transferirá datos como exportador de datos al importador de datos de conformidad con las Cláusulas Contractuales Estándares.

**Importador de datos**
El importador de datos es (por favor, especificar brevemente las actividades relacionadas con la transferencia):
El importador de datos es una entidad legal que puede procesar datos como importador de datos de acuerdo con las Cláusulas Contractuales Estándares.

**Sujetos a los que se refieren los datos**
Los datos personales transferidos relacionados con las siguientes categorías de personas a los que se refieren los datos (por favor, especificar):
Los datos personales transferidos podrán relacionarse a [Insertar descripción de aquellos individuos cuyos datos personales sean procesados, por ejemplo, personal de Hitachi, clientes de Hitachi, proveedores de Hitachi, etc.].

**Categorías de datos**
Los datos personales transferidos relacionados con las siguientes categorías de datos (por favor, especificar):
Los datos personales transferidos podrán incluir [Insertar lista de categorías de datos personales a procesar].

**Categorías especiales de datos (si corresponde)**
Los datos personales transferidos se relacionan a las siguientes categorías de datos especiales (por favor, especificar):

**Operaciones de procesamiento**
Los datos personales transferidos estarán sujetos a las siguientes actividades básicas de procesamiento (por favor, especificar):
Los datos personales transferidos estarán sujetos a las actividades básicas de procesamiento de conformidad con las Cláusulas Contractuales Estándares, incluyendo, pero no limitado a la recolección, registro, organización, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación mediante transmisión, difusión o puesta a disposición de alguna otra manera, alineación o combinación, restricción, eliminación o destrucción.

EXPORTADOR DE DATOS

Nombre:……

Firma Autorizada……

IMPORTADOR DE DATOS

Nombre:……

Firma Autorizada……

HITACHI
Inspire the Next

**APÉNDICE 2 A LAS CLÁUSULAS CONTRACTUALES ESTÁNDARES**

Este Apéndice forma parte de las cláusulas y debe ser completado y firmado por las partes.

**Descripción de las medidas de seguridad técnica y organizativa implementadas por el importador de datos de conformidad con las Cláusulas 4(d) y 5(c) (o documento/legislación adjunta):**

Por favor, referirse al Anexo 2 al Acuerdo de Protección de Datos.

HITACHI
Inspire the Next

**ANEXO 2**
**AL ACUERDO DE PROTECCIÓN DE DATOS**

# REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

**1. Introducción**

Estos Requerimientos de Seguridad de la Información (los "**ISR**" (por sus siglas en inglés)) reflejan el acuerdo entre las Partes respecto de los estándares mínimos que el Proveedor deberá emplear durante todo el término del Acuerdo Maestro incluyendo las SOWs (encargos de trabajo) en virtud de este (en conjunto, el "**Acuerdo Maestro**").

**2. Definiciones**

A menos que se defina expresamente en este IRS, todos los términos en mayúscula tendrán el mismo significado que aquél asignado en el Acuerdo Maestro. En este ISR, los siguientes términos tendrán los siguientes significados:

**Datos de Hitachi:** todo Dato de Hitachi incluyendo, pero no limitado a los datos compartidos en virtud o en referencia al Acuerdo Maestro, Servicios, Entregables, procesos de facturación y comerciales. Los Datos de Hitachi incluyen los datos del Cliente de Hitachi.

**Sistemas de Hitachi:** toda red, sistema de computación, aplicaciones, servicios en nube de Hitachi que brinden acceso o almacenen, procesen o transmitan Datos de Hitachi.

**Entorno de Producción:** Sistemas del Proveedor utilizados para prestar Servicios o Entregables a Hitachi.

**Datos Restringidos de Hitachi:** Datos de Hitachi clasificados como Restringidos de Hitachi Vantara, incluyendo, pero no limitado a la información personal, propiedad intelectual, planes financieros y cualquier otra información confidencial.

**Sistemas del Proveedor**: Redes, sistemas de computación, aplicaciones y/o servicios en nube del Proveedor que brinden acceso, accedan, almacenen o transmitan Datos de Hitachi o accedan a Sistemas de Hitachi.

