CONTRATO DE TRATAMIENTO DE DATOS

Este Contrato de tratamiento de datos (el "Contrato") se suscribe entre Siemens Product Lifecycle Management Software Inc., también conocida como Siemens Industry Software (que en lo sucesivo se denominará "SISW") y el cliente, que ha manifestado la aceptación de los términos y las condiciones de este Contrato (el "Cliente"). SISW conserva el derecho de utilizar sus empresas afiliadas para ejercer cualquiera de los derechos y cumplir cualquiera de las obligaciones que se especifican en este Contrato. Por consiguiente, el término "SISW" tal y como se utiliza aquí, también puede referirse a empresas afiliadas que son propiedad de forma directa o indirecta o que están controladas de forma directa o indirecta por la empresa matriz de Siemens Product Lifecycle Management Software Inc. y que han sido autorizadas por Siemens Product Lifecycle Management Software Inc. para distribuir los servicios en la nube de SISW (el "Servicio en la nube").

El Cliente será el único responsable de determinar el tipo de los datos y las personas a los que afecta el tratamiento y deberá garantizar la legitimidad de dicho tratamiento por medio del servicio en la nube. El Cliente también será responsable de cualquier corrección, eliminación o bloqueo de datos personales que se realice mediante las funcionalidades ofrecidas por el servicio en la nube. El Cliente puede exportar y eliminar sus datos, incluidos datos personales, utilizando las funcionalidades ofrecidas por el servicio en la nube. Al finalizar este Contrato de tratamiento de datos, el Cliente tendrá 30 días para enviar una solicitud por escrito a SISW para que los datos del Cliente se pongan a disposición del Cliente para que pueda descargarlos. Tras el vencimiento de cualquier período estipulado por SISW en respuesta a dicha solicitud, cualquier dato restante del Cliente quedará sujeto a la eliminación y ya no estará disponible para el Cliente. SISW y el Cliente acuerdan que, dentro del ámbito del servicio en la nube, el derecho del Cliente a emitir instrucciones se ejercerá exclusivamente mediante el uso de las funcionalidades ofrecidas por el servicio en la nube. Las instrucciones adicionales referentes a los datos del Cliente requieren un contrato independiente por escrito entre SISW y el Cliente que incluya un acuerdo sobre cualquier importe que el Cliente tenga que pagar para poner en práctica dichas instrucciones. El Cliente se compromete a no cargar ni almacenar información médica protegida (IMP) en el servicio en la nube, a no ser que SISW y el Cliente hayan suscrito un contrato independiente por escrito que permita expresamente el almacenamiento de IMP en el servicio en la nube.

Al proporcionar el servicio en la nube, por lo que respecta al sistema de producción, SISW deberá cumplir las medidas técnicas y organizativas descritas en el Apéndice 2 del Anexo A de este Contrato de tratamiento de datos. Los sistemas que no sean de producción relacionados con el servicio en la nube pueden cumplir o no las medidas descritas en el Apéndice 2 del Anexo A. Además, SISW puede cambiar las medidas técnicas y organizativas aplicables al sistema de producción de vez en cuando, siempre que dichos cambios no afecten negativamente al nivel de protección que dichas medidas ofrecen de cualquier modo material. SISW restringirá la recopilación, el tratamiento o el uso de datos personales sin autorización por parte de sus empleados y solo empleará para el tratamiento de los datos personales del Cliente a personal que haya recibido formación específica de conformidad con los requisitos de protección de la privacidad de los datos.

SISW tendrá derecho a recurrir a subencargados de tratamiento de datos para la prestación del servicio en la nube. En la medida en que el acceso de los subencargados de tratamiento de datos a los datos personales del Cliente no puede excluirse, SISW proporcionará al Cliente si este la solicita una lista de dichos subencargados de tratamiento de datos y sus respectivas ubicaciones y actualizará dicha lista cuando sea necesario antes de otorgar acceso a cualquier subencargado de tratamiento de datos nuevo a los datos personales del Cliente. En caso que el Cliente se oponga de manera razonable a cualquier subencargado de tratamiento de datos nuevo, el Cliente deberá informar a SISW de dicha objeción y, si SISW insiste en recurrir a este subencargado de tratamiento de datos nuevo, tendrá derecho a rescindir este Contrato de tratamiento de datos por motivo justificado. En la medida en que la contratación de cualquier subencargado de tratamiento de datos implique una transferencia transfronteriza de datos personales, SISW procurará que dicho subencargado de tratamiento de datos mantenga un nivel adecuado de protección de los datos por lo que respecta a dichos datos personales.

SISW verificará frecuentemente el cumplimiento de las medidas técnicas y organizativas aplicables y, ante una petición razonable del Cliente, confirmará al Cliente que se cumplen las medidas técnicas y organizativas aplicables. En caso que el Cliente tenga motivos para creer que una confirmación emitida por SISW es errónea, el Cliente tendrá derecho a confirmar el cumplimiento de las medidas técnicas y organizativas programando una auditoría con SISW, sujeta a previo aviso razonable. Los gastos de dicha auditoría correrán por cuenta del Cliente.