**Pruebas y Entorno de Desarrollo:** Sistemas del Proveedor utilizados con el fin de desarrollar y/o evaluar un servicio pero que no se utilicen directamente para prestar Servicios o Entregables a Hitachi o al Cliente de Hitachi.

**3. Requerimientos Generales**

(a) El Proveedor deberá mantener garantías organizativas, físicas y técnicas que cumplan o superen las mejores prácticas de la industria, por ejemplo, tal como se establece en las normas ISO/IEC 27001:2013/27002:2013 o NIST SP 800-53 y entregar a Hitachi una copia de la documentación sobre su sistema de seguridad de la información y prácticas siempre que se lo solicite.

(b) El Proveedor deberá mantener un programa de seguridad de la información bajo la supervisión de un Director de Seguridad de la Información (CISO) o un líder senior responsable de un programa efectivo para la seguridad de la información y que ejerza la supervisión necesaria y pertinente del Personal adecuado para mantener la confidencialidad, integridad, disponibilidad y seguridad de los Datos de Hitachi y los Sistemas de Hitachi.

(c) El Proveedor deberá brindar durante la vigencia del Acuerdo Maestro un Informe SOC 2 Tipo II o la certificación de la norma ISO/IEC 27001:2013 con la Declaración de Aplicabilidad asociada o una autenticación o certificación equivalente, de un tercero independiente que cubra su operación en relación con los Servicios o los Entregables.

**4. Gestión Independiente**

(a) El Proveedor deberá evaluar los riesgos de seguridad de la información asociados con servicios de terceros que sean importantes para la prestación de los Servicios o Entregables e identificar acciones correctoras para mitigar dichos riesgos. Los servicios de terceros existentes deberán ser monitoreados y evaluados de manera periódica a fin de controlar los riesgos de seguridad a la información y el Proveedor deberá tomar medidas para la mitigación de los riesgos.

(b) El Proveedor deberá divulgar por adelantado los nombres de los subcontratistas que pueden acceder, procesar, almacenar o transmitir los Datos de Hitachi.

**5. Seguridad del Personal**

(a) El Proveedor deberá asegurar que todo Personal que acceda a los Datos de Hitachi o a los Sistemas de Hitachi participen de una capacitación formal anual sobre concientización en seguridad de la información.

(b) El Proveedor deberá asegurar que todo el Personal con acceso a los Datos de Hitachi o a los Sistemas de Hitachi cuenten con la información sobre los requerimientos específicos sobre seguridad de la información relacionados a los Servicios o Entregables.

(c) El Proveedor deberá asegurar que todo el Personal con acceso a los Datos de Hitachi o a los Sistemas de Hitachi hayan participado de una verificación adecuada de antecedentes antes de acceder a los Datos de Hitachi y a los Sistemas de Hitachi.

(d) El Proveedor deberá asegurar que todo el Personal ha suscrito cláusulas de confidencialidad en sus ocntratos de trabajo.

**6. Access Control**

(a) El Proveedor deberá asegurar el acceso a los Datos de Hitachi, a los Sistemas de Hitachi y a los Sistemas del Proveedor pertinente múltiples niveles y técnicas que cumplan con los estándares y lineamientos de la industria sobre seguridad, tal como la combinación de identificadores únicos y contraseñas seguras.

(b) El acceso a los Datos de Hitachi se otorgará estrictamente en base a una necesidad comercial.

(c) El Proveedor deberá asegurar que todo el personal que se conecte de manera remota (desde fuera de las instalaciones del Proveedor) para acceder a los Datos de Hitachi, Sistemas de Hitachi u otros Sistemas pertinentes del Proveedor sean autenticados utilizando múltiples factores y VPN.

**7. Seguridad del Sistema**

El Proveedor deberá utilizar medios técnicos y de procedimiento para asegurar permanentemente los Sistemas del Proveedor, incluyendo, pero no limitado a:

(a) anti-malware, protección avanzada contra amenazas;

(b) firewalls, puerta de enlace segura, seguridad de acceso a redes, sistemas de prevención de intrusión (IPS), sistemas de detección de intrusión (IDS);

(c) securización y configuración de los Sistemas del Proveedor;

(d) exploración periódica de vulnerabilidad y corrección de vulnerabilidades proporcional a la severidad de las vulnerabilidades;

(e) parches de firmware, OS, middleware, aplicaciones para el último parche disponible;

(f) prueba de penetración de Sistemas de Seguridad que pueden accederse de manera externa por lo menos una vez por año; y

(g) registro, control y respuesta a eventos de seguridad de la información y condiciones anormales.

Hitachi se reserva el derecho a solicitar en cualquier momento las evidencias y auditorias destinadas a acreditar el cumplimiento de las obligaciones de seguridad indicadas en este numeral.

**8. Protección de Datos**

El Proveedor deberá asegurar que los siguientes controles técnicos y de procedimiento se encuentran vigentes para proteger los Datos de Hitachi a menos Hitachi apruebe por escrito con anterioridad de otro modo:

(a) Los Datos de Hitachi se almacenan y procesan física o lógicamente separados de los datos de otros clientes del Proveedor o separados de otros entornos del Proveedor.

(b) Los Datos de Hitachi se encuentran encriptados cuando estén en tránsito (transmitidos) utilizando métodos y protocolos de encriptación sólidos y seguros (en particular TLS 1.2 y superior).

(c) El acceso a los Datos de Hitachi y los Sistemas de Hitachi se otorga estrictamente sobre una base de necesidad de conocerlos y el acceso queda inmediatamente revocado cuando ya dicha necesidad deja de existir.

(d) El acceso programático a los Datos de Hitachi o los Sistemas de Hitachi está asegurado utilizando tokens o certificados de autenticación y los tokens o certificados se rotan periódicamente.

(e) Los Entornos de Producción son independientes de los Entornos de Prueba y Desarrollo y los datos de Hitachi son independientes. Las actividades de prueba y desarrollo no se realizan en los Entornos de Producción ni en los Datos de Hitachi almacenados en cualquier Entorno de Producción.

(f) Todo Dato de Hitachi utilizado para prueba o desarrollo se encuentra adecuadamente protegido, es decir, mediante el uso de datos de prueba solamente (no datos de producción) o enmascaramiento u ofuscación de los datos de producción.

(g) El acceso a los Datos de Hitachi se registra y los registros se mantienen por al menos 1 año.

(h) Los Datos Restringidos de Hitachi siempre se encuentran encriptados cuando se los almacena, incluyendo en un dispositivo de almacenamiento como copia de seguridad o cuando se lo almacena temporalmente durante el traslado utilizando métodos de encriptación seguros.

(i) No se almacenan Datos Restringidos de Hitachi en dispositivos extraíbles personales, tales como disco duro portátil, puertos USB, DVDs, etc.

(j) No se almacenan Datos Restringidos de Hitachi en servicios de nube de terceros sin la previa aprobación escrita de Hitachi.

(k) Los Datos de Hitachi y los Sistemas del Proveedor están protegidos para soportar Objetivo de Punto de Recuperación (RPO) y Objetivo de Tiempo de Recuperación (RTO) de los Entregables y los Servicios.

(l) Todos los Datos de Hitachi, incluyendo los dispositivos que contienen los Datos de Hitachi, deberán devolverse a Hitachi o declararse totalmente irrecuperables al término del Acuerdo Maestro o una SOW aplicable.

**9. Seguridad Física**

(a) El Proveedor deberá garantizar que solo Personal autorizado podrá almacenar, procesar o acceder a los Datos de Hitachi en un entorno seguro.

(b) El Proveedor deberá garantizar que solo Personal autorizado acceda y almacene todos los dispositivos que contengan Datos de Hitachi en un entorno seguro.

(c) El Proveedor deberá asegurar que los Sistemas del Proveedor solo puedan eliminarse o agregarse con autorización de la gerencia del proveedor.