SISW y el Cliente acuerdan que cualquier transferencia de datos personales del Cliente de países de la Unión europea a países fuera de la UE que la UE haya considerado que no tienen el nivel adecuado de protección de datos personales se realizará según las disposiciones de las cláusulas contractuales tipo de la UE, estipuladas en el Anexo A y plenamente incorporadas al presente documento. En caso de producirse un conflicto entre los términos de este Contrato de tratamiento de datos y los términos de las cláusulas contractuales tipo, prevalecerán las disposiciones de las cláusulas contractuales tipo. Las

cláusulas contractuales tipo se regirán por las leyes del estado miembro de la UE en que esté establecido el exportador de datos (tal como se define en el Anexo A).

Anexo A
Cláusulas contractuales tipo de la UE

A efectos del artículo 26, apartado 2, de la Directiva 95/46/CE para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países que no garanticen una adecuada protección de los datos.

por y entre

El Cliente o una empresa afiliada del Cliente establecida en la UE

(en lo sucesivo, el "**exportador de datos**")

y

Siemens Product Lifecycle Management Software Inc., también conocida como Siemens Industry Software, incluida cualquier empresa afiliada de propiedad directa o indirecta o controlada directa o indirectamente por la empresa matriz de Siemens Product Lifecycle Management Software Inc. y a las que Siemens Product Lifecycle Management Software Inc. haya concedido su autorización para tratar datos en su nombre

(en lo sucesivo, el "**importador de datos**")

cada una de ellas "la parte"; conjuntamente "las partes",

ACUERDAN las siguientes cláusulas contractuales (en lo sucesivo, las Cláusulas) con objeto de ofrecer garantías suficientes respecto de la protección de la vida privada y los derechos y libertades fundamentales de las personas para la transferencia por el exportador de datos al importador de datos de los datos personales especificados en el Apéndice 1.

Sección 1. Definiciones

A los efectos de las presentes Cláusulas:

(a) "datos personales", "categorías especiales de datos", "tratamiento", "responsable del tratamiento", "encargado del tratamiento", "interesado" y "autoridad de control" tendrán el mismo significado que en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos;

(b) por "exportador de datos" se entenderá el responsable del tratamiento que transfiera los datos personales;

(c) por "importador de datos" se entenderá el encargado del tratamiento que convenga en recibir del exportador datos personales para su posterior tratamiento en nombre de este, de conformidad con sus instrucciones y de los términos de las Cláusulas, y que no esté sujeto al sistema de un tercer país por el que se garantice la protección adecuada en el sentido del artículo 25, apartado 1, de la Directiva 95/46/CE;

(d) por "subencargado del tratamiento" se entenderá cualquier encargado del tratamiento contratado por el importador de datos o por cualquier otro subencargado de este que convenga en recibir del importador de datos, o de cualquier otro subencargado de este, datos personales exclusivamente para las posteriores actividades de tratamiento que se hayan de llevar a cabo en nombre del exportador de datos, de conformidad con sus instrucciones, los términos de las Cláusulas y los términos del contrato que se haya concluido por escrito;

(e) por "legislación de protección de datos aplicable" se entenderá la legislación que protege los derechos y libertades fundamentales de las personas y, en particular, su derecho a la vida privada respecto del tratamiento de los datos personales, aplicable al responsable del tratamiento en el Estado miembro en que está establecido el exportador de datos;

(f) por "medidas de seguridad técnicas y organizativas" se entenderán las destinadas a proteger los datos personales contra su destrucción accidental o ilícita o su pérdida accidental, su alteración, divulgación o acceso no autorizados, especialmente cuando el tratamiento suponga la transmisión de los datos por redes, o cualquier otra forma ilícita de tratamiento.

Sección 2. Detalles de la transferencia

Los detalles de la transferencia, en particular, las categorías especiales de los datos personales, quedan especificados si procede en el Apéndice 1, que forma parte integrante de las presentes Cláusulas.

Sección 3. Cláusula de tercero beneficiario

1. Los interesados podrán exigir al exportador de datos el cumplimiento de la presente Cláusula, las letras b) a i) de la Cláusula 4, las letras a) a e) y g) a j) de la Cláusula 5, los apartados 1 y 2 de la Cláusula 6, la Cláusula 7, el apartado 2 de la Cláusula 8 y las Cláusulas 9 a 12, como terceros beneficiarios.

2. Los interesados podrán exigir al importador de datos el cumplimiento de la presente Cláusula, las letras a) a e) y g) de la Cláusula 5, la Cláusula 6, la Cláusula 7, el apartado 2 de la Cláusula 8 y las Cláusulas 9 a 12, cuando el exportador de datos haya desaparecido de facto o haya cesado de existir jurídicamente, a menos que cualquier entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos en virtud de contrato o por ministerio de la ley y a resultas de lo cual asuma los derechos y las obligaciones del exportador de datos, en cuyo caso los interesados podrán exigirlos a dicha entidad.

3. Los interesados podrán exigir al subencargado del tratamiento de datos el cumplimiento de la presente Cláusula, las letras a) a e) y g) de la Cláusula 5, la Cláusula 6, la Cláusula 7, el apartado 2 de la Cláusula 8 y las Cláusulas 9 a 12, en aquellos casos en que ambos, el exportador de datos y el importador de datos, hayan desaparecido de facto o hayan cesado de existir jurídicamente o sean insolventes, a menos que cualquier entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos en virtud de contrato o por ministerio de la ley, a resultas de lo cual asuma los derechos y las obligaciones del exportador de datos, en cuyo caso los interesados podrán exigirlos a dicha entidad. Dicha responsabilidad civil del subencargado del tratamiento de datos se limitará a sus propias operaciones de tratamiento de datos con arreglo a las Cláusulas.

4. Las partes no se oponen a que los interesados estén representados por una asociación u otras entidades, si así lo desean expresamente y lo permite el Derecho nacional.

Sección 4. Obligaciones del exportador de datos

El exportador de datos acuerda y garantiza lo siguiente:

(a) el tratamiento de los datos personales, incluida la propia transferencia, ha sido efectuado y seguirá efectuándose de conformidad con las normas pertinentes de la legislación de protección de datos aplicable (y, si procede, se ha notificado a las autoridades correspondientes del Estado miembro de establecimiento del exportador de datos) y no infringe las disposiciones legales o reglamentarias en vigor en dicho Estado miembro;

(b) ha dado al importador de datos, y dará durante la prestación de los servicios de tratamiento de los datos personales, instrucciones para que el tratamiento de los datos personales transferidos se lleve a cabo exclusivamente en nombre del exportador de datos y de conformidad con la legislación de protección de datos aplicable y con las Cláusulas;

(c) el importador de datos ofrecerá garantías suficientes en lo que respecta a las medidas de seguridad técnicas y organizativas especificadas en el Apéndice 2 del presente contrato;

(d) ha verificado que, de conformidad con la legislación de protección de datos aplicable, dichas medidas resultan apropiadas para proteger los datos personales contra su destrucción accidental o ilícita o su pérdida accidental, su alteración, divulgación o acceso no autorizados, especialmente cuando el tratamiento suponga la transmisión de los datos por redes, o contra cualquier otra forma ilícita de tratamiento y que dichas medidas garantizan un nivel de seguridad apropiado a los riesgos que entraña el tratamiento y la naturaleza de los datos que han de protegerse, habida cuenta del estado de la técnica y del coste de su aplicación;

(e) asegurará que dichas medidas se lleven a la práctica;

(f) si la transferencia incluye categorías especiales de datos, se habrá informado a los interesados, o serán informados antes de que se efectúe aquella, o en cuanto sea posible, de que sus datos podrían ser transferidos a un tercer país que no proporciona la protección adecuada en el sentido de la Directiva 95/46/CE;

(g) enviará la notificación recibida del importador de datos o de cualquier subencargado del tratamiento de datos a la autoridad de control de la protección de datos, de conformidad con la letra b) de la Cláusula 5 y el apartado 3 de la Cláusula 8, en caso de que decida proseguir la transferencia o levantar la suspensión;

(h) pondrá a disposición de los interesados, previa petición de estos, una copia de las Cláusulas, a excepción del Apéndice 2, y una descripción sumaria de las medidas de seguridad, así como una copia de cualquier contrato para los servicios de subtratamiento de los datos que debe efectuarse de conformidad con las Cláusulas, a menos que las Cláusulas o el contrato contengan información comercial, en cuyo caso podrá eliminar dicha información comercial;

(i) que, en caso de subtratamiento, la actividad de tratamiento se llevará a cabo de conformidad con la Cláusula 11 por un subencargado del tratamiento que proporcionará por lo menos el mismo nivel de protección de los datos personales y los derechos de los interesados que el importador de datos en virtud de las presentes Cláusulas; y

(j) que asegurará que las letras a) a i) de la Cláusula 4 se lleven a la práctica.

Sección 5. Obligaciones del importador de datos

El importador de datos acuerda y garantiza lo siguiente:

(a) tratará los datos personales transferidos solo en nombre del exportador de datos, de conformidad con sus instrucciones y las Cláusulas. En caso de que no pueda cumplir estos requisitos por la razón que fuere, informará de ello sin demora al exportador de datos, en cuyo caso este estará facultado para suspender la transferencia de los datos o rescindir el contrato;

(b) no tiene motivos para creer que la legislación que le es de aplicación le impida cumplir las instrucciones del exportador de datos y sus obligaciones a tenor del contrato y que, en caso de modificación de la legislación que pueda tener un importante efecto negativo sobre las garantías y obligaciones estipuladas en las Cláusulas, notificará al exportador de datos dicho cambio en cuanto tenga conocimiento de él, en cuyo caso este estará facultado para suspender la transferencia de los datos o rescindir el contrato;

(c) ha puesto en práctica las medidas de seguridad técnicas y organizativas que se indican en el Apéndice 2 antes de efectuar el tratamiento de los datos personales transferidos;

(d) notificará sin demora al exportador de datos sobre:

(i) toda solicitud jurídicamente vinculante de divulgar los datos personales presentada por una autoridad encargada de la aplicación de ley a menos que esté prohibido, por ejemplo, por el Derecho penal para preservar la confidencialidad de una investigación llevada a cabo por una de dichas autoridades,
(ii) todo acceso accidental o no autorizado, y
(iii) toda solicitud sin respuesta recibida directamente de los interesados, a menos que se le autorice;

(e) tratará adecuadamente en los períodos de tiempo prescritos todas las consultas del exportador de datos relacionadas con el tratamiento que este realice de los datos personales sujetos a transferencia y se atendrá a la opinión de la autoridad de control en lo que respecta al tratamiento de los datos transferidos;

(f) ofrecerá a petición del exportador de datos sus instalaciones de tratamiento de datos para que se lleve a cabo la auditoría de las actividades de tratamiento cubiertas por las Cláusulas. Esta será realizada por el exportador de datos o por un organismo de inspección, compuesto por miembros independientes con las cualificaciones profesionales necesarias y sujetos a la confidencialidad, seleccionado por el exportador de datos y, cuando corresponda, de conformidad con la autoridad de control;

(g) pondrá a disposición de los interesados, previa petición de estos, una copia de las Cláusulas, o de cualquier contrato existente para el subtratamiento de los datos, a menos que las Cláusulas o el contrato contengan información comercial, en cuyo caso podrá eliminar dicha información comercial, a excepción del Apéndice 2 que será sustituido por una descripción sumaria de las medidas de seguridad, en aquellos casos en que el interesado no pueda obtenerlas directamente del exportador de datos;

(h) que, en caso de subtratamiento de los datos, habrá informado previamente al exportador de datos y obtenido previamente su consentimiento por escrito;

(i) que los servicios de tratamiento por el subencargado del tratamiento se llevarán a cabo de conformidad con la Cláusula 11;

(j) enviará sin demora al exportador de datos una copia de cualquier acuerdo con el subencargado del tratamiento que concluya con arreglo a las Cláusulas.

Sección 6. Responsabilidad

1. Las partes acuerdan que los interesados que hayan sufrido daños como resultado del incumplimiento de las obligaciones mencionadas en la Cláusula 3 o en la Cláusula 11 por cualquier parte o subencargado del tratamiento tendrán derecho a percibir una indemnización del exportador de datos por el daño sufrido.

2. En caso de que el interesado no pueda interponer contra el exportador de datos la demanda de indemnización a que se refiere el apartado 1 por incumplimiento por parte del importador de datos o su subencargado de sus obligaciones impuestas en la Cláusula 3 o en la Cláusula 11, por haber desaparecido de facto, cesado de existir jurídicamente o ser insolvente, el importador de datos acepta que el interesado pueda demandarle a él en el lugar del 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 ministerio de la ley, en cuyo caso los interesados podrán exigir sus derechos a dicha entidad.

El importador de datos no podrá basarse en un incumplimiento de un subencargado del tratamiento de sus obligaciones para eludir sus propias responsabilidades.

3. En caso de que el interesado 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 subencargado del tratamiento de datos 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 subencargado del tratamiento de datos acepta que el interesado pueda demandarle a él en cuanto a sus propias operaciones de tratamiento de datos en virtud de las Cláusulas en el lugar del 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 ministerio de la ley, en cuyo caso los interesados podrán exigir sus derechos a dicha entidad. La responsabilidad del subencargado del tratamiento se limitará a sus propias operaciones de tratamiento de datos con arreglo a las presentes Cláusulas.

Sección 7. Mediación y jurisdicción

1. El importador de datos acuerda que, si el interesado invoca en su contra derechos de tercero beneficiario o reclama una indemnización por daños y perjuicios con arreglo a las Cláusulas, aceptará la decisión del interesado de:

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

   (b) someter el conflicto a los tribunales del Estado miembro de establecimiento del exportador de datos.

2. Las partes acuerdan que las opciones del interesado no obstaculizarán sus derechos sustantivos ni procedimentales a obtener reparación de conformidad con otras disposiciones de Derecho nacional o internacional.

Sección 8. Cooperación con las 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, o a cualquier subencargado, en 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 sin demora al exportador de datos en el caso de que la legislación existente aplicable a él o a cualquier subencargado no permita auditar al importador de datos ni a los subencargados, con arreglo al apartado 2. En tal caso, el importador de datos estará autorizado a adoptar las medidas previstas en la letra b) de la Cláusula 5.

Sección 9. Legislación aplicable

Las Cláusulas se regirán por la legislación del Estado miembro de establecimiento del exportador de datos.

Sección 10. Variación del contrato

Las partes se comprometen a no variar ni modificar las presentes Cláusulas. Esto no excluye que las partes añadan cláusulas relacionadas con sus negocios en caso necesario siempre que no contradigan las Cláusulas.

Sección 11. Subtratamiento de datos

1. El importador de datos no subcontratará ninguna de sus operaciones de tratamiento llevadas a cabo en nombre del exportador de datos con arreglo a las Cláusulas sin previo consentimiento por escrito del exportador de datos. Si el

importador de datos subcontrata sus obligaciones con arreglo a las Cláusulas, con el consentimiento del exportador de datos, lo hará exclusivamente mediante un acuerdo por escrito con el subencargado del tratamiento de datos, en el que se le impongan a este las mismas obligaciones impuestas al importador de datos con arreglo a las Cláusulas. En los casos en que el subencargado del tratamiento de datos no pueda cumplir sus obligaciones de protección de los datos con arreglo a dicho acuerdo por escrito, el importador de datos seguirá siendo plenamente responsable frente al exportador de datos del cumplimiento de las obligaciones del subencargado del tratamiento de datos con arreglo a dicho acuerdo.

2. El contrato por escrito previo entre el importador de datos y el subencargado del tratamiento contendrá asimismo una cláusula de tercero beneficiario, tal como se establece en la Cláusula 3, para los casos en que el interesado 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 contrato o por ministerio de la ley. Dicha responsabilidad civil del subencargado del tratamiento de datos se limitará a sus propias operaciones de tratamiento de datos con arreglo a las Cláusulas.

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

4. El exportador de datos conservará la lista de los contratos de subtratamiento celebrados con arreglo a las Cláusulas y notificados por el importador de datos de conformidad con la letra j) de la Cláusula 5, lista que 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.

Sección 12. Obligaciones una vez finalizada la prestación de los servicios de tratamiento de los 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 subencargado deberán, a discreción del exportador, o bien devolver todos los datos personales transferidos y sus copias, o bien destruirlos por completo y certificar esta circunstancia al exportador, a menos que la legislación aplicable al importador le impida devolver o destruir total o parcialmente los datos personales transferidos. En tal caso, el importador de datos garantiza que guardará el secreto de los datos personales transferidos y que no volverá a someterlos a tratamiento.

2. El importador de datos y el subencargado garantizan que, a petición del exportador o de la autoridad de control, pondrán a disposición sus instalaciones de tratamiento de los datos para que se lleve a cabo la auditoría de las medidas mencionadas en el apartado 1.

APÉNDICE 1 A LAS CLÁUSULAS CONTRACTUALES TIPO

Exportador de datos
El exportador de datos es (especifique brevemente sus actividades correspondientes a la transferencia):

El Cliente es un suscriptor a un servicio en la nube proporcionado por SISW, que permite a los usuarios finales autorizados por el Cliente introducir, modificar, usar, eliminar, descargar y tratar de cualquier otro modo los datos del Cliente, entre los cuales puede haber datos personales, tal como se describe en el Contrato y en la documentación pertinente del servicio en la nube.

Importador de datos
El importador de datos es (especifique brevemente sus actividades correspondientes a la transferencia):

Siemens Product Lifecycle Management Software Inc., por sus propios medios o por medio de sus subencargados del tratamiento de datos, presta el servicio en la nube, que incluye: el mantenimiento en los Estados Unidos y en la Unión Europea de la infraestructura informática sobre la cual se presta el servicio en la nube; el almacenamiento en la infraestructura de los datos del Cliente cargados en el servicio en la nube por el Cliente; el control de la disponibilidad y el funcionamiento continuo del servicio en la nube y la infraestructura; y el mantenimiento de la seguridad de la infraestructura tal como se estipula en el Contrato y la documentación pertinente del servicio en la nube.

Interesados
Los datos personales transferidos se refieren a las siguientes categorías de interesados (especifíquense):

A menos que el exportador de datos lo especifique por escrito, entre los interesados pueden encontrarse usuarios finales autorizados por el Cliente para utilizar el servicio en la nube y otros empleados del Cliente cuyos datos personales estén almacenados en el servicio en la nube.

Categorías de datos
Los datos personales transferidos se refieren a las siguientes categorías de datos (especifíquense):

Las categorías de datos específicas que se deben almacenar en el servicio en la nube están sujetas a una configuración significativa por parte del Cliente, aunque algunas categorías comunes de datos que se pueden almacenar en el servicio en la nube son, por ejemplo, entre otras: nombre, dirección de correo electrónico, nombre de la empresa, número de teléfono, emplazamiento laboral, nacionalidad o ciudadanía, e información referente al acceso y al uso del servicio en la nube. Según la configuración del servicio en la nube del Cliente, podría haber muchas más categorías de datos en los datos de Cliente.

Categorías especiales de datos (si es pertinente)
Los datos personales transferidos se refieren a las siguientes categorías especiales de datos (especifíquense):

Cualquier categoría especial de datos que se tenga que almacenar en el servicio en la nube sería la acordada entre las partes en el Contrato o en un pedido, o la estipulada en un plan de trabajo para servicios profesionales a prestar al Cliente como parte de la implementación del servicio en la nube.

Operaciones de tratamiento
Los datos personales transferidos serán sometidos a las operaciones básicas de tratamiento siguientes (especifíquense):

Los datos personales pueden tratarse: como parte del funcionamiento normal del servicio en la nube, en función de la configuración del Cliente; por medio del almacenamiento o archivado en la infraestructura informática mantenida por el exportador de datos, en entornos de un solo usuario o de varios usuarios; accediendo a ellos o transmitiéndolos según las instrucciones emitidas al servicio en la nube por un usuario final autorizado por el Cliente para utilizar el servicio en la nube; y como parte de las operaciones de mantenimiento del servicio en la nube realizadas por el exportador de datos.

APÉNDICE 2 A LAS CLÁUSULAS CONTRACTUALES TIPO

Algunas ofertas de servicios en la nube se proporcionan conforme a distintos términos que, si procede, se estipularán en un pedido. De lo contrario, el importador de datos emprenderá las medidas técnicas y organizativas descritas a continuación por lo que respecta a los datos personales almacenados en el sistema, de conformidad con la letra d) de la Cláusula 4 y la letra c) de la Cláusula 5 de las Cláusulas.

Descripción de las medidas de seguridad técnicas y organizativas puestas en práctica por el importador de datos de conformidad con la letra d) de la Cláusula 4 y la letra c) de la Cláusula 5:

1. Control de acceso físico. Se impedirá a las personas no autorizadas obtener acceso físico a las instalaciones, los edificios o las salas donde se encuentren los sistemas de tratamiento de datos que realizan el tratamiento de datos personales o utilizan dichos datos.

   Medidas: Todos los centros de datos cumplen estrictos procedimientos de seguridad aplicados por personal de seguridad, equipos de vigilancia, detectores de movimiento, mecanismos de control de acceso y otras medidas para impedir que los equipos y las instalaciones de los centros de datos peligren. Solo los representantes autorizados tienen acceso a los sistemas y a la infraestructura de las instalaciones de los centros de datos. Para garantizar un funcionamiento adecuado, los equipos de seguridad físicos (por ejemplo, sensores de movimiento, cámaras, etc.) se someten periódicamente a tareas de mantenimiento. De forma detallada, en todos los centros de datos se ponen en práctica las siguientes medidas de seguridad físicas:

   a. En general, los edificios están protegidos mediante sistemas de control de acceso (sistema de acceso con tarjetas inteligentes).
   b. Se proporcionan al personal autorizado credenciales de autorización, entre las que figuran una tarjeta de acceso electrónico (exclusiva de cada empleado, proveedor o contratista), para permitirles acceder físicamente a las instalaciones de los centros de datos.
   c. El acceso físico a los centros de datos dentro de los límites del sistema se controla mediante un sistema de control de acceso electrónico, que consta de lectores de tarjetas y teclados de PIN para la entrada a los edificios y a las salas y lectores de tarjetas solo para la salida de los edificios y las salas.
   d. En función de la clasificación de seguridad, los edificios, las áreas individuales y las instalaciones circundantes también se protegen mediante medidas adicionales. Entre estas medidas se encuentran perfiles de acceso específicos, videovigilancia, sistemas de alarma contra intrusos y sistemas biométricos de control de acceso.
   e. Se otorgarán derechos de acceso al personal autorizado individualmente de acuerdo con las medidas de control de acceso al sistema y a los datos que se estipulan a continuación. Esto también se aplica al acceso a visitantes. Los invitados y los visitantes de los edificios de SISW tienen que registrar sus nombres en recepción y deben ir acompañados de personal autorizado de SISW. SISW y todos los proveedores de centros de datos externos registran los nombres y los tiempos de las personas que entran en las áreas privadas de SISW dentro de los centros de datos.
   f. Los empleados y el personal externo de SISW tienen que llevar sus tarjetas de identificación en todas las ubicaciones de SISW.

2. Control de acceso al sistema. Se debe impedir el uso sin autorización de los sistemas de tratamiento de datos utilizados para prestar el servicio en la nube.

   Medidas:
   a. SISW o sus subencargados de tratamiento gestionan el entorno para cumplir con NIST SP 800-53 Rev 4 Requisitos de Control de Acceso (AC) e Identificación y Autentificación (IA).
   b. Se utilizan diversos niveles de autorización para otorgar acceso a sistemas sensibles, incluidos los que almacenan y tratan datos personales. Se dispone de procesos para garantizar que solo los usuarios autorizados dispongan de la autorización apropiada para añadir, eliminar o modificar usuarios.
   c. Todos los usuarios acceden a los sistemas de SISW con un nombre de usuario y una contraseña exclusivos que deben cumplir ciertos criterios de complejidad mínimos.
   d. SISW y sus subencargadados del tratamiento de datos disponen de procedimientos para garantizar que los cambios de autorización solicitados solo se implementen de acuerdo con las directrices (por ejemplo, que no se otorguen derechos sin autorización). Si un usuario de SISW cambia de función o deja de trabajar en la empresa, se realiza un proceso para revocar los derechos de acceso al entorno.
   e. SISW y sus subencargados de tratamiento de datos han establecido una política de contraseñas que prohíbe el uso compartido de contraseñas, estipula qué se debe hacer si se revela una contraseña, exige cambios periódicos

de todas las contraseñas de los usuarios, y exige el cambio de las contraseñas predeterminadas. Se asignan ID de usuario personalizados para la autentificación. Todas las contraseñas tienen que cumplir requisitos de complejidad mínimos y almacenarse en un formato cifrado. En el caso de las contraseñas de dominio, el sistema fuerza un cambio de contraseña cada 60 días que cumple con los requisitos mínimos de complejidad. Cada ordenador de SISW tiene un protector de pantalla protegido por contraseña.

f. SISW o sus subencargados de tratamiento de datos auditan automáticamente los siguientes eventos relacionados con las cuentas: creación, modificación, activación, desactivación y eliminación. Un administrador del sistema revisa los registros periódicamente.
g. Las redes de SISW y sus subencargados de tratamiento de datos se protegen del Internet público mediante cortafuegos.
h. SISW y sus subencargados de tratamiento de datos utilizan software antivirus actualizado en los puntos de acceso a la red de la empresa, para las cuentas de correo electrónico y en todos los servidores de archivos y todas las estaciones de trabajo.
i. SISW y sus subencargados de tratamiento de datos implementan la gestión de parches de seguridad para garantizar la aplicación de las actualizaciones de seguridad pertinentes.
j. El acceso remoto completo a la red corporativa de SISW y a la infraestructura crítica está protegido mediante autentificación multifactor de alta seguridad.

3. Control de acceso a los datos. El personal autorizado para utilizar los sistemas de tratamiento de datos solo obtendrá acceso a los datos personales a los que tengan derecho a acceder, y los datos personales no se deben leer, copiar, modificar ni eliminar sin autorización durante el transcurso del tratamiento, el uso y el almacenamiento.

   Medidas:

   a. El acceso a información personal, confidencial o sensible se otorga según el principio de la necesidad de conocimiento. En otras palabras, los empleados o terceros tienen acceso a la información que necesitan para poder realizar su trabajo. SISW utiliza conceptos de autorización que documentan cómo se asignan las autorizaciones y qué autorizaciones se asignan. Todo los datos personales, confidenciales o sensibles se protegen de acuerdo con las políticas de seguridad y los estándares de SISW.
   b. Todos los servidores de producción de cualquier servicio en la nube de SISW se controlan en los centros de datos pertinentes. Las medidas de seguridad que protegen las aplicaciones que realizan el tratamiento de información personal, confidencial o sensible se comprueban frecuentemente. Con este fin, SISW también incorpora auditorías externas periódicas para confirmar que estas medidas se apliquen de la manera adecuada.
   c. SISW no permite la instalación de software personal o de otro tipo que no esté aprobado por SISW en los sistemas utilizados para cualquier servicio en la nube.
   d. Si hubiese una necesidad de transferir datos debido al fallo de soportes de almacenamiento de datos subyacentes, al finalizar dicha transferencia, el soporte de almacenamiento estropeado se deberá desmagnetizar (en el caso de los soportes de almacenamiento magnéticos) o destruir (en el caso de los soportes de almacenamiento de estado sólido u ópticos).

4. Control de transmisión de datos. Los datos personales no se deben leer, copiar, modificar ni eliminar sin autorización durante la transferencia.

   Medidas:

   a. SISW o sus subencargados de tratamiento de datos gestionarán la infraestructura y la configuración de modo que cumplan con NIST SP 800-53 Rev 4 Requisitos de los sistemas y de protección de las comunicaciones (SC). Esto incluye los sistemas de prevención de intrusos de red (NIPS) y los cortafuegos en los límites del sistema para protegerse contra comunicaciones malintencionadas en el límite exterior de la infraestructura. Los NIPS y los cortafuegos se configuran de acuerdo con las normas de DISA STIG. Los datos se cifran en tránsito mediante módulos criptográficos que cumplen con FIPS 140-2.
   b. Cuando los soportes de datos se transportan físicamente, se implementan medidas adecuadas en SISW para garantizar los niveles de servicio acordados (por ejemplo, cifrado y contenedores con revestimiento de plomo).
   c. La transmisión de los datos personales sobre las redes internas de SISW se protege de la misma manera que cualesquiera otros datos confidenciales de acuerdo con las políticas de seguridad de SISW.
   d. Cuándo se transfieren los datos entre SISW y el Cliente, las medidas de protección para los datos personales transferidos se estipulan en el Contrato o en la documentación pertinente del servicio en la nube. Esto se aplica tanto a la transferencia de datos física como a la basada en la red. El Cliente asume la responsabilidad de cualquier transferencia de datos desde el punto de demarcación de SISW (por ejemplo, un cortafuegos de salida del centro de datos en el que se aloja el servicio en la nube).

5. Control de entrada de datos. El servicio en la nube permitirá determinar retrospectivamente si se han introducido, modificado o eliminado datos personales en la infraestructura utilizada para prestar el servicio en la nube y quién ha realizado estas operaciones.

   Medidas:
   a. SISW solo permite al personal autorizado acceder a los datos personales necesarios para su trabajo. SISW ha implementado un sistema de registro para la entrada, la modificación y la eliminación o el bloqueo de datos personales por parte de SISW o de sus subencargados de tratamiento de datos en la mayor medida que lo permita el servicio en la nube.
   b. Los seguimientos de auditoría proporcionan los detalles suficientes necesarios para facilitar la reconstrucción de sucesos si se producen o se sospecha que se se han producido actividades no autorizadas o fallos. Cada registro de eventos del sistema operativo incluye el tipo de evento, un cronomarcador, el origen del evento, la ubicación del evento, el resultado del evento y el usuario relacionado con el evento.

6. Control de trabajos. Los datos personales solo se procesarán de acuerdo con los términos del Contrato y cualquier instrucción relacionada proporcionada por el Cliente.

   Medidas:
   a. SISW utiliza controles y procesos para garantizar la conformidad con los contratos entre SISW y sus clientes, subencargados de tratamiento de datos u otros proveedores de servicios.
   b. Los datos del Cliente estarán sujetos como mínimo al mismo nivel de protección que la información confidencial según el estándar de clasificación de la información de SISW.
   c. Todos los empleados y socios contractuales de SISW están obligados por contrato a respetar la confidencialidad de toda la información sensible, que incluye los secretos comerciales de los clientes y socios de SISW.

7. Control de la disponibilidad. Los datos personales se protegerán contra la destrucción accidental o no autorizada o contra pérdidas.

   Medidas:
   a. SISW emplea procesos de copia de seguridad y otras medidas que garantizan una rápida restauración de los sistemas empresariales críticos cómo y cuándo sea necesario.
   b. SISW recurre a proveedores de servicios en la nube de todo el mundo para garantizar la disponibilidad de energía en los centros de datos.
   c. SISW ha definido planes de contingencia, además de estrategias de recuperación empresarial y tras desastres para los servicios en la nube.

8. Control de separación de datos. Los datos recopilados para diferentes objetivos se pueden tratar por separado.

   Medidas:
   a. Cuando resulta pertinente, SISW utiliza las capacidades técnicas del software implementado (por ejemplo: entorno para múltiples usuarios o entornos de sistemas separados) para conseguir la separación de datos entre los datos personales del Cliente y los de cualquier otro cliente.
   b. SISW mantiene instancias específicas (con separación lógica o física) para cada cliente.
   c. El Cliente (incluidos sus afiliados) solo tiene acceso a sus propias instancias de cliente.

9. Control de la integridad de los datos. Garantiza que los datos personales se mantendrán intactos, íntegros y actualizados durante las actividades de tratamiento:

   Medidas: SISW ha implementado una estrategia de defensa de varios niveles como protección contra modificaciones no autorizadas. Hace referencia a los controles indicados en las secciones de control y a medidas descritas anteriormente. Debido a la configuración de los cortafuegos, habrá diversos segmentos de red que separan el acceso público y el privado. Cada conjunto de reglas de cortafuegos tendrá controles de acceso concretos que especifican las comunicaciones permitidas entre estos segmentos.

   a. Centro de control de seguridad: Se utilizará software de detección de intrusiones automatizado junto con otros procesos y software forense y de prevención de seguridad para alertar, investigar y, si es necesario, notificar y ayudar a remediar cualquier incidente de seguridad.

b. Software antivirus: todos los sistemas tendrán definiciones de antivirus actualizadas configuradas para proteger contra virus, gusanos, troyanos y otras formas de malware.
c. Copia de seguridad y recuperación: todos los sistemas tendrán un nivel base de instantáneas de copia de seguridad de los datos y la configuración. Si procede, SISW y sus subencargados de tratamiento de datos también gestionarán la instancia de un cliente con una configuración de alta disponibilidad que garantizará que los datos estén almacenados en dos centros de datos distintos separados por una distancia suficiente entre ellos.
d. Auditorías externas periódicas para probar las medidas de seguridad. SISW y sus subencargados de tratamiento de datos se someterán a auditorías externas periódicas para poner a prueba las medidas de seguridad indicadas anteriormente